Measuring the Effectiveness of an Information Security Training and Awareness Program

Roshan Dhakal

Doctor of IT, Charles Sturt University

This thesis is in total fulfilment of the requirements of the degree of: Doctor of IT, Charles Sturt University

March 2018

Protected by Copyright
# Table of Contents

Certificate of authorship.............................................................................................................................................. vi
Acknowledgement .......................................................................................................................................................... vii
List of publications ......................................................................................................................................................... viii
List of figures and tables .................................................................................................................................................. ix
List of Abbreviations ..................................................................................................................................................... xi
Definitions.......................................................................................................................................................................... xii
Abstract.............................................................................................................................................................................. xiii

Chapter 1. Introduction ..................................................................................................................................................... 1
  1.1 Preamble ................................................................................................................................................................. 1
  1.2 Background to the problem ....................................................................................................................................... 3
  1.3 Information security culture ...................................................................................................................................... 4
  1.4 Information security policy ....................................................................................................................................... 5
  1.5 Research problem ..................................................................................................................................................... 7
  1.6 Significance of the research ...................................................................................................................................... 10
  1.7 Research aims ........................................................................................................................................................ 12
  1.8 Research hypotheses ................................................................................................................................................ 13
  1.9 Research questions .................................................................................................................................................. 14
  1.10 Thesis structure ...................................................................................................................................................... 15
  1.11 Summary ............................................................................................................................................................... 17

Chapter 2. Literature review ........................................................................................................................................... 18
  2.1 Overview .................................................................................................................................................................. 18
  2.2 Information security lifecycle .................................................................................................................................. 20
    2.2.1 Plan .................................................................................................................................................................. 20
    2.2.2 Do ................................................................................................................................................................. 20
    2.2.3 Check ............................................................................................................................................................ 21
    2.2.4 Act ............................................................................................................................................................... 21
  2.3 Information security program ................................................................................................................................... 21
  2.4 Information security awareness ............................................................................................................................... 23
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4.1 Delivering information security awareness programs</td>
<td>26</td>
</tr>
<tr>
<td>2.4.2 The effectiveness of information security awareness programs</td>
<td>27</td>
</tr>
<tr>
<td>2.4.3 Implementing an effective security awareness program</td>
<td>29</td>
</tr>
<tr>
<td>2.4.4 Measuring the effectiveness of an information security awareness program</td>
<td>30</td>
</tr>
<tr>
<td>2.4.5 Identifying the gaps in information security awareness</td>
<td>31</td>
</tr>
<tr>
<td>2.5 Information security training</td>
<td>32</td>
</tr>
<tr>
<td>2.5.1 Organising training methods</td>
<td>32</td>
</tr>
<tr>
<td>2.5.2 Delivering the information security training program</td>
<td>34</td>
</tr>
<tr>
<td>2.5.3 The effectiveness of the information security training program</td>
<td>35</td>
</tr>
<tr>
<td>2.5.4 Implementing an effective information security training program</td>
<td>36</td>
</tr>
<tr>
<td>2.5.5 Measuring the effectiveness of an information security training program</td>
<td>37</td>
</tr>
<tr>
<td>2.5.6 Identifying the gaps in information security training</td>
<td>39</td>
</tr>
<tr>
<td>2.6 Information security investment</td>
<td>42</td>
</tr>
<tr>
<td>2.6.1 An Integrated model for information security costing</td>
<td>43</td>
</tr>
<tr>
<td>2.6.2 Information security investment research gaps</td>
<td>46</td>
</tr>
<tr>
<td>2.6.3 Identifying the gaps in information security investment</td>
<td>48</td>
</tr>
<tr>
<td>2.7 Management support</td>
<td>49</td>
</tr>
<tr>
<td>2.8 Information security policy</td>
<td>51</td>
</tr>
<tr>
<td>2.9 Information security behaviour</td>
<td>54</td>
</tr>
<tr>
<td>2.9.1 Theory related to information security behaviour</td>
<td>54</td>
</tr>
<tr>
<td>2.9.2 Procedural-based information security behaviour</td>
<td>56</td>
</tr>
<tr>
<td>2.9.3 Relationship between awareness and behaviour</td>
<td>58</td>
</tr>
<tr>
<td>2.10 Summary</td>
<td>61</td>
</tr>
<tr>
<td>Chapter 3. Research methodology overview</td>
<td>62</td>
</tr>
<tr>
<td>3.1 Research phase</td>
<td>62</td>
</tr>
<tr>
<td>3.1.1 Proposed framework</td>
<td>62</td>
</tr>
<tr>
<td>3.1.2 Research questions design</td>
<td>63</td>
</tr>
<tr>
<td>3.1.3 Research process</td>
<td>63</td>
</tr>
<tr>
<td>3.2 Data collection process</td>
<td>66</td>
</tr>
<tr>
<td>3.2.1 Survey questions design</td>
<td>66</td>
</tr>
<tr>
<td>3.2.2 Data collection tools</td>
<td>70</td>
</tr>
<tr>
<td>3.2.3 Description of sample</td>
<td>71</td>
</tr>
<tr>
<td>3.2.4 Validity and reliability of data collection tools</td>
<td>72</td>
</tr>
<tr>
<td>3.2.5 Research ethical considerations</td>
<td>73</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>3.2.6. Quality control of data</td>
<td>75</td>
</tr>
<tr>
<td>3.2.7 Ongoing benefit of the research</td>
<td>76</td>
</tr>
<tr>
<td>3.2.8 Research development stage</td>
<td>76</td>
</tr>
<tr>
<td>3.3 Data analysis</td>
<td>76</td>
</tr>
<tr>
<td>3.3.1 Data-analysis procedure</td>
<td>77</td>
</tr>
<tr>
<td>3.3.2 Research sample and size analysis</td>
<td>78</td>
</tr>
<tr>
<td>3.4 Summary</td>
<td>83</td>
</tr>
<tr>
<td>Chapter 4. Results and discussion</td>
<td>85</td>
</tr>
<tr>
<td>4.1 Measuring awareness level of participants</td>
<td>86</td>
</tr>
<tr>
<td>4.1.1 Password and sensitive information handling</td>
<td>86</td>
</tr>
<tr>
<td>4.1.2 Identifying and managing threats</td>
<td>87</td>
</tr>
<tr>
<td>4.1.3 Improving organisational information security</td>
<td>88</td>
</tr>
<tr>
<td>4.1.4 Incident response and reporting actions</td>
<td>89</td>
</tr>
<tr>
<td>4.1.5 Delivering a training and awareness program</td>
<td>90</td>
</tr>
<tr>
<td>4.1.6 Awareness level of the functional department</td>
<td>91</td>
</tr>
<tr>
<td>4.1.7 Training methods influenced by age</td>
<td>92</td>
</tr>
<tr>
<td>4.2 Research hypotheses</td>
<td>93</td>
</tr>
<tr>
<td>4.3 Summary</td>
<td>103</td>
</tr>
<tr>
<td>Chapter 5. Building an effective information security training and awareness program</td>
<td>104</td>
</tr>
<tr>
<td>5.1 Goals of an information security training and awareness program</td>
<td>104</td>
</tr>
<tr>
<td>5.2 Designing an information security training and awareness program</td>
<td>106</td>
</tr>
<tr>
<td>5.2.1 Identifying customer needs</td>
<td>107</td>
</tr>
<tr>
<td>5.2.2 Reviewing the previous security program</td>
<td>107</td>
</tr>
<tr>
<td>5.2.3 Identifying the training and awareness tools</td>
<td>108</td>
</tr>
<tr>
<td>5.2.4 Identifying user knowledge through metrics</td>
<td>108</td>
</tr>
<tr>
<td>5.2.5 Target audience</td>
<td>108</td>
</tr>
<tr>
<td>5.2.6 Outlining the security training and awareness program strategy and plan</td>
<td>109</td>
</tr>
<tr>
<td>5.2.7 Setting up priorities</td>
<td>109</td>
</tr>
<tr>
<td>5.3 Developing the security training and awareness program</td>
<td>110</td>
</tr>
<tr>
<td>5.3.1 Creating training and awareness resources</td>
<td>111</td>
</tr>
<tr>
<td>5.3.2 Choosing appropriate content</td>
<td>112</td>
</tr>
<tr>
<td>5.3.3 Content sources</td>
<td>112</td>
</tr>
<tr>
<td>5.3.4 The learning process</td>
<td>113</td>
</tr>
<tr>
<td>5.3.5 Previous knowledge and experience</td>
<td>114</td>
</tr>
</tbody>
</table>
5.4 Implementing an information security training and awareness program ................................................. 114
  5.4.1 Awareness and training resources delivery method ................................................................. 115
  5.4.2 Challenges in implementing a security training and awareness program ........................................ 115
5.5 Post implementation of the information security training and awareness program ......................... 116
5.6 Summary ............................................................................................................................................. 117

Chapter 6. Measuring the effectiveness of the training and awareness program ...................................... 118
  6.1 Reason for measuring effectiveness of the training program .......................................................... 118
  6.2 Performance planning ....................................................................................................................... 120
    6.2.1 Estimating the possible actions .................................................................................................. 120
    6.2.2 The degree of achievement ...................................................................................................... 120
  6.3 Measuring procedures ....................................................................................................................... 121
    6.3.1 First test (measuring the participant’s knowledge) .................................................................. 121
    6.3.2 Second test (measuring training and learning satisfaction) ....................................................... 121
    6.3.3 Third test (measuring participant behaviour) ......................................................................... 122
    6.3.4 Fourth test (measuring the training and awareness program) ................................................. 122
  6.4 Framework for measuring the training and awareness program ......................................................... 123
    6.4.1 Information security program .................................................................................................. 125
    6.4.2 Measuring information security program attributes ............................................................... 133
    6.4.3 Advanced measures of efficiency of training and awareness program ..................................... 137
    6.4.4 Review and analysis ................................................................................................................. 142
  6.5 Outsourcing the information security program .................................................................................... 144
    6.5.1 Is outsourcing friend or foe? ..................................................................................................... 145
    6.5.2 Risk of outsourcing the security program ............................................................................... 146
    6.5.3 Measuring the success of outsourcing ..................................................................................... 146
    6.5.4 Measuring the effectiveness of outsourcing ............................................................................. 147
  6.6 Training and awareness partnership program ..................................................................................... 148
    6.6.1 Partnering security training and awareness program: friend or foe? ........................................ 149
    6.6.2 Measuring the effectiveness of the partnership program ......................................................... 150
  6.7 Failure of the training and awareness program ................................................................................... 151
    6.7.1 Management ............................................................................................................................. 151
    6.7.2 User .......................................................................................................................................... 152
    6.7.3 Technical .................................................................................................................................... 154
    6.7.4 Measuring the failure of the information security training and awareness program .................. 155
  6.8 Summary ............................................................................................................................................. 156
Chapter 7. Conclusion ................................................................................................................................. 157
7.1 Objectives .............................................................................................................................................. 157
7.2 Findings .................................................................................................................................................. 158
  7.2.3 Primary research question: How is measuring the information security education training and awareness framework effective in minimising organisational information security incidents? ................................................................................................................................. 158
  7.2.2 The first research sub-question: How does employee behaviour affect the overall information security in an organisation? ................................................................................................................................. 159
  7.2.3 The second research sub-question: Will employee behaviour be changed after implementing the information security training and awareness program? ................................................................................................. 159
  7.2.4 The third research question: How is an information security training and awareness framework is evaluated, and its success measured? ................................................................................................. 160
  7.2.5 The fourth research sub-question: How does the age factor affect the training and awareness framework? ........................................................................................................................................ 160
7.3 Implications of the findings ..................................................................................................................... 160
  7.3.1 Theoretical .......................................................................................................................................... 160
  7.3.2 Practical ............................................................................................................................................. 160
7.4 Research limitations ................................................................................................................................. 161
7.5 Future directions ..................................................................................................................................... 161
Bibliography .................................................................................................................................................. 163
Appendix 1: Ethics approval .......................................................................................................................... 191
Appendix 2a: First survey of support group and initial survey of control group .................................................. 192
Appendix 2b: Second survey with the scenario .................................................................................................. 194
Appendix 2c: Third survey of support group and final survey of the control group ............................................. 199
Appendix 3: Consent form ............................................................................................................................ 201
Appendix 4a: Measuring the effectiveness of training and awareness program (basic measures) ......................... 202
Appendix 4b: Measuring the effectiveness of training and awareness program (advanced measures) ................. 204
Certificate of authorship

Certificate of Authorship

I hereby declare that this submission is my own work and to the best of my knowledge and belief, understand that it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at Charles Sturt University or any other educational institution, except where due acknowledgement is made in the thesis [or dissertation, as appropriate]. Any contribution made to the research by colleagues with whom I have worked at Charles Sturt University or elsewhere during my candidature is fully acknowledged. I agree that this thesis be accessible for the purpose of study and research in accordance with normal conditions established by the Executive Director, Library Services, Charles Sturt University or nominee, for the care, loan and reproduction of thesis, subject to confidentiality provisions as approved by the University.

Name: Roshan Dhakal
Signature:
Date: 23/03/2018
Acknowledgement

Firstly, I would like to thank Charles Sturt University for providing me with the chance to study for the Doctor of IT and the Research Committee for ongoing support. My thankfulness further extends to the coordinator and other staff who are directly or indirectly related to my study.

I also would like to sincerely thank to my principal supervisor MD Rafiqual Islam and co-supervisor Champake Mendis for their continuous support during my study. Their valuable guidance and productive suggestions always encouraged me to move forward on my research work, and they also helped me to publish my two papers. Their feedback and advice have always been fruitful. Their readiness in allocating time munificently during the research was much appreciated. I would also like to thank other lecturers who supported me and showed the right path during my coursework.

I also acknowledge professional editor, Rosemary Purcell, who provided copyediting and proofreading services according to the guidelines laid out in the university-endorsed national Guidelines for Editing Research Theses.

At last, I would like to thank my family and friends who always supported me in every step of my life, especially during my doctoral study. Their continuous support, love, and care encouraged me to write the thesis.
List of publications


List of figures and tables

Figure 1.1: Identifying the organisational goals
Figure 1.10: Structure of the thesis
Figure 2.1: Confidentiality, integrity and availability triangle
Figure 2.2: Information security lifecycle
Figure 2.6.1: Integrated model for information security investment
Figure 2.9.1: Commonly used behavioural theories in information security awareness
Figure 2.9.2: Information security behaviour methods
Figure 2.9.3: Two-factor categorisation of security behaviour
Figure 3.1: Research process
Figure 3.3.2: Survey Monkey as data collection tool
Table 3.2.5: Ethical research considerations
Figure 3.3.2a: Survey sample from all three surveys
Figure 3.3.2b: Distribution of samples
Figure 3.3.2c: Participants based on industry
Figure 3.3.2d: Research participants according to location
Figure 3.3.2e: Participant distribution according to employer size
Figure 3.3.2f: Participant responses according to organisation size
Figure 4.1.1: Password and sensitive information handling
Figure 4.1.2: Identifying and managing information security risks and threats
Figure 4.1.3: Improving organisational information security
Figure 4.1.4: Incident response and reporting
Figure 4.1.5: Training and awareness program delivery
Figure 4.1.6: Comparison of functional department
Figure 4.1.7: Classification of training method according to age
Table 4.2a: ANOVA results for Hypothesis 1
Table 4.2b: t-test results for Hypothesis 1
Table 4.2c: ANOVA results for Hypothesis 2
Table 4.2d: t-test results for Hypothesis 2
Table 4.2e: ANOVA results for Hypothesis 3
Table 4.2f: t-test results for Hypothesis 3
Table 4.2g: ANOVA results for Hypothesis 4
Table 4.2h: t-test results for Hypothesis 4
Table 4.2i: ANOVA results for Hypothesis 5
Table 4.2j: t-test results for Hypothesis 5
Table 4.2k: ANOVA results for Hypothesis 6
Table 4.2l: t-test results for Hypothesis 6
Table 4.2m: ANOVA test results for Hypothesis 7
Figure 5.1: Building an effective security training and awareness program
Table 5.2.5: Target audience
Table 5.4.1: Training and awareness delivery methods
Figure 6.4: Theoretical framework for measuring the effectiveness of an information security program
Figure 6.4.1a: Identified information security threats
Figure 6.4.1b: Information security program
Figure 6.4.2a: Attributes of an information security program: knowledge, attitude, and awareness
Figure 6.4.2b: Sample question to measure knowledge, attitude and behaviour
List of Abbreviations

ANOVA: analysis of variance
APA: Australian Privacy Act
APP: Australian Privacy Principles
CIO: chief information officer
ENISA: European Network and Information Security Agency
GDT: general deterrence theory
IP: internet protocol
IS: information security
ISA: information security awareness
ISB: information security behaviour
ISF: International Security Forum
ISP: information security policy
IT: information technology
ITS: information technology security
NIST: National Institute of Standards and Technology
PMT: protection motivation theory
ROI: return on investment
SANS: SysAdmin, Audit, Network and Security
SETA: security education, training and awareness
TAM: Technology Acceptance Model
TPB: theory of planned behaviour
VOIP: voice over internet protocol
Definitions

**Information security culture**: a procedure for safeguarding the organisation’s resources.

**Organisational information security**: related to protecting the organisation’s all resources.

**Information security lifecycle**: the entire process of the IS from initial to the final phase.

**Information security behaviour**: actions which affect the IS process

**Information security awareness**: making people aware of an organisation’s IS

**SETA program**: a formal program designed to raise awareness of the organisation’s users either through education or training or awareness methods.

**Information security policy**: a formal document which consists of a set of procedures, rules and regulations on how to conduct or perform IS practices safely and securely.

**Risk management**: procedure for identifying, prioritising, managing and mitigating the organisation’s vulnerability and threats.

**Security metrics**: tool used to measure IS practices.

**Outsourcing**: contracting the products or goods to a third party experienced in providing the best solutions or buying goods from other parties who could give the best answer.

**Partnering**: sharing the resources with two or more organisations through agreements.

**Learning process**: the procedure for gaining knowledge through various sources.

**Research hypothesis**: statistical assumptions carried out by the researcher to predict the outcomes of the research before starting the study.

**Support group**: the group supported by the training and awareness program. The participants in this group undertook the training and awareness session.

**Control group**: the group that did not receive any training and were not involved in the training and awareness session.
Abstract

Information security education, training, and awareness programs are designed to raise awareness of users in organisations about their roles and responsibilities in organisational information security policy. Organisational information security policy is a formal document where the set of rules and regulations on using information technology is explained. In most organisations, information security policy is not readily accessible to end users, which results in human error, either knowingly or unknowingly. This research aims to educate, train, and make users aware of information security policy; identify the organisation’s risks; report any security incidents through a security training and awareness program; and measure its effectiveness. The effectiveness of the training and awareness program could be measured by how it helps change the security behaviour of the user regarding knowledge, attitude and behaviour. In the literature review, users’ responses are investigated from both a theoretical and practical point of view. Many organisations assume that humans are the weakest link and are vulnerable to information security breaches. This research also attempts to measure the other factors that are responsible for organisational information security. Thus, this thesis describes how training and awareness program content affects the success of the program, how the experience of the training coordinator changes the program, and how the training program, outsourced program, partnering program and methods for delivering and communication affect the effectiveness of the program. This thesis further explains the implemented framework for measuring the effectiveness of the training and awareness program, and the framework for information security investment. This thesis also estimates the success factors of the training and awareness program and the reasons for the failure of the program.

Keywords: Information security training and awareness program, knowledge, attitude, and behaviour, security behaviour, effectiveness.
Chapter 1. Introduction

This introductory chapter provides background to the research problem, looks at definitions of IS culture from the literature, outlines what an ISP is, presents the research problem and the significance of the research, outlines the research aims, and lists the hypotheses and research questions. The chapter concludes with an outline of the thesis.

1.1 Preamble

Most organisations today are dependent on IT (information technology), and protecting it is a crucial factor for all organisations. IS (information security) is integral to an organisation and cannot be segregated from its business. Before proceeding, it is therefore essential to be familiar with what IS is, as organisations have various ways of defining it.

Infosec defines information as assets of the person or of the organisation, with IS implying that individual and organisational information is protected (Infosec, 2017). Properties related to IS include all electronic data and information, server and networks where collected data are manipulated, any intellectual papers and printed documents of people and the organisation, and any physical devices (Australian Government, 2016). The business directory describes IS as protecting an organisation’s data and information from unauthorised users, ensuring the confidentiality, integrity and availability of an organisation’s data and information (Business Directory, 2017).

Rapid changes in the global network and distribution of information technologies and information systems have led to significant changes in an organisation’s communication processes (Lee, 2003). It is well known that everything in this universe has positive and negative aspects. As information systems and technologies make some positive changes in an organisational information system, there are some drawbacks as well. The global network and IT in government and non-government organisations are at risk of cyber attacks, such as data and identity theft, and theft of the customer and business information that are the resources required for organisational survival (Wong, 2016). There have been many IS attacks in an organisation’s IS system that have severe results for both the public and the economy. Information security attacks from external factors such as hackers, crackers and script kiddies, and organisation’s disgruntled users whose intention is to harm the organisation, all have the same motives. Incentives could be financial gain, damaging an organisation’s reputation by decreasing market value or considering they smart enough to bring down the organisation (Kshetri, 2010). According to the Australian Government Cybersecurity report (Australian Information Industry Association, 2015) most government organisations experience around 47% of total attacks in the form of phishing attacks (Osman, 2017). Data breaches, denial-of-service attacks, theft of official documentation and
compromising of web servers are the primary IS attacks that government organisations are facing today. Private organisations are also not isolated from IS attacks. Compromised systems at 56%, and malicious emails at 22% of total attacks make up the primary IS attacks, followed by data loss and denial-of-service attacks (Lines, 2017).

The literature shows that organisations are investing heavily in technical countermeasures, such as installing anti-virus, firewall and encryption technologies. But many researchers argue that technical countermeasures are not sufficient for the overall organisation’s IS, and believe that more than half (50-75%) of an organisation’s IS incidents arise from employee negligence (Haeussinger, 2015). Therefore, investment in an organisation’s IS requires both technical and employee countermeasures. Today, many researchers and practitioners have moved their interest to the human aspect of IS by analysing the theory of behavioural change and human psychology. SETA (security education, training and awareness) programs are known as the best possible solution for ISB (information security behaviour) for playing a significant role in employee performance strategy (Evans, Maglaras, He, & Janicke, 2016). The main purpose of IS education, training and awareness is to make employees aware of organisational information security policy (ISP) and procedures, and to handle the organisational IS system securely and responsibly. When employees are aware of ISP, they will know and understand the organisation’s risks and threats, and they will also work hard to maintain the organisational IS system (Wright, 2005). In other words, IS training and awareness helps employees protect the organisation’s confidential data and information, and employees are also less likely to be abused for IS incidents (Haeussinger, 2015). SETA programs are considered as a measuring device for successful organisational IS system strategy and performance.

Before implementing any IS training and awareness program, an organisation should look at its position. Where are we now? What is the current situation and status of the organisation? What IS-related incidents are the organisation facing? How can they be minimised? What are the plans and strategies that need to be implemented to reduce the security incidents? After reaching the desired target, how can it be maintained and? (Applied Trust, 2008) The answers to the above questions need analysing before implementing any security training and awareness program. Figure 1.1 illustrates the organisational goals.
1.2 Background to the problem

The examples listed below are the most common IT problems people face, and are usually ignored because victims are reluctant to discussing such problems. Technical countermeasures are effective in mitigating these issues.

**Phone and email scams:** Nowadays more and more Australian organisations are becoming victims of email and phone scammers. The scammer does a lot of research and investigation to collect personal and organisational information before targeting the organisation or user (Vincent, 2017). For example, during tax time, scammers target individuals and tell them that their tax file number is compromised and that they are liable for a hefty fine, but if payment is made to the nominated account, then the fine will be waived. Another example is a scammer sending an email to employees saying that they have won one million dollars in a draw that took place last week, and to please confirm and grab a win. The email is sent from an organisational email address pretending that it is genuine. A further example is scammers calling using VOIP (voice over internet protocol) using a virtual IP (internet protocol) address so they will not be caught. They call organisational management saying that the organisation is dealing with drugs in Australia, and this is a call from the Australian Federal Police. They say the organisation will be shut down, with the only option being payment of AUD20,000.00, which is the initial legal cost of the local court. The scammers say that after getting clearance from the local court the funds will be refunded.

These kinds of scammers collect personal information and pretend to help us from being a victim. If the organisation and its users are not aware of these kinds of threats, then security incidents frequently occur. It is important that users are encouraged to report these kinds of threats, rather than being punished; otherwise these kinds of incidents are not reported for fear of losing their job, and other employees could be targeted (Dascalescu, 2018).

**Information collected from social networking sites:** Social networking sites are a common medium for collecting personal information, such as name, address, date of birth, contact
information and facial information—the critical for identification of a person. IS attacks or an incident could happen as a result of that information getting into the wrong hands where there is no specific rule for reporting security incidents. The motivation for using such information could be financial, denial-of-service or disturbing the service, jealousy, revenge, or getting confidential information and selling it to competitors (Office of the Australian Information Commissioner, 2015). Man-in-the-middle attacks cause security incidents in Australian banks, where the most common attackers are spoofing the conversation between bank servers. In such attacks, the attacker presents as a genuine user by providing identification information along with the security question of genuine users gained from social networks (Okesola, 2014; Turner, 2016).

**Social engineering:** The intention of the user involved in social engineering attacks is unknown unless caught. The most significant consideration is the user’s fear and emotion. In most cases, attackers use fear as a weapon, which causes users to believe the attackers (PhishMe, 2017). For example, an attacker calls the user saying that it has been noticed that they are funding terrorist organisations in the country, and that such practice could lead them to a lifetime in prison or a million-dollar fine, or both. When ordinary users get such messages or calls, they prefer to pay instead of getting in trouble. In some cases, co-workers watch when users type their password, and can therefore access their computer when users are on a short break or go to the restroom. In social engineering, attackers always stay on the safe side and only give trouble to others (Waugh, 2013).

### 1.3 Information security culture

Many researchers have different viewpoints about defining IS culture, and there is no such thing as a specific boundary around it. Dhillon (2000) defines IS culture as an example of the entire performance within an organisation that is liable for safeguarding any information (Pevchikh, 2015). Schlienger and Teufel (2003) define IS culture as the whole social and cultural attitude to practice that maintains technological action mode, so that IS becomes an integral part of the user’s everyday actions (O’Brien, Islam, Bao, Weng, Xiong, & Ma, 2013; Schlienger & Teufel, 2003).

Schlienger and Teufel (2003) argue that organisational IS culture should cover all communities and traditions that technically support their IS methods (Alnatheer, Chan, & Nelson, 2012). This results in organisational IS being an integral part of the everyday activity of all employees (O’Brien et al., 2013). Organisational IS culture plays a significant role in improving trust between employees (Petri, 2006). Sasse, Brostoff, and Weirich (2001) classify and associate the main features of IS culture in an organisation, such as business effect, reward and punishment, and awareness (O’Brien et al., 2013; Petri, 2006), while arguing for the establishment of a fear-based method to convince users to comply with IS behaviour (Dojkovski, Lichtenstein, & Warren, 2006).
Adams and Blandford (2005) make clear that organisational IS culture must support corporate business policy in combination with a general operational plan (O’Brien et al., 2013). In addition, they point out that users should be made aware of the issues by introducing a training and awareness program. They further discuss the significance of an aware management, because IS culture and an IS training and awareness program would not be triumphant without the full support of organisational management. Thomson, von Solms and Louw (2006) state that corporate culture inspires IS culture, and that management and users have an equal impact (O’Brien et al., 2013). Gaining knowledge and maturity are crucial to ensure user awareness of IS matters and encourage users to take part in the organisation’s social activities so they can learn by watching others. Ruighaver, Maynard and Chang (2007) argue that measurement of the performance of IS culture cannot be cut off from the culture of the whole organisation (Alnatheer et al., 2012), because a corporate internal culture has a massive impression on IS culture (O’Brien et al., 2013).

Whiteman and Mattord (2012) argue that employee attitudes from different cultures and backgrounds affect organisational IS culture (O’Brien et al., 2013), with education making significant changes along with training and awareness to assist in building organisational IS culture. In addition, Whiteman and Mattord explain that actions involving ignorance, accidents and intention could affect an organisation’s IS culture. Ignorance and accidents could be minimised by raising awareness and employing training sessions. Intention is hard to manage; however, it can be reduced by educating the users. Operating new activities, such as a rewards, along with a training and awareness program that could divert the mind from negative to positive thinking, and appropriate IS policies and procedures can assist (Chartered Institute of Management Accountants, 2009).

1.4 Information security policy

ISP is the organisation’s group of plans that have been released to make sure that all users follow the rules and regulations (Doyle, 2017). The primary purpose of an ISP is to make sure that proper methods are in place to safeguard the organisational business processes and IT system. In other words, ISP is defined as the organisation’s formal document that says how it can protect its physical, rational and technical assets. For example, the physical asset includes all electronic devices and the organisation’s premises, the rational asset includes intellectual property and confidential documents, and the technical asset includes firewalls, intrusion detection systems, virus protection, and servers (Doyle, 2017). Some researchers state that an ISP is a document that is never ending and requires additional support for continuous upgrading as technology and organisational goals change (Paquet, 2013). An ISP is considered as the constitution of the organisation, and is a handbook giving detailed information on what employees should and should not. Some organisations use existing ISP booklets, while other organisations create new ones and implement IS through the ISP, or get help from professionals who are expert in writing corporate policy and procedures. The other purpose of an ISP is to explain how an organisation plans to teach its users regarding the protection of administrative resources and how IS procedures are applied and executed (Rouse, 2017).
When organisations do not have an ISP, their users will perform the organisation’s activities their way, correctly or incorrectly, if they are unaware of the consequences of their actions (Krzyzewski, 2017). ISP provides users guidelines on what things need to be done, how to perform, and when to act (Yeagley, 2015).

As its primary purpose, an ISP must enable users to recognise potential business threats and IS risks, and mitigate against them. An organisation’s managers and security managers are responsible for developing the ISP. Before preparing an ISP, managers need to consult with end users and managers from different disciplines and include the identified risks from respective departments.

The secondary purpose of the ISP is to maintain standards within the organisation (Caballero, 2014). Reyes (2015) describes several features that should be considered while developing the ISP: why it is required; what should be included; what happens if there is no ISP and how can it be enforced. For example, in password policy, the ISP explains why the password is required—whether it is for access control or for securing confidential information. There need to be guidelines on password length and strength; for example, that it has a minimum of eight characters including numbers, letters and symbols (Microsoft TechNet, 2018) and that it needs to be changed in every month. Users need to be told that if they choose their birth date, address or the name of the city they live in as the password, it can be easily guessed and would be compromised; even if users use the same password for a long time it would be speculated on and compromised (Thomas, 2005).

An ISP needs periodic review after its deployment. The reason for its implementation is that technology is ever-changing and new threats and risks arise which need addressing before the occurrence of IS incidents (Reyes, 2015). The ISP also needs to be handed over to all users. Security policy developers should teach every user about the ISP according to their functional department, ensure that they understand the policy, enforce them to implement it in their workplace, and measure its success.

Organisational management and IS professionals always suggest implementing the best ISP, but what is meant by the best ISP is not always clear. An ISP could be a 10-page document or even a 100-page document. The central theme that needs to be included in an ISP is a focus on the organisational IS system in a well mannered, complete and integral mode (Applied Trust, 2008). The IS training and awareness program must talk about the importance of the ISP and make it clear to all users so they understand and implement it in their workplace. Again, users should be made aware that protecting the organisational IS system means not only preserving the organisation but protecting themselves (Yeagley, 2015). Here the question that could arise is how safeguarding the organisation helps in protecting the users. One wrong move from the users could make the organisation vulnerable to attack, resulting in compromising the data and information of the organisation, as well as the users. When user identity leaks, they could be susceptible to another type of attack resulting in them experiencing unnecessary trouble and losing their
job. Therefore, user awareness and training about organisational ISP is central to safeguarding the organisation from IS incidents (Caldwell, 2013).

1.5 Research problem

The research problem focuses on the issues that are currently being experienced in the IS discipline by addressing the gaps identified in the literature review. This section describes these issues.

Today most organisations have an ISP and an IS training and awareness program. So why are most organisations facing or experiencing IS-related incidents? Why are technical countermeasures and an ISP not enough to protect the organisation’s IS system? Why are the IS training and awareness programs that organisations implement not being fruitful for the organisation? Also, why have IS-related incidents been unknown and hidden for a long time (Herold, 2010)?

Many questions arise in this area, but the answer will remain unknown unless there is further investigation (Australian Government, 2016). An IS training and awareness program will be ineffective unless its success factors are measured and the targeted objectives are attained. While measuring the effectiveness of the IS training and awareness program, the program should measure both employees and management. According to a report from the Australian Government, there is a shortage of requirements in IS training and awareness programs, and the limited subject areas included in the programs are the primary concern (Australian Information Industry Association, 2015). Employees from different disciplines, backgrounds and cultures can compromise the achievement of an adequate training and awareness program. The level of understanding varies from beginners to expert staff, staff who are from English speaking background and non-English speaking background, staff who are familiar with IT and the team who does not have specific knowledge about IT.

The message-sending procedures in an awareness and training program should be implemented according to the employee’s discipline (Santa, 2007). The organisational ISP should be given to different discipline users in a clear and understandable manner they understand. This is the critical factor for the success of IS training and awareness programs that most organisations overlook. For example, while implementing IS training and awareness sessions, technical terms and jargon should be avoided for users who are not familiar with IS. Also, training should change as the technology changes and new threats and risks arise. In most organisations, the ISP is not reviewed and updated, and many still follow the same policy implemented decades earlier (Santa, 2007).

The primary role of the organisation is to make sure that all employees perform correctly while handling information, and this is only possible when all employees are trained and aware of the organisation’s ISP. IS training and awareness is an ongoing method of gaining
knowledge which is essential for users and results in massive profit to the organisation by transforming its performance in the long term (Santa, 2007).

The secondary role of the organisation is to run its business by implementing IT without affecting its ROI (return on investment). This will not be possible unless there is a clear set of organisational IS-related policy and procedures. An ISP is not effective unless organisational users understand it. Therefore, management must ensure that the organisation’s users read it, understand it and apply it in their workplace (NSW Government, 2013). The corporate ISP and procedures could be handed over to new employees during induction or in the organisation’s training and awareness session. Individual discussion with employees gives them an opportunity to express their views on IS, and this kind of interaction with individual employees is essential to change their attitude and to assist them to learn (Santa, 2007). All employees’ point of view on IS would be different, and the way they see the IS threats and risks are also different. Many organisations have revealed that the training and awareness provided to employees during induction are insufficient (Navarro, 2007). It is also essential that employees receive the training and knowledge of organisational ISP promptly. Organisational managers should act as the leading hand in delivering the message, and can work as role models (Broudy, 2010).

In many organisations, management believes it has implemented the best IS training and awareness program before analysing the organisation’s needs. This is the primary issue that most organisations face today. The IS training and awareness program is ineffective unless the organisation’s management identifies the needs of the organisation, understands their users, understands why there are many IS-related incidents even after implementing the training and awareness program, and implements appropriate measures to measure the effectiveness of the IS training and awareness program (Brecht, 2016). Many organisations fail to manage the implementation of IS training and awareness programs. For example, organisations need to clarify with employees why an IS training and awareness program is needed, what the result for employees and the organisation would be, and the consequences of complying. IS training and awareness courses are usually brief, and there is not enough time to design a new one to measure proficiency and intelligence. There is no review carried out to evaluate employee performance in an organisation. Some participants selected for training and awareness programs have problems with language and sincerity towards embarking on IS practice (Australian Skills Quality Authority, 2016). IS training and awareness programs are useful when employees understand the theme of the program and implement correct practices in the workplace, and when management designs the training and awareness program according to the needs of the organisation. Most organisations implement poor quality training and awareness programs and use inappropriate methods to measure them. Moreover, many organisations implement a training and awareness program that was designed earlier, and still follow the same assessment practices (Australian Skills Quality Authority, 2016).
Another reason for the failure of training and awareness programs is that the organisation focuses on only one mode of training, and today most organisations are attracted towards computer-based training because of its cost-effectiveness and ease of use (Kim & Homan, 2012). However, organisations should concentrate more on which training method would be suitable for its users. Users should be able to choose the training method rather than being pushed to undertake the particular training method the organisation has implemented. This kind of freedom to select practice encourages users to take part in training and awareness programs, and also help users to express their ideas and views concerning organisational IS (Training Today, 2016).

Additionally, organisational management often ignores its users for participation in the training program, with its management team only participating. This kind of practice inspires users to skip the training program and makes them feel that IS responsibility is just for the managers and security professionals (7 Barriers to Organisational Learning, 2017). Untrained users do not know how to report issues, and during IS incidents are fearful of losing their job, thus many events are not reported. Some organisations conduct a pre-test before the training program and a post-test after the program, but some only attend the post-test, not the pre-test. While performing the training program, organisations rely on just one method of communication and delivering the message without realising which training method suits their training program and without knowing the participant’s preference (The Most Effective Training Techniques, 2016). Since the IS training and awareness program is an ongoing process, failing to periodically review or invest in the program are other issues that could lead to its failure.

Many Australian organisations outsource to IS companies, which deal with all the issues and challenges that arise or will arise in an organisation’s IS system. Any issues and incidents related to IS are between management and the outsourcing companies, and employees are isolated (Colwill, 2006). Moreover, some outsourcing companies are located overseas, and policies and procedures conform to overseas companies’ rules and regulations. Therefore, employees are not interested in knowing about the security-related incidents that are happening in their organisation, and they might think that outsourcing companies are liable for security incidents. This results in gaps in communication between outsourcing companies, organisational management and employees, with employees thinking that IT is not a technical issue anymore, but rather a business issue.

The security behaviour of the users determines the success and failure of the training and awareness program. Therefore, it is necessary to know the success and failure factors of the training and awareness program so that the user’s behaviour is measurable. Organisational users have a right to use the organisation’s confidential information, and the protection of that information depends on the level of knowledge users have got. It is well known that knowledgeable and skilled users can perform and make better decisions (Manke & Winkler, 2013). However, the issue here is that after knowing experienced and trained users are the
pillars of organisations, why organisations overlook them in providing the essential knowledge in regard to the organisation’s ISP and risks. Users are the first ones who experience security incidents, and trained users could act as “first aid” to the security incidents. IT is evolving rapidly, and new threats and risks are growing that could compromise IS (Hight, 2005). Training and awareness provides the additional knowledge and awareness to end users, and information about new risks and threats for managers and security professionals.

1.6 Significance of the research

From an IS professional and researcher viewpoint, working in the organisational environment means complicated interaction with both people and the system. IS is a process that is known as a necessity, but the priority given is not proportionate to its significance. There is always an argument in an organisation about how much security measures need to be employed, and how to manage the related effects (Ruch, 2018). This kind of divergence creates an intricate balance about how to organise IS. A method that presents a significant structure for systematic organisational IS systems in defying situation where the main concerns for the struggle to exist is needed. Thus, identifying a process that measures how organisational IS management is enhanced in Australian organisations through the process of IS training and awareness program is the central area of this research.

There are very few published research papers that concentrate on organisational IS training and awareness programs (Tsohou, Kokolakis, Karyda, & Kiountouzis, 2008). At the same time, however, the concept and description of organisational IS training and awareness programs are being enhanced because of their significance in securing the organisation’s data and information. Realising an IS training and awareness program is complex, both academically and commercially. To make an organisational IS system active there is a need for a proper IS training and awareness program. An IS training and awareness program would be more useful when organisational management employs it as a business requirement and measures it (Herold, 2010; PCI Data Security Standard, 2014).

The concept of IS in many small and medium-sized organisations is still little known and ambiguous because of the organisation’s culture and its working environment. The possible employment of an IS system and its related procedures in organisations needs a reliable basis (Khan, 2010). Regardless of the significance of IS in organisations, current strategies, methods and policy and procedures for IS is not all-encompassing. An organisation’s management often does not consider the procedure of organising IS and has no control in handling it. Therefore, identifying how an organisational IS system could be enhanced and investigating the success factors that lead to IS in an organisation is needed (Al-Awadi & Renaud, 2007). Investigating the challenges and issues through this research guided the
prototype or organisational model to support IS professional in an organisation to gain valuable methodology in measuring IS training and awareness.

This research investigates organisations’ current status from an IS point of view, the IS issues and challenges, and gives practical suggestions on how changes for the better can be implemented. This research represents an initial effort to benchmark the IS knowledge of employees and organisations. This research further boosts IS to an advanced position where more organisations will contribute to increasing knowledge and awareness of IS as a progressively more renowned topic in practice (Navarro, 2007).

The significance of this research can be categorised into theoretical and practical aspects. On the theoretical side, this research gives an overview of a theoretical framework that can be implemented by IS professionals for successful employment of IS in an organisation. The theoretical framework assists IS professionals to perceive the profession as designed for critical thinking rather than commencing an action, and provides a roadmap for security professionals to concentrate on the changes to their knowledge, and other employees to retain information about security operations. IS professionals can implement the proposed research framework into other organisations, with implementation of this framework in other organisations based on the organisation’s needs and size being an area for future research. This research also underlines possible IS standards in an organisation as future research. Until now the research concentrating on IS management in an organisation has an unsatisfactory academic contribution. The research conducted on organisational IS management concentrates on a management paradigm or behavioural paradigm in dealing with IS. The management paradigm concentrates on managing IS-related risks and threats, whereas the behavioural paradigm concentrates on an organisation’s ISP (Lane, 2007). The gap here is that an organisation requires a logical method of managing IS that combines both approaches (Botha, 2011).

On the practical side, this research gives an overview of the current status of IS management. The areas include, but are not limited to, problems and challenges, impediments and obstacle that affect the employment of ISP and training and awareness programs, and suggestions for addressing those areas. This research also explains how the employment of a theoretical framework helps IS professionals develop IS management in an organisation by extracting from earlier research and encompassing them in current prerequisites. For example, inheriting some of the objectives and strategies, and policy and procedures from earlier research into the current research, gives the model an overall structure that significantly increases the integrity of IS management and is appropriate to the coexisting IT design. Measuring the efficiency of the theoretical model should be done for both management and employees (Tasmanian Government, 2017). Measuring from the management side should find that after training organisational management believes in gathering knowledge, whereas from the employee side it should result in increasing in awareness and active involvement in other aspects of IS procedures.
1.7 Research aims

This overall aim of this research is to measure the effectiveness of the IS training and awareness program in an organisation. The program’s effectiveness is determined by an improved level of the ISA of users, their capacity to insist on the specifics of the ISA paradigm and maintaining their knowledge.

Measuring the effectiveness of IS an education training and awareness program should not only focus on changing user performance based on their knowledge, attitudes and behaviour but should also improve ROI (Boxa & Pottasa, 2013; Stephanou & Dagada, 2008). For example, organisations spend a massive budget on IS training and awareness programs to change user performance, and the program helps to change user behaviour; but after a couple of months, some users may leave due to personal or family reasons. How do the organisations then cope with a situation whereby their qualified and trained users are no more? How do they manage the situation so it positively affects the organisation’s business effectiveness and security culture?

In achieving these aims, this research:

- further examines other training types and how those training methods influence the success of the IS training and awareness program (Abawajy, 2014)
- investigates the different methods that are presented in the literature review
- assists IS professionals select the mode that is appropriate to the goals of an organisation, and to view the success factor of that method in that particular organisation instead of selecting randomly (Olusegun & Ithnin, 2013)
- plays a vital role in establishing the theoretical background of current IS training and awareness methods. The reason behind this is to make academic researchers and experts familiar with the theoretical knowledge which broadens their view on why this particular IS training and awareness program is believed to have an expected effect on users
- identifies the limitation of IS training and awareness methods which contains experimental facts based on their practical success
- evaluates the current organisational IS culture and prioritises human factors in IS systems and also identifies the interrelationship between users, IS threats and risks and the IS budget for building IS system
- examines how changes are happening in organisational IS systems direct the significance of ISA
• investigates previous training and awareness programs and results to help IS professionals understand what has happened before, why the training and awareness program did not work, and whether the failure is on the user or management side
• further implements the new ideas and techniques in measuring the effectiveness of delivering training and awareness methods.

1.8 Research hypotheses

In most research studies, the hypothesis gives an initial prospect of the research study before starting the research and in some cases decides the research plan and process (Lavrakas, 2008). The hypothesis consists of two or more variables and prefigures the relationship between those variables (Center for Innovation in Research and Teaching, 2018). The result of a hypothesis is determined by either accepting the hypothesis or rejecting the hypothesis, and is mostly applied in quantitative research methodology (Reading craze, 2013). The hypotheses for this research follow.

1. H0: There is a significant variation in the results of the first survey and the second survey.
   
   H1: There is no significant variation in the results of the first survey and the second survey.

2. H0: There is no significant variation in the results of the first survey and third survey.
   
   H1: There is a significant variation in the results of the first survey and third survey.

3. H0: There is a significant variation in the results of the second survey and third survey.
   
   H1: There is no significant variation in the results of the second survey and third survey.

4. H0: There is a significant variation in the results of the initial survey of the support group and the control group.
   
   H1: There is no significant variation in the results of the initial survey of the support group and the control group.

5. H0: There is a significant variation in the result of the initial control group and result of the final control group.
   
   H1: There is no significant variation in the result of the initial control group and result of the final control group.
6. H0: There is a significant variation in the result of final support group and result of the final control group.

   H1: There is no significant variation in the result of final support group and result of the final control group.

7. H0: There is a significant variation in the relationship in between ISA and IS performance.

   H1: There is no significant variation in the relationship in between ISA and IS performance.

1.9 Research questions

There is a specific relationship between employees’ access to ISA and employee’s attitude about IS performance (Banfield, 2016). There is a specific relationship between employee’s age and background and IS training methods.

The research question and its sub-questions are:

How is measuring the IS education training and awareness framework effective in minimising organisational IS incidents?

- How does employee behaviour affect the overall IS in an organisation?
- Will employee behaviour be changed after implementing the IS training and awareness program?
- How is the IS training and awareness framework evaluated, and its success factor measured?
- How does the age factor affect the training and awareness framework?

The primary research question asks how an IS education training and awareness program helps to reduce the number of IS-related incidents in an organisation. The research question also asks how an IS education training and awareness program is measured to maintain its effectiveness in reducing the number of IS-related incidents and risks. The first research sub-question asks how employee performance influences organisational IS culture. The first question further discusses how a change in employee behaviour (either a positive change in employee performance or adverse change in employee performance) reforms the overall IS management system. The second research sub-question describes the possibility of change in employee performance after an employee receives IS education training and awareness program. The second research sub-question further discuss the effectiveness of the training and awareness program, and if the IS education training and awareness programs fulfil the organisational needs or whether there is a need to upgrade the program. The third research
sub-question discusses the method of measuring the effectiveness of the IS education training and awareness program. The third research sub-questions further discuss on the evaluating the success factor of the IS education training and awareness program. The fourth research sub-question discuss how age affects the implementation of the IS education training and awareness program. The fourth research sub-question further describes why young employees are attracted towards web-based training rather than instructor-based training and how group discussion encourages employees to express their ideas.

1.10 Thesis structure

This thesis consists of seven chapters.

Chapter 1 provides a general introduction to the research including the reason for the study, objectives of the research, and research aims and questions.

Chapter 2 presents the literature review on the theory of IS and how these theories are executed in the present environment. In this chapter, some of the terms that are related to IS are defined. In addition, the employee factor and its relationship to organisational IS are investigated by looking at the challenges from a social point of view to find the hidden and mysterious actions that lead to IS incidents. Organisational culture is reviewed along with its relationship to IS to identify the relationship between the success of IS training and awareness programs and developing a suitable organisational culture where employees are conscious about IS incidents and are also proficient to act in response.

Chapter 3 describes the research methodology for exploring raising ISA in an organisation by measuring its effectiveness within employees. Online data collection is the method used to collect the data and SurveyMonkey is the tool for investigating the current level of ISA within employees and the needs of organisational ISA. Three separate surveys were conducted with the support group, and two independent studies were done with the control group. The initial review was performed to measure employee level of understanding IS. The second survey was conducted after implementing the IS training and awareness program. The third survey was performed after a specific interval of time to measure whether employees forgot their IS training and awareness program or whether anything needed updating. This chapter also describes the analysis of the detailed statistical data that was collected through the online surveys. In addition, this chapter creates the hypothesis for testing and examining the results of ISA on employee IS performance in organisations. The collected data were checked for consistency and authenticity and verified as standard after slight modification.

Chapter 4 describes the results and discusses the findings, which were clarified after the statistical analysis and hypothesis testing.
Chapter 5 describes the building of an effective IS training and awareness program. This chapter discusses how IS training and awareness programs are developed, designed and implemented in detail. The organisational, individual and other factors that are directly involved in managing the IS training and awareness program are presented.

Chapter 6 describes the theoretical framework for measuring the effectiveness of IS training and awareness programs. Some other theories and models for measuring the effectiveness of the program are also discussed and are compared with the proposed framework. Chapter 6 also describes the impact of outsourcing an IS training and awareness program and discusses the risk factors related to outsourcing. Further, the impact of partnering the IS training and awareness program is discussed. Finally, the chapter describes the factors that are responsible for failure of the program.

Chapter 7 presents the conclusion of the thesis, with the findings, and outlines its limitations and suggestions for future research. New and unique solutions for the effectiveness of the IS training and awareness program are discussed and the chapter also verifies the discussions and opinions of the earlier chapters.

Figure 1.10 provides a diagrammatic view of the structure of the thesis.
1.11 Summary

This chapter provided an introduction and background to IS and IS education, training and awareness programs. The IS issues were discussed, and how a training and awareness program assists users to address IS-related issues was considered. Nowadays, every organisation has an ISP but many still face IS attacks through ignorance from management about ISP, unclear security policy or end users being unaware of security policy. Thus, this chapter detailed how emphasising significance of ISP in an organisation assists building a robust information security culture. The research problems were described and the necessity for this research was outlined. The research hypotheses are included in this chapter in order to provide early view of the research study.

Chapter 2 consists of the literature review and related work on IS and training and awareness programs.
Chapter 2. Literature review

The literature review for this thesis involved the study of existing literature from multiple sources; books, conference papers, newspapers, magazines, PowerPoint slides, journal articles, published theses, reports, case studies, forums and discussion, and all other IS resources that are accessible through the internet. While reviewing the literature, information relating to IS was regularly refreshed and revised, and I also searched for any further knowledge in the field of ISA. The literature review involved verifying significant areas and focusing on the issues related to the success of ISA. This process helped establish knowledge via an early learning process and continual re-reading of the IS literature.

2.1 Overview

This literature review criticises the research concept previously accepted as real by researchers. It also determined the research dilemma by recognising the hypothesis and gaps that need resolution. A literature review plays a significant role in the research methodology by explaining the proposal, directing the theoretical model and associating the correlation between the research proposal and the research model idea. The main aim of this literature review was to establish a relationship between recent research studies and focusing on the gaps in ISA that have occurred in other organisations. The literature review found that IS in an organisation would be successful only through a SETA program. The ISO (International Organization for Standardization) also states that a SETA program is an initial step in minimising IS-related incidents in an organisation by making employees aware of their organisation’s ISP.

The goal of an ISP is to reduce the risks and threats, which is difficult to achieve when it is related to organisational culture. Thus, this literature review concentrates on those areas directly related to the research goals and questions. The gaps identified in the literature review should therefore be connected to the framework for the management of IS in organisations. The organisational ISP and organisational IS culture are significant areas that are complicated to develop, and most organisations face the same challenges.

IS is defined as safeguarding the confidentiality, integrity and availability of data and information systems from malicious acts. Confidentiality, integrity and availability are also called the confidentiality, integrity and availability triangle (Technopedia, 2017), see Figure 2.1. Rouse (2017) defines IS as the approach for controlling the methods, devices, policies and procedures to protect and respond to threats and risks to data and information. The aim is not only to protect data and information, but also understand how the data and information are collected, processed and made available.
The confidentiality, integrity and availability triangle is an IS framework that outlines the ISP of an organisation. The three elements of the triangle are believed to be the most critical aspects of IS. **Confidentiality** represents the protection of data and information and not revealing those data and information to anyone (TAFE NSW, 2009). Some examples of confidential data are birth date, bank details, driver licence number, medical records, social security number, travel documents, institutional reports and biometric data. These information details are required to identify the person, and need to be confidential. Trust between client and organisation is built when clients know their details are in safe hands. The purpose of confidentiality is to conceal the data and information from unauthorised users, made possible through encryption technology and cryptography (Summers & Tickner, 2004).

**Integrity** in IS refers to making sure that entered data and information are correct and that only authorised users can modify it. The purpose of integrity is to protect data from unauthorised parties during entering, transferring and storing processes. Some illegal parties can attempt security attacks to intercept significant data and modify it before sending it to the allocated receiver; some malicious users intentionally modify the data.

**Availability** refers to making sure that the data and information are available to authorised users all the time (Summers & Tickner, 2004). Authorised users could be the organisation’s customers, users, contractors or stakeholders. IS attacks concerning availability are denial-of-service attacks and website attacks (redirecting to the error page). Attackers who are responsible for these attacks may have ego or jealousy problems, and want revenge or to blackmail, and some competitors hire attackers to disrupt an opponent’s website.
2.2 Information security lifecycle

IS also has a lifecycle, and Figure 2.2 shows its four steps, commonly known as plan, do, check and act. The IS lifecycle provides direction to ensure that IS is continuously progressing. IS is not a statistical review or results, but it needs frequent consideration and ongoing support, and to maintain the IS lifecycle, policies and procedures require implementing at the beginning. ISP is considered as the heart of IS, playing a fundamental role in measuring and safeguarding the steps of the IS lifecycle. The following sections briefly discuss each stage of the IS lifecycle.

![Information security lifecycle](image)

**Figure 2.2: Information security lifecycle (Lodgaard & Aasland, 2011)**

2.2.1 Plan

Planning is an initial step in any program that explains the planning of the program. For example, what is the goal of the program? How to get there? How can organisational assets be protected while organisations have no idea about them? The planning phase in IS includes an organisation’s roadmap, its resources that need safeguarding, the IT that requires protecting, organisational assets, the policy and procedures to maintain the organisational IS, and risk management. Identifying the organisational information system is the purpose of the planning phase.

2.2.2 Do

The do phase of the IS lifecycle begins after the planning phase. After all the organisational assets have been identified, a further step is to conduct the IS estimation. This stage goes through various tasks from consideration to investigation. It applies to all small and medium-sized organisations. In big organisations, when there are multiple tasks, the job should be prioritised. The function that has the highest importance should be prioritised first and work that has low significance should be prioritised lower. It is precisely the same as a risk matrix in which the job is to prioritise according to risk and vulnerability. The purpose of the do phase is to investigate assets in all areas to detect any threats or vulnerabilities and collect more in-depth information about assets. An advance observation
during the planning phase needs upgrading with further descriptions, and this stage acts as benchmarking for the IS. While concluding the IS lifecycle, the status of organisational IS could be compared with the IS benchmark to find out the progress of the IS in an organisation (Pfau, 2003).

2.2.3 Check

After outlining the organisational information system and networks, which are assets, and classifying the threats and vulnerabilities, the next step is to incorporate or bind them with the organisation’s ISP. In other words, the check phase is defined as protecting the organisation’s information systems because this phase minimises the identified risks in the do phase of the lifecycle. The purpose of this phase is to organise and upgrade the information system and network security, which increases the potency of IS and meet the terms of organisational ISP. The check phase ensures that every corporate resource meets the basic IS standard (Pfau, 2003). Apart from the basic IS standard, a different kind of defence technique can be employed, and suitable defence techniques need to operate according to the significance of the resource at risk.

2.2.4 Act

Act is the final phase of the IS lifecycle, and supervises the IS the organisation implemented. After reinforcement of the organisational IS, this phase makes sure that the amendment stays in place. Moreover, this phase also supervises the performance of the newly implemented system and technology in an organisation. Protection of the organisational resources depends upon the value of the resources, and so does the monitoring. Every resource needs assessment within the corporate information system, but some resources need to be evaluated over and over again more than others (Pfau, 2003). The purpose of this phase is security performance and affirmation, and this could be possible through assessment. The act stage includes assessing the information system to find out whether it meets the terms and conditions of the organisation’s ISP, or if any modifications happened recently. Evaluating the information system should be done by applying the data into an experimental configuration and then making a comparison. This comparison allows an organisation to monitor the progress or fall of the IS in an organisation.

2.3 Information security program

An organisational IS program depends upon employees because they are the primary users of an organisation’s data and information, which are the organisational assets. Therefore, security incidents caused by employees could result in massive destruction—more so than security incidents from an outsider. Nowadays, attackers are targeting organisational employees in such a way that employees are barely aware of the attacks, and their identity is stolen through social engineering or phishing attacks. So if organisations intend to implement the IS program then the program must meet the international standard, such as ISO 9001:2000, ISO 27001 and 27002, Standard of Good Practice, NIST (National Institute of
Standards and Technology), Consortium for IT Software Quality (International Organization for Standardization, 2013; Wikipedia, 2017). These international standards emphasise the significance of IS training and awareness, make clear the reason for specifying and complying with the standards, and exist as an authority (Veseli, 2011).

Organisations would encounter many security-related issues during the process of risk assessment. When organisations face external security attacks, the organisation might lose its data and information during the time of the attack, but when organisations undergo an internal security attack, and then organisational data and information are always compromised. Therefore, it is essential to employ ISP to reduce IS incidents. An organisation would be unlikely to quote the value of losses due to security incidents, or the cost of installing the new technology. ISA plays a vital role in getting rid of these kinds of losses and introduces a general but effective program where organisational management could talk about the results of risks and defensive techniques that could be implemented to safeguard the information (Deerwood Technologies, 2013).

The significance of ISA includes, but is not limited to, the following:

- It assists employees to recognise and respond to the IS incidents.
- It helps employees to be aware of organisational IS systems.
- It gives practical knowledge on how to mitigate with scammers, thief, and fraudster.
- It helps in minimising the number of IS incidents.
- It allows employees to comply with the organisation’s policy procedures and standards.

The objectives of IT security awareness are as follows:

- Employees will recognise the necessity of IS and risk management.
- Organisations will distinguish the different types of risks that are related to the organisation’s business and determine the effective methods of control.
- An organisation’s employees could notice and detect irregular movements, which could reduce the possibility of security incidents.
- It will teach organisation’s employees to use its resources appropriately so that there will be no risk of mishandling.
- Overall, it maintains the organisation’s reputation and constancy, and creates a positive ROI.

From these objectives, the significance and necessity of an ISA program in an organisation is clear (Labuschagne, 2015). With those objectives and needs, security awareness would
suggest additional information about the threats and risks, and assist in filling the gap once support from management is gained (Botha, 2011; Deerwood Technologies, 2013).

2.4 Information security awareness

ISA is an official organisational program designed to make sure that organisational management and users are conscious of, and interested in, minimising IS threats and risks, and comply with ISP. In other words, ISA corresponds with the organisation’s IS department to ensure that organisational management and its users are aware of, familiar with, pursue and value organisational ISP. ISA would be unsuccessful if users are aware of organisational ISP, but ignore acting according to policy and procedures. According to Siponen (2000) and Straub, Keil, and Brenner (1997), ISA is a crucial factor in the prevention of information system abuse. Developing IS in an organisation through security awareness is often a complicated task. While implementing ISA, there arise a couple of issues. Awareness of performance needs to be considered, and problems need to be found that motivate user interest in complying. ISA compliance could fluctuate, affecting the overall performance of organisational security (Tsohou et al., 2008).

The other factor concerning ISA effectiveness is that it relies on the attention and curiosity of the recipient. ISA programs are unsuccessful when implemented with insufficient attention and interest in IS by users. According to Cohen (1999), enhancing ISA requires significant and effective actions, which is only possible when participating users are positively impressed with IS. Therefore, user attitude and behaviour are the most important factors in the implementation of an ISA program, with changes in these factors leading to complications in IS (Labuschagne, 2015).

Much of the research shows that some ISA programs are built in an assessable fashion, while other organisations avoid implementation. A survey conducted in Australian educational institutions illustrates that only one-third of educational institutions had correctly reviewed an ISA program (Labuschagne, 2015). Furthermore, a survey conducted by Ernst and Young shows that one-third of the organisations surveyed had successfully implemented an ISA program, but had not allocated sufficient budget for its continuation (Bennett, 2004). Another survey conducted in 2002 on medium-sized and large organisations, found that according to organisational security managers no more than 50% of organisations had an ISA program in effect (Tsohou et al., 2008). The difference in survey results means that the effectiveness of ISA programs is always low when compared to organisational needs. Leach (2003) agrees that more than half of security incidents arise from user behaviour compared to insufficient technical solutions, and proposes that a well-documented ISA program is capable of minimising that number.

Schlienger and Teufel (2003) include all three elements of IS (security education, awareness and training) in the design of their program. Xiong (2011) further argues that such a program is the most effective method for delivering the message, especially in face-to-face
training, but many researchers conclude that organisations overlook performing necessary training and awareness programs (Banfield, 2016). Okeni and Owens (2007) support Schlienger and Teufel’s (2003) security program, and state that the learning process is initiated by increasing awareness, which is possible by identifying a suitable training program. Siponen (2000) recommends that ISA is an essential factor in IS, confirmed by the Security Awareness Index Report. Thomson and von Solms (1998) view on ISA is that security awareness is designed to make end users aware of the meaning and worth of organisational ISP, which could be achieved by educating and training end users. Qing, Ng, and Kankanhalli (2007) support ISA programs as essential for end-user education to preclude IS-related incidents. Spurling (1995) does not mention anything about security education, but suggests that security awareness projects consist of security training. Johnson (2006) advises that if an ISA program complicates IS, then those complications could be handled with appropriate training and education. The various published journals reviewed for ISA procedures disclose that all three elements of SETA are combined to design a framework for developing an effective IS program. This program consists of instructor-based and computer-based training with the purpose of educating end users, changing performance and undertaking periodical endeavours (Tsohou et al., 2008). Vroom and von Solms (2002) combine the three elements of IS to create an effective IS program that educates users about why it is necessary to protect organisational data and information and how organisations can make sure that users are getting appropriate training and education regarding IS threats and risks. Bray (2002) suggests that ISA is a result of security training, and both security training and awareness programs are designed with the help of appropriate knowledge and education about IS. In some reviewed journal articles, researchers overlooked security awareness, but looked at ISA through security education and training, that is, users not only know what ISP is, but also understand why we it is needed. Charoen, Raman, and Olfman (2008) argue that many researchers are still unclear about the theory and definitions of IS training and awareness, with researchers believing that security awareness is also known as security training. They also think that training enhances security, and ISA is an effective way for an organisation to ensure that users are aware of risks and threats, and also how to mitigate them. Puhakainen (2006) separates security education from security awareness and training, but he mixes up the concept of security awareness and training. He implemented the idea of security awareness training to indicate that security awareness could be gained through the training and learning process, and his research on ISA consists of analysis and evaluation of security training (Tsohou et al., 2008).

There are a large number of definitions of ISA in the literature, but the open coding process concluded that there are three features: cognitive, behavioural, and process. The three features are described further in detail as follows.

**Cognitive perspective:** In most cases, ISA is defined from a cognitive perspective, which means ISA could describe a user’s way of thinking that is influenced by knowing and
realising the meaning of an IS system. Such users are interested and cognisant of IS, aware of IS threats and risk, and can handle the organisation’s IS system maturely (Haeussinger, 2015).

The Siponen (2000) definition of ISA has both a cognitive and behavioural viewpoint: “Information security awareness is a position where an organisation’s IS users are fully aware and entirely loyal to the organisation’s security goals and objectives” (p. 31). In this definition, users being fully aware of organisational IS represents the cognitive point of view and users being loyal or faithful to the organisation’s security goals represents the behavioural perspective as users pursue the given rules and regulations of organisational objectives.

Bulgurcu, Cavusoglu, and Benbasat (2010) also define ISA from the cognitive perspective, but they separate the ISP awareness component from the general meaning of ISA. General ISA represents a user’s entire knowledge, and the realisation of IS challenges and prospective results, but ISP awareness represents user knowledge and awareness of the organisation’s ISP. For example, users can use a swipe card for getting access to organisational premises, which shows that the user is aware of access control and IS. However, they might not know that the swipe card cannot be shared with anyone, and cannot be used outside of business hours as represented in the organisation’s ISP on access control. As a consequence, the user could have enough knowledge and be fully aware of organisational IS, but still require a certain level of awareness and understanding of policies and procedures approved by the organisation. Therefore, both components (general ISA and ISP awareness) need to be addressed for the appropriate definition of ISA.

D’Arcy and Hovav (2007) follow the cognitive perspective, and describe ISA as user awareness of organisational IS processes. User awareness consists of ISP, IS training and awareness program, and controlling users’ actions instead of measuring their level of understanding and familiarity with IS challenges and intimidation. Banerjee and Pandey (2010) limit ISA to the knowledge of IS only, and describe ISA as the knowledge every user requires to safeguard the organisation’s physical and logical resources. Spears and Barki (2010) also follow the cognitive perspective, but describe ISA differently. Their viewpoint focuses on various groups in organisations, such as the management group, the IS expertise group, general users, and third-party stakeholders (such as cleaners, security guards, contractors and delivery person).

**Behavioural perspective:** While many definitions of ISA come from the cognitive perspective, some descriptions also refer to the actual behaviour related to IS. The behaviour action starts from identification and knowing the organisation’s IS governance to responding and being dedicated to the organisational goals. From the behavioural perspective, a user’s ISB symbolises the organisation’s ISA. So there is no precise definition of ISA from a behavioural point of view because ISA and ISB interact intimately with each other (Haeussinger, 2015).
Process perspective: The process perspective defines the actual process of raising organisational security awareness and running awareness campaigns. NIST values the process perspective of ISA the most because ISA attempts to motivate users about IS and assimilates the cognitive and behavioural approaches from a user’s position to identify and react to IS-related affairs (Wilson & Hash, 2003). Kritzinger and Smith (2008) define ISA as an effort to make sure that every organisational user is aware of their roles and responsibility to safeguard the data and information they deal with. Bray (2002) defines ISA as an attempt to educate all users and make them aware of organisational ISP, and advising users about what the organisation expects from them.

2.4.1 Delivering information security awareness programs

The purpose of an ISA program is to make users aware of IS (Labuschagne, 2015). The awareness program is regarded as successful when the message is adequately conveyed and delivered to users. Therefore, the delivery method plays a significant role in the success of the program, and there are various options for delivery. This section further analyses the different modes of providing ISA.

Abawajy (2014) mentions that the standard way of conveying ISA messages is either through paper or the internet. The paper method of delivery incorporates utilising advertising materials such as posters, brochures, leaflets and flyers that contain eye-catching catchphrases on security-related matters. Delivery through the internet includes using security interaction forums and emails containing security newsletters. Wilson and Hash (2003) compared both delivery modes and found that awareness materials delivered via the internet are efficient because multiple sets of information can be delivered compared to messages conveyed on paper. They also argue that messages delivered through the internet are exclusive to selected users who need specific delivery methods, but that there is no assurance that users view and understand the contents of the internet-based security awareness programs.

Valentine (2006) mentions that the classroom-based security awareness delivery method is costly because awareness program coordinators needs to change the awareness content, workout the feedback provided by the participants and interact with the participants many times. Leach (2003) argues that the success of an awareness program depends on the proficiency of the program coordinator, because if they are incompetent, users get bored and might skip the program in the middle of the session or not show up in future awareness programs. Cone, Irvine, Thompson and Nguyen (2007) argue that the periodic nature of the delivery of security awareness programs affects users because they might not think critically about the security concepts. Albrechtsen and Hovden (2010) suggest that a security awareness program is successful only if there is two-way communication between program coordinators and participants sharing their knowledge and experiences during the session.
Cone et al. (2007) introduced the concept of video games as a method for delivering ISA. Fung, Khera, Depickere, Tantatsanawong, and Boonbrahm (2008) compared the video-game method of delivery with classroom-based methodology, finding that the participants who participated in classroom-based programs performed better than those using video games. On the other hand, Abawajy (2014) considers that videos designed for educational purposes are an effective method for delivering ISA. He further suggests that online videos are time flexible and users could repeat the videos as many times as they like. Repeating security awareness content could be another useful mode in raising user awareness. Abawajy comments that in the repeating process, organisational management sent phishing emails to the users to identify and understand the threats of phishing attacks. After determining the user’s knowledge on phishing attacks, the organisation conducted the awareness program on phishing attacks and again sent the phishing emails to users to find out whether they could detect the phishing emails or not. Kumaraguru, Rhee, Acquisti, Cranor, Hong, and Nunge (2007) implemented a similar process, whereby they inserted information about phishing attacks in a phishing email with the intention of educating users.

2.4.2 The effectiveness of information security awareness programs

Users are the most critical element in IS, yet they present a potential and astonishing vulnerability and unmanaged factor (Xuemei et al., 2009). An example could be when users believe that they are using a secure password to access the organisation’s computer or to access the server room, but the secure password is readily guessable. Sharing the password with a partner or workmate, or writing it on the desk or on sticky notes to stick on the computer are other insecure practices. These kinds of incidents could be experienced in an organisation because users are not aware of the importance of passwords and the potential impact of breaches on organisational IS.

Despite this, most organisations are interested in carrying out technological and academic measures to achieve organisational IS goals. IS is a vast and complicated subject, and implementing passwords is not only the solution. Sveen, Rich, and Jager (2007) agree that passwords could work as an effective measure for IS if they are kept secret and cannot be guessed easily. Many IS training and awareness programs look at technical aspects such as access control, physical security and anti-virus measures rather than user knowledge. Moreover, in most cases, IS training and awareness is implemented after the occurrence of IS incidents, and such training and awareness programs only focus on event-related issues (Veseli, 2011).

According to Hansche (2001), users are critical to ensuring organisational IS, and most users are not aware of how their behaviour and actions result in experiencing many vulnerable IS-related incidents. Hansche also mentions that many users think of IS as a burden. Iivari and Hirschheim (1996) highlight that from the technological point of view about IS incidents, a user’s defence against the IS causes a problem in the execution of IS in an organisation. Hansche further mentions that users who are aware of IS can intellectually identify and
circumvent IS-related incidents. Therefore, looking from a user’s viewpoint, an organisation’s assets for organisational security represent IS from the social point of view, and the combination of the social and technical perspective provides a framework for an organisational role in IS. The ISF agrees that looking at IS from a socio-technical point of view keeps the technical, organisational and human aspects of IS stable (Durbin, 2016). The ISO agrees and believes in the technical, human and organisational issues surrounding IS, further stating that users who are new to the job must go through an IS training and awareness program. New users must undergo induction before conducting any task (SAI Global, 2006). So, if a user does not take any IS training and awareness program, then they would not be able to finish the job properly because they have no idea about how to access the organisation’s data and information. Bosworth, Kabay, and Whyne (2014) believe that IS relies on users rather than technology. Their research deals with IS user performance, such as social awakening, control status and group schism. These kinds of practices and performance from users show the social point of view, but to gain consistency in IS, the technical aspect should also be taken into account, which indicates that the organisational role regarding IS is socio-technical.

Lafleur (1992) mentioned in his research that IS relies upon the technical and organisational aspects that IS-related incidents can experience from the organisational and technical point of view. Martins and Eloff (2002) agree that the success of an IS program relies on the technological methods and end users. They also agree that organisational ISP should be designed in such a way that they support organisational goals and strategy, and this is the social aspect. They further argue that the success of any IS program relies on a computerised system, which is a professional aspect. This kind of socio-technical point of view posits that equal attention needs to be given to addressing the socio-technical related issues. McLean (1992) mentions that changing behaviour, attitude and opinion is essential to gain a reasonable level of IS. McLean’s study further focuses on user attitude and performance, and how an IS training and awareness program imposes a change in a user’s perspective and performance. NIST executes a process for implementing an IS training and awareness program according to a user’s particular role (Wilson & Hash, 2003). NIST further mentions that IS is a user-related issue, and the result to IS is achieved through users. It formulated a different kind of essential endorsing environment to change user performance and address the technical challenges in regard to IS. Thus, the technical, human and organisational aspects of IS are united, which represents a socio-technical viewpoint. Pipkin (2000) agrees that an IS training and awareness program is an approach that is designed for users to understand the organisation’s ISP, how to evaluate IS and how to report when the organisation experiences IS-related incidents. Proctor and Byrnes (2002) suggest that IS execution necessarily needs to attend to people, process and technology.

Spears and Barki (2010) investigated the relationship between user involvement in an organisational risk-mitigation program and organisational IS compliance. The investigation revealed that user involvement in a risk-mitigation program has a significant impact in
increasing security behaviour because of a better correlation between IS risk management, organisational business and improved ISP compliance, which leads to enhanced ISA. The investigation did not reveal IS training and awareness as a significant attribute of effective ISP, but it emphasised that ISA acts as a substantial factor (Chan & Mubarak, 2012). Spears and Barki (2010) further considered different technical challenges that could influence IS to build a prerequisite for ISA. On the other hand, they reflect on awareness topics because it is impractical to manage successful IS with only physical and technical measures. Therefore, their study focused on user performance and ISA from a socio-psychological point of view. Tudor (2006) also emphasises the need for user ISA, and reflects on how to motivate users to comply with IS. On the other hand, Tudor implemented the principle of avoidance (which is a method of accomplishing IS) to gain a welcome change in user performance and also to refer to the different aspects of technological approaches.

2.4.3 Implementing an effective security awareness program

There is a direct relationship between an implemented ISA program and ISB (Labuschagne, 2015). Many researchers have reviewed this relationship, while others have overlooked it. D’Arcy and Hovav (2007) researched how user awareness levels affect some abusing behaviour; their study was based on the general deterrence theory (GDT). They implemented the deterrence principle, which is a more active measure for screening IS, and conclude that some IS abuse is controllable. But they also implemented ISP and training and awareness programs as passive measures, which seem to be more effective against various violations (abuse ranges from medium level to high-level strictness) of IS. They generalised the model and started using IS-related protective software with the aim of increasing security awareness and minimising the user’s abusive intent. In a separate study based on the GDT, they observed that the IS user’s awareness before implementing any tactical methods for IS are kept under control by the user’s skills. For instance, if the user has expert knowledge of computer skills they use that ability to efficiently and practically handle the situation (Haeussinger, 2015). They concluded with the implementation of the deterrence principle in the training and awareness program and found that it is less efficient with users who know computers, and IS is more efficient for those users who work overtime and remotely. When they implemented the deterrence principle with the IS policy, however, they found that users cannot control the whole IS system even if they are skilled in IS. This is because security awareness makes users aware of risks and hazards so they can control those risks, but in security policy users need to follow the procedures from the security policy (D’Arcy & Hovav, 2007).

Bulgurcu et al. (2010) implemented a theory by merging ISA and ISP to reveal that the TPB builds a positive attitude to comply with ISP. Users’ positive values and morals affect their intention to act according to the organisation’s ISP. They also found that the results of a review on complying or not complying depends on user attitude and ISA being employed to enhance the user’s intention clearly or unclearly through opinion and resulting ideas. They further argue that an ISA program needs developing in such a way that it enhances user
attitude. Their prerequisite for an ISP is that users have the attitude to act in accordance with ISP (Bulgurcu et al., 2010).

2.4.4 Measuring the effectiveness of an information and security awareness program

The effectiveness of an ISA program cannot be measured as college grades are, such as with a distinction, credit and pass. But that does not mean that such a program is not measurable. The success of an awareness program depends on a reduced number of IS incidents, positive change in IS behaviour in employees, business processes being executed without interruption, and employees believing that IS is not only for the organisation but also for them. Portney and Watkins (2015) agree that multiple surveys to the same participants in a specified time are required to measure the effectiveness of the program. Their research also found that ISA programs are deemed effective when the results of multiple surveys are the same, or results have only changed a little.

Other factors also influence the accurate measurement of the effectiveness of the ISA over a specified time interval, such as employees leaving the job, being transferred to other departments or different locations, being promoted, or being on leave during the next survey (McCormac, Calic, Butavicius, Parsons, Zwaans, & Pattinson, 2017).

Allen and Yen (2002) also support the technique of surveying the same participants multiple times, and argue that if the time duration between surveys is a little bit longer it could show that employees still remember the content they learned in the training, and that the training is still effective in changing IS behaviour. Grimm (2010) suggests that the survey questions need to be designed in such a way that survey participants are encouraged to respond openly, freely and genuinely, because incorrect responses do not provide the desired measurement outcomes. Bowling (2005) introduced the concept of anonymity and privacy of the participants. For example, collecting the responses online and hiding the participant’s identity encourages participants to make a genuine response whereby they are not being judged (Duffy, Smith, Terhanian, & Bremer, 2005).

Eminagaoglu, Ucar, and Eren (2009) suggest that security awareness positively influences minimising IS-related threats. Their investigation found that an employee’s practice of using a weak password dramatically reduced after implementing IS password policy in the awareness program. They also found that to make the awareness program efficient, there needs to be continuity. Knapp, Marshall, Jr, and Ford (2007) support the concept of continuing the awareness program to keep employees refreshed. Kruger and Kearney (2006) argue that a security program should not only continue but also needs to be measured so new upcoming threats and risks can be managed. Cone et al. (2007) argue that the size and limitation of security challenges related to employee security awareness leads to oversights in the awareness program. Abawajy, Thatcher, and Kim (2008) suggest that
while measuring the efficiency of the awareness program, user awareness should not be the only focus, but also the program coordinator’s experience and proficiency.

2.4.5 Identifying the gaps in information security awareness

The research for this thesis identified the following gaps about IS awareness:

1. There have been various frameworks and models for IS training and awareness programs, but the studies have lacked a framework by which to measures its effectiveness.
2. The success of a security awareness program depends upon the active involvement of the participants, but the literature fails to measure the degree of involvement.
3. In computer-based delivery methods for awareness of IS, the literature provides no assurance that users have read and understood the contents.
4. The combination of social-technical factors has been shown to be more effective in changing user behaviour, such as user-friendly technology, clear ISP, and organisational culture, than pushing users to undertake a security awareness program.
5. While measuring the effectiveness of IS awareness, the literature fails to measure the user’s self-awareness level about the organisations IS before implementing the awareness program.
6. Most of the literature discusses organisations implementing an IS awareness program after the organisation has experienced a security attack.
7. For success of an IS awareness program, continuity of the awareness program and measuring procedure is required; however, the studies in the literature fail to measure when users leave the organisation, move to other states, or are promoted to higher positions.
8. The literature mentions that organisational users need to keep engaged in security awareness programs at certain time intervals, but fail to provide the exact time frame.
9. There is need for the continuity of the security awareness program, but the literature does not focus on updating awareness contents as new threats and challenges emerge.
10. The introduction of rewards in changing user behaviour results in users only being attracted to the position rather than changing their attitude, and penalties only create differences in the relationship between users and managers.
2.5 Information security training

In IS programs, security training and education plays a vital role in developing security awareness, and are more effective than preventive measures and controls. Various researches prove that organisations overlook assigning sufficient security training. Therefore, it is an essential aspect of an IS program to reflect on how managing and organising training modes assist in an effective IS program. Many training programs are designed to convey a message in one direction from single users to many with the help of professional skills. Alternatively, quite a few researchers state that implementing local knowledge during the process implicating the user’s presence is compulsory and proficient in achieving change in an organisation (Xiong, 2011). This process focuses on the significance of a user’s involvement, full consideration, and arrangement for enhancing their ISA and actions.

2.5.1 Organising training methods

Albrechtsen and Hovden (2010) investigated and assessed a process for a SETA program that consisted of various types of training and conclude that this sort of training process is useful in changing user performance for a temporary period. But implementing and conducting this sort of training program is not easy, and requires a lot of funds, and finding the time to attend the training program for busy users during working hours is often challenging. Therefore, more users and organisations are currently paying attention to computer-based training methods and e-learning. A survey conducted by ENISA found that more than half of European organisations implement computer-based training methods (Santa, 2007; Silva, Menezes, & Costa, 2012). Merete Hagen and Albrechtsen (2009) discovered that e-learning provides temporary progress in user knowledge, attitude and performance. E-learning consists of some essential features derived from IS courses from the organisation’s work process via verbal prologue, figures, songs, short videos on IS threats and risks, and motivational practice to think over. The e-learning process concludes with a test or exam that consists of multiple-choice questions with correct answers, comments, user opinions and discussion (Xiong, 2011).

Computer-based training is now more commercial, with no restriction on time management, and users can choose their own time to undertake this training. There is a set up cost in implementing computer-based training, but once it has been organised, there will be no extra cost in its delivery. So, computer-based training is more reliable compared to instructor-based training, and also works well when practice requires continuity for a large number of users in an organisation. Developing the end-of-training test in computer-based training acknowledges user evaluation about their understanding of the training method (Xiong, 2011). Wilson and Hash (2003) designed a security awareness online video conference, which is also an active method of e-learning for delivering training ideas. Online video conference methodology comes under computer-based training, using shared audio and video conferencing. The concept of audio-video conferencing is more effective, but is
more costly. It works the same as classroom-based training and managing user time is often a challenging factor. Wilson and Hash further discuss that mixing multiple training methods and delivery ideas in a single training session could professionally deliver information and attract the user’s attention. For instance, long PowerPoint presentations are often boring, so this kind of practice could be replaced by introducing animated videos, cartoons, short clips from a movie related to IS and taking users to real-time work zones. Users who undertake training sessions with multiple training delivery modes understand more and estimate IS challenges better compared to those who undertake training sessions with only one delivery mode (Shaw et al., 2009).

According to the Computer Security Handbook, an alternative way of presenting the message, such as IS-related posters, screensavers on desktops and laptops, pens, mouse pads and coffee cups, is relatively significant in raising ISA (Rudolph, Warshawsky, & Numkin, 2002). The handbook further suggests that posters or pictures need to be colourful and attractive and give a meaningful message, should be of standard size and font for quick notice. The pictures and posters need to be changed or moved frequently, and should be positioned in such a place where users always go, such as the kitchen, bathroom, meeting room, lift walls and walkway corridors. An organisation’s IS department could create the pictures or images, and some pictures could be downloaded from the internet. While downloading the pictures from the internet, it is always recommended to check for copyright infringement (some pictures can be downloaded for free, while some pictures require payment to download) (Xiong, 2011). According to Mathisen (2002), most organisations in western countries implement pictures as a method for conveying messages about IS to end users. But this method of transmitting a message to users has a temporary perimeter, and it would be demanding for security professionals to determine how much information is required when designing new posters and pictures. The pictures should be disseminated throughout the organisation and how many users look at the message and how many users neglect could be questioned.

An American company named Aetna introduced a compulsory method of undertaking an annual test on ISA (Janakiram, 2014). In this method, essential IS messages were conveyed to users, and taking the test would increase the user’s level of ISA. The test is based on the effectiveness of an earlier test and tried to cover its drawbacks. The test has been revised every year so that it includes Aetna’s IS-related subjects. Each test concentrates on motivating various IS subjects, and every user needs to attend to this test annually. This method of undertaking a test obliges users to remember their responsibilities and raises awareness of IS-related challenges on a minimal budget. Designing questions to focus on the organisation’s IS needs and assessing its security needs is often a challenge (Xiong, 2011).

Skinner (1999) suggests the idea of a reward in respect of a user’s performance; however, the user’s performance is possibly not repeatable in coming days in the same situation. Also, when a user’s performance is penalised, there is less chance of occurrence of the same
incidents in coming days. Therefore, proper management of social psychology (reward or penalty) techniques along with various methods of delivering a message to end users that end up with behavioural change, while designing proper terms and conditions of reward and punishment, carry some weight. Festinger and Carlsmith (1959) argue that the technique of rewarding does not result in an expected change in user attitude. The experimental evidence justifies the findings that huge rewards could be a reason for attracting a person to the position rather than the user’s preceding attitude. So, the challenge of user behaviour followed by reward techniques brings together the user’s attitude and behaviour even if user action is not related to beliefs. As an alternative, small rewards may be of more value when continuing behavioural changes indicate rewarding techniques are valued. Alternatively, while implementing punishment as valid in IS, the potential effect of a pessimistic by-product should not be overlooked. Driscoll (2014) found that the value of a penalty appears to be temporary, and it also has by-products, such as a decrease in the relationship and communication with the manager, not reporting security-related incident behaviour, anger and revenge, and fear to learn. Moreover, it needs to be kept in mind that reward and penalty practice needs particularising. What works for one person may not work for another person. So favourable results rely on user choice, and decision-makers should have some knowledge about how specific outcomes affect particular people, and facts and figures need to be collected from users for successful fortification (Xiong, 2011).

2.5.2 Delivering the information security training program

There has been very little research conducted in the field of delivering an IS training program, with the literature only focusing on computer-based and classroom-based training methods. Rudolph et al. (2002) suggest that there are various ways of delivering IS training, such as IS stories, videos, weekly meetings and group discussion on recent security incidents, and seminars and conferences. Peltier (2002) mentions that security newsletters, books, security-related videos, and books selected with the help of training coordinators are active mediums for delivering the security training message to users. Mitnick and Simon (2002) agrees that the continuity of a security training program is an effective way for increasing user knowledge and improving attitude towards IS, which ultimately changes user behaviour. Puhakainen and Siponen (2010) propose that there are other factors that need consideration while delivering the training session, for example, management should act as a role model by analysing the security incidents of competing organisations and discussing mitigating strategies of those incidents in the weekly meeting through animated videos. Tudor (2006) suggests the several stages of the IS program include designing training, reviewing ISP, identifying organisational strategy, creating a security training team, analysing security devices, ongoing training routines, delivery procedures, advertising security materials, making security training as a part of organisational business processes, and responding and reporting security incidents.

Kim and Homan (2012) conducted a comparative study on instructor and computer-based training, and found that the instructor-based training delivery method had a positive impact
in conveying the message. They conducted a couple of surveys with an interval of two and three months and found that instructor-based training delivery method had a high score. The outcome of their study suggests that organisations should not rely on one mode of delivery but should look for an alternative method for conveying the message to employees.

A separate study conducted by Reid, Jacobsen, and Katz (2005) on users maintaining information, found that computer-based training is useful in preserving the training message compared to other methods. Argyris and Schon (2007) suggest that organisations conducting the training program should deliver the training materials on a routine basis to make sure users do not forget the content. They further mention that users need to keep refreshed about the training content so that they do not forget to implement it in their work.

Jagatic, Johnson, Jakobsson, and Menczer (2007) and Okesola (2014) applied the concept of related training where information related to phishing attacks was downloaded from social networks and conveyed to users. In their research, they sent phishing emails pretending that they came from friends in social networks, and found that over half the users opened the phishing emails.

2.5.3 The effectiveness of the information security training program

Much of the literature shows that IS training is evolving, but lacks proof to support the effectiveness of training programs and their effect in the workplace (Waly, 2013). Cone et al. (2007) state that most security training programs are ineffective because they only focus on providing information about organisational security, rather than teaching users how their actions jeopardise the organisation’s IS. Ghazvini and Shukur (2016) mention that organisations implement security training programs only once, which is ineffective in changing the performance of users. A single training session does not make users think that the program is for them, and therefore they do not pay attention to the picture of the organisation’s security. Samy and Ahmad (2009) believe such traditional thoughts and practices are ineffective approaches to the success of any security training program.

Nowadays, there are many effective techniques that can be implemented in training programs, such as computer-based training, audio and video, workshops, and fun interactive programs. The main reason for implementing such activities is to keep users engaged in the training program so they will learn and understand the concepts and purpose of the training program, thereby making it fruitful. Sometimes, though, the training materials are too innovative for participants and they have difficulty understanding them, especially those who are new to IS (Ghazvini & Shukur, 2016). Those participants might need another training program that only focuses on the basic information about IS rather than fitting all users into the same training program.

Some studies have found that participants undertaking training programs who learn and understand the materials do not seem to implement those skills and knowledge in their
workplace (Asai & Perez, 2012; Shahri, Ismail, & Rahim, 2012). Many researchers have failed to evaluate participants’ behaviour before and after the training session, which then does not signify the effectiveness of the training program. Moreover, in some programs the coordinator does not introduce any productive activities that could attract more participants (Monk, Van Niekerk, & Von Solms, 2009). For example, the coordinator resents using the same boring lectures and PowerPoint slides, and does not include critical thinking or fun activities to motivate participants to understand that the training is not only for organisational purpose but also for them. For an effective security training program, it is necessary to identify and differentiate the factors that led the training program to fail in the past (Nagarajan, Allbeck, Sood, & Janssen, 2012).

The gaps that arise in the literature identifying the factors for inefficient training programs require further processing to develop an effective training program (Parks, Chu, & Xu, 2011). Waly (2013) and Yamnill and McLean (2001) suggest that to make the training program successful, participants need to be motivated and inspired in such a way that they implement the knowledge and skills gained during the training session into their daily tasks. Additionally, to make training programs effective they should incorporate the organisational ISP, risk management and business contingency plan. There should be different training programs based on the participant’s job role and qualifications. The primary purpose of the training program is to teach the participants about IS, how their activities make the organisation vulnerable to attack, how to mitigate new threats, and making organisation’s information systems secure (Shaw et al., 2009). For example, a general employee training program should focus on basic IS and participant security activities, such as sharing passwords, browsing social networking sites on the company’s devices and downloading free and pirated software. For managers, the training program should focus on risk assessment, and how IS influences business processes and decision-making. For security professionals, the training program should focus on designing the training program, researching new threats in the computing environment, preparing security audits and reports to managers, and maintaining security processes and business performance.

The delivery process also affects the efficiency of the training program. For example, some participants prefer classroom-based training while others like online training and workshops. The delivery of the training content depends on the participant’s learning capacity. For example, some learn through listening, while others learn through videos, games and discussion. Therefore, the security professionals who are designing the training program should focus on various ways of making the training program effective (Ghazvini & Shukur, 2016).

2.5.4 Implementing an effective information security training program

The organisation should implement security training to every user, and to make the content effective it should focus on proper handling of organisational IS and the possible outcomes
of mishandling it (Wipawayangkool, 2009). Marks and Rezqui (2009) agree that security training is an efficient way to improve the user’s knowledge so the content should be relevant to training expectations. They further argue that security training should be performed on a continuous basis and that every training session needs updating as there is the possibility of new threats and risks in the future (Ahlan & Lubis, 2011; Pastor et al., 2010; Wipawayangkool, 2009). Rotvold (2008) states that an IS training program conducted by security professionals on a yearly basis would be adequate in including any new material. Rotvold’s study found that the content and materials used were same for all groups, suggesting that the training should be designed to assist employees doing their tasks.

Wright (2005) suggests that seven factors require consideration when implementing an effective IS training program: identifying the goals, selecting the training coordinator, choosing the participants, executing the training, schedule maintenance, cyclic measurement, and describing the supportive goals. Maqousi, Balikhina, and Mackay (2013) propose three methods for implementing a security training program and delivering the message: implementing the training program on the organisation’s website and intranet, implementing the training content through organisational management, and designing another site for the IS training program. Their study found that implementing a training program through the organisational intranet is useful because every user could access the organisation’s website. Toth and Klein (2013) suggest three levels of implementation to make the security training program efficient: basic, educational and higher. The basic level contains the necessary information about ISP and risk management for those general users. The educational level provides in-depth knowledge for managers and IS professionals who are responsible for the ongoing learning process in a changing security environment. The higher level is for IS professionals so they can anticipate tackling security issues and challenges, and design and update the ISP (Beyer & Brummel, 2015). Stahl and Pease (2011) suggest that the training program must incorporate commitment from employees, management and security professional for its effectiveness.

2.5.5 Measuring the effectiveness of an information security training program

Orgill, Romney, Bailey, and Orgill (2004) measured the efficiency of the IS training program by conducting a training session on phishing and social engineering attacks and reviewing through phishing and social engineering audits. Before conducting the social engineering attacks, they send a phishing email asking for the employee’s login details, such as username and password, pretending that it came through the organisation’s management. They found that more than half of the employees gave their login details. Their investigation further concludes that there is no consistency in employee awareness level on phishing and social engineering attacks in other departments.

Schiffman (2008) conducted another social engineering survey in the United Kingdom, showing that employees exchange their login details for a bar of chocolate. In another study (Aloul, 2012), more than half of the employees became the victim of social engineering
attacks by providing their login details when the attacker pretended they were calling from
the IS department. That survey further found that many employees use the same password
for different purposes and never change them, even after security training on social
engineering attacks and password policy.

Kumaraguru, Sheng, Acquisti, Cranor, and Hong (2008) conducted phishing audits in a
Portuguese company, and found that after implementing phishing training, the user’s ability
to identify the phishing emails increased by more than half in the first audit and increased
further in the second audit, which emphasises that the user’s training on phishing attacks,
was effective.

Argyris and Schon (2007) argue that the effectiveness of information training depends on
how users learn. They propose a theory on the user’s learning process that highlights that
they learn according to stages. The effectiveness of the learning process is measured after
delivering the training material. They evaluated the user’s learning process by
differentiating the user’s expected action and the user’s actual action.

Grohmann and Kauffeld (2013) measured the efficiency of training questions based on the
user’s psychology that not only evaluates their responses, but is also universally acceptable
for various training materials that assess security training in a company or within many
companies. Danziger and Yee (2000) measured the efficiency of computer-based training
and instructor-based training, and found that users receiving instructor-based training
perform better because every user can communicate with the instructor. Rehberg, Gazzillo,
Diaz, and Middlemas (2009) also support the efficiency of instructor-based training because
the instructor provides the training content to every participant and they can mark the
training content if they do not understand for discussion with the instructor later, which
cannot be done in computer-based training. Kim and Homan (2012) measured the efficiency
of instructor-based and computer-based training by surveying both kinds of training at two
and three-month intervals and found that participants retained content in both methods
after two months, but forgot after three months. They further suggest that organisations
must continue the training program after a specific time interval to maintain its
effectiveness. They also mention that both kinds of training enhance a user’s level of
knowledge and that users memorise training content but do not retain it for a long time.

McElroy and Weakland (2013) state that before implementing the IS training and awareness
program organisations must be aware of how a designed program could provide practical
and realistic measures. They further state that implementing an open-door policy is critical
for the success of a training and awareness program. In an open-door policy, organisation’s
management conducts frequent meetings with its functional departments to discuss how to
train and educate their employees and departments, and provide feedback about the
training and awareness program to management.
Pironti (2007) and Merete Hagen, Albrechtsen, and Hovden (2008) agree that IS training and awareness programs should be evaluated from every aspect of the organisation, including technical, cultural, economic, ethical, management, individual and environmental aspects. This process is desirable, but is also challenging and unrealistic because of organisational policy limitations. Merete et al. (2008) further implemented a combined research method: using a quantitative research process for large organisations and a qualitative research process for small organisations, to measure the effectiveness of the training and awareness program. Savola (2013), Posey et al. (2014) and Goel and Shawky (2009), however, argue that most research concentrates on evaluating detached factors and acquaintances, which results in limited rational experiments, and that all training and awareness programs cannot be measured only through qualitative and quantitative research processes. The results gained from those analyses could be biased because the outcomes of training programs are evaluated using opinion and intelligence.

Parsons et al. (2013) support the Human Aspects of Information Security Questionnaires (HAIS-Q) model, which measures most areas of IS, such as individual, technical and organisational. However, this model only evaluates the theoretical variables and could be subjective to employee behaviour because behaviour is affected by personality, organisational security culture, working environment and co-worker attitude. In 2017, the HAIS-Q model was implemented in many Australian organisations and universities to measure the effectiveness of information security training and awareness programs, with the research conducted on university students and organisational employees revealing that participants scoring high in the HAIS-Q also scored high on the phishing assessment (Parsons et al., 2017). Wissen (2017) conducted research in European organisations and implemented the HAIS-Q model because it follows the theory of knowledge, attitude and behaviour of Kruger and Kearney (2006), which ensures that increasing user knowledge on organisational policy and procedures, would make positive changes in their attitude and behaviour towards organisational policy and procedures. The HAIS-Q model also mixes up the quantitative and qualitative research process for data collection and analysis that had been already implemented by Karjalainen and Siponen (2011). However, their survey only measured certain aspects of an organisation’s security and employee behavioural change because it is not efficient in covering recent changes in IT globally (Schaeken, 2018).

McCormac et al. (2017) state that organisations and IS researchers could implement the HAIS-Q to measure the effectiveness of information security training and awareness programs, the organisation’s information security cultural changes, and the effect of information security concerns. They further mention that the HAIS-Q is a reliable instrument for measuring the effectiveness of information security awareness training of employees, and to establish the potency and limitations of participants and organisations. Their research also found that participants who completed the HAIS-Q are more aware and cautious. They highlight that further research is required to investigate the difference in individual behaviour, such as why there is change in behaviour in some participants after
implementing the HAIS-Q and why other participants are resistant to change. They also recommend that while measuring participant behaviour, it would be effective if further details are provided, such as who the participant is and which organisation they belong to.

Montesdioca and Maçada (2015) initiated a model of employee satisfaction through the information security policy and training implemented by various organisations in Brazil. Their model emphasises that employee awareness about information security program performance and the act-benefit ratio influences employee satisfaction with information security policy and training.

Vaezi and Chin (2015) argue for the significance of evaluating participant satisfaction with information security and designed evaluation survey questions. Their intention was to evaluate participant satisfaction with various features of information system security. The outcomes verified that surveys can be consistently implemented to evaluate participant satisfaction and could be implemented in the future as well.

Scholl, Leiner, and Fuhrmann (2017) conducted surveys to measure the effectiveness of security training and awareness programs and found that various organisations still struggle to implement an effective measure to evaluate the success of such programs. They also found that some organisations still do not know which metrics to measure to establish the success of information security training and awareness programs, and if security metrics are implemented to measure success, organisations still struggle to determine why employee security awareness does not improve after implementing the program. They further mention that before evaluating the success of an information security program, it is essential to understand the current position of an organisation and what it is expecting from the program, so its current position will be benchmarked against the outcomes of the program and its effectiveness measured. They also introduce the concept of digital benchmarking in the form of digital games, where information security related issues are conveyed through games and participant knowledge and awareness levels are measured based on how they respond to the security issues and scenarios. Scholl, Leiner, and Fuhrmann (2017) also suggest that one method would not be sufficient; incorporation of various methods is required when it comes to measuring the effectiveness of information security training and awareness programs. For example, while measuring participant awareness, a survey could be implemented to monitor the organisation’s security procedure to recognise the organisation’s problems and benchmark against the security measures. The implementation of various methods relies on the organisation’s measuring attributes, such as size and culture, and whether it is within allocated funds.

Shoshan (2017) states that participant’s information security awareness training programs are always ineffective when measuring phishing attacks for a couple of reasons. First, humans are by nature curious and second, phishing attacks are highly advanced, more so than whatever is taught in phishing training programs. For example, humans are always curious when a phishing email has eye catching subjects and phishing attackers use machine
learning systems, which let the attacker know whether the phishing email has been opened and the malicious files are installed in employee’s device or not.

Kurowski (2018) agrees that individual knowledge on information security policy forms the significant background for compliance of information security policy, which means that if an individual does not know about the information security policy then they would not act according to the policy or coincidently follow it. Kurowski further introduces an evaluation tool for measuring user knowledge on information security policy and their behaviour after complying with information security policy in two dimensions. The first dimension establishes the user’s compliance using self-reporting, and survey questions are focused on user behaviour and topics from the information security policy. The second dimension establishes the reliability of the user’s compliance using self-reporting by evaluating the difference between the user’s individual knowledge on information security policy topics and the knowledge gained after reading the information security policy.

2.5.6 Identifying the gaps in information security training

The research for this thesis identified the following gaps in IS training:

1. Most organisations implement a training program only once, which fails to measure the productivity of the program.

2. In most organisations, users do not have freedom to choose the training methods that affects their performance.

3. The concept of “one size fits all” is still implemented in many organisations, which means that organisations fail to provide training to its users according to their job position.

4. Organisation’s users often do not change their attitude and behaviour even after they have received the security-related training, for example, about changing their password.

5. Most of the literature shows that organisation management fails to measure the effectiveness of the training content and the organisation’s expectations before implementing.

6. Much training program content consists of lectures and slides, which is not effective, but the organisation fails to conduct a training program that could be made innovative by implementing real-time scenarios in the actual workplace.

7. Most organisations include posters and videos in training content, but fail to weight how much information needs to be included when designing them.
2.6 Information security investment

Research on IS training and awareness investment has been carried out by many researchers. It is not an easy task to build up the conceptual model for IS investment because it has to deal with various strategies, policies and procedures, and legal and technical issues. The essential thing in IS investment is that investment in other areas aims to have some earning in return. That return can be visible, but investment in IS does not make an apparent return; rather it reduces the risk (Bohme & Nowey, 2008). If the investment in IS is successful, then the results are probably indefinable and cannot be viewed. Investing in an organisation’s IS does not give the immediate results, but it could lead to having positive effects on the organisational culture by minimising possible risks and threats. Two prospects need consideration before investing in ISA; they are commonly known as previous stake and previous position. Stake prospects are intended to sustain judgement by evaluating the expenses and reimbursement of potential investment. The previous position prospect points towards the investment that has been done earlier and assessing whether the investment that an organisation has assigned was well organised or not (Weishäupl, Yasasin, & Schryen, 2015). The issues discussed above deal with the resource-basis concept (such as organisational information systems, data and procedures could be prototyped as resources, and definite and indefinite resources could be precisely measured) and the organisational learning process (which does not concentrate on an organisation’s mechanism in depth), as both are well-known concepts in IS literature. The resource-basis concept is naturally fixed, which focuses only on the ownership of resources and aptitude. It signifies that the resource-basis concept does not report actual and sequential results. On the other hand, the organisational learning process thinks of useful and subsequent results, and models a learning evolution gained from the organisation’s previous error that eventually guarantees the organisation will change information into admired wisdom, which results in raising its long-lasting amending aptitude. Organisational learning processes allow organisations to respond enthusiastically to altering their background (Kwon & Johnson, 2014). Resource-basis concepts administer and manage the significant features that need to be borne in mind while deciding on investment, and make assumptions on multiple sections of the organisational environment and their relationships between one another (Wade & Hulland, 2004; Weishäupl et al., 2015).

The resource-basis concept is considered an essential theory in the history of management theories that could indicate how the organisation works. The primary intention of the resource-basis concept is that organisations have to get control of useful, exceptional, unique and irreplaceable resources, and get an aptitude to gain an endurable competitive benefit. Organisational resources are defined as the organisation’s properties, competence, procedures, features, skills and intelligence that are ruled by the organisation with the intention of allowing and employing the policy to enhance an organisation’s efficacy and competence (Demirhan, 2005). Many researchers and practitioners agree that investment in organisational ISA is the subset of whole IT investment (Weishäupl et al., 2015). The
resource-basis concept is therefore suitable for outlining IS investment for the following causes:

- The non-IT resources, which require safeguarding and which safeguard the organisation’s assets, could be modelled as resources.
- The resource-basis concept has been already implemented in the IS literature to outline IS investment (Cavusoglu, Mishra, & Raghunathan, 2004).

Due to the global emergence of IT and its activity in the competitive environment, organisations must enhance their goods regularly and make progress to create and retain their competitive benefit. At the new curiosity in the organisational learning process by researchers and practitioners suggests, this is an innovative and competing idea (Culnan & Williams, 2009). Here learning is defined as the identification and resolution of mistakes, and the mistakes refer to any aspect of skills or a craft that leads to the action being unsuccessful. The identification and resolution of errors makes the lack of identification or resolutions impede the learning process (Culnan, Foxman, & Ray, 2008). Additionally, complicated and impulsive issues are likely to be more indefinite, and are related to an advanced error rate that creates difficulty in employing valuable plans and performance (Argote, 2011). It is evident that investment in IS is a complicated issue; it would therefore be advantageous from the organisational learning process point of view in particular to explain how the effectiveness of the decision could be progressed by reporting the previous experiences in the comment field (Kwon & Johnson, 2014). Also, the organisational learning process gives a dynamic look that is continuously employed to investigate the results of investment in IS. Theoretically, the impacts that affect IS investment determination could be outlined as a principal variable, and resources for IS investment could be summarised as an action policy that results in advanced ISA (Weishäupl et al., 2015). The organisational learning processes employed as a recommendation in the framework of IS investment is explained as a transformation of the organisation’s performance as it congregates skills. Organisational learning processes consist of three elements; principal variables, action policy and results. These elements are explained in the next section.

2.6.1 An Integrated model for information security costing

Principal variables are the goals organisations attempt to reach. When an organisation sets up its activities with goals, principal variables act as a motivational factor in determining IS investments. For example, a specific purpose could be operating under government and trade partners and union rules.

Action policy defines a series of processes that are premeditated to accomplish specified objectives and assessed by principal variables. Here, action policy means investment in organisational IS assets, such as installing anti-virus, firewalls and cryptography technology, which produce the results. For instance, organisations investigating the SETA program
anticipate minimising IS incidents from employees. Results consist of entire outcomes related to investment in IS, either planned or unplanned, and practical or impractical (Weishäupl et al., 2015). Results could be compared with the principal variables; whether organisations have implemented the proper action policy or not, and standard results mean the diminution of IS incidents and magnifying service convenience.

Both the resource-basis concept and organisational learning processes are related to a multi-theoretical model that keeps the benefits in an incorporated model for standardised assessment of IS investments. Moreover, this integrated model outlines the organisational features, such as business procedures and security asset management submissive within the known area of investigation. The innovative idea is that government features combine industrial features, trade partners and union features, and business procedures that affect the organisation’s judgement in IS are classified as principal variables. Principal variables influence determining the investment in IS assets, which be in accord with action policy. For instance, assessment in IS investment must meet the national accreditation standard to get ahead of IS appraisal. IS investment in technical assets or human factors relates to action policy, which signifies that actual investment in SETA is the component of action policy referred to as the human resources of IS. IS investment affects the results as described by the effects of action policy on the outcomes (Ghose & Rajan, 2006). The consequences involve an impact the security investment has on unsecured assets, security procedure, security procedure performance and whole organisational performance (Weishäupl et al., 2015).

Figure 2.6.1: Integrated model for information security investment (Weishäupl et al., 2015)
Figure 2.6.1 makes it clear that principal variables, such as government rules, industry regulation, and trade partners and union rules, have a significant effect on the action policy. The organisation’s business processes have an impact on judgement in the organisation’s IS investment (Anderson, Bohme, Clayton, & Moore, 2008; Melville, Kraemer, & Gurbaxani, 2004). For example, organisations need to implement further IS capital to satisfy national accreditation. Action policy also has a significant impact on the results, for example, investments in the IS also affect non-IS resources, organisational business processes and performance and organisational security processes and performance (Khansa & Liginlal, 2009). For example, investment in biometric technology helps an organisation preclude unauthorised admission to an organisation’s property, and biometric techniques do not affect the organisation’s data and systems (Weishäupl et al., 2015). Security processes and business processes are not standalone now (Wang, Chaudhury, & Rao, 2008). A business process is always vulnerable to the risks and threats, and is still required to operate consistently to assure the organisation’s triumph (Neubauer & Heurix, 2008). For example, in biometric technology identification and verification are the security processes that affect the business process because when the identification and verification process is interrupted or disturbed, the organisation’s workflow is impeded. Security processes also affect security process performance because the effectiveness of security processes is addressed or measured by security process performance. For example, the number of attempts rate (which is acceptance rate and failure rate) in biometric technology for identification and verification determines the effectiveness of the biometric system’s performance. Security process performance also affects business process (Rowe, 2007). For example, in biometric systems, a low rate of failure during the identification and verification process ensures that the organisation’s workflow is not disturbed. Organisational business value has a direct impact on the organisation’s overall performance, such as its assets, process and workflow. An organisation is said to be successful when its effectiveness and competency is enhanced, and an organisation’s workflow occasionally interferes and is promptly restored and retrieved (Weishäupl et al., 2015).

The single loop in Figure 2.6.1 consists of changes that are dependent on current rules and regulations, and does not implicate the principal variables. A single loop exists when the outcomes of the action policy warn of IS incidents and the organisation measures the assured findings to make sure that the implemented strategy is pre- eminent, exclusive of changes in principal variables. The double loop consists of the changes in the principal rules and regulations in action and performance. The double loop exists when the outcomes of investment decisions do not comply with the organisation’s goals, and encourage an organisation to reassess the principal variables and investment separately. The main difference in a single loop and double loop is that a single loop provides the conventional example of action, but a double loop includes comment and opinion that are more valuable during the decision-making process (Shen & Jones, 2005). On the other hand, the tremendous amount of learning conducted in an organisation is a single loop, as it
recognises and fixes the mistakes and ensures that the task is completed and the action stays within the specific rules (Weishäupl et al., 2015).

2.6.2 Information security investment research gaps

The external attributes, such as government rules, corporate rules and trade union rules, affect an organisation’s IS investment judgement (where to invest, how much to invest and when to invest). For instance, there are government rules in the context of the Australian Privacy Act 1988 for all organisations, Office of the Australian Information Commissioner for all agencies, Australian Privacy Principles for all credit providers and Healthcare Identifiers Act 2010 for healthcare providers (Office of the Australian Information Commissioner, 2015). There have been fewer studies conducted that focus on IS investment judgement in the area of government rules and regulations, and the results of those studies found that government rules have a negative impression in IS investment judgement (Weishäupl et al., 2015). Ghose and Rajan investigated the results of governance obligation and information assertion in the practical manner of investments in IS (Ghose & Rajan, 2006). In the context of Australia, a new trade rule where large multinational organisations have to pay 40% tax on their net profit to the government has resulted in organisations minimising practical investment in other IS resources such as SETA programs and the monitoring of their effectiveness. For medical and healthcare providers, an external factor such as changes in the government and its policies affect investment in IS, sometimes leading to cuts. Whenever there are arguments and controversy about cutting investment in IS, concerns are raised about ISA and need for IS investment. International standards for IS such as NIST, ISO/ International Electrotechnical Commission (IEC) 27001 and 27002, ISF (International Security Forum) and others also affect an organisation’s decisions in relation to IS investment (International Organization for Standardization, 2013; Wikipedia, 2014). Another factor that affects IS investment decisions is the country’s development status. For example, organisations in developed countries are more concerned about ISA and investment because the background and culture of the country decide the requirement for IS investment and awareness (Weishäupl et al., 2015).

Industry rules affect how IT is implemented in an organisation to generate business revenue. For example, the main important aspect of organisational IS is an incorporation of an organisation’s IS resources, which continues the organisational business processes with the intention in reality that investment in organisational IS does not only relates to the organisation’s structural design, but also needs to generate revenue. Here, the issue or gap for an organisation is that there needs to be a joint balance between implemented IS resources and the best possible investment, which is mostly not included in the academic literature (Botha, 2011; Weishäupl et al., 2015).

The effect of the organisation’s trading partners and union rules in relation to IS outsourcing also needs to be contemplated. According to Anderson (2001), outsourcing causes a reduction of the investment in improved security levels, as organisations study from the
errors that another organisation experiences. It would not be a good idea to share data and
information related to an organisation’s IS because they are highly sensitive and contain an
organisation’s classified information that signifies business secrets. Thus, sharing highly
classified information could get it into the wrong hands, resulting in a drop in the
organisation’s trust and reputation, with a negative impact on market value. It would be
difficult to regain consumer trust and reputation once an organisation loses it. In order to
address the gaps in information sharing, Gordon encourages organisations to share only
information that has been administrated by legal requirements (Gordon & Loeb, 2002).

Nowadays information sharing and outsourcing have become critical because of
complicated IT. When organisations share or outsource their data and information for
processing, the total budget from installation to ongoing costs and savings that will be
gained by outsourcing needs to be evaluated. Because of this, organisations hardly ever
outsource IS-related tasks. There have been fewer studies conducted in the area of
information sharing and outsourcing where general employees are isolated. If organisations
realise that IS is no longer a technical issue, but is now a business issue, everyone has a role
to play and none of the employees (including top management to general employees)
should be isolated. This research also addresses this issue (Weishäupl et al, 2015).

Investment in IS, both human or technical, affect non-IS-related resources such as whole
organisational resources, its procedures and execution. For example, a biometric technology
that precludes unofficial admission to an organisation affects non-IS resources, such as
organisational data and information, and also physical devices. It is well known that the
majority of IS-related incidents are due to human negligence and error rather than
technological malfunctioning, therefore investment in the human factor as an IS resource
should not be overlooked (Weishäupl et al., 2015). Here investment in the human factor
represents the SETA program, workshops related to IS, group meetings and discussion on
issues relating IS.

Investing in IS has a positive effect on organisational security processes as it protects the
organisation’s overall security. A security process would be considered as advantageous
when it is periodically accessed and considered to employ frequent assessment according to
organisational policy and procedures. In other words, it could be said an IS process should
be customised along with changing situations in the long run.

Jakoubi, Neubauer, and Tjoa (2009) define the business process as the continuous and
professional operation of organisational business processes, which is the key element for
successful business. Due to the rising number of IS risks and threats, an organisation needs
to consider security processes that assure the accurate functioning of the business process.
Jakoubi, Neubauer, and Tjoa also consider the security of business processes from a risk-
management approach and recommend a model for risk-based awareness business process
management. They found that investigating in securing the organisation’s business process
is still evolving, which has lots of possibilities. Still, securing the organisation’s business
process all the way through to the IS process has been paid no attention in the academic literature whatsoever (Jakoubi, Neubauer, & Tjoa, 2009).

The effectiveness of IS processes can be evaluated through IS process performance. For instance, the effectiveness of a biometric authentication process could be evaluated by counting the number of attempts for identification and the verification process. These types of IS process performances are practical in equating the other IS processes to estimate investment for IS. There has been no research carried out in relation to the IS process performance method (Weishäupl et al., 2015). As discussed earlier, the IS process affects an organisation’s business processes. There is also influence between IS process performance and an organisation’s business process performance that needs research that agrees with this influence.

The overall performance of an organisation is significantly affected by the organisation’s business process performance and its IS progress performance. As IS processes safeguard an organisation’s business process, IS process performance and its organisation’s business process performance and overall organisational performance are exactly related to the common logic that the higher the IS process the better the quality of organisational performance. There has been no research conducted until now on how the IS process performance influences a whole organisation’s performance. Also, it is still uncertain how an organisation’s overall performance is affected by the organisation’s learning process (Weishäupl et al., 2015).

2.6.3 Identifying the gaps in information security investment

The research for this thesis identified the following gaps about IS investment:

1. The literature review identified that external factors such as government policy affects the investment in an organisation’s IT but there is a gap in the literature about measuring the volume of investment affected by external factors.

2. There is need for continuous support of IT to sustain the organisation’s business; however, the literature does not show how the investment in IT generates an organisation’s ROI.

3. The literature addresses IT outsourcing and partnership programs for sharing information, but does not justify the cost for that information sharing, or information about the resultant ROI.

4. The literature fails to measure the effectiveness of IT outsourcing programs on general users because the communication and information sharing happens between outsourcing companies, and the organisation’s managers and general users are isolated.
5. Most organisations still believe that IS investment means investment in the technical side of information systems, such as hardware, software and networks, but overlooks non-technical factors, such as implementing, measuring and monitoring of IS training and awareness programs. Most of organisations fail to periodically measure IS awareness programs because there is no investment for ongoing support.

6. Securing the organisation’s business processes and business performance is still a challenge in a competitive environment, and the literature fails to measure how investment in IS secures the organisation’s overall business processes.

7. When an organisation minimises or cuts off IT budget, the first thing to get rid of is its investment in training and awareness programs. The investment in training and awareness programs does not mean buying the program from third parties; organisations could design the training and awareness program in-house by communicating with IT security professionals and organisation managers. Therefore, the literature lacks information about implementing and continuing training and awareness programs when there is a low or no budget.

2.7 Management support

Bulgurcu et al. (2010) describe IS training and awareness as user understanding of ISP. They also explore employee logic by ISA performance and its consequences on IS accordance. They found that user thoughts and values inspire employee’s outlook to act under IS, and these thoughts and values are induced by the level of IS training and awareness (Chan & Mubarak, 2012). Additionally, putting more weight on IS training and awareness programs could hopefully result in change in employee thoughts and support.

Spears and Barki (2010) investigated the affiliation between employee involvement in organisational risk management and the organisation’s security agreement. Their investigation found that employee participation in organisational risk management seriously assisted in enhancing organisational security control performance because of an association between organisational IS risk management and its business environment, enhancement in IS-related policy and procedures and also outshining the IS training and awareness program. Their research focused on a SETA program as a significant contributor, but their study lacks consideration that SETA programs act as a substantial contributor to an organisation’s successful ISP (Spears & Barki, 2010).

It is necessary to review the current literature on IS training and awareness from the management point of view. McFadzean, Ezingeard and Birchall (2007) agree that top-level management awareness about IS plays an active role in organisational security processes.
They state that top-level management has an overall view of the organisation and authority to remodel the organisation. Their study also reveals that top-level management decisions and an organisational IS training and awareness program determine the organisation’s strategic performance. Knapp, Marshall, Rainer, and Ford’s (2006) investigation also reveals that top-level management encouragement is directly proportional to the organisational IS culture and policy and procedure implementation. However, their investigation did not wholly look at the role of management in IS training and awareness as an estimator for an organisation’s security performance, but rather focused on the significance of management support and its importance in changing the organisation’s IS dedication.

Mouratidis, Jahankhani, and Nkhoma (2008) explored the variation of organisational network security opinion between organisational management and organisational IS professionals. Their study discovered that management has a different opinion concerning organisational network security from IS management. IS professionals can have better knowledge about how to ensure adequate network security, monitoring network security and how to respond if anything goes wrong with the organisational network security. Organisational management represents the decision-maker, who may or may not implement the security measures recommended by IS management, or organisational management may have another approach to securing an organisational network. Organisational management and its IS professionals having the same attitude is the best solution, but a difference in opinion results in a cynical effect on the organisation’s ISP. In other words, it could be said that there is a need for IS training and awareness for management.

Choi, Kim, Goo, and Whitmore (2008) emphasise the significance of ISA in organisational management by studying the correlation between security awareness and undertaking action. Their study found a definite relationship between security awareness and undertaking the actions. When a high level of ISA is required in organisational management, there is more probability that administration will take steps towards defensive measures. They find that management implements defensive measures after a security incident occurs. Thus, organisational management will not enforce any defensive rules unless security incidents happen. Therefore, increasing the ISA level within organisational management can advance in organisational IS performance.

Lane experimented with IS management in Australian institutions, and found that IS training and awareness is still a challenge in Australian institutions (Lane, 2007). Lane’s experiment proposed that Australian institutions do not have sufficient IS training and awareness programs, which results in low performance. Therefore, it is necessary for an organisation to employ IS training and awareness programs to promote organisational IS cultural commitment that finally progresses to user responsibility in regard to IS.

A separate study conducted by Spears and Barki (2010) not only reflected on the effect of the human factor in ISA, but also implemented an IS training and awareness program. They
conclude that humans are an essential factor that needs evaluating as an element of the organisational risk-assessment procedure. User unresponsiveness represents critical threats to organisations, and IS training and awareness interacts with commitment. They state that organisations should execute user risk assessment to understand user ISA level, and this process needs to be a part of an organisation’s overall risk assessment procedure to spot the area that needs more attention. Therefore, inadequate IS training and awareness in an organisation causes significant threats to its information system and business that requires proper evaluation and subsequent reduction.

A study conducted by Merete Hagen, Albrechtsen, and Johnsen (2011) in organisations in western countries found that organisations focus more on policy and procedures while employing any methods, but they focused less on IS training and awareness. Their study also reveals that ISA methods were predominantly successful in IS practice. The result shows that the relationship between the execution of IS practice is inversely proportional to its success (Khan, Alghathbar, Nabi, & Khan, 2011). For example, IS training and awareness and IT control weight equally to achieve a successful IS program. This kind of structure is applicable in most western organisations, which is evidence that Australian institutions and companies are in the same circumstances. Another study carried out by Laaksonen and Niemimaa (2011) found that IS training and awareness have a positive effect on users’ views about ISP, and it needs consideration while planning such policies. They also found that the number of security problems involved in ISP was minimal and focused more on a technological approach rather than the human factor of IS management.

2.8 Information security policy

Researchers discuss ISP as being tremendously significant, and carrying additional weight to organisational IS. ISP covers the issues that organisations face due to misapprehension of the meaning of ISP and its operation. Olson and Abrams (1995) define ISP as a set of organisational rules and regulations that authorise how the organisation handles, deals with and distributes its resources to reach identified ISP goals. While considering these rules and regulations, it should utilise users to judge whether their activities and performance breach or meet the terms of ISP. In other words, ISP plays a strategic role in outlining an organisation’s direction and also acts as a convenient procedure for end users. Therefore, ISP requires focus on advanced management and end-user supervision (Lane, 2007). Höne and Eloff (2002) outline the primary purpose of ISP as the rights and responsibilities of users who utilise the organisational resources. According to Higgins (1999), ISP acts as a foundation for organisational IS management. It is known that successful IS management relies on the endurance and realistic use of ISP. In much research, ISP has been extensively discussed and employed, and its relationship with IS is significant. Wood explains that ISP is a critical factor that manages the procedures of organisations (Wood, 2002). ISP is now becoming more sensible in carrying out the process of organisational information systems and other aspects of organisational strategy, which means that organisational ISP requires
more focus and should be promoted to the leading position of the organisation. The literature verifies that ISP is widely accepted and has more value in the organisation. Fulford and Doherty (2003) studied the execution of ISP in big organisations in western countries. They launched several thousand questionnaires to IS experts, but only got responses from a few hundred participants. Their research was based on ISP regarding IS distribution, publicity of ISP and features that influence the success of ISP. Their study found that there is a high rate of policy subsistence, and many organisations depend upon only one method for distribution. In other words, just one way for distributing ISP is more likely to drop down the target because it might not be accessible to each interested user. Their research concludes that there is a shortage of academic research in some areas of ISP and an organisation’s lack of concentration in those areas. The survey conducted by Ernst and Young focuses on the acceptance, or implementation value of ISP instead of identifying the areas included, and their study does not highlight an organisation’s effect on ISP (Bennett, 2004).

According to the research conducted by Xiong (2011), an organisational ISP employed on the organisational website has no positive effect on employees over providing the hard copy. The study illustrates that those employees who read organisational ISP on the organisational website result in increasing the positive attitudes of organisational ISP compared to employees who were provided with the hard copy. But in the case of reporting IS-related incidents, hardcopy recipients’ employees perform better than web-based recipients.

Little research has been conducted on the challenges of how organisations are developing ISP, or whether the expanded ISP is useful or not and if the organisation states that the ISP they are implementing is effective, then how organisations measure the effectiveness of implemented ISP. Maynard and Ruighaver (2002) propose that studies on ISP are more likely to be following the standards rather than focusing on what is occurring in organisations. As a result, there is a shortage of broad study in developing effective operation of ISP, and more research needs to be conducted to find out whether ISP acts as a benchmark for organisational IS or ISP acts as a prototype for IS. Bayuk (1996) suggests a method for developing ISP in which all organisational resources need to be protected, documenting the model and composing it into a strategy. Global Information Assurance Certification incorporation with SysAdmin, Audit, Network and Security Institute suggests another program for developing ISP, which includes policy, execution and declaration methods (Naidu, 2002). This program not only gives information on the procedure, but also provides information on how policy needs designing. Dhillon (2000) proposes a model for ISP by categorising it into entity, component and inclusive, and defining and explaining all methods. Here entity means every technology, and components means a little bit varied, but combining technologies and general means law or rule-based that is related to entire technologies, people, and processes. Dhillon further investigates the needs of the organisation, which focuses on IS using successful ISP, and found that ISP adoption is minimal and therefore more effective methods of implementation are needed. Getting
control over information systems through ISP is a primary concern of IS, which otherwise remains unprotected. Even though ISP in organisations can be well known, the literature points out that building and employing a reliable ISP is often incomplete (Lane, 2007).

Baskerville (1993) discusses the rising awareness of growing organisations, and found increasing policy with minimal supervision on how IS policies need to be established. Baskerville further discusses how growing organisations understand assumptions based on standard organisational policies where constant designs do not act according to IS. Other researchers agree; conveying that extensive investigation on ISP has committed to satisfying IS, in contrast to security policy development. As a result, a further study is required that not only includes ISP but also assesses the improvement of processes in educational providers. Baskerville examines the policy that is related to a supporter of meta-policy, which is implementing policy on policies. It gives a significant overview of IS policy improvement since it assists on a traditionally complicated part of development. Meta-policy is employed by certain educational providers, but the level of meta-policy acceptance and performance is as yet unidentified. Still, in general, it is relevant and involves the effectiveness of meta-policy, and its potency and drawbacks form another valuable motivation for research.

ISP acts as a vision for organisational success, and is essential for organisational IS and accompanying users in doing their duties. Höne and Eloff (2002) agree that the employment of an active ISP from a user’s point of view could be enormously tricky because ISP might not be handed over to users effectively. The ISP could be too lengthy and contain too much technical jargon, and the relationships between IS and user performance is anonymous. The fundamental belief of ISP is that users need to perform their duties according to security policy. On the other hand, Wood’s thinking on ISP is changeable; requiring distributed IS policies with the aim of connecting the organisation’s duties with security policy assertion by various methods (Wood, 2002). In multiple types of research, there is agreement of the magnitude of ISP. The ineffective and unproductive operation of ISP is expected to weaken the progression of organisational IS, and the upshot is that ISP is awkward, problematic and out of control.

From the organisation’s management point of view, management could believe that IS is the final objective, but IS needs consideration and an organisation’s precedence instead of goals. The organisation also needs to think about the scarcity of ISA and being unfamiliar with features of IS. IS should act as an ability to perform organisational precedence; an organisation’s ability could be influenced by the improper and unacceptable functioning of ISP. A successfully employed ISP signifies the expected user’s performance, and also points towards organisational objectives with the intention that users will not believe ISP as horrible. Therefore, ISP needs to be implemented in such a manner that is reliable and encouraging to users and also correctly exhibits the organisation’s route. ISP which acts as the main character in coordinating organisational IS should connect with top-level
managers, while merging it to user awareness gives an overview of the proper organisational framework for execution and action under IS (Lane, 2007). ISP is more likely to focus on how organisations function, and it should run when employed in a suitable functional environment and act following them. ISP should make clear to users their roles and responsibilities, and acquiescence should finalise the procedures.

The integral roles and responsibility for developing ISP sometimes fails because IS technicians and security professionals do not have enough knowledge of the organisation’s advanced goals. This sometimes happens because the user viewpoint is on IS as information technology security rather than information security; that is, they think ITS is an IT issue, and IS is now a business issue. Therefore, IS policies built up under these criteria fallback to rights and other users’ cooperation. It concludes that some of the organisation’s significant and advanced goals, such as business goals, are overlooked (Lane, 2007). In some organisations, the manager implements a review of ISP without having proper authority, whether they are disappointed with the executed procedure or they think it is not part of their duty. In such circumstances, it could be clear that the people who are building up ISP are not aware of, and do not have any idea of, the organisation’s advanced goals, and these policy builders are involved in appointing other users in organisations to employ a successful ISP. Hence, the previously occurred complicated task during policy building would be more complicated when implementing policy, largely unsuccessful, and at last evaded.

2.9 Information security behaviour

Much of the research on ISA finds that ISB is the predecessor of ISA. Many researchers have studied the procedure of applying ISA to ISB and compliance. A short description of theory-based ISB is therefore included here to review the relationship between ISB and ISA.

2.9.1 Theory related to information security behaviour

The purpose of introducing IS behavioural research in ISA is to illuminate why some users act per ISP, while others do not. Based on this concern, researchers have studied the various models and concepts that describe ISB. Lebek, Uffen, Neumann, Hohler, and Breitner (2014) propose four theories from many theories that define the ISB commonly known as the TPB (theory of planned behaviour), GDT (general deterrence theory), PMT (protection motivation theory), and TAM (technology acceptance model) (Bada & Sasse, 2014; Lebek et al., 2014). These theories of ISB are briefly described in Figure2.9.1 to achieve advanced knowledge from other research regarding the correlation between ISB and ISA.
Figure 2.9.1: Commonly used behavioural theories in ISA (Lebek et al., 2014)

**Theory of planned behaviour**

Prior to introducing the TPB, Fishbein and Ajzen (2015) introduced the theory of action reason (in 1975) to study the fact that people’s behaviour is decided based upon their intention, which acknowledges their propensity to conduct that behaviour. In other words, behaviour is decided by intention, and behaviour is inspired by a viewpoint to conduct such behaviour with the addition of some external forces that compel that behaviour. The theory of action reason was updated in 1985 with the new name of TPB, and it has been implemented in different disciplines of IS. The TPB is more involved with risk assessment and user behaviour in IS, and both theories are effective in investigating human behaviour. The theory stands on the belief that a user’s actual behaviour comes from user intention but intention, does not actually substitute for the behaviour. The TPB states that intention stems from three principles; attitude towards behaviour, attitude towards external forces, and perceptible behavioural control (Alfawaz, Nelson, & Mohannak, 2010). Attitude towards behaviour represents the principle regarding the results of behaviour (for example in the context of IS, users are encouraged and motivated towards ISP, which results in changing their positive behaviour towards IS). Attitude towards external forces represents that attitude is persuaded by external forces to conduct the behaviour (for example, the organisation’s IS culture, strategy and standards assist in changing user behaviour). Perceptible behavioural control represents the control principle and discernment on a simple or complex way of executing the behaviour; for example, users should be trained and aware about organisational ISP to notice how they behave and act in accordance with IS (Haeussinger, 2015).

**General deterrence theory**

GDT was initiated in 1975 to investigate criminal offences, and crime departments have been using this theory to prophesy different crimes and offensive behaviour by employing the deterrence principle and supporting fear policy. The GDT signifies that when a user sees...
support for strictness in an aggressive response, offensive action is unlikely to occur because users are committed to the related law. In 1993, the GDT was employed in IS, such that user actions on IS would dissuade users from perpetrating prohibited actions (Alfawaz et al. 2010). The deterrence principle has been implemented in IS to enhance policy and procedures, raise awareness, safeguard organisational resources, and extend roles and responsibility by inspiring users. One researcher notes that the GDT inherits TPB principles to review and assess a user’s ISBs (Haeussinger, 2015).

**Protection motivation theory**

The PMT was initiated in 1975, and in 1983 its framework was developed further to understand why users turn away from potential dangers, for example, by carrying out organisational duties according to organisational policy and implementing the password policy to avoid unauthorised access. The purpose of this theory is to propose a behaviour created by a couple of cognitive principles; threat principle and coping principle. These principles arise from various fear appeals. Threat principle originates from user fear relating to the professed strictness of the danger and susceptibility of the threat (Haeussinger, 2015). Coping principle depends upon the fact that a user is proficient in carrying out the proposed behaviour. These two principles are implemented in IS to encourage users and comply with organisational ISP.

**Technology acceptance model**

TAM was initiated in 1989 with the intention of adopting new technology that relies on a user’s viewpoint. This theory constitutes two principles: perceptible effectiveness and perceptible convenience. Perceptible effectiveness represents the user’s level of understanding, such as implementing ISP could improve a user’s job performance by complying with security policy. Perceptible convenience represents a user who feels it is hard to comply with ISP, which is similar to the TPB. Perceptible behavioural control could be managed through an IS training and education program (Haeussinger, 2015).

2.9.2 Procedural-based information security behaviour

Apart from the above-described theories, another descriptive method related to ISB known as classification theory is also relevant. In classification theory, a user’s behaviour is classified according to the concepts of adaption, opinion and character of the idea. According to Stanton, Stam, Mastrangelo, and Jolton (2005), it is essential to improve and implement appropriate regular appraisals and reviews of users from a security behaviour viewpoint. Classification theory highlights the features of organisational issues where an action is lawful or against the law is assisted in knowing the ISB of the user. Classification of organisational issues provides two motivational factors for an organisation; there is more chance of the periodical review of IS in an organisation, and it could help the organisation set up their IS priorities. Classification theory has four categories: 1. Not knowing–not doing 2. Not knowing–doing 3. Knowing–not doing 4. Knowing–doing.
Not knowing–not doing

In this category, users have neither an idea of the organisational requirements for security behaviour nor any knowledge about IS. When users do not know what to do, and do nothing, they breach IS rules and regulations, which results in compromising the organisational IS. Appointing a new employee without giving training and induction about the job role, and promoting employees to a new level without proper induction and training are two examples of not knowing–not doing. These types of practices are considered as cognitive failure, leading to confusion in ISP, overlooking updating the policy, and weak management (Alfawaz et al., 2010).

Not knowing–doing

In this category, users do not know the organisational ISP and do not have a proper understanding of IS, but have appropriate ISB. For example, a user does not know about organisational ISP but consults with workmates and seniors prior to taking any particular actions, which results in the organisational IS not being compromised. Some users are more careful than others when determining how to act in indistinct situations, and these users always prefer less risky actions. Users call this kind of behaviour self-regulatory practice, in which they discover the rules from their own innate tendency to pursue organisational regulations (Alfawaz et al., 2010).

Knowing–not doing

In this category, the user has all the knowledge and is proficient in ISB, but they are not conducting appropriate ISB. An example is, on appointing new employees after giving them all the necessary training and induction sessions, the employees do not execute the knowledge and skills as expected, resulting in compromising the organisation’s IS (Alfawaz et al., 2010). The question is, why is the user not performing when they know everything? Dhillon (2001) suggests that the user’s principles, traditions and sincerity could affect their working style. Dhillon further indicates that informing users about the result of their ignorance could change the behaviour of users.

Knowing–doing

In this category, users have all the knowledge and skills to perform ISB. For example, an employee has obtained all the necessary training and induction, and is complying with the security policy. As knowing–not doing, this category is also related to self-regulatory practice; however, it seems to be ideal practice. There are a couple of drawbacks alerting organisations not to rely entirely on this category. The first drawback is that IS dramatically changes frequently, which means a new level of threats are also growing that require a new level of skills and knowledge that is often expensive and demanding. The second drawback is that when all users are proficient in conducting their tasks according to ISB, organisation risk management could be overlooked or ignored (Alfawaz et al., 2010). Moreover, when an organisation changes its strategy and technology, or when the user changes their behaviour
from one category to another, ISB is compromised because the change in the user’s response is unpredictable.

Figure 2.9.2 illustrates the ISB categories.

2.9.3 Relationship between awareness and behaviour

Mancha and Dietrich (2007) designed a model whereby user behaviour is affected by human and environmental characteristics, and judged by the user’s level of belief on each effect. In this model, the user’s level of understanding is affected by other organisational factors and the user’s opinion is developed about IS with the intention of gaining necessary or unnecessary inducement. They recommend that a user’s level of belief is the degree to which users are aware of the organisation’s IS strategy, which can improve ISB. Anderson and Agarwal (2010) suggest that user awareness of IS threats affect their opinion of the potential risks and danger, their ideas are valued according to their attitude and effectiveness of their performance, and their behaviour has an impact on IS. Galvez and Guzman’s (2009) study found that individual factors and environmental factors make workplace IS procedure clear to users. Individual factors include a user’s expected results from IS effort and a user’s value in IS and environmental factors comprises motivating users in IS through computer literacy to expected results. They also conclude that ISA is a prominent factor with a concept that it is directly proportional to IS practice. Ryan (2007) agrees that a user’s high degree of awareness has a positive influence on workplace IS procedure. Siponen (2000) found that the shortage of user awareness level is the main reason for delinquency in IS. Siponen also agrees with several researchers who believe that
some behavioural theories could be employed to emphasise the motivating factor that remains in the midst of ISA and ISP submissive behaviour. Siponen further highlights that those fundamental physical factors (such as user ethics and belief, sentiment, welfare and confidence) and relevant factors (such as user problem-solving and critical thinking skills) stimulate the user to comply with the organisational IS system. Yayla (2011) provides a summary of how IS managers and professionals could manage intentional and unintentional internal IS risks and hazards. Yayla recommends solutions for accidental internal risks (such as enhancing a user’s security awareness level, implementing security training and awareness programs, and minimising workload and time pressure) and intentional internal threats (such as applying fear policy, improving user dedication, and employing technology-based countermeasures).

Spears and Barki’s (2010) studies reflect on the task of ISA risk and how users could be engaged in managing IS risk. They conclude that user engagement in risk-management procedure and advanced knowledge in IS risk-management procedures gives additional growth in organisational IS management performance through a coalition between IS risk management and the business environment. Takemura (2011) studied the ISA and ISB correlation and discovered that advanced security awareness assists while assessing organisational IS.

Many organisations are now more worried about the risks and threats from inside than outside users, and many survey results show that most of the dangers that organisations experience are from inside users. So, it is essential to understand user behaviour and the consequences of their actions (Mittal, 2016). To study user behaviour and how it affects organisational IS, researchers developed a classification of user behaviour into two categories: intentional behaviour and unintentional behaviour. Intentional user behaviour is action that is intentionally malicious, advantageous or accidental, and technical knowledge represents the professional skills and proficiency needed to conduct such activities (Banfield, 2016). Unintentional user behaviour is the inadvertent errors and ignorant behaviour from the user. These users are always monitored by intentional users so they can gain advantages from unintentional user mistakes and actions. Figure 2.9.3 explains the two-factor categorisation of ISB and also proves that user intention and expertise are the main factors for success (Banfield, 2016). The figure also describes how the user’s degree of skill and knowledge encourages particular purposes ranging from intentional damage to innocent mistakes. Intention and expertise both act as independent variables, but in the case of IS, they act as dependent variables (Stanton et al., 2005).
Figure 2.9.3: Two-factor categorisation of security behaviour (Stanton, et al., 2005; Stephanou & Dagada, 2008)
2.10 Summary

Most of the literature focuses on end users as the main reason for security breaches in an organisation, neglecting the other factors. This literature review thus provided a broad review of recent literature on IS training and awareness. Like many other literature reviews, this one also has some weaknesses. This literature review mainly depends on journal articles, conference papers, articles, and some documents from websites. Moreover, this literature review only includes some published books, reduces the journal articles to those which only meet the minimum standard for peer review, so some other research effort could be missing. This literature review attempted to address a significant amount of ISA literature and detailed analysis of the factors responsible for IS training and awareness. It also reviewed the relationship between ISA and ISB, the impact of training methods in security awareness, and deep evaluation methods for organisational security awareness.

Chapter 3 details the research methodology and analysis of the first survey.
Chapter 3. Research methodology overview

This chapter includes the overview of the research methodology, and discussion of the particular steps taken, including the research process, the data-collection process and data analysis.

3.1 Research phase

The research phase consists of the proposed research framework, question design and process.

3.1.1 Proposed framework

According to researchers, research is an innovative action which is carried out to enhance the skills and knowledge about human society, technology, psychology and so on, and the implementation of knowledge and skills to work out novel theory and purpose. Moreover, research is an organised way of investigating and developing new experiences and discovering the answers to particular issues. The choice of a relevant research aim relies on the research trends and limitations of earlier studies. There are a variety of methods for conducting research within various disciplines and subjects, with the techniques classified into scientific and social methods (Maynard, 2010). The research method uses an orderly process to deal with the particular research issues, and with respect to IS, the social science discipline is applied. The research conducted on IS systems generally focuses on people, processes and technology.

As research on IS systems comes under social science, the other related disciplines are also briefly touched on, such as psychology, anthropology and sociology. Psychology relates to behavioural research to provide practical guidance on relationships, mental health and addiction. Anthropology refers to the study of various aspects of humans within past and present societies. Sociology relates to the exciting and illuminating field of study that analyses and explains essential matters about our personal lives, our communities and the world.

The chosen research method needs to be guided by the research issue, the aim of the researcher, and also determined by research questions. Social science in the IS field implements both qualitative and quantitative research methods (Neuman, 2014).

Quantitative research uses statistics to evaluate issues that rely on data and establishes theory and interactions. Quantitative research investigates the real-time problems through experiments, surveys, questionnaires, interviews and modelling. Quantitative research also relies on the validity, reliability and repeatability of the data, which means it includes a
massive number of samples that is not possible in other research methods. The results are shown in the form of graphical and statistical descriptions (Gravetter & Wallnau, 2011).

The proposed framework for this research is explained in detail in Chapter 6.

### 3.1.2 Research questions design

The research methodology explains and analyses the research process, which was designed to look for the answer to the research questions listed in Section 1.9. The research process started with queries such as how this research could assist in measuring the effectiveness of the security program, and whether during the measurement process the researcher is implementing the same measurement indicator or metrics, and whether the results are practical. This research proposed a research model based on the research questions. The objective of the research methodology was to understand user knowledge about IS training and awareness programs and to investigate the areas that need improvement.

Both investigative and hypothetical tests compromise this research. The investigative research involved primary research methods, such as collecting data obtained from the survey, making it a quantitative study. This research method involved the investigation of the people (general users, management and informational technology users) and their practice of IS. The survey was administered to a group of the sample population to take a broad view of their knowledge, understanding, attitude and performance. An additional cross-sectional survey was then implemented to another group of the sample population to minimise the chance of unfairness. The gaps exposed in the literature review were explored during the design of the survey question, confirming the theories and verifying the hypothesis. The collected data from the survey were analysed to give numeric and statistical notification to evaluate the IS. After the evaluation of the survey data, the relationship between the end-user’s level of ISA and ISB was identified and recognised through quantitative data analysis.

### 3.1.3 Research process

The research process started with identifying gaps that arose from the literature review. The IS issues found in the literature review and the proposed research framework informed the research questions. But this was not the only reason for this research: the research questions and research process was also based on the needs of an organisation. Thus, this research is based on both theoretical knowledge and practical implications. So, after analysing the theoretical and practical side of the study, the investigation commenced its first survey without implementing the ISA program.

The purpose of the first survey was to understand the end-user’s level of knowledge and understanding about various disciplines related to IS, such as security policy, meaning, purpose and the final goal of IS. The survey was intended to provide some information on what end users already know and what they do not know. Based on this information, the IS
training and awareness program was designed. The security experts, corresponding
departments, and organisational management approved the training and awareness
program for further verification. The actual implementation of the program began after
finalising the verification process.

A training and awareness program should be appropriate to the end-user’s requirements. In
other words, if a user wants an instructor-based training and awareness program, they
should not be forced into another mode of training and awareness. Chapter 5 discusses
these issues in detail.

After the training and awareness program, a second survey was conducted to establish
whether end users understood the program or not. The results of the second survey were
compared with the results of the first survey. No significant changes between the results of
the first and second survey would indicate a need for improvement in the training and
awareness program, while a dramatic change between survey results would indicate that
the program was working. Finally, a third survey was conducted after four months, with the
intention of finding out if end users had forgotten the training and awareness program or
not, and whether there was a need for continuation of the program to keep end users
refreshed.

The purpose of surveying the control group at the beginning and the end of the program
was to establish if end-user behaviour changed due to external factors of the organisation,
such as a change in policy and culture, intention of complying, or change in cyber security
governance. The comparison of the final survey result of the support group and control
group indicates whether the organisation needs to implement the outsourced training and
awareness program, or whether an organisation’s IS is proficient in changing end-user
behaviour and complying with IS.

Figure 3.1 illustrates the research process.
Figure 3.1: Research process (Dhakal, Islam, & Mendis, 2017)
3.2 Data collection process

This research was conducted in Australia with the intention of collecting the data locally. Several Australian Government and non-government organisations were requested to undertake the survey, but all refused, mentioning organisational security as a reason. This meant that online data collection was the other option for the survey. In conducting the online survey through SurveyMonkey, all of the respondents were from the United States. However, it does not matter where the participants were from because IS is a global problem and IS issues in Australia and the United States are likely to be identical.

The survey was implemented as a method for data collection and conducted through SurveyMonkey. The purpose of choosing SurveyMonkey, a web-based technique for data collection, was because it is beneficial for the statistical analysis and allows comparison and evaluation of the outcomes for different groups. The whole survey consists of three sets of questionnaires created to focus on the intended target and addressing the research question and sub-questions. In this research three surveys were conducted: one before the training and awareness program; the second after the training and awareness program; and third after a four-month time interval from the training and awareness program. The first survey was intended to measure the end-user’s level of understanding of IS. The second survey was designed to measure whether the end-user’s knowledge and behaviour changed after the training and awareness program. The third survey was designed to measure whether users forgot the training and awareness program or not, and whether the program needed to be continued afterwards. The survey questions were uploaded in SurveyMonkey and participants could view and respond to the survey questions through SurveyMonkey. The survey process lasted for six months due to the timeframe for completing the second and third surveys, but the time taken to complete each survey was one week. Since humans were involved in this research, the data collection process started after getting approval from Charles Sturt University Research Committee which approved the ethics application (see Appendix 1). The remaining steps involved in data collection are discussed below in detail.

3.2.1 Survey questions design

The list of questions implemented in this research verifies that the designed questions assist in considering ISA both from the practical and theoretical side. The questions refer to necessity, significance, practical implications, and other disciplines of IS. Three sets of questionnaires were developed, with each collection consisting of 10 questions. Three questions are multiple choices, where participants were given a choice of answers to select from. These questions need roughly between five and 10 minutes to complete, and were collected instantly. The next group of questions are scenario-based, and the questions are provided at the end of the scenario, thus acting as a case study. The information contained in the script could be information on different disciplines of IS or real IS incident scenes or some animated videos related to IS. The intention of providing a scenario before the
questions is to provide some awareness of IS. Since all participants must go through the
script to answer the questions, reading the situation aids their understandable prior
answering the questions. Moreover, it is practically not possible to provide a training and
awareness program to web users (web user here means participants who use the web or
the internet to participate in the survey) as in an instructor-based training program. In
instructor-based training and awareness programs, an instructor physically presents the
training and awareness session in a classroom.

According to Bulgurcu et al. (2010), questionnaires designed according to ISA have the
intention of measuring users’ level of knowledge about IS and measuring afterwards to
check the level of understandings on organisational ISP (Bulgurcu et al., 2010; Chan &
Mubarak, 2012). Chapter 5 describes the further analyses of user ISB. The intention of the
questionnaires is also to gain the participant’s experience on IS breaches in mathematical
descriptions.

While designing the questionnaires, many questions arose from the literature review about
investigating and measuring the awareness level of every user instead of those with security
expertise or professionals. The questions designed for the initial survey of the control group
(another group not participating in any training and awareness program) are same as the
questions in the first survey. The initial survey also measures the user’s level of knowledge
and understanding of IS, and the questions are related to frequent security attacks,
accessibility of ISP, the role of management, backup, and identification of threats. The
questions are based on the fact that there is a significant relationship between IS theory and
behaviour. The questions designed for the support group measure the participant’s
responses and actions from an earlier survey, and the scenario is intended to provide
knowledge about IS. The formation of questions in the second set links with the related IS
type that measures the first set of questionnaires. The second set of questions for the
final survey of the control group are the same as the support group’s third survey
questionnaires, and are also concerned with the meaning of ISA. The reasons for
implementing the same questions in the two surveys is to measure the effectiveness of the
training and awareness program when the same proposals are responded to by two groups;
a support group who will receive the training and awareness program, and the control
group who were not involved in the security awareness program. The result of final survey
of the control group could be compared to the second or third survey of the support group.

Because the survey questionnaires were in different modes, the responses would be
different, which creates complications in measuring the differences and comparing with
another survey. The knowledge of IS theory when combined with ISA assists in improving
user awareness of ISP. In some organisations, the reason users do not access organisational
ISP is that the information relating to ISP is considered as classified and confidential. The
questions also concern the abuse of computers and mishandling of IS. These kinds of
problems attempt to understand users’ experiences on IS incidents, what has happened and
how they responded. The reason is to understand the user’s opinion in those incidents so that the appropriate actions are undertaken to combat those incidents. The response from the participants could be a bit longer, and considering the circumstances the control group questions are open-ended rather than closed and multiple choice. The same questions for support group were implemented for the control group, and participants were divided into three groups; IS professionals, managers and general users. Participants from different backgrounds, ethnic and racial groups and educational backgrounds were encouraged to participate so that the research would be more reliable and valid.

Appendix 2 provides the sets of questionnaires.

**First survey**

The first survey was designed to recognise the end-user’s level of knowledge and awareness of IS and organisational security policy. The first survey further aimed to understand the vulnerable areas of the organisation’s security that end users were not focusing on. There is a need for potential control measures concerning perceived risks and threats, and to enhance security awareness in that area. IS training and awareness programs should focus on the areas that need more attention. Therefore, the results of the first survey assisted the researcher create a training and awareness program concentrating on those areas that require more attention to improve ISA in an organisation. The first survey questions are based on the reviewed literature, known hypotheses, and organisational security incidents, and focused on measuring the end-user’s knowledge, attitude and behaviour. The organisational security incidents were recognised, and were related to risk evaluation, IT management and those incidents that repeatedly appear in an organisation. The questions in the first survey are associated with other factors such as job role, functioning department and employment period. The reason behind asking such questions was to compare whether users from the IT department are more aware of IS than those in other functional departments, whether managers are more knowledgeable than regular users or not, and whether users who have worked for a long time are more aware than those who have worked for short time or those who have recently joined the organisation. The questions relating to user behaviour, such as phishing attacks, social engineering attacks, password handling and physical protection, are also contained in the first survey. The intention of including those questions in the survey was to establish whether users respond to those attacks according to ISP.

**Second survey**

The second survey was designed to evaluate the effectiveness of the IS training and awareness program; the foundation of this research. Before going into further detail, it is important to note that conducting the online survey through SurveyMonkey meant that it was not possible to conduct a computer-based training and awareness program, especially after not receiving enough responses from the first survey. Therefore, in the second survey scenario-based information and some other information related to IS were provided along
with the survey questions. All participants needed to go through the scenario and choose the appropriate answer, but if participants they were not satisfied with the given answers, they could express their ideas in the text box, which was the last option in every question. If the survey was conducted in an organisation where the participants are known, there would be a training and awareness program, and the survey questions would be designed according to the functional departments, but that is unlikely in a web-based survey.

The purpose of evaluating the effectiveness of a training and awareness program is to ensure whether the aim was reached or not, assessing the outcomes of the program, and whether the program’s goal was partially or wholly fulfilled. Not all the responses could reach the goal in the first survey, but some of the questions are repeated in the second survey, such as the participant’s experiences of the first survey and the training methods that assist in measuring the effectiveness of the training methods. Chapter 5 discusses the effectiveness of training methods in detail. Since the second survey includes scenario-based questions, an extra option was added to the answer list where participants could express their ideas and opinions when they were uncertain about the given choice of answers. For example, if the question in the first survey was about password management, such as how often do you change the password, the answer could be in numbers, but if the same question was repeated in the second survey, then the effectiveness of the training and awareness program could not be measured.

Third survey
The third survey was designed to measure whether users forgot or remembered what they learned in the training and awareness program. In most organisations, management implements the training and awareness program and conducts a test to measure it. Organisations know that after the training program users retain some knowledge and information about IS, and if the survey is conducted immediately after the training, the success rate is always high. The third survey in this research was carried out some months after the training and awareness program, and if the survey result shows a decline in awareness level, another training and awareness program should be implemented to keep users refreshed and updated on organisational IS. The questions in the third survey consist of a mixture of the first and second surveys, with multiple-choice answers. The training and awareness program and review should continue after the third survey in continuous mode.

Initial survey of the control group
The control group comprised mixed users from all functional departments. The control group was intended for comparison purposes only. The participants of the control group did not participate in any training and awareness program. Rather, the control group was used to compare whether the training and awareness program was effective in achieving organisational goals, or if the organisations are more than enough to change behaviour and achieve organisational goals. In other words, it seeks to find the answer to the question: Do organisations require IS training and awareness programs?
The questions designed for the initial survey of the control group are same as the questions asked of the first survey of the support group. The purpose of the first survey of the support group is to measure the user’s level of knowledge, but that is not the intention of the initial survey of the control group. The initial survey of the control group would be completed at the same time as the first survey of the support group.

**Final survey of the control group**

The final survey of the control group could be implemented at the same time as the second or third survey of the support group. The time interval of the initial survey of the control group and final group would be around two to four months. The outcomes of the final survey of the control group play a vital role in comparing the effectiveness of the training program. The result of the final survey of the control group could be evaluated with the second or third survey result of the control group, depending on what the organisation wants to measure. If the results of the final survey of the control group are compared with the results of the second survey of the support group, it measures the effectiveness of the training and awareness program. If the final survey results of the control group are compared with the results of the third survey, it measures how long users memorise the content of the training and awareness program and whether the organisation needs to continue training and awareness programs to keep users refreshed.

**3.2.2 Data collection tools**

This research chose SurveyMonkey as a data collection tool because of its convenient nature and benefits during the statistical analysis. The questions designed for the participants are in an appropriate mode; questions are short and easy to understand, technical terms and answers are avoided, and questions are in the form of multiple choice. All the selected responses are from given choices, except in the second survey where an extra option was added in the comment field in which participants could express their response when they were not satisfied with the given answers. Survey question distribution was organised according to the participant’s job role and position, the organisation’s size, risks and threats to business processes, the organisation’s reliance on the information system and security, and security incident occurrences and mitigation strategies. The survey was carried out with the intention of collecting the participant’s decisions on the expected threats and risks described in their response and evaluating it with the identified threats and risks in the literature review. This process assists in reflecting on the identified threats and risks so that preventive strategies could be implemented. The aim of this research was not to canvass all the possible threats and risks in the IS training and awareness program, but to support the practical measures employed by organisations to minimise those threats rather than threats and risks defined by users.

Figure 3.3.2 illustrates SurveyMonkey.
3.2.3 Description of sample

This research implemented the survey through SurveyMonkey, and all participants were from various states of the United States of America. In both surveys, 100 participants were invited, but only 66 people responded in the first survey, and 56 responded in the second survey. The SurveyMonkey team was contacted to ask why there was not a 100% response to both surveys. The help and support team from SurveyMonkey apologized and made a partial refund, explaining that the survey was opened for two days and no one had responded, so it was closed. The survey questions were subsequently rechecked to ensure that the questions were easy to understand.

The difference in the sample size does not mean that it did not address the issues. For example, in the survey, if questions related to password protection are asked of two groups with sample sizes of 50 and 500, the number of participant’s response would still be from the given options. The only difference would be the number of options chosen by two sample groups.

The sample size would make a difference if qualitative research were applied where individual participants have different opinions and responses.

In the first survey, 100 participants were invited to take part, and 66 people responded. The majority of participants were over 45-years-old, less than half participants were between 18 and 45 years, and there were more female participants than male. In the second survey,
invitations were sent to the same participants, but only 56 participants took part. As in the first survey, the highest responding age group was above 45, and less than half were between the ages of 18 and 44. Again, there were more female participants than male.

In the third survey, however, there was a dramatic change in the response rate. Invitations were sent to the 100 participants, but 102 participants responded. The reason for the extra responses is that an email was sent to the SurveyMonkey team asking why the survey had not reached the target in the earlier surveys. The SurveyMonkey team encouraged respondents to participate and a few completed the survey at exactly the same time, before the target of 100 was reached, so there are two extra responses in this survey.

The number of respondents in the 18 to 44-year age group rose, but the peak group was above 45-years. Again, there were more female participants than male.

Most participants used their desktop as a medium for taking part in the surveys, while some used tablets, phones, iPads or laptops. SurveyMonkey did not ask for the participant’s job role, but suggested they input their annual earnings, and job roles were based on that. The participants whose salary ranged from USD25,000 to USD65,000 were general users, and their participation was around 50% of the total. The participants whose income ranged from USD65,000 to USD90,000 were managers, and their participation was approximately 30% of the total. Participants whose salary was above USD100,000 were top-level executives and chief IS officers, and their participation was around 20% of the total.

3.2.4 Validity and reliability of data collection tools

The validity of the research relates to the amount of precise data and how the framework employed the data. When the collected data are independently reliable, higher validity could be accepted. Validity also depends on the choice of research methodology (Mortazavi-Alavi, 2016). According to Heale and Twycross (2015), the weight of research should not be provided only to the outcomes, but also needs to value the rigour of the study. Here, rigour represents the degree of researcher effort to improve the quality of the research, and since this research adopted the quantitative research methodology, assessing the reliability and validity of the data helped to achieve rigour. Validity in quantitative analysis describes the degree to which the theory or hypothesis in the quantitative study is measured. Reliability in quantitative research is defined as the degree to which research tools reliably have similar outcomes when employed in the same circumstances on repeating events. For example, in the context of ISA, a survey conducted to measure the knowledge of organisational ISP not only gives the result in numbers, it measures the degree of knowledge which could be believed to be valid. Data and information could change over time, but the assumption and methods remain the same. Facts and figures could adjust from one organisation to another, but the occurrences of the IS incidents stay the same.

Validity classifies quantitative research into three groups, described here briefly. The first is content validity, whereby the data collection tools, such as survey questionnaires,
encompass all expected areas. IS professionals were asked to give their view on whether the data collection tools implemented were appropriated or not to ensure validity. The second is construct validity, which gives suggestions on the survey results to the model for consideration of the hypothesis. The third is criterion validity, whereby other data collection tools evaluate the related variables. Other data collection tools, such as observation of end-user behaviour, could be implemented to measure the same variables (Heale & Twycross, 2015).

Evidence that shows the survey as a valid data collection tool includes:

1. The homogeneity principle of validity represents that the survey measured the results and scores.
2. The convergence principle of validity represents that survey measures the theory like other tools.
3. The theory evidence principle represents that when a survey estimates a high score in ISA, then users are more likely to be aware when undertaking their daily organisational activities.

Reliability means uniformity of measures. For example, a participant completing the survey is expected to complete it in almost the same way every time they take part in the survey. Reliability is used to verify the inherent reliability of the study, for example, when a survey has questions in which participants select two or more options. This research implemented repeated reliability where survey repetition occurs more than once, and the data collection process employed the survey as a tool for data collection. The participant’s responses could be compared every time they were involved, which also verifies that the data collection tools are reliable. Of primary importance is to assess the research critically and make a judgement on whether it makes a significant impact in the field of IS or not. In quantitative analysis, validity and reliability of the implemented data collection tools assist researchers in determining whether to apply the results in the research discipline (Heale & Twycross, 2015).

3.2.5 Research ethical considerations

Since this research process involved human participants, the moral values and ethical principles needed to be considered throughout the research to make sure that risk and threats related to ethics had a minor effect on the study. Ethical issues were discussed from the beginning to the end of the research, and possible ethical issues were attended to as per the requirement of Charles Sturt University ethics application and approval procedure. Appendix1 includes the ethics approval letter from Charles Sturt University Ethics Committee. The ethical issues and control measures identified in this research is described in Table 3.2.5 according to the principle of ethics (Dudovskiy, 2017).
Table 3.2.5: Ethical research considerations

<table>
<thead>
<tr>
<th>Prospective ethical issue</th>
<th>Prospective effects</th>
<th>Prospective preventive measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant identification</td>
<td>Participants might fear that their name and responses could be made public.</td>
<td>Participants were assured that their names would be deleted after collecting the data from the survey and during the analysis process. Participants were assured that taking part in this survey was optional and participants’ names and responses remain confidential.</td>
</tr>
<tr>
<td>Participant concern on time-frequency</td>
<td>Participants might worry about the time to undertake the survey and frequency of the review.</td>
<td>Participants were assured that survey questions would be short and straightforward so that the minimum time could be taken to complete, and for the second and third surveys participants were previously informed about the date and time.</td>
</tr>
<tr>
<td>Research Copyright and Intellectual property</td>
<td>Researcher or organisation (under which researcher is working) could claim for intellectual property ownership for the results of the research and any contribution made by the researcher throughout the study.</td>
<td>The consent form of the survey clarifies that the result of the research could be published, not the response of participants. Any other assistance provided by participants other than their survey responses would be prescribed.</td>
</tr>
<tr>
<td>Participant respect and dignity</td>
<td>Participants might worry about being respected.</td>
<td>In any circumstances, if participants feel their responses have not been valued and their dignity has not been given highest priority, then participants could just leave.</td>
</tr>
<tr>
<td>Participant communications</td>
<td>Participants could worry about communicating with the researcher throughout the data collection process.</td>
<td>Participants were assured that participants could interact with the researcher at any time throughout the research process. Furthermore, participants were assured that communication would be done with honesty, with no misleading or false information.</td>
</tr>
<tr>
<td>Participant privacy and security</td>
<td>Participants could be concerned about their personal life being exposed.</td>
<td>Participants were assured that there would be no personal questions in the research that could expose their privacy and security.</td>
</tr>
</tbody>
</table>
3.2.6. Quality control of data

Since the quality of data was essential to this research, and is also the basis for the results, control procedures were employed to sustain high-quality standards. Some control measures implemented in this research to maintain high-quality standards are briefly described below.

Data accuracy

The survey questions consist of multiple-choice questions where answers are in the form of multiple choice and participants have to choose from the given options. This means there is no chance of manipulating or modifying the responses. The collected responses were checked to make sure the responses were from the participants who took part in the survey and not edited by any third parties. All the participant responses were genuine, and none of the responses were modified, which verifies that collected data were accurate.

Data independence

This research focused on measuring the effectiveness of a training and awareness program, which means participants who have undertaken the program could participate as well as participants who did not attend any training and awareness program. The participants who did not participate in the program responded according to their knowledge and understanding, which also verifies that collected data were independent and not altered.

Data appropriateness

The data obtained from SurveyMonkey assures prevents needless errors that could occur during manual data entry and extraction for statistical analysis. The SurveyMonkey website does not allow the researcher to manipulate participant responses, and participants cannot modify the survey questions and options in the answer list, thus verifying that the collected and analysed data were appropriate for the research.

Data authority

The survey questions were related to the literature review, research questions, and aim of the research and potential organisational issues with IS. The responses obtained from these questions authorised that the data were related to the investigation. The survey responses were confidential, and further processes were handled confidentially. Anonymity was assured while managing the data. The consent form provided to every participant assured and declared the anonymity that it was entirely the participant’s choice to participate in the survey or not. Appendix 3 provides the consent form. Considering the facts provided, it is believed that if multiple surveys were conducted, the outcomes would be similar, which confirms that the survey data were valid and reliable.
3.2.7 Ongoing benefit of the research

Since this research reflects on measuring the effectiveness of a security training and awareness program, many organisations that may or may not have implemented a security awareness program would benefit from this research. The results of this research should encourage organisations to understand how an IS training and awareness program assists in changing user behaviour and leads to a change in organisational culture. This research also allows organisations to observe how other organisations benefit from security programs before implementing them in their own organisation. Furthermore, the improvement in IS training and awareness programs as a result of this research assists in identifying and mitigating the risks and threats, and raises awareness in users about potential security issues and techniques and how to respond to them professionally. This research will also help those organisations that already have a security awareness program by explaining how to measure it. The organisations will learn how measuring attributes such as knowledge, attitude and behaviour can have a significant impact on security programs. This research also describes how to invest in security and the ROI possibilities. In the end, security programs are continuing and ongoing, technology is changing day by day, and organisations are relying more on electronic sources for business, so organisations have to understand that ISA is not optional for their business, and ignorance could result in a massive loss.

3.2.8 Research development stage

The research development stages for this research were:

1. Planning stage: The baseline of the research started with getting an ethics approval letter from the university’s ethics committee and then classifying the prospective survey participants.
2. Data collection stage: The actual implementation of the survey questions into online data collection tools (SurveyMonkey).
3. Data-analysis stage: Extraction of data from SurveyMonkey for statistical analysis and preparing the result of the research for the thesis.
4. Thesis writing: Consisted of writing up the literature review, discussion, limitations and conclusion of the research, and drafting the thesis for multiple reviews and finalising any remaining tasks.

3.3 Data analysis

After the completion of the data collection procedure, the analysis of the data began. Microsoft Excel was utilised to execute the data-analysis procedure. Analysis of the collected responses was executed according to the research questions and similar issues
identified during the literature review. The data-analysis tools executed an in-depth data-analysis process, and the results are displayed tables and figures.

As previously mentioned, the survey acts as a tool for data collection that verifies the conditions for validity and reliability, and also assists in fairness during data-analysis procedures. This thesis also describes the results, and discusses the data-analysis procedures.

In this research, multiple surveys were carried out to measure and compare results that would be effective in changing the behaviour of end users through the IS training and awareness program.

### 3.3.1 Data-analysis procedure

Data-analysis plans and procedure steps are discussed below.

**Respond to and describe the survey**

The answers to the survey were categorised according to the groups of participants to compare the responses between groups through statistical presentations such as pie charts and bar diagrams. Further descriptions of the variables were set through statistical calculations, such as mean, median, mode and standard deviation.

**Participant’s awareness level and security awareness program**

From the responses to the first survey, the awareness level of participants was evaluated, illustrated and explained. These responses also indicated significant areas for inclusion in the training and awareness program. With the intention of creating awareness, the second survey contains a scenario, and participants should respond according to the information provided in the scenario. The participants were categorised according to their job role, functional departments and how long they have worked in that department and organisation.

**Evaluation of the security training and awareness program**

Knowledge, attitude and behaviour were measured to ascertain the effectiveness of the training and awareness program that was initiated after evaluating and comparing the outcomes from the first and second surveys showing participant awareness levels. Comparisons between the training types also indicated the effectiveness of the training and awareness program. Comparing the mean between the two groups was measured through a \(t\)-test for the dependent sample and sample \(t\)-test for the independent sample. To evaluate the means between various groups and to be more accurate an ANOVA (analysis of variance) test was employed with the confidence level of the interval at 95%, which is standard for socio-technical analysis (Veseli, 2011). This research implemented the paired sample \(t\)-test, which is also known as dependent sample \(t\)-test. A paired sample \(t\)-test is a statistical process or method which calculates whether the mean variation of two survey
The paired t-test measured every question or article two times in pairs of the study. The primary purpose of the paired sample t-test was to investigate case studies and repeated survey calculation (Statistical Solutions, 2018). For both tests, the value of $p$ was calculated, and the hypothesis tested by the following:

If $p \leq 0.05$, the result is significant. If $p > 0.05$, the result is not significant (Statistic Solutions, 2018).

### 3.3.2 Research sample and size analysis

It is difficult to identify the correct number of participants for research, but generally the more participants, the better the sample. In this research, the number of participants varied according to the survey. The numbers of participants were different in all three surveys according to profession, industry, location, employer size and organisations that implement or do not implement a security program. Therefore, each survey sample needs to be analysed differently. In the first survey, out of 100 invited participants more than half (66) completed the survey with a completion rate of 66%. In the second survey, 100 participants were asked to take part, but only 56 completed the survey with the completion rate of 56%. The time allocation was exactly same as in the first survey. But in the third survey, 100 participants were invited, and 102 participants completed the survey with 100% completion rate. As previously stated, the likely reason for the extra participants was due the last participants completing the survey at exactly the same time. The time allocation for all three surveys was a week, but all the participants responded in two days, and SurveyMonkey closed the survey. Figure 3.3.2a illustrates the survey sample size and their completion rate.

<table>
<thead>
<tr>
<th>First Survey</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Survey invitation</td>
<td>100</td>
</tr>
<tr>
<td>Participant who</td>
<td>66</td>
</tr>
<tr>
<td>completed the survey</td>
<td></td>
</tr>
<tr>
<td>Survey success rate</td>
<td>66%</td>
</tr>
<tr>
<td>Survey completion time</td>
<td>2 days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Second Survey</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Survey invitation</td>
<td>100</td>
</tr>
<tr>
<td>Participant who</td>
<td>56</td>
</tr>
<tr>
<td>completed the survey</td>
<td></td>
</tr>
<tr>
<td>Survey success rate</td>
<td>56%</td>
</tr>
<tr>
<td>Survey completion time</td>
<td>2 days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Third Survey</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Survey invitation</td>
<td>100</td>
</tr>
<tr>
<td>Participant who</td>
<td>102</td>
</tr>
<tr>
<td>completed the survey</td>
<td></td>
</tr>
<tr>
<td>Survey success rate</td>
<td>100%</td>
</tr>
<tr>
<td>Survey completion time</td>
<td>2 days</td>
</tr>
</tbody>
</table>

Figure 3.3.2a: Survey sample from all three surveys
In the first survey, the participants were from different groups, such as IT professionals (26%), management groups (36%), and general users (38%). In the second survey, 24% were IT professionals, 40% were managers, and the remaining 36% were general users. In the third survey, 35% were IT professionals, 42% were managers, and the remaining 23% were general users.

Figure 3.3.2b is the chart explaining the distribution of the samples according to job role.

The survey managed the research samples according to industry type. In the first survey, 22% of the participants were from the health and insurance sector, 19% from educational and training institutes, 16% from the IT sector, 13% industrial and trade workers, 12% from banking and finance, 11% from service organisations and 7% from the government sector. The second survey consisted of 22% of participants from service organisations, 17% banking and finance, 15% government sector, 15% education and training institutes, 13% industrial and trade workers, 12% IT sector and 6% from the health and insurance sector. The third survey consisted of 20% of participants from the government sector, 16% from banking and finance, 15% health and insurance sector, 14% from service organisations, 13% IT professionals, 12% education and training institutes, and 10% industrial and trade workers.

Figure 3.3.2c is a chart of participants based on industry sector.
This research was conducted through SurveyMonkey, and participants came from various states in the United States of America. Looking at the participants based on their geographic location, the survey shows that a high proportion of participants were from the South Atlantic, a few participants were from the East South Central and Mountain region, and participants from the New England and West North Central areas were in a similar ratio. In the second survey, most participants were from the South Atlantic, a few participants were from the New England and Mountain regions, and the ratio of participants from the West North Central, West South Central, and Pacific regions were similar. In the third survey, most of the participants were from the East North Central and South Atlantic regions, and a few participants were from the New England and East South Atlantic regions.

Figure 3.4.2d illustrates the participant ratio according to their geographical location in all three surveys.
The survey distributed research participants according to the size of their organisation. Figure 3.3.2e illustrates the sample distribution according to organisational size in all three surveys. The purpose of analysing the organisation according to size is because of its significant role in research. In the first survey, 49% of participants came from organisations with more than 5000 users, 24% from organisations having 2000–5000 users, 10% from organisations having 500–1999 users and the remaining 27% from organisations with up to 500 users. The second survey consisted of 38% participants from organisations with more than 5000 users, 29% from organisations with 2000–5000 users, 23% from organisations with 500–1999 users, and the remaining 10% from organisations with up to 500 users. In the third survey, 29% of participants were from organisations with more than 5000 users, 34% from organisations with 2000–5000 users, 22% from organisation with 500–1999 users, and the remaining 15% from organisations with up to 500 users.
Organisations implementing training and awareness programs are more aware of the risks and threats compared to other organisations. Figure 3.3.2f illustrates that an organisational training and awareness program has a more significant impact on minimising security risks and threats compared to organisations that do not have a training and awareness program in all three surveys.

The figure explains that in the first survey more than 75% of participants who belong to organisations with more than 5000 users benefit from security programs and more than 60% of participants from organisations with 2000–5000 users outsource their training and awareness programs. 50% of participants belonging to organisations with 500–1999 users have security training and awareness programs created by their IT departments and 40% of participants belonging to organisations with up to 500 users have a security program, but it is only implemented during the induction session before appointment to the job.

In the second survey, more than 65% of participants belonging to organisations with more than 5000 users benefit from security programs and more than 55% of participants belonging to organisations with 2000–5000 users indicated that they use outsourced training and awareness programs. The second survey also showed that 40% of participants belonging to organisations with 500–1999 users identified that they have security training and awareness programs created by their IT departments and 35% of participants from organisations with up to 500 users have a security program, but it is only implemented during the induction session before appointment to the job.

In the third survey, more than 55% of participants belonging to organisations with more than 5000 users benefit from security programs, and more than 40% of participants belonging to organisations with 2000–5000 users indicated that they use outsourced training and awareness programs. The third survey also showed that 35% of participants belonging to organisations of 500–1999 users identified that they have security training and
awareness programs created by their IT departments, and 65% of participants belonging to organisations with up to 500 users explained that they have a security program that is only implemented during the induction session before appointment to the job. Figure 3.3.2f shows participant responses according to organisation size.

![First Survey](image1)

![Second survey](image2)

![Third Survey](image3)

**Figure 3.3.2f: Participant responses according to organisation size**

### 3.4 Summary

This chapter provided an overview of the research methodology, which included planning the research and procedures for data collection and analysis. The research methodology was designed based on the research problems, goals and research questions. The aim of the research methodology was to recognise the end-user’s knowledge about organisational IS through investigative analysis and hypothesis testing to find out the areas that need attention. The research process involved identifying the gaps from literature review and how the research questions address the needs of the organisation. The data collection process included designing the survey questions, establishing the tools for data collection, and description of the sample. The survey questions were approved from experts for reliability and validity. An online survey was implemented as a tool for data collection. The samples were described according to age, gender and location. The research involved the participation of human beings and therefore required ethical approval to ensure that moral values and ethical principles were adhered to. An online survey meant there was less chance of data modification by participants or third parties, which means that the collected data is accurate and appropriate. The collected data was analysed and illustrated in figures based
on the participants’ level of awareness about the security awareness program and an evaluation of the security training and awareness program.

Chapter 4 discusses the statistical evaluation in measuring the effectiveness of the training and awareness program and hypothesis testing.
Chapter 4. Results and discussion

This research focused on user ISA gaps as identified in the literature review. Much of the literature acknowledges that ISA relies on end-user’s compliance with security procedures, but other factors have a significant impact on that compliance. This research model was evaluated and illustrates that there is a substantial amount of inconsistency in ISA. The results should motivate security professionals, management and research fellows to raise the awareness of end users about IS issues and to present them in organisational security policies and procedures in simple and clear language that is understandable to every user, and available anytime without any difficulty.

Much of the literature on IS education training and awareness programs argues that such programs improve awareness levels, but their results are not adequately assured. The results of this research also support the constructive impact of training and awareness programs on the user’s level of awareness, their compliance behaviour, and how security professionals and managers should deliver proper training and awareness programs. Initially, an end-user’s knowledge of IS is fundamental to an analysis of ISA, which means additional knowledge and understanding about IS makes users more aware of organisational IS incidents. Organisations therefore need to focus on the factors that are responsible for increasing the knowledge of those users who do not even have general knowledge of organisational IS in order to avoid accidental and careless actions. When organisations encounter security incidents, there are both positive and negative effects, and organisations should encourage and motivate users who are entirely or partially influenced by such events to enhance awareness levels about security issues. In order to improve ISA, organisations should focus on delivering information on security attacks; developing risk-management plans, incident response and reaction plans; and identifying how user carelessness makes the organisation’s IS vulnerable to attacks. Organisations should not only focus on internal security incidents, but also on delivering information on external security incidents, as that can also increase the user’s awareness level. Workmates or colleagues’ behaviour is also another factor that affects ISA, because sometimes one user follows the same procedure as a co-worker without knowing whether the co-worker is doing their job according to organisational security policy or not. But this kind of practice does not apply to every user, and end users cannot be isolated from this practice, especially when joining new organisations. The results also show that female participants are more aware of ISA, more dedicated to the compliance of ISP, and always motivated towards security behaviour.

This chapter presents the results of the three surveys and the test results for each of the hypotheses.
4.1 Measuring awareness level of participants

The survey results from the three surveys were analysed by password and sensitive information handling, identifying and managing IS risks and threats, improving organisational IS, incident response and reporting actions and delivering security programs from all three surveys, and are presented here. In addition, the factors that affect the effectiveness of the program (awareness of the functional department, and how training methods are affected by age) are also discussed.

4.1.1 Password and sensitive information handling

The password and sensitive information handling results of all three surveys are illustrated in the bar diagram in Figure 4.1.1 to provide information about how effective the training and awareness program is in raising awareness of the participants.

In the first survey, one question relates to password protection and sharing: Have you noticed in your organisation whether or not employees are sharing the password? Nearly half of the participants replied no to password sharing, one-fifth replied yes, another one-fifth responded do not know, and the remaining participants replied differently. Six said they share the password with workmates because sometimes they are sick or on annual leave and their absence could affect the workflow of the organisation. Some participants replied that they share the password with their partners, and others that there is a standard password for the entire team. A few participants responded that they write a password on a sticky note and stick it on the computer. Gross and Rosson (2007) argue that a single user’s carelessness in handling password and sensitive information could leave the organisation vulnerable. Those who replied yes, do not know or unsure for password sharing are of interest in that these participants need significant attention in training and awareness on password handling, and the training should reflect the importance of password handling and the consequences of sharing in detail. Furthermore, password protection and sensitive information handling policy should be included in organisational security policy and explained to every user.

The results of the second survey show a significant amount of change in the password handling response because participants were then more aware of the issues due to the training and awareness program.

The third survey showed that more than 90% of users did not share their password.
4.1.2 Identifying and managing threats

In the first survey, a question related to identifying and managing threats was asked: *Who is responsible for identifying and managing IS threats in your organisation?* This question intended to establish whether participants knew that IS is not a technical issue, but is a business issue, and every user in the organisation is responsible for IS. Nearly 43% of participants responded that IS professionals are responsible for managing threats, 19% responded that organisational managers are responsible, 36% responded that all employees are responsible, and 9% responded that others are responsible for identifying and managing threats. Six participants responded that their organisation outsources IT from other companies so whatever issues arise, outsourcing companies are liable. Twenty-nine participants still assumed that IS professionals are responsible for any IS-related issues in organisations and 13 believe that it is a manager’s role to manage IS-associated threats and risks. With more than 60% of participants still thinking that it is the responsibility of IS professionals and organisational managers to be liable for IS-related incidents rather than all employees there is a need for a proper training and awareness program that focuses on the responsibility of all users for IS incidents in an organisation, and that none of the users should be isolated from the IS training and awareness program. The threat mitigation and identification process is also part of organisational risk management, and should be made clear to all users.

After the training and awareness program, an increase of awareness in the second survey showed that all users are responsible for identifying and managing threats. The awareness level increased further in the third survey, with participants more aware that every employee is liable for identifying and managing threats. The bar diagram in Figure 4.1.2 illustrates the comparison between all three surveys concerning identifying and managing IS risks and threats.
4.1.3 Improving organisational information security

In the first survey a question related to enhancing IS was asked: *In your opinion how would you improve more IS in your organisation?* The purpose of this question was to identify what measures or precautions could be practical to maintain IS in an organisation, whether it could be implementing the latest control technology, applying for a training and awareness program or both technology and security awareness programs, or any other programs. This question also had the intention of establishing whether participants chose the latest technology or security awareness program, or both.

The results of the first survey showed that 19% of participants responded that there was a need for new technology to improve IS, and another 19% acknowledged that there are other factors responsible for IS, such as outsourcing. A total of 21% of participants responded that there is a need for a security awareness program, and 39% responded that there is a need for both new technologies along with the security awareness program. Outsourcing could be an option for transferring organisational risk to related parties but is not the total solution. Most incidents come from human error, and technical countermeasures are not sufficient to measure human error. Without proper knowledge and awareness of the latest technology, there would be no enhancement in organisational IS. Furthermore, organisations should not only rely on security awareness programs because the increase in awareness level does not protect the organisational assets from external factors such as viruses, script kiddies, Trojan horse attacks and denial-of-service attacks. Therefore, to control these external attacks, there is a need for technical countermeasures. So, both control measures need to be directly proportional to each other.

In the second survey, after the training and awareness program, there was an increased awareness level in participants, and more than half believed that both are required to improve ISA. In the third survey, more participants assumed that technical countermeasures in conjunction with a security awareness program would be more fruitful and successful in
improving organisational IS. Figure 4.1.3 is a bar diagram that illustrates the comparison between the three surveys regarding improving IS.

![Figure 4.1.3: Improving organisational information security](image)

4.1.4 Incident response and reporting actions

A question regarding the incident response and reporting actions was: *If you noticed any IS incidents in your organisation, what would you do?* The purpose of this question was to find out whether participants were aware of incident response and reporting procedures. In answer to the question, 74% of participants responded that it needs reporting to managers straightaway, 19% responded that employees should handle it and respond to the incidents, and 3% replied to just leave or ignore it. The ignorance behaviour of users could lead to potential damage to the organisation. User reaction behaviour could make organisations more vulnerable to attack because the user assumed that they had solved the problems, but that is not the case, and attackers get more time and resources to attack. Therefore, additional training needed to be carried out to raise awareness about incident responses, and an incident response and reporting policy should be included in organisational ISP and explained to all users. User reaction to security incidents could be confusion while solving it, creating a habit of not reporting. Moreover, users do not want to report the security behaviour of their workmate because they do not want to be an enemy of their workmates, and some users are scared to report a workmate’s security incidents because of their violent nature.

After the training and awareness program in the second survey, an increased rate of reporting security incidents to the managers and security professionals with a lower ignorance rate was shown. The reporting rate rose further in the third survey with a zero ignorance rate. The reason for the high increase rate in reporting behaviour rate and zero ignorance rate in the third survey is because when the actual incidents occur in organisations, users can see how their workmates and co-workers report to managers. Users also further notice what procedures their workmates followed, and moreover co-workers could discuss how well they handled the security incidents with other workmates,
thereby increasing awareness level. Figure 4.1.4 is a bar diagram which illustrates the comparison between all three surveys regarding incident response and reporting.

![Bar diagram](image)

Figure 4.1.4: Incident response and reporting

4.1.5 Delivering a training and awareness program

In the first survey there is a question related to the delivery of the training and awareness program: *In your organisation, how often management implements the IS education training and awareness program to employees?* The purpose of this question is to find out from the participant’s point of view in what timeframe the organisation conducts training and awareness programs. Is the timescale effective in maintaining the awareness level of users, or is there a need for a regular schedule? A total of 33% responded that training is conducted during the induction session when they join the organisation, 15% that it occurs every month, 18% that it occurs biannually, and 33% responded with other factors. Among the 22 participants who chose other factors, 10 replied that organisation implements the training and awareness session only after incidents, and the remaining participants answered that there is not a proper training and awareness program in their organisation. In organisations that conduct the training and awareness program during induction, 22 participants responded that it is one-time awareness program. The reason could be that the organisation has implemented the best security measures, or the organisation had not experienced any substantial security incidents, and they just want to inform new users that they are aware of IS and all users need to follow organisational ISP. There is no particular advice indicating that organisations should conduct training and awareness programs in a particular timeframe, and security training and awareness programs should be performed according to the needs of the organisation as part of security policy.

In the second survey, participant’s responses increased marginally in all three answers. But in the third survey, participant’s responses changed dramatically. Participants focused more on biannual training instead of one-time training and monthly training because they assumed that one-time training was not enough in maintaining the awareness level of the user and monthly training was too quick to catch up with all training events, resulting in
more users skipping the training. Figure 4.1.5 is a bar diagram illustrating the comparison between all three surveys about the delivery of the training and awareness program.

![Bar diagram](image.png)

**Figure 4.1.5: Training and awareness program delivery**

### 4.1.6 Awareness level of the functional department

The purpose of evaluating the functional department was to establish whether IS professionals and managers are more aware than personnel in other sectors. The sectors assessed were IT, banking and finance, government, services, health and insurance, education and training, and industry workers and trades. The questions related to password handling, incident response and reaction, identifying and managing IS risks and threats, improving organisational IS, incidents and delivering security programs. The results of the first survey show that security professionals, bank staff, and users from the education and training sector are more aware than other users. The reason is that they are frequently updated about IS by their management. In the second survey, the awareness level increased in all users across sectors. The results of the third survey showed a slight increase in awareness level of all users, illustrating that the training and awareness program was functioning.

Figure 4.1.6 is a bar diagram comparing the three surveys.
4.1.7 Training methods influenced by age

The purpose of evaluating the training method by age was to determine which training method was effective in delivering the message to end users. Some participants prefer classroom-based training methods, others like computer or web-based training methods, and still others like group discussion or case studies. The training method is also affected by age. The younger generation is more attracted to computer-based training methods compared to classroom-based training. All training methods have their advantages and disadvantages. Moreover, user background and interest affect the preferred training method. According to the survey participants aged 18–35, 25% prefer classroom-based training, 35% prefer computer-based training, 32% prefer discussion and group meetings, and the remaining 8% prefer other training methods such as online forums and chats. In participants aged 35–55, 35% prefer classroom-based training, 20% prefer computer-based training, 30% prefer discussion and group meetings, and the remaining 15% prefer other training methods. In participants aged above 55 years, 40% prefer classroom-based training, 15% prefer computer-based training, 35% prefer discussion and group meetings, and the remaining 10% prefer other training methods.

Figure 4.1.7 illustrates the preferred training method according to age group.
4.2 Research hypotheses

Hypothesis testing was done through ANOVA and t-tests to maintain the accuracy of the survey data, and the results for each hypothesis are presented below.

Hypothesis 1:

H0: There is a significant variation in the results of the first survey and the second survey.

H1: There is no significant variation in the results of the first survey and the second survey.

Table 4.2a: ANOVA results for Hypothesis 1

<table>
<thead>
<tr>
<th>Treatments</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>T X</td>
<td>24.53</td>
<td>25.71</td>
<td></td>
<td></td>
<td></td>
<td>53.24</td>
</tr>
<tr>
<td>Mean</td>
<td>2.453</td>
<td>2.871</td>
<td></td>
<td></td>
<td></td>
<td>2.642</td>
</tr>
<tr>
<td>T X^2</td>
<td>60.6165</td>
<td>65.7323</td>
<td></td>
<td></td>
<td></td>
<td>146.3508</td>
</tr>
<tr>
<td>Std.Dev.</td>
<td>0.2227</td>
<td>0.6061</td>
<td></td>
<td></td>
<td></td>
<td>0.4934</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>SS</th>
<th>df</th>
<th>MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Between treatments</td>
<td>0.8736</td>
<td>1</td>
<td>0.8736</td>
</tr>
<tr>
<td></td>
<td><em>F</em> = 4.19081</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Within treatments</td>
<td>3.7523</td>
<td>18</td>
<td>0.2085</td>
</tr>
<tr>
<td>Total</td>
<td>4.6259</td>
<td>19</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.2a shows that the *f*-ratio value is 4.19081 and *p*-value is 0.055528; therefore the result is significant at *p*>0.05 and the alternative hypothesis is accepted.
Table 4.2b: t-test results for Hypothesis 1

Table 4.2b shows the $t$-value is 1.766 at 9 degrees of freedom, and the $p$-value is 0.1112 at 95% confidence interval and $p>0.05$, which means there is a significant variation in the results and the alternative hypothesis is accepted. Based on the outcome of two surveys, there is significant variation between the results of first and second surveys. The first survey was conducted to measure the participant’s basic knowledge of IS. After that, the training and awareness program was implemented, based on the results of the first survey. It is evident that after receiving the training and awareness session there was an increase in user knowledge and a change in behaviour.

Hypothesis 2:

H0: There is no significant variation in the results of the first survey and third survey.

H1: There is a significant variation in the results of the first survey and third survey.
Table 4.2c: ANOVA results for Hypothesis 2

<table>
<thead>
<tr>
<th>Treatments</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>ΣX</td>
<td>24.53</td>
<td>20.71</td>
<td></td>
<td></td>
<td></td>
<td>45.24</td>
</tr>
<tr>
<td>Mean</td>
<td>2.453</td>
<td>2.071</td>
<td></td>
<td></td>
<td></td>
<td>2.282</td>
</tr>
<tr>
<td>ΣX²</td>
<td>60.5185</td>
<td>45.6257</td>
<td></td>
<td></td>
<td></td>
<td>106.2442</td>
</tr>
<tr>
<td>Std.Dev.</td>
<td>0.2227</td>
<td>0.5513</td>
<td></td>
<td></td>
<td></td>
<td>0.4537</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>SS</th>
<th>df</th>
<th>MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Between-treatments</td>
<td>0.7296</td>
<td>1</td>
<td>0.7296</td>
</tr>
<tr>
<td></td>
<td>F  = 4.12772</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Within-treatments</td>
<td>3.1817</td>
<td>19</td>
<td>0.1768</td>
</tr>
<tr>
<td>Total</td>
<td>3.9113</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

From Table 4.2c, the f-ratio value is 4.12772 and p-value is 0.057217; therefore the result is significant at $p>0.05$ and the alternative hypothesis is accepted.

Table 4.2d: t-test results for Hypothesis 2

<table>
<thead>
<tr>
<th>Sample 1</th>
<th>Sample 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>First_Survey</td>
<td>Third_Survey</td>
</tr>
<tr>
<td>Sample size</td>
<td>10</td>
</tr>
<tr>
<td>Arithmetic mean</td>
<td>2.4530</td>
</tr>
<tr>
<td>95% CI for the mean</td>
<td>2.2937 to 2.6123</td>
</tr>
<tr>
<td>Variance</td>
<td>0.04960</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>0.2227</td>
</tr>
<tr>
<td>Standard error of the mean</td>
<td>0.07043</td>
</tr>
</tbody>
</table>

From Table 4.2d, the $t$-value is $-1.911$ at 9 degrees of freedom, the $p$-value is 0.0883 at 95% confidence interval and $p>0.05$, which means there is a significant variation in the results and the alternative hypothesis is accepted. The results of the first and third surveys show a slight variation. The third survey was conducted five months after the implementation of the security training and awareness program because it took one month to analyse the results of the first survey and design the training and awareness program. The purpose was
to establish whether the participants forgot what they had learned in the security awareness program or not, whether it was still effective, or if they needed to refresh with another short awareness program or a continuation of the program. The results further show a slight decline in the awareness level of the participants, which verifies that participants forgot some aspects of the awareness program and there is a need for another short refresher awareness course to update the participants.

Hypothesis 3:

H0: There is a significant variation in the results of the second survey and third survey.

H1: There is no significant variation in the results of the second survey and third survey.

Table 4.2e: ANOVA results for Hypothesis 3

<table>
<thead>
<tr>
<th>Summary of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Treatments</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td><strong>N</strong></td>
</tr>
<tr>
<td><strong>Σx</strong></td>
</tr>
<tr>
<td>Mean</td>
</tr>
<tr>
<td>Σx²</td>
</tr>
<tr>
<td>Std.Dev.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>SS</th>
<th>df</th>
<th>MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Between-treatments</td>
<td>3.2</td>
<td>1</td>
<td>3.2</td>
</tr>
<tr>
<td>Within-treatments</td>
<td>6.0412</td>
<td>18</td>
<td>0.3356</td>
</tr>
<tr>
<td>Total</td>
<td>9.2412</td>
<td>19</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.2e shows that the $f$-ratio value is 9.53456 and $p$-value is 0.0063466; therefore the result is not significant at $p<0.05$ and the null hypothesis is accepted.
Table 4.2f: t-test results for Hypothesis 3

Table 4.2f shows the t-value is –3.069 at 9 degrees of freedom, the p-value is 0.0134 at 95% confidence interval and p<0.05, which means there is no significant variation in the results and the null hypothesis is accepted. The survey results of the second and third surveys show no significant variation. Both surveys were conducted after the implementation of the security training and awareness program, which means participants were more aware because of the security program and the result has no significant difference. It is evident that after a particular time interval participants could forget the awareness program, but the time interval between the second and third surveys was around four months, which is acceptable. As mentioned earlier, the time interval between the first and second survey was five months. It takes a couple of months to conduct the first survey, analyse it, design the training and awareness program based on the results of the first survey, and conduct the second survey.

Hypothesis 4:

H0: There is a significant variation in the results of the initial survey of support group and control group.

H1: There is no significant variation in the results of the initial survey of support group and control group.
Table 4.2g: ANOVA results for Hypothesis 4

Table 4.2g shows the $f$-ratio value is 0.32603 and $p$-value is 0.575069; therefore the result is significant at $p>0.05$ and the null hypothesis is accepted.

Table 4.2h: $t$-test results for Hypothesis 4

Table 4.2h shows the $t$-value is 1.066 at 9 degrees of freedom; the $p$-value is 0.3143 at 95% confidence interval and $p>0.05$, which means there is no significant difference in the results and the null hypothesis is accepted. The results of the first survey of the support group and the first survey of the control group show no major variation in the outcome. Both surveys
were conducted at the same time before implementing the security training and awareness program.

Hypothesis 5:

H0: There is a significant variation in the result of the initial control group and result of the final control group.
H1: There is no significant variation in the result of the initial control group and result of the final control group.

Table 4.2i: ANOVA results for Hypothesis 5

<table>
<thead>
<tr>
<th>Summary of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Treatments</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>N</td>
</tr>
<tr>
<td>ΣX</td>
</tr>
<tr>
<td>Mean</td>
</tr>
<tr>
<td>ΣX²</td>
</tr>
<tr>
<td>Std.Dev.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Result Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source</strong></td>
</tr>
<tr>
<td>Between-</td>
</tr>
<tr>
<td>treatments</td>
</tr>
<tr>
<td>Within-</td>
</tr>
<tr>
<td>treatments</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

Table 4.2i shows the \( f \)-ratio value is 0.21985 and \( p \)-value is 0.644784; therefore the result is not significant at \( p > 0.05 \) and the null hypothesis is accepted.
Table 4.2j: t-test results for Hypothesis 5

Table 4.2j shows the t-value is 0.415 at 9 degrees of freedom, the p-value is 0.6878 at 95% confidence interval and p>0.05, which means there is no significant difference in the results and the null hypothesis is accepted. According to the initial result of the control group and final result of the control group, there is no major variation in the result. There is no difference in the result because none of these participants attended the security training and awareness program. The purpose of this evaluation was to observe whether the change in organisational security culture and policy made positive influences by increasing awareness levels and change in behaviour or not, and whether the user’s own consciousness of IS has any impact in changing security behaviour.

Hypothesis 6:

H0: there is a significant variation in the result of final support group and result of the final control group.

H1: there is no significant variation in the result of final support group and result of the final control group.
Table 4.2k: ANOVA results for Hypothesis 6

<table>
<thead>
<tr>
<th>Treatments</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>$\Sigma X$</td>
<td>20.71</td>
<td>25.69</td>
<td></td>
<td></td>
<td></td>
<td>46.4</td>
</tr>
<tr>
<td>Mean</td>
<td>2.071</td>
<td>2.569</td>
<td></td>
<td></td>
<td></td>
<td>2.32</td>
</tr>
<tr>
<td>$\Sigma X^2$</td>
<td>45.6257</td>
<td>66.4983</td>
<td></td>
<td></td>
<td></td>
<td>112.124</td>
</tr>
<tr>
<td>Std.Dev.</td>
<td>0.3513</td>
<td>0.2339</td>
<td></td>
<td></td>
<td></td>
<td>0.4534</td>
</tr>
</tbody>
</table>

Table 4.2k shows the $f$-ratio value is 6.89756, and the $p$-value is 0.017124; therefore the result is significant at $p<0.05$ and the null hypothesis is accepted.

Table 4.2l: t-test results for Hypothesis 6

Table 4.2l shows the $t$-value is 2.375 at 9 degrees of freedom, the $p$-value is 0.0416 at 95% confidence interval and $p<0.05$, which means there is no significant change in the results.
and the null hypothesis is accepted. The results of the third surveys of the support group and the control group show no major variation. Both surveys were conducted six months after first survey, and the results show that participants either forgot the training or did not comply with the security program. Alternatively, the participants from the control group could have become more aware of the organisational ISP, or following organisational change. The results show a decline in awareness level of the support group and increase in the awareness level in the control group, which means that there was no major variation between the groups.

Hypothesis 7:

H0: There is a significant variation in the relationship between ISA and ISP performance.
H1: There is no significant variation in the relationship between ISA and IS performance.

Table 4.2m: ANOVA results for Hypothesis 7

<table>
<thead>
<tr>
<th>Summary of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treatments</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>N</td>
</tr>
<tr>
<td>ΣX</td>
</tr>
<tr>
<td>Mean</td>
</tr>
<tr>
<td>ΣX²</td>
</tr>
<tr>
<td>Std.Dev.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Result Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
</tr>
<tr>
<td>Between-treatments</td>
</tr>
<tr>
<td>Within-treatments</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

Table 4.2m shows the $f$-ratio value is 6.66336, and the $p$-value is 0.004445; therefore the result is significant at $p<0.05$ and the alternative hypothesis is accepted. To measure organisational security awareness, the results of all the three surveys from the support group were compared. The participant’s awareness level was measured before the security program, after implementation of the security program and then after a specific time interval to gives a comparative analysis. The results show that participants with minimal knowledge of IS and organisational security policy dramatically increased their knowledge after the security training and awareness program, and the number of IS incidents reduced. And, after a specific time interval, some participants maintained their awareness level, whereas some participants forgot the security awareness program. Some participant’s behaviour exhibited knowing but not doing (as explained in Section 2.9.2). The results
conclude that ISA has a positive influence in changing user security behaviour, which ultimately changes IS performance.

4.3 Summary

This chapter provided analytical discussion and the results of hypothesis testing. The end-user’s awareness level was measured based on password and sensitive information handling, identifying and managing threats, enhancing organisational IS, incident response and reporting of actions, delivery of the training and awareness program, awareness level of the functional department, and evaluating the training method by age. The research hypothesis testing was conducted through two tests: ANOVA and t-test. The t-test was implemented because the survey needed to be carried out to similar participants multiple times.

Chapter 5 describes building an effective IS training and awareness program.
Chapter 5. Building an effective information security training and awareness program

An Information security training and awareness program is a perfect way of teaching users about organisational IS and security policy to ensure that users follow the same guidelines during their work. In some organisations, users assume that IS belongs to IT and the security program is related to technological measures (Sanghavi, 2015). This can lead to unintentional mistakes, or users incorrectly performing their duties. Sometimes users do not know how and where to report suspicious behaviour they identify in an organisation (National Offshore Petroleum Safety and Environmental Management Authority, 2018). IS programs are designed to overcome such situations. Security programs do not teach users how to do their job, but teach them how to perform tasks safely and securely (Gilbert, 2003).

This chapter describes the development and implementation of the security training and awareness program. This chapter also details the design and implementation of the program, and the influence training methods have. Before developing the program, certain things need to be considered, such as organisational needs, the goal of the security program, risk management and business contingency. The three attributes of IS; that is, confidentiality, integrity and availability, are the main pillars of the training program. The program needs to align with the organisation’s mission to meet its business goals (Breithaupt & Merkow, 2014). The purpose of a training and awareness program is to improve the user’s view, and encourage them to understand and follow proper ISB about organisational IS (Maeyer, 2017). Teaching users about ISA could help in solving primary security and privacy challenges (Ghazvini & Shukur, 2017). However, there are some security training and awareness programs that fail, and the main reason for this is providing too much information during the training (Burnette, 2017).

5.1 Goals of an information security training and awareness program

Generally, in most organisations, the IT and security department is liable for the protection of the organisation’s physical and technical resources. The primary intention of an IS training and awareness program is to make clear that organisational IS is the concern of all users at all levels, rather than being the responsibility of the IT and security department. When an organisation expects correct ISB from all users, it is the responsibility of the organisation to train, educate and make users aware of organisational IS, and also their role in safeguarding the organisation’s confidentiality, integrity and availability (Brecht, 2017).

The goal of the IS training and awareness program is to deliver a clear, accurate and detailed message in such a way that is easily understandable. The message should focus more on why and how we protect organisational IS. The security program contributes to building a positive security environment in an organisation, and emphasising its significance.
contributes to ongoing enhancement. An information security training and awareness program should address all users in an organisation, and management should act as a role model in establishing ISB at all levels, therefore the security program should be implemented as appropriate to all levels (O'Donnell, 2016). An IS training and awareness program should be employed according to the user’s job and position, rather than applying the policy of one size fits all. For example, the awareness program deployed for general users would be inappropriate for security professionals and managers; this kind of practice does not assist in achieving success in security programs (Ramalingam, Khan, & Mohammed, 2016).

Another goal of the IS training and awareness program is achieving business objectives, so it also needs to focus on it helps achieve the business goals. Today all business is conducted electronically, and business success relies on the information that is given by information systems with business processes that are stable and ongoing. Information plays a significant role in decision-making and organisations classify, prioritise and protect the information according to their importance (Kaplan, 2015). Since users are the primary source for handling data, security training and awareness programs educate, train and raise awareness about how to handle the organisation’s business information without risking confidentiality, integrity and availability. Organisations must have a renowned and good reputation to sustain their competitive business environment (Hudgens, 2017). Customers expect that all their information will be confidential and should only be utilised for given reasons. Organisations should therefore have well-written security policy and procedures, and implement regular security training and awareness programs to ensure that users are aware and alert in safeguarding organisational information and resources (Russell, 2002). Security training and awareness programs assist users to know why they have to focus on protecting the organisation’s business information, what will happen when business information gets breached, and how to safeguard the organisation’s business information by raising the awareness of users (Ashraf, 2005).

This chapter concentrates on the design, development, implementation, measuring and monitoring of the security training and awareness program. It further reflects on the model and methodologies that apply to proper participation and encouragement of users. ISA is valuable in achieving the targeted objectives of organisations, and this chapter discusses implementation procedures and the difficulties in implementing methods for raising awareness. The significance of, and relationship between, IS programs and users and also those features that inspire users to participate in the program are also discussed. An IS program should concentrate and inspire all users about the rules and regulations for ensuring organisational IS.

Figure 5.1 illustrates how to build an effective security training and awareness program, which is explained in detail in the next section.
5.2 Designing an information security training and awareness program

The designing phase is the initial step in building the IS training and awareness program. During the designing period, the organisation’s mission should be kept in mind. The mission is a significant part of the training and awareness program, showing how the business requirements are related to organisational IS and culture. While designing the program, it should be kept in mind that the content must refer to the organisational IS topics and subjects, rather than meaningless issues. The designing phase identifies organisational needs, expectations of the training and awareness program, and how to deliver it. The designing phase includes identifying the organisational needs, target audience, an outline of the training and awareness plan, setting up the priorities and benchmarks, the budget, risk-management plan and business contingency plan.

Many researchers identify other factors that require consideration. For instance, von Solms and von Solms (2006) state there are internal and external factors. Internal factors can be controlled and maintained by organisations, such as the organisation’s values, strategies and business challenges. External factors, which cannot be controlled, include changes in technology and threat levels, the government and legislative environment, and changes to the global market. Upfold and Sewry (2005) consider organisational security policy, prioritising information and resources, physical and logical security, access control, and risk management and business continuity as critical factors. ISO Security considers security
compliance and incident management as essential factors of IS programs (International Organization for Standardization, 2013). Chang and Ho (2006) propose other factors, such as organisational position and rank, and IT aptitude as having a positive impact on designing training and awareness programs. Knapp, Marshall, Rainer, and Morrow (2006) and Singh, Gupta, and Ojha, (2013) identify technical and non-technical factors that need to be addressed while designing the security program.

There are some factors that need an explanation before moving on to the development phase of an IS training and awareness program. Below is a detailed explanation about how each element influences the training and awareness program.

5.2.1 Identifying customer needs

Identifying customer needs is the initial step in creating an effective IS training and awareness program. In this research, customers mean end users, managers and security professionals. Before developing a training and awareness program, management has to research its organisation to identify weakness and the areas that are most vulnerable. IS audits also needed to be reviewed, what advice has been given and the response. After the diagnosis of an organisation, its intention regarding a security program needs to be looked at; why the organisation wants to implement a security program, and what are its expectations. The expectations of end users and security professionals also need to be addressed. For example, users do not generally tell managers they do not know how to perform a particular task and ask for training, but if managers understand and recognise that a user’s action is not appropriate, they could request and recommend users for training. Another way to identify the user’s needs is to work with them as a colleague or workmate, because in many cases, co-workers are the first to be asked for help, with some users scared of asking for help from managers. Working as a friend with end users encourages sharing of work experiences and motivates them towards understanding IS. Understanding user interest is another factor to consider.

5.2.2 Reviewing the previous security program

Some organisations have had security training and awareness programs before, and some have not. If an organisation has not had a previous security program then a new security program could be created based on their needs, but if the organisation already has had a security program, it needs to be reviewed; what has happened, what topics they covered, why the metrics are not effective in measuring outcomes, was the security program continued or did it stop, and what they want now, are the questions that need an answer. The organisational security policy and programs that were designed and implemented 10 years earlier might not be practical now because technology is changing, and so is the risk and threat level.
5.2.3 Identifying the training and awareness tools

Awareness tools and methods play a significant role in program effectiveness. The tools should be based according to the user’s choice if possible. The approach in one organisation may not suit all users. Users need to have the freedom to choose the training method where possible. The security program should also be readily understood, well organised and delivered without any obstacles (Arash & Zarina, 2017).

5.2.4 Identifying user knowledge through metrics

Metrics are valuable and significant tools for identifying security training and awareness program needs. Metrics measure the success of training and awareness programs by calculating the effectiveness of the program, evaluating the competence of the program and determining potential growth. The metrics should further measure what users already know about IS, what users believe about IS, and how they perform organisational IS (Veseli, 2011). Further analysis to identify the gaps is required; what happened before, what is currently being implemented, and what are the plans. After completion of the needs assessment, the outcomes could be presented to managers to persuade them that appropriate resources are required to enable the identified training and awareness needs to be met and to develop the outline of the program. The outline should cover all organisational needs and set up priorities based on their importance. Identifying end-user knowledge about organisational IS is very important in deciding the content for a security awareness program. Some researchers also call this needs assessment (Wilson & Hash, 2003).

5.2.5 Target audience

The target audience is the intended users for the specific purpose. Organisations must identify the right people for the right training to gain success in the security program, and the security program must directly influence the target audience. The organisation needs to establish the problem that is being experienced by the target audience. In this research, the target audience includes technical and non-technical users as described in Table 5.2.5.

Table 5.2.5: Target audience

<table>
<thead>
<tr>
<th>Targeted Audiences</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>Chief Information Security Officer (CISO)</td>
</tr>
<tr>
<td></td>
<td>All security professionals</td>
</tr>
<tr>
<td></td>
<td>Help desk support</td>
</tr>
<tr>
<td></td>
<td>System and network administrator</td>
</tr>
<tr>
<td>Non-Technical</td>
<td>Executives and decision makers</td>
</tr>
<tr>
<td></td>
<td>Managers</td>
</tr>
<tr>
<td></td>
<td>All users from other departments</td>
</tr>
<tr>
<td></td>
<td>General users</td>
</tr>
<tr>
<td></td>
<td>Cleaners and security guards</td>
</tr>
</tbody>
</table>
5.2.6 Outlining the security training and awareness program strategy and plan

After finalising the identified needs, the next phase is to develop the strategy and plan for the training and awareness program. This plan is the operational manuscript that consists of the factors responsible for the strategy, such as current government and legislative policy which states that organisations need to complete the training and awareness program. The manuscript also comprises training and awareness program opportunities, description of the training and program coordinator, target audience, expected goals of the training and awareness program, content, delivery method, and comments and suggestions for the program.

5.2.7 Setting up priorities

After completion of the planning, there arise some factors that determine what resources or elements should be scheduled, in order and prioritised. Training and awareness program materials and supplies need to be prioritised according to the availability of the resources. If the training and awareness program materials are available early, it could be scheduled first, but if the equipment is not available then the coordinator needs to assign and develop the program, and this should be considered as a high priority. Priority needs arrangement according to the risks and threats identified during the risk-management process. The security training and awareness plan should prioritise users according to their position in an organisation, because the job determines the sort of access that users hold. Identified gaps need preferencing according to their goal in the particular areas. If the training and awareness program is dependent on any other factors, then positive elements need to be prioritised based on their necessity and condition for the program.

Setting up the barrier

When complications arise from the training and awareness program materials during the planning phase, the target audience needs consideration. The training and awareness materials must focus on two areas: target audience position in the organisation and IS experience needed for the position. While setting up the barrier in developing awareness materials, more attention should be paid to the behaviour of employing the information system. Setting up the barrier while developing the training resources is significant, and the objectives of the training are to create the related skills and knowledge, identifying the necessary responsibilities, actions, and training requirements of the target audience. The training resources need designing in such a way that they offer essential skills and knowledge for participants to achieve IS responsibility related to their position, from beginning level to top level. For example, basic training resources on organisational IS are for general users, further advanced training materials are for managers, and highly developed training resources are for security professionals, executives, and decision-makers who are entrusted with more responsibility to address IS responsibility. Setting up the barrier for educating materials is more complicated because educational providers create these materials and they are less useful when implemented temporarily. If there is a need
for educational resources in the security program, educational providers who offer such degrees and certificates can be found easily, and their syllabus fulfills the resources and materials criteria.

**Information security training and awareness budget**

Budget plays a significant role in planning a training and awareness program. A decision needs to be made on the budget for the security program with full support from the executives. The budget for the training and awareness program should be allocated as part of the organisation’s IS budget, or additional budget needs to be assigned based on the priority of the security program. The training and awareness plan requires minimum criteria to meet, and the requirements need to be sponsored by the organisation’s budget or viewed through the contract. When the training and awareness plan requires prioritising at a lower level, there could be an issue in deploying the training and awareness plan. Therefore, the chief information officer (CIO) is liable for investigating all the priorities and for building a program that refers any insufficiency and shortage in the budget that could affect the current security training prerequisite, that is, fitting the training and awareness plan according to the existing budget, pushing for extra budget, restructuring of current resources, and deploying the training and awareness plan when the budget is accessible over the specified time interval.

5.3 Developing the security training and awareness program

After the designing phase, the next step is to develop the training and awareness program. Before preparing training and awareness resources, two factors need to be considered: training (knowledge and education based on target audience needs) and awareness (highlighting the behaviour). Training and awareness both need to concentrate on the designed resources that the participant uses for their work (Knapp & Ferrante, 2014). During the training and awareness session, if materials and content relate to the participant’s job role, they concentrate more on the course. In order to make the training and awareness program successful, the training and awareness resources need to be remarkable, motivating, attention-grabbing, relevant and topical. Normally the objective of the awareness resources is just to concentrate on the best security preparation, so the awareness message needs to be brief and straightforward (Pullman & Streff, 2009). The awareness message could cover one area or multiple areas depending on the areas the participants should be made aware of (Wilson & Hash, 2003). The message delivered or communicated during the awareness session should ensure that every user is aware of general IS roles and responsibilities. But the message conveyed in the training session must focus on the particular and intended audience only. The message that needs to be delivered during the training session should cover the entire resources related to IS that participants must know to perform their duties safely and securely (Olzak, 2017). Therefore, training resources are further discussed in detail in the following sections (Wilson & Hash, 2003).
5.3.1 Creating training and awareness resources

Organisations should seek to understand what the target audience wish to learn prior to creating resources for training. Before creating training resources, the training coordinator needs to find out who the target audience is and what their roles and responsibility in IS are. IS training needs to focus on the latest computing technology rather than outdated technology (deZafra, Pitcher, Tressler, & Ippolito, 1998). The training materials should emphasise the level of responsibility for IS, and training methods should be flexible, with the capacity for future technologies and organisational expectations because technology and expectations change over time. The training methods should be developed at basic, intermediate and advanced levels, and sample learning objectives need to be given for every level as a manual for a module developer. This research does not focus on learning objectives, but provides a brief description (Wilson & Hash, 2003).

During the creation of the awareness resources, the first query is what all users want to be aware of; whether it is related to underlying knowledge about organisational security or about social engineering attacks, phishing attacks, password handling or any other specific area of IS. The training and awareness materials need to be clear and precise. The training materials do not need to be advanced and intricate. Most organisations complete their training and awareness sessions with flexible funding and average involvement. The purpose of an IS training and awareness session is to make every end user aware of IS, rather than certifying them in IS. Security professionals could develop security awareness resources by consulting with managers, or buy them from security agencies. If the organisation finds a specific security issue, they could implement a short awareness program which focuses on that particular issue rather than waiting for the formal awareness program to launch (Alageel, 2003).

It is often a difficult task to change the user’s behaviour and attitude, but it is not impossible. Some techniques could be tried, such as rewarding, appreciating, encouraging and building positive thoughts to help users change. But if the user intends not to change their behaviour and is stubborn, then they tend to change their job. Awareness resources should focus more on how end-user security behaviour affects organisational IS culture, business processes and lifestyle. Resources should also focus on how and why rather than what. For example, what is IS should be replaced by why do we need IS and how do we maintain IS in our organisation.

Awareness resources need to discuss the importance, and the potential impact, of not complying, and during the session there needs to be two-way communication. Two-way communication encourages end users to speak up and share their experiences and opinions. It should be kept in mind that the user’s skills and ideas are another resource which might not be in the awareness content, and these issues could be of interest for future reference for the awareness program coordinator. The most important thing is that awareness resources must be designed according to the job role of the users (Wilson & Hash, 2003).
5.3.2 Choosing appropriate content

The organisation can choose to develop its training program by consulting with management, executives and security professionals, and examining organisational IS needs. There are many IS disciplines, but those that address the organisation’s expectations need to be selected. The content should include, but not be limited to, the following: IS attacks; password handling; how to use new technology; emergency procedures, and incident response and reaction procedures; and training on evacuation during major emergencies (Wilson & Hash, 2003). While choosing training content, it is crucial to address the level of the training program (basic, intermediate and advanced).

As mentioned earlier, training and awareness resources should focus on designing the program according to the user’s position in an organisation. There are hundreds of topics in IS. Selecting appropriate materials should be based on the organisational needs, the results of the risk matrix, what users want to learn, vulnerable areas of IS, and managers and security professionals’ expectations; for example, awareness of phishing attacks, social engineering attacks, password policy, accessibility of ISP, cyber terrorism, scammers and reporting policy. Security professionals should be aware of new security threats and how that threat affects the organisation’s IS system. Managers should be mindful of how unintentional and small mistakes could jeopardise the whole IS and business processes. General IS content should be designed for the general user, general content along with additional materials should be developed for managers, and advanced content should be planned for security professionals’ awareness (Alageel, 2003).

5.3.3 Content sources

Before creating the training program, the first thing to consider is whether the security professionals should develop the program or whether it should be outsourced to a security agency. In this research three types of sources for training content are discussed: in-house built in, partnering, and outsourcing the entire training program. Many organisations can develop an in-house training program by using their own resources, getting assistance from IS professionals, security websites and online security courses, and bearing all the expenses for the program.

In partnering, many organisations unite and share their resources to build up a training program. For example, in Australia, many organisations combine their resources and create a training program. When there is only content included in the training program, others could contribute their assets to that content and modify it in such a way that the training program only consists of the organisation’s resources. Sometimes combining training resources cannot meet the objectives. In such cases, special attention to training resources that meet the participant’s expectations are required (Wilson & Hash, 2003). Therefore, organisations should scan training resources created by combining resources, and check whether the training content and resources are appropriate for their organisation or not before deploying the training program.
Outsourcing the training program requires organisations to consult with outsourcing agencies who are expert in building training and awareness programs. Sometimes there are already built-in security training program samples, and sometimes outsourcing agencies could create one based on the organisation’s needs and expectations.

Much awareness content is found easily on the internet, which can be practice for awareness sessions (Alageel, 2003). Awareness content should focus on a particular issue, and sometimes a single resource could cover the whole awareness session. Sometimes, ISA content is readily available from electronic and non-electronic sources. For example, electronic sources could be IS-related movies and serials on television, security training institute websites, journal articles, white papers, conference papers, eBooks, conference papers, seminars, research papers and theses. Non-electronic sources are course books, newspapers, security magazines and articles, security posters and pictures, and security essays (Wilson & Hash, 2003).

5.3.4 The learning process

People learn in many ways, and a single rule does not apply to all. Since there is no appropriate training method or resource that suits all organisations, the training coordinator and training course developer are responsible for choosing training resources that fit the organisational and target audience expectations. The most successful learning process for people depends on their learning technique, knowledge and previous experience. A Chinese saying best defines the learning objectives, I hear I not remember, I see I understand, and I do I learn.

Learning objectives are classified into two sections: learning techniques, and previous knowledge and experience. Learning techniques are different for everybody, but personalities sometimes determine particular learning techniques. Both instructor-based and computer-based learning techniques could have an optimistic or pessimistic impact on audience performance and the technique is determined based on suitability for the target audience’s preference. Both for theoretical and practical learning processes, some audiences like to listen to the content and others may wish to experience audio-visual learning, group discussion and image description. During the learning process, the training coordinator sometimes gets confused between teaching and telling (deZafra et al., 1998). During the teaching procedure, they find out whether audiences are listening or not so they can implement an alternative method. In the telling procedure, the training coordinator merely conveys the message from the training resources. The training program should consist of many delivery approaches, such as presentations, audio-video, pictures and diagrams, and end-of-training test. These approaches suit both instructor-based and computer-based training methodology.
5.3.5 Previous knowledge and experience

The training coordinator should focus on the knowledge and experience of the target audience prior to deploying the training session. For example, an audience with advanced-level IS skills could identify and learn more compared to an audience that does not have an advanced level of knowledge. If the target audience is made up of recent graduates, then they could be more dedicated to computer-based training methods because they are familiar with those methods from their study period (deZafra et al., 1998).

The training coordinator should also focus on the target audience’s job position prior to developing the training program. For example, if it is intended to train general users about different types of attacks, such as phishing, social engineering and spoofing, then a couple of training days need to be deployed. But if the same training session is applied to security professionals, then a one-hour period would be enough because they are already familiar with those terms. But if the training coordinator pushes security professionals to attend the same training program for a couple of days, they would be not interested and might skip other training programs in future.

5.4 Implementing an information security training and awareness program

As soon as the organisation identifies the needs and training programs goals, designs the training strategy and plan, and develops the training and awareness content and resources, the next step is to implement the program. Implementing the security training and awareness program is not only the responsibility of security program coordinator but is the responsibility of all end users and at all levels. Before implementing the security program, its potential benefits should be fully explained, ensuring that the program gets full support from management and end users. The training and awareness program budget needs to be discussed to ensure either the IT department allocates the budget as a part of the total IT budget or management fully covers the expenses of the security program. Furthermore, the training timetable and closing the procedure with a short test needs to be discussed.

Training and awareness programs are not successful unless management is involved because management has the final decision about accepting and implementing the program. End users are also responsible for implementing the security program. User interest, full support and positive involvement at every level motivate and encourage the implementation of IS. There is a saying in IS: the organisation does not change but users change, and user behaviour changes the shape of the organisation.

Before implementing the training and awareness session, a sample test needs to be conducted with a pilot group (a general group designed to quickly test the program to provide advice and comment). The pilot testing needs to be done by security professionals in a given period to receive timely suggestions so that necessary changes are made before implementing the program or session.
5.4.1 Awareness and training resources delivery method

Some awareness delivery methods are freely available on the internet and others could be created. Awareness resources should be deployed in those areas users frequently go, or in forms they are likely to see, such as posters and pictures, mouse pad, pens, coffee cups, kitchen walls, toilet walls and screensavers. Awareness resources are more effective when they are colourful, attractive and provide meaningful messages. Cartoon pictures with awareness message need changing over a specified time interval. One of the most robust awareness methods for raising awareness is through television programs, but that is not practical within an organisation. For example, the government could implement an awareness campaign through comedy and informative programs on television and broadcast through the radio.

The training delivery method depends on the development of the training program; either in-house, partnered or outsourced. Some examples of training methods are instructor-based, web-based and group discussion. The security training and awareness program must execute more than one delivery mode for success of the program. Funding needs to be considered as some modes, for example animated videos, are costly to either buy or make.

Table 5.4.1 outlines awareness and training methods.

<table>
<thead>
<tr>
<th>Delivering awareness methods:</th>
<th>Delivering training methods:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pictures and posters</td>
<td>Instructor based training</td>
</tr>
<tr>
<td>Mouse pad</td>
<td>Computer based training</td>
</tr>
<tr>
<td>Screensavers</td>
<td>Scenario based training</td>
</tr>
<tr>
<td>Coffee cups</td>
<td>Online forum and interaction</td>
</tr>
<tr>
<td>Pens</td>
<td>Group discussion</td>
</tr>
<tr>
<td>Videos</td>
<td>Focus group</td>
</tr>
<tr>
<td>Cartoons</td>
<td>Seminar</td>
</tr>
<tr>
<td>Newspaper</td>
<td>Monthly meeting</td>
</tr>
<tr>
<td>Security magazines</td>
<td>Conference</td>
</tr>
<tr>
<td>Crossword puzzles such as Sudoku</td>
<td>Case study</td>
</tr>
<tr>
<td>Calendars</td>
<td>Distance learning and elearning</td>
</tr>
<tr>
<td>Security news on Television and radio</td>
<td>Self study (education is training in progress)</td>
</tr>
<tr>
<td>Video games</td>
<td></td>
</tr>
</tbody>
</table>

Table 5.4.1: Training and awareness delivery methods

5.4.2 Challenges in implementing a security training and awareness program

Sometimes unwanted challenges arise during the implementation phase. Some of the difficulties that arise in implementing the training and awareness program are:

- management not in favour of implementation
- the program lacks definition of ongoing benefits
- insufficient resources and materials
- ineffective or loss of communication
- undefined funds for the security program
- pushing all participants for a single program
• participants leaving in the middle of the program (Ashraf, 2005; Topic 1: Obstacles to Successful Implementation, 2014; Wood, 2011)

5.5 Post implementation of the information security training and awareness program

The final step in building an effective IS security training and awareness program is the post-implementation phase. As it is well known that IS training and awareness is not a one-time program, and to make the program more effective, there is a need for continuous and ongoing support from management and users. The reason for constant backing is that technology is changing, people are changing, and even organisational strategy and expectations are changing. The continuous and ongoing support includes measurement, monitoring, change management and measuring success factors of the program (Wilson & Hash, 2003), which is discussed further in the next chapter.

An IS training and awareness program is outdated and redundant if proper consideration is not given to changing the technological and organisational environment when the organisation’s values and goals are changed. Organisational management and IS managers need to be aware of these kinds of possible issues and should include some procedures in security policy to make sure that the ongoing IS training and awareness program is an essential part of meeting the organisation’s goals. Ongoing IS training and awareness programs should be considered of interest for continual progress. Monitoring the effectiveness of the IS training and awareness program is essential for the continuous improvement of the training program because monitoring outlines and tracks the critical information about the training program’s activity (Wilson and Hash, 2003).

The monitoring process also summarises the training’s activity, such as the training syllabus, schedule and participants, and provides a further mechanism for standard reporting and analysis of the IS training program. Monitoring the program includes evaluating its level according to the report of the program, and being consistent with the standard determined by the organisation. The report’s recommendations could be implemented to identify the gaps in IS so that necessary remedial actions can be taken and followed up. This process assists managers to recommend additional ongoing training and implement corrective strategies for success. An ongoing IS training program would not be successful unless proper assessment and feedback procedures are undertaken. The feedback procedure should focus on the goals of the training program that were established in the beginning. The feedback procedure could be implemented after the essential benchmarking is outlined. The feedback procedure should include all the essential factors that affect the quality of the training program and also provide any further advice or recommendations for the change (Wilson & Hash, 2003).

There is also a need for change in the IS training and awareness program as the technology changes and new threats appear. The training and awareness program content and delivery
methods need to be changed as the organisation’s mission changes, for example when the organisational structure changes, business expectation changes, external global market changes, and national rules and regulation related to information systems changes. Therefore, managing change ensures the training and awareness program is functioning well and is appropriate in addressing the actual problems confronted by the organisation. Managing change should also focus on changing IS policy as indicated by the organisational culture.

Continual development concentrates on generating training and awareness to a standard that ensures comprehensive IS. During continual development, the training and awareness content and delivery mode should be built in and related to the organisation’s business strategy. Therefore, a good IS training and awareness program should classify the dimension of the program, monitor procedure to acquire data, and send standard reports to responsible executives on time and as agreed (Wilson & Hash, 2003).

5.6 Summary

This chapter provided an overview of building an effective IS training and awareness program in detail, which included its design, development, implementation, measurement and monitoring. It also described the influence of the program delivery method on measuring its effectiveness. The IS training and awareness program should be developed in such way that it covers the expectations of the organisation, objectives of the program, and any issues that arose in the risk management and business contingency plan. With business being conducted electronically and over the internet, the achievement of business goals depends upon the organisational information system. Thus, the goal of the training and awareness program should not only be limited to achieving security goals, but also needs to achieve business goals.

This chapter further described the implementation process and the barriers to success of the IS training and awareness program. The importance of, and relationships between, the IS training and awareness program and participants, as well as those aspects that influence participation were explained.

With a need for ongoing support from management for the success of the program, this chapter also discussed on feedback, monitoring and updating the program and implementing change management.

Chapter 6 presents an overview of measuring the effectiveness of an IS training and awareness program, discusses outsourcing and partnerships, and provides reasons for failure of the program.
Chapter 6. Measuring the effectiveness of the training and awareness program

The effectiveness of an IS training and awareness program would be unknown unless it was measured. Measuring effectiveness is critical to making sure that the implemented security training and awareness program has a significant effect. Measuring the effectiveness of the program ensures it addresses and satisfied all the needs of end users, organisations, and the needs of the training program itself, discussion of which constitutes this chapter. For example, if the training resources and materials do not satisfy the training needs, such as using inappropriate topics that are obsolete and not suitable in today’s context, then the training and awareness program does not comply with the user’s and the organisation’s needs. An inappropriate method of delivering the training and awareness program, whether a complicated process of delivery or a random way of mixing different delivery methods such as lectures, audio-visual, pictures and images, and discussion, would not satisfy the training and awareness program needs. When the training and awareness program fails to achieve the targeted outcomes, additional time and funds need to be deployed to support the program. But in most cases, instead of allocating extra funds and time for preventive measures such as training and awareness programs when there is a security attack, most organisations spend the additional resources on the recovery of the system (Davis, 2008).

Often only one aspect of IS, the end user, is considered the main reason for IS incidents in an organisation. Rather than end users, many other factors are responsible for IS incidents, and those factors also need to be addressed during the development, implementation and measurement of the security program. For example, the effectiveness of installed technology needs to be regulated, and should gauge the user’s opinion about the technology that has been implemented; whether it supports them at work or not. Also, the applied technology should measure whether the allocated funds for the training program are sufficient or not, as well the request procedure for additional funds.

6.1 Reason for measuring effectiveness of the training program

The standard methods for delivery are instructor-based, computer-based, group discussion or through monthly meetings. Albrechtsen and Hovden (2010) argue that user involvement in group training, such as group discussion and workshops verify that such programs are effective in changing user attitude and behaviour. In their group training workshop, Chen, Li, Hoang, and Lou (2013) had very few participants, but the training conveyed and communicated the message briefly with a minimum of time allocated. When they measured the effectiveness of the workshop after six months, they found that while changed participant behaviour was maintained, they could not explain their knowledge about the organisation’s IS and issues as they had forgotten it in that time interval. Moreover, the participants in the workshops had not concentrated as intended.
Siponen (2000) states that there should be some interesting and exciting activities during the training and awareness program to encourage participants, as well as the program coordinator. Supporting Siponen’s idea, Merete Hagen et al. (2011) emphasise implementation of the fun factor related to IS (such as games and play that users would remember for a long time) could be another effective way of keeping participants and the training coordinator motivated. Another study by Goucher (2009) also supports group training’s effectiveness in changing user attitude and behaviour.

Kim and Homan (2012) compared the effectiveness of computer-based and instructor-based training methods and found that computer-based training is more successful in maintaining knowledge. They performed a follow-up survey two and three months after training, and found that after two months the knowledge transfer rate was high in instructor-based training, but it was low in the survey conducted after three months. Additionally, they found no change in the level of knowledge after three months; the result of the initial survey before the training program was similar to the three-month survey results.

Usually, organisations expect that after a training and awareness program there will be an increase in the performance of users, but there arises a question: how much improvement has the training and awareness program instigated to change the user’s performance. There is no accurate measurement of the training and awareness program and user performance, only an approximation, because user performance is not only related to training—there are other external factors involved. The training and awareness program is considered useful in enhancing business processes and performance, and it should be compared to other methods and chosen according to their functioning. When the IS budget is low, the training and awareness program is often abandoned. As mentioned earlier, while designing the training and awareness plan there is a need to plan for continuity and improvement of the program. Measuring the effectiveness of a training and awareness program assists in choosing appropriate training methods because organisations can compare the selected mode with other organisations that have already implemented that method to check its effectiveness. Measuring effectiveness assists in understanding the success of the program by knowing the potency and limitations of the training and awareness program, which is necessary to recognise user performance and interest.

Below are some of the reasons why it is essential to measure the success of the security training and awareness program.

1. To estimate that the resources and materials deployed were appropriate for learning and satisfied the participants.
4. To measure what the participants learned from the training and awareness program.
5. To measure training and awareness effectiveness by looking at the participant’s results.
6. To measure the effectiveness of the training and awareness method by comparing it to alternative methods (Ashraf, 2005).

7. To give meaningful information that helps users to evaluate their own work performance and managers to monitor and supervise work performance.

8. To provide statistical and numeric data that is used by the training coordinator to further enhance the teaching and learning process (deZafra et al., 1998; Skillnets, 2005).

Prior to measuring the effectiveness of the training and awareness program it is essential to plan the evaluation. It is necessary to have a learning plan to measure the participant learning process. There is a need for the plan to measure training effectiveness, and finally, the organisation’s strategy and goals allied with the learning process need to be identified to measure the ROI. The evaluation plan consists of three attributes: measuring the performance plan, measuring the level, and deploying the measuring plan.

6.2 Performance planning

To measure performance planning, two attributes known as estimating the possible actions and degree of achievement are required.

6.2.1 Estimating the possible actions

The prerequisite of action is a well-written document that forecasts the activities that are required before and during the learning process. In other words, there is a specific prerequisite that needs to be communicated to foretell training and awareness program effectiveness. For example, during the training and awareness session, does the training coordinator need a hardcopy of the course, materials such as projectors and some coloured and printed pictures for audio-visual presentations, and is there a need for special arrangements for participant comfort. The performance planning should advise that the actions are achievable in such a way that allows the training coordinator to look at the actions used by participants either in class or the workplace. But it is a challenging task to measure participant attitude through their work. During the measuring process, the training coordinator could evaluate the answers or any specific knowledge the participants apply to solve the problem or task. For example, in computer-based training, participant’s actions could be planned and measured during the training session and in instructor-based training, the training coordinator could change the evaluation plan according to the quality of the questions asked.

6.2.2 The degree of achievement

The degree of achievement depends upon the user’s regular work habit. Instead of conducting an assessment in class, the user behaviour, which directly influences the organisation’s ambition, could be assessed. The degree of achievement obtained could be
established by setting up a scale, such as to pass the test participants should score six out of ten. In some organisations, there would be no scale, meaning participants must pass all the questions in the test. The quality of the training and awareness session, the objective of the training session, and the organisational expectations determine the level of success measures. In performance planning, if the degree of achievement is not mentioned, then it would be difficult to measure the participant’s achievement and learning process as well.

6.3 Measuring procedures

There are four types of measuring procedures to evaluate the effectiveness of the program and participants.

6.3.1 First test (measuring the participant’s knowledge)

Measuring the participant’s knowledge can be done by conducting an end-of-session test. The questions in this type of test rely on the participant’s satisfaction about how they experienced the session, the training and awareness delivery method, whether the content was helpful or not. The questions also include whether participants were comfortable with the training coordinator and the way they presented the training materials, and if the training session met their expectations, and where the participant’s responses ranked on the scale of very poor to excellent. This test does not provide detailed analysis of the participant’s response data, but gives quick suggestions and comments from the participant’s point of view (Sethi, 2013). Some of the demographic data are gathered during or at the end of the session, but participant satisfaction and expectations are measured only after the training and awareness session. The measurement process also depends on the participant’s job position and knowledge level. For example, designed training and awareness program’s results presented to managers would be more effective than that offered to security professionals and general users.

6.3.2 Second test (measuring training and learning satisfaction)

This test evaluates the amount of knowledge that has been communicated or delivered from the training session to the participants. The testing process varies according to the level of the training. For example, in basic training a multiple-choice test or fill in the blanks could be deployed before and after the training. For intermediate and advanced levels, the training session should be focused more on a behavioural test, such as scenario-based, natural based or case study, and the testing procedure must be related to the performance planning of the learning process and highlighting the training materials presented during the session(Sethi, 2013). Performance planning also gives more constructive and immediate responses and advice compared to the end-of-session test. The performance-planning test also evaluates the amount of knowledge gained by participants during the training session, and further evaluation could be applied during the middle of the session at the end of a section rather than testing at the end of the session. For example, if the training session is about the different types of IS attacks in organisations, the training coordinator could
implement the performance-planning test after the completion of the training and awareness session on social engineering attacks instead of waiting for the whole session to be completed. In other words, a performance-planning test evaluates the effectiveness of the teaching and learning process because it assesses how successfully the content is communicated or delivered to participants. The training coordinator could then decide on how the participants are learning (either they need revision of the session one more time, or need the same training and awareness via the alternative methods). Sometimes it is challenging to evaluate performance-planning tests because some participants are already familiar with the training and awareness content and materials before the session, which means the session has a minimal effect on those participants. Therefore, training and awareness materials and content should be designed according to the participant’s educational background as well. Sometimes there is a time gap between training and awareness sessions and evaluation procedures, which provides a challenge in deciding what the training was about and when the session occurred (Botha, 2011). So, to determine the satisfaction of the learning and learning process, additional methods of initial testing procedures could be implemented before training, and the final testing procedure executed afterwards.

6.3.3 Third test (measuring participant behaviour)
Measuring participant behaviour is often challenging and cannot be gained by one test only (Sethi, 2013). Multiple tests during a specified interval of time after deploying the training and awareness program are required. For example, in the research process for this thesis, three surveys were implemented in the specified time interval. After the training and awareness program, two surveys were conducted to measure the participant’s behaviour. The first was immediately after the training, and the second after four to five months. It is often challenging to measure progress of the participants in that time interval because some participants may have left the organisation, some may have been promoted, and some may have transferred to another department or location.

6.3.4 Fourth test (measuring the training and awareness program)
Kruger and Kearney (2006) emphasise the significance of the security program by providing the reason why measurement is essential. When an organisation employs an IS training and awareness program it does not certify that all of its users are aware of ISP and applying them in their workplace. So, to get the maximum benefit of the employed security program, there is a need for a proper method for its measurement. The measurement process is useful when there are the right people to measure at the right time and using the right metrics (Sethi, 2013). Three key attributes need to be explained to measure the effectiveness of the training and awareness program: what needs to be measured, how to measure, and when to measure. Before describing the attributes, this thesis proposes a theoretical framework for measuring the effectiveness of the training and awareness program which is illustrated in the next section.
6.4 Framework for measuring the training and awareness program

The proposed framework in Figure 6.4 explains the entire process for measuring the effectiveness of the security program. But before measurement, it is essential to know what factors need to be measured. In the top left corner, some of the attributes essential for an organisational IS program are listed, and each attribute is explained below.
Figure 6.4: Theoretical framework for measuring the efficiency of an information security program

Information security program
- Risk Management
- Security policy
- Training and awareness program
- Monitoring and continuation

No (Update program)

Yes (Satisfied Program)

Review and Analysis

Assessment & analysis

Measuring Attributes
- Knowledge
- Attitude
- Behaviour

Measuring process

Basic Measurement
- User’s knowledge on organizational security
- User’s knowledge on common attack types
- User’s knowledge on organizational security policy

Advanced Measurement
- Outsourcing security performance
- Overall Organizational security performance
- Organizational security and business performance
- Organizational security process
- User’s behaviour
- Other factors
- Management knowledge and attitude to security

Security metrics and measures

Information security behavioural change
Information security awareness performance change
6.4.1 Information security program

IGI Global (2018) defines an IS program as a public collection of ISP, parameters, and benchmarks employed to give shape to a successful IS management system. An IS program is designed to protect the attributes of IS through sets of rules and regulations. IS varies from one organisation to another, and depends on the requirements of management. Every user in an organisation, from managers to general users, are liable for making sure they act according to the IS program’s attributes, such as security policy and organisational risk management, and the IS program is aligned with organisational business processes (Canavan & Diver, 2006). ISP should be written in simple, logical and understandable language so that users can understand it; if the policy is unclear and confusing to comprehend, users do not follow it. Lack of clarity is one of the most important reasons for users not supporting ISP. If the security policy is not well-written and does not include the some of the critical topics, then it should be revised and updated. Sometimes organisations implement a policy written 10 years previously. In that case, the policy should be updated and changed, and if new issues or challenges arise that could affect organisational IS, then the policy must include those issues and problems. Many organisations have an IS program that consists of organisational law, rules and regulations, standards, and practice (Akamai, 2018). This thesis describes the attributes that are involved in creating the IS training and awareness program are described. This training and awareness program intends to give information and knowledge about an organisational IS program and its attributes so that users are more aware of the organisational IS program, which ultimately improves and strengthens IS. The attributes in IS are many, but only those attributes that are related to the training and awareness program are discussed here (Behm, 2003).

Risk management

A risk is defined as the possible harm that comes from the existing system and unexpected events. Regarding IS, the risk is the danger that occurs within the system or from an external force that does unintended harm to the information system. Risk management is the procedure for identifying, knowing, and then reacting to the issues that could affect the three pillars of the information system: confidentiality, integrity and availability. The risk could be measured only after knowing the potential threats and vulnerabilities, and deciding on the probability and effect of every risk (Caballero, 2014). Before discussing risk measurement, it is essential to know what the threats and vulnerabilities are and how to identify them. Threat is defined as the possibility of harm that can be sourced to particular weaknesses in the system. Threat source is the planned method of intentional abuse of the weakness. In some circumstances, some procedures accidentally or unintentionally fire up the weakness. Threats are not dangerous unless activation of the threat source follows. Therefore, it is essential to identify the threat source during the risk-management process, and each threat source must be considered according to the possibility of its occurrence and the potential harm it could cause. Possible threats regarding IS include, but are not limited to, human threats (such as intentional and intentional harm to the information system),
natural threats (such as flood, fire, earthquakes and hurricanes), environmental threats (such as pollution and chemicals), and terrorist threats (such as intentional harm to the information for targeted motives which could lead society to fear and terror).

Figure 6.4.1a illustrates the identified threats in the context of IS. The vulnerability is defined as the error or defect within the IS system which could be used to breach and violate the information system. The failure in the information system comes not only from the technical side, but also from the person who is operating the information system (Kebbel-Wyen, 2014). The design phase of security policy identifies and defines the vulnerabilities of IS, and the identification process involves network scanning, ethical hacking and vulnerabilities testing.

**Figure 6.4.1a: Identified information security threats**

IS risk management is the procedure of maintaining the organisational IS system from possible harm (Elky, 2006). Including the risk-management approach in the IS training and awareness program strengthens the security program because it describes the risk process and mitigating strategy. Some of the mitigating risk strategies are discussed below.

**Risk acceptance:** Risk acceptance is the procedure of accepting the known risk to continue the business and information system. The classification of risk is according to importance, cost and potential damage the risk can cause. Managers are often involved in accepting the risks, and distribute the risk according to their field. For example, distributing the risk that is related to IS to security professionals means that IS professionals are accepting the risk so that they could generate a mitigating strategy for the accepted risk.

**Risk mitigation:** The risk-mitigation process in risk management is also known as the strategy or policy for managing the risks. After identifying and accepting the risk, the next
procedure is to combat or organise management of the risk and deploy some preventive techniques to minimise the possibility of damage that risk can cause.

**Risk avoidance:** Risk avoidance is the procedure of evading the weak and suspicious area of the organisational information system. For example, in the biometric authentication system, if the organisation found that the biometrics devices are fooled, then there is a risk of stealing user data and information, so the organisation could implement another access method such as a password to avoid the risk caused by the biometric system.

**Risk transference:** Transferring the risk is a procedure where a third party is interested in taking the risk of the organisation. Insurance is one example of moving the risk. In the context of organisational IS, it entails outsourcing the IS products to a concerned third party that is more experienced in handling IS risks and issues. This chapter also discuss the impact of outsourcing in IS training and awareness programs. It should be kept in mind that risk transference does not minimise the possibility of patching up the errors, but it does protect the organisation from entire breakdown.

Proper education, training and awareness can assist users in knowing how IS risks could affect the organisation and what necessary actions could be employed in mitigating those risks. In many organisations during the risk-management process, management concentrates more on deploying the new technology instead of addressing the end users. Some general IS mistakes by end users are an insecure password (such as date of birth, name and address, and some familiar names that could be easily guessed by friends and colleagues), checking the emails and profiles of social media in the organisation’s devices (such as opening a spam email on an organisation’s computer), as well as other things that users may think of as unnecessary. These unnecessary things could be necessary for intruders, who can collect this information, and along with the intruder’s skills can be enough to attack the organisation. Therefore, employing an effective IS training and awareness program could reduce the time and money consumed while responding to security issues and challenges, which can result in a one-fourth saving on the organisation’s manufacturing and production costs (Hamm, 2009).

Security is not a standalone job, but is the responsibility of all users. When risk is involved, therefore, all three attributes—people, process and technology—also need to be involved. Without providing any awareness and training on IS to users, it would be impractical to expect that they could handle the challenges and IS issues. So, during the designing phase of the IS training and awareness program, organisations should focus on risk-management modes, such as incident response and reaction, and categorising and safeguarding intellectual property. The designing phase also includes educating end users about the significance of the security program; avoiding unsafe transmission networks; being aware of common types of security attacks, and backup and recovery; addressing system performance; and complying with IS prevention requirements and business strategy with compliance standards. IS resources need to be safeguarded at all levels from bottom to top,
and users should receive the essential knowledge about ISP and security risks. These days, security professionals should always address IS incidents and discuss them with employees during monthly meetings. This kind of practical approach encourages and motivates users towards a risk-management plan and strategy, which is the way to minimise the allocated budget and time, and endorse IS at all levels (Hamm, 2009).

**Business contingency plan**

The business contingency plan is employed straight after identifying the threats and risks. It is known as a corresponding method that includes the plan, process and practical procedures that allow the rescue and retrieval of information processes during an emergency (Caballero, 2014). A contingency plan normally involves responding, continuity, recovering and restoring the business. An IT contingency plan signifies the full range of actions that are planned to support and regain the significant IS resources during the emergency (CDC Unified Process, 2008). The contingency plan suits the emergency situation, which involves continuity and regaining organisational business processes.

Organisations could implement a preparation plan for response, continuity and backup, and recovery actions to combat the interruption actions that influence the organisational IS and business process (Connecticut Interlocal Risk Management Agency, 2011). Since there is an intrinsic relationship between organisational business procedures and information systems, there is a need for a similar contingency plan to make sure that the recovery plan and back up resources do not work against each other.

There is no single description of a contingency plan that fits all organisations (Qayoumi, 2010). The contingency plan differs from one organisation to another and the resources that one organisation implements may not be suitable or fit for another organisation. The reason for this difference is due to identified risk in the risk-management plan, and the contingency plan relies on the identified risk (Gregg, 2009). Therefore, the contingency plan is directly attached to the outcomes of risk management and its reduction procedure (Swanson, Wohl, Pope, Grance, Hash, & Thomas, 2002). There are various plans for contingency, but three plans are widely accepted and used in many organisations. They are commonly known as incident response plan, business continuity plan, and disaster recovery plan, and are briefly described below.

**Incident response plan:** The incident response plan acts as first aid during the emergency. It determines the process to address the IS attack in an organisation. It is one central critical aspect that needs to be included in the IS training and awareness program because a well-trained user can handle the situation professionally by responding and reporting to seniors compared to an untrained user who tries to respond to the situation without proper knowledge, thereby allowing more time for attackers to do more damage. These incident response procedures should be designed to provide IS professionals with procedures for identifying, responding and reporting processes, and finally recovering from IS incidents.
**Business continuity plan:** The business continuity plan ensures organisational businesses process can continue during and after an IS incident and interruption (Caballero, 2014). The IS professionals and managers are liable for the continuity of the business process because they have the necessary skills and knowledge to manage them during security attacks. In some conditions, the business continuity plan does not solve the entire problem for the organisational business procedure to continue. In that case, the business continuity plan acts as a temporary solution for the continuity of the business.

**Disaster recovery plan:** The disaster recovery plan focuses on destructive incidents that decline right of entry to the IS system for a specified time interval. Additionally, the disaster recovery plan addresses an alternative to the re-establishment of the infected system. For example, backup and recovery of the information system allows the smooth running of the business even after security attacks in the system, which sometimes could go beyond the contingency plan (Swanson, et al., 2002).

**Information security policy and procedure**

ISP is a formal and well-written document about the rules and regulations of organisational IS and the guidelines to follow those rules. In other words, ISP is the constitution of the organisation. It sets instructions on how to safeguard organisational data and information, what processes need to be followed in the workplace, and what will happen if users do not comply with the rules and regulations. Additionally, ISP describes the organisation’s view on safeguarding the organisational resources, business data and processes, customers and its own user data and information from misuse, unsanctioned conversion, and unofficial release. ISP consists of three attributes: policy, procedure and practices. The policy is the formal document that sets the direction for the organisation. Standards provide the benchmark for the policy, which represents that policy needs specific standards for compliance. Procedures are the proposed set of rules and regulations that manage the policy and standards. There is a need for particular methods during policy development and setting up the minimum standard. Practices are the detailed explanation about actions that are taken to reach the targeted goal by setting up the policy, procedure and guidelines (Qayoumi, 2010). There are many kinds of ISP, depending on importance and priorities, but organisations need to include all the policy in their organisational ISP. For example, policy and procedures for password protection, sensitive information handling, access control, information disclosure, IS attack and response, user awareness and training, and monitoring and compliance. Management must enforce ISP and ensure that its users are aware of all procedures. However, users do not need to know and understand all the policies of organisations, and only need to know those related to their role and position. For example, general users in organisations should know the basic policy of IS rather than knowing about technology policy. Security policy could be five pages, or maybe 5,000 pages, and more pages do not signify that the organisation is safe unless it has conveyed the policy to its users.
It is the responsibility of the organisation to not only teach but also to ensure that users know and apply the ISP in their work. Many participants in the survey in this research responded that they did not have any formal ISP in their organisation, and some answered that they have, but management did not communicate it. The ignorance of management in teaching and delivering ISP to end users leaves their organisation vulnerable to attack. So in the IS training and awareness program, end users are informed more about ISP rather than responding to incidents. ISP teaches users how to do the job safely and securely by complying with the organisational ISP. Unaware users in the organisation mean that there is a massive possibility of IS being violated from accidental or unintentional mistakes of the user, or being violated by external forces.

**Information security education training and awareness program**

Many researchers have their view of defining the information security education training and awareness program, but in general, it is an educational, training and awareness program that is designed to make people aware of organisational IS. It does not teach employees how to do their job, but it does explain to employees how to do their job safely and securely (Hight, 2005). The purpose of an IS education training and awareness program is to make sure that users are aware of the risk factors they are facing, and how to handle those risks initially. Implementing the program in an organisation means employees can recognise the possible threats and vulnerabilities, problems and affairs that are still functioning in the workplace. The program explains to employees how they can safeguard the organisation’s resources and the necessary steps to inhibit IS infringement. The goal of the program is to create positive changes in employee attitude and performance. A practical IS education training and awareness program justifies the rules and regulations for use of the organisation’s IT system. An effective IS education training and awareness program starts with an attempt that can be applied and executed in different modes and experienced in every department and every level, from general employees to senior managers. The program is beneficial when the resources used in the program act according to the organisation’s ISP. When the policy is written clearly and briefly, the developed resources rely on it according to the organisation’s processes (Wilson & Hash, 2003). The program consists of three attributes that are discussed briefly: security education; security training and security awareness, and illustrated in Figure 6.4.1b.

![Figure 6.4.1b: Information security program](image-url)
NIST defines IS security education as education that incorporates each security proficiency and experiences of the multi-operative area in the general categorisation of knowledge. It also combines the study of multiple subjects in the field of theory, principles and challenges, and attempts to create IS professionals who are competent in predicting and positive in reacting (Wilson & Hash, 2003). Security education is a formal educational course that is delivered by educational institutes and universities. Security education aims to increase user knowledge about IS and qualify them in the field of IS. In some cases, training acts converse to education. Some institutions provide IS courses consisting of four to six units or more, and students are awarded a certificate after finishing the course. Some of the designed subjects are delivered in conjunction with educational providers and IS merchants who highlight more training features rather than education. Therefore, IS professionals need to analyse both programs, IS training and IS education, and come to a decision about which one suits organisational needs (Goucher, 2009).

NIST defines IS training as a learning process that attempts to create appropriate and required IS proficiency and aptitude in an operating department rather than the IT department (Wilson & Hash, 2003). It is not apparent that the training program should be similar to the degree or certificate provided by educational providers, but the training syllabus might include a certain percentage of material which is identical to the educational provider’s curriculum. A security training program is a short course designed to train users about IS according to the necessity of the organisation. In many organisations, IS training is conducted during the induction session when employees join the organisation. For instance, training about the IS program for system administrators or system analysts could be an in-depth explanation of technical control (which includes authentication and access control, auditing and follow-up reporting, and protecting the information from third parties). For managers, the training content should relate to management control (which provides for implementing policy and procedures, risk management, IS life cycle and monitoring the IS management program). And for the functional departments, the training content should include operational control (which include issues and challenges, disaster recovery planning, IS training and awareness, physical and logical security, monitoring and maintenance, and changes happening at the workplace). Security training is also an educational program, but it is distinct from security education. Security training is different to security awareness because security training aims to educate the user in such a way that they can proficiently accomplish the given task, while security awareness seeks to concentrate on user interest in one issue or many issues. The knowledge and credentials gained throughout the training period and awareness developed during the session must focus on the essential security and learning materials.

NIST defines security awareness as a program that is designed to change the performance and attitude of the users and implement an excellent IS system (Wilson & Hash, 2003). Security awareness aims to concentrate on awareness of IS through awareness presentations. An awareness presentation is planned so users understand IS issues and
reacts appropriately. Awareness targets general participants with interesting and productive methods. For instance, an awareness program on social engineering should describe what social engineering is, what happens when you are affected by a social engineering attack, how you can prevent social engineering attacks, and how you should report if you experience or are suspicious about social engineering attacks.

Security awareness is different from security training (Veseli, 2011). In a security awareness program, users receive information that is designed to change behaviour. In a security training program, users not only get the information, they also have to show that they are proficient in the knowledge and skills they learned during the training session through a skills test or examination (Albrechtsen & Hovden, 2010). Security training reflects a formal program with the intention of gaining knowledge to be more competent in carrying out work. The intermediate stage between security awareness and security training is composed of IS principles and knowledge. When organisations implement a security training and awareness program, the IS principles and knowledge form the active awareness program, which is the basis for the training program. Sometimes jokes and comedy on security awareness could be designed to make users aware of ISP. Security awareness is often achieved through writing the message on community notice boards, posters, flyers, coffee cups, pens, screensaver, mouse pad or desk that users frequently see (Merete Hagen et al., 2011).

**Monitoring and continuation**

An IS training and awareness program would be useless without continuity of the program and monitoring of its effectiveness. Since IS is a never-ending process, there is a need for continuation of the program. The survey results in the research for this thesis verified that when participants are surveyed four to five months after training, their performance level decreases. If the same practice continues, the result of participant’s performance levels will gradually reduce to be the same as in the first survey. In most cases, after the second survey, organisations ignored the training program and failed to monitor whether it was proficient in changing the user’s behaviour or not.

Monitoring does not only mean monitoring the users, but also other factors related to the training and awareness program, such as security policy, training and awareness resources and materials, and delivery methods. Continuing the training and awareness program can be a quick catch up to ensure that users have not forgotten the program and are complying with it. Continuation does not mean that it should be executed every month or every quarter, but needs to be executed when organisational management thinks it is the right time to continue, or possibly regularly, such as biannually. After continuing the training and awareness program, the program’s effectiveness needs to be monitored according to organisational policy. When the results of the monitoring process are available, it is easier for security professionals to determine the issues and further the remedial steps for the follow-up (Wilson & Hash, 2003).
6.4.2 Measuring information security program attributes

Three attributes need consideration when measuring the effectiveness of the security program: knowledge, attitude and behaviour (Security Awareness: Measuring Attitudes, Knowledge, 2008). Knowledge represents how users understand and look at organisational IS (Essays, UK, 2015a). Before implementing any IS program, it is necessary to measure what users know and think about the components of an IS program. Attitude represents the user’s way of thinking about organisational IS and how they approach IS. Behaviour represents how the user’s actions or activities affect the organisation’s IS, either knowingly or unknowingly (Kaur & Mustafa, 2013). Figure 6.4.2a illustrates how all three attributes are directly related to the organisation’s ISA. These attributes are measured using three components; what to measure, how to measure and when to measure.

![Diagram of attributes of an information security program: knowledge, attitude, and awareness](image)

**What to measure**

The first component, *what to measure*, measures the user’s knowledge (what knowledge users already know or awareness of IS), attitude (what user’s thoughts are about IS), and behaviour (what instructions users need to follow while conducting the organisation’s tasks). In the context of this thesis, this component also identifies the needs of the training and awareness program, and the content included during the building process is explained here. What to measure is further categorised into the following sections:

- organisational IS policy and procedures
- risk management
- business contingency plan
- monitoring and compliance.

Kruger and Kearney (2006) developed a model where they structured the issues in a tree format to measure the effectiveness of an IS training and awareness program. They assigned categories and sub-categories to the problems in particular sections of the tree according to
their significant values. They further sub-categorised these four categories according to their importance. For example, information policy on handling sensitive information was further sub-categorised according to the significance and weight of the information, such as confidential information and highly confidential information. These sub-categorised sections further divided into level of confidentiality and access control authority to handle that information (Veseli, 2011).

In this research, the IS program established what users know about organisational ISP, what the user’s role is in identifying and mitigating the organisation’s IS risks and threats, and how to respond and comply during IS attacks in the organisation. The first question relates to the user’s knowledge and understanding of organisational ISP. The response to this question assists the security program coordinator in identifying the reason, such as why security policy is not handy to all users; whether it is ignorance from the management team or that users are not interested in knowing ISP because some users might think it is for managers and supervisors. The second question is related to IS threats and risks. The response to this question assists in identifying the threats and risks that an organisation is currently experiencing and potential risks that may arise soon. An IS training and awareness program coordinator could include those threats and risks in a security program to make its users aware. The third question is related to business continuity during an emergency. The response to this question assists the program coordinator to know what users could do to respond during an emergency situation; whether users would report it to their senior managers, or defend, or let it go (Gross & Rosson, 2007).

**How to measure**

The second component represents how to measure the IS program and user behaviour. There are various methods to measure the user’s response, such as interview, survey and case study questions. But it should be kept in mind that one survey response does not reflect user behaviour and the scale do not necessarily determine that the user is proficient or weak in IS. Additionally, users does not want to show their weakness in front of others and could lie in their response about their behaviour, and some users get help from their co-workers in completing the answer sheet. Some users could tell the truth, some lie, and some pretend and tell different stories about their behaviour. The mixture of all kinds of users makes the measuring process interesting and productive because the result could be useful in determining the actual action of the users. User behaviour can be measured by survey, interview, group discussion, and scenario-based questions and answers. One of the practical ways to measure user behaviour is to ask the next user who is a co-worker and works closely to another user, but in some cases, it is unethical to inquire about other users’ behaviour with the help of co-workers.

Figure 6.4.2b includes sample measurement questions.
When to measure

The famous saying for getting the desired result is, the right thing needs to be done in the right way and in the right time. While measuring user behaviour, the survey should be conducted in a certain interval of time after the training and awareness program, and again the next survey should be performed after a specified time interval. The reason for this kind of practice is that if the end-of-session test is conducted immediately after the training and awareness program, then it is evident that the user’s results and score could be pretty good. But it does not signify that users could implement the knowledge and skills that are gained in their actual job. The real measurement of user behaviour should be conducted when users employ the knowledge and skills they learned from the training and awareness program in their workplace (Kruger & Kearney, 2006). The time interval should be allocated in such a way that it is not too soon or too late for the training and awareness program to be repeated (Chant, 2017). For example, conducting the training and awareness program every month would be too soon and users could be annoyed or might skip the program, and every year could be too late to catch up with the program. Another way to keep users refreshed and updated with the training and awareness content is to implement a quick refresher program (a group discussion or short awareness program on a few chosen topics) quarterly and a formal training and awareness program every year. This practice ensures that users do not forget the content of the program and perform according to the organisational ISP (Veseli, 2011).

Figure 6.4.2b: Sample question to measure knowledge, attitude and behaviour

<table>
<thead>
<tr>
<th>Question related to measure the knowledge of user</th>
<th>Information security policy is a written document which sets the rules and regulations of the organization and every user must comply with the organization’s information security policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ I agree</td>
<td>□ I disagree</td>
</tr>
<tr>
<td>□ I disagree</td>
<td>□ Don’t know</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question related to measure the attitude of user</th>
<th>Organization information security is responsibility of all users because it is not a technical issue anymore but is now a business issue.</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ I agree</td>
<td>□ I disagree</td>
</tr>
<tr>
<td>□ I disagree</td>
<td>□ Don’t know</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question related to measure the behaviour of user</th>
<th>Before I leave the office, I shut down the computer properly, clean up the desk, shred up the unwanted documents and remove any stick notes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ I agree</td>
<td>□ I disagree</td>
</tr>
<tr>
<td>□ I disagree</td>
<td>□ Don’t know</td>
</tr>
</tbody>
</table>
Security metrics and measurement

There is no clear-cut or exact description of security metrics, but in most cases, security metrics vary according to their nature and how they are executed to get the desired results (Wright, 2006). In this research, security metrics measure the performance of users, the training and awareness program, and the IS program; detect user knowledge, attitude and behaviour about IS; and provide outcomes that are realistic in decision-making (Rathbun, 2009). Online surveys execute security metrics which does both jobs: first, it collects the data from the users and second, its computerised code helps to generate numeric and statistical data which is handy and practical in the decision-making process. Nowadays there is various software available in the market and online mainly designed for processing survey data.

Basic measures of effectiveness of user performance

In the IT world, basic measures refer to the process or method of protecting organisational assets and information. The essential knowledge or information that should be known by all users about organisational IS is basic knowledge, and measurement of basic knowledge is known as basic measures. In this research, basic measures are defined as measuring the user’s primary understanding of IS. The basic knowledge includes the ISP, risk management, user roles and responsibility in protecting the organisation’s assets, incident response and handling, the organisation’s physical and digital protection, access control, organisational mission, and the training and awareness program. It would be difficult to know to what extent users know the necessary information about organisation security unless measured. The measures give management the information to decide whether users are fully aware of organisational IS or not. The reason behind this is that fully aware general users are the first line of defence for organisations. In basic measures, user knowledge of organisational security including security policy and common attacks that organisation experiences are described below.

User’s knowledge of organisational IS: Management should provide all the necessary information to every user about the organisation’s IS. The required information includes the technology they are using to protect the organisation’s resources and physical security, the organisation’s ISP, access control, users’ rights and obligations, how user error could jeopardise the organisation, and what would happen if not complying with the organisation’s rules and regulations. In some organisations, basic information is provided only during the training and induction session while appointing new users. The purpose of measuring the user’s basic knowledge on organisational IS is to determine whether users are aware of their roles and responsibilities, are complying with the organisation’s security policy, or need additional training to boost their knowledge.

User’s knowledge of common attack types: The IS training and awareness program coordinator should focus on IS attacks both internal and external that an organisation is
experiencing. For example, general users could experience social engineering and phishing attacks, and technical users could experience virus attacks, script kiddies and denial-of-service attacks. The intention of measuring user knowledge in common attack types is to determine how familiar users are with those attacks and how they are responding; either reporting to managers or just letting it go. Additionally, organisations would know how user error and negligence could make organisational resources vulnerable to attack so that management could implement the training and awareness program to make users aware of attacks.

**User’s knowledge of organisational information security policy:** The IS training and awareness program intends making the user aware of organisational ISP. ISP guides users and organisations in the right direction by making them aware of their roles and responsibilities and also reflecting on how their security behaviour affects organisational IS processes. Most organisations should have an ISP, but sometimes only make it accessible to managers and security professionals. In Australia, many small and medium-sized businesses do not have an ISP, and if they do, it is not accessible to all users. The reason behind this is that many medium-sized businesses outsource IT services from security agencies and the policy is only communicated between outsourced agencies and the organisation’s managers. The impact of outsourcing is discussed later in this chapter. In large and multinational organisations, ISP exists because they have an IT department and the CIO is responsible for creating ISP and also the training and awareness program in a timely way. In IS training and awareness programs, users are taught about the security policy. The purpose of measuring user knowledge about the organisation’s security policy is to check whether users are aware of organisational ISP or not, and also to monitor whether user activities comply.

The reason behind measuring user knowledge is to ensure that users understand the necessary security requirements, and how their one small mistake could have a massive impact on the organisation’s IS system. It also makes users aware of ISP and how to get access and implement it in their workplace. Another reason for this measure is that management should encourage and motivate their users in teaching the policy, and ensure that they understand and apply it in the workplace. Explaining ISP could be through training either in the classroom or online and providing notes.

### 6.4.3 Advanced measures of efficiency of training and awareness program

Advanced measurement applies to managers and IS professionals because their training program includes high-level knowledge and skills about IS, and it is often considered a complicated task. There is a need for follow-up survey measures and results need comparison with all participants’ survey results. Training effectiveness is determined by participant behaviour, and as explained earlier, it is difficult to measure participant reaction. Advanced measures include management knowledge and attitude towards IS, user behaviour, organisational security processes, business and security performance, overall
organisational performance, the effect of outsourcing, and other factors that are essential for the success of training and awareness programs.

Management knowledge and attitude towards IS

The result of the first survey showed that management was not aware of how IS affects business processes because they believed that IS was related to the IT department while management deals with the organisation’s business processes. After the training and awareness program, managers were aware of how IS helps in managing the organisation’s business processes and what would happen to the organisation’s business data and information when compromised. Management changed their attitude: IS is now no more a technical issue, it is now a security issue. This kind of positive change from management encourages and motivates other users to change their attitude because management acts as a role model. When management is aware of, and understands, IS, they can focus on those areas that need more attention (McElroy & Weakland, 2013).

The survey question that best defines management knowledge and attitude towards IS is: How could management improve the IS systems in their organisation?

The participants responded that management should encourage end users to share their opinions freely, consult with end users about the challenges and issues they are experiencing, and should make end users aware of the organisation’s ISP.

User behaviour

User behaviour is often challenging to evaluate, and one survey result does not determine the user’s expression of all behaviour. There is a need for additional follow-up training and other methods such as problem-solving skills to measure user behaviour because in an advanced-level evaluation process a survey would be not practical. The content of the training should also be related to changing behaviour activities. The training coordinator should be proficient in communicating and delivering the message to participants because user behaviour also depends on how the training coordinator conveys the messages. Sometimes users need to undertake the training program for a second time if they have not understood the training content. Also, if the training coordinator did not explain the training content adequately, the training program could not change user behaviour. To measure the user’s response, the training coordinator could send a phishing email after the training program to find out how the user responds to that email: whether the user opens the email, reports to the manager or supervisor, or does not open the email. Some other real-time case scenarios related to the training content could be given to the participants after the training program to check how users understand and respond. If user behaviour is unintentional, then the training coordinator should explain that their reaction is incorrect and teach them the correct procedures. But if the user is intentionally reacting incorrectly, it should be reported to the manager, who should find out the reason why the user is intentionally damaging the organisation’s IS before punishing them.
Organisational security processes

The IS process needs periodic evaluation, and the evaluation process includes ISP (Kanungo, 2006). IS changes over time and so does the IS process (Weishäupl et al., 2015). The IS training program for security professionals should include emerging threats to IS processes. Measuring the security process of an organisation gives the current status and how security professionals are responsible for the securing IS processes. The security processes measure the number of IS incidents before and after the training program. Also, they assist security professionals to determine whether the security training program has a positive influence on organisational security process or not (Steinklauber, 2003).

Organisational security and business performance

Organisational business performance refers to the continuous operation of the organisation’s business processes without any delays and without compromising its data and information. Trained users are the reason for successful business processes because they know more about IS risks and threats. And also educated users could identify the potential harm it could do to the business and how IS processes and business processes are directly proportional to each other (Jakoubi, Tjoa, Goluch, & Kitzler, 2009). Measuring security and business performance assists management and security professions to be aware of how IS processes could help safeguard the organisation’s business processes and how to include organisational business processes into the organisation’s IS risk management (Jakoubi, Tjoa, Goluch, & Quirchmayr, 2009).

Overall organisational security performance

Measuring overall performance means measuring the performance of IS processes, because security processes safeguard the organisation’s business processes and success, economic value, and its position in the market (Melville et al., 2004). Overall organisational performance relates to how security processes have influence on an organisation’s business performance. Measuring the entire operation makes it easier to reflect on current security performance and business performance, and how security performance has a significant impact on organisational business performance (Weishäupl, Yasasin, & Schryen, 2015).

Outsourcing security performance

Outsourcing refers to getting the products and services from a third party. Outsourcing the IS training and awareness program could be beneficial because outsourcing agencies are highly proficient and expert. Measuring the performance of outsourcing assists managers and security professionals develop the benchmark for performance and identify user satisfaction using performance metrics (Technology and Business Integrator, 2017) (Axelrod, 2005). In outsourcing procedures, most organisations implement an outsourced training and awareness program once, and they do not have any follow-up plan to keep users updated. All communication goes between management and outsourcing agencies, and end users are
isolated because the training and awareness program depends on management’s needs (Overby, 2007).

Other factors

The human aspects of the IS have been discussed and measured, but there are other factors also responsible for the effectiveness of the IS training and awareness program. Many researchers only consider humans and how their behaviour affects the effectiveness of training and awareness programs, but they have not thought that there are other factors which have a high impact on humans and changing their behaviour. The other elements which have a significant effect on information training and awareness programs follow.

User interest in security training and awareness program: It is well known that every user is different and their interest in IS training and awareness program is the one critical factor that needs consideration. The user’s job role and educational background should be identified before measuring because if the training content is already known, or users are already familiar, then users may not be interested in undertaking the training program. The training delivery method also influences user participation. For example, in most organisations, only one training and awareness program methodology is employed, and management compels every user to undertake it. This kind of practice does not give any valid output because through fear of losing their job, users could award an excellent score at the end of the session even though they did not understand the content (Chew, Swanson, Stine, Bartol, Brown, & Robinson, 2008). Additionally, they might get help from their colleagues, and sometimes colleagues could do their training program, including the test, if a computer-based method is used. In this way, users are happy, which makes the training coordinator pleased and finally, the excellent score makes the organisation blissful; this kind of practice is still executed in many small and medium-sized Australian organisations.

Some users feel shy expressing their ideas in front of people, and they are not interested in taking part in a training and awareness program. The training coordinator should arrange an alternative method specially designed for those users, and during the planning and development phase the training coordinator should implement multiple modes of delivery, and users could freely select the training method suitable for them. The interest and active participation of managers and security professionals in building and measuring the training and awareness program gives them a feeling of control over the security measures, which measures the effectiveness of the training and awareness program.

Appropriate aims and ambitions of the security training and awareness program: Measuring the objectives of the security training and awareness program identifies and describes the security program’s performance. The IS program’s aims and objectives should reflect the organisation’s mission and strategy and be expressed in the security program’s performance. Appropriate aims and ambitions from the organisation’s strategy should be included in the training and awareness program. The extracted organisational purpose
should adequately fit the training and awareness program and again needs to be reassessed and approved. If the aim of the security program is not clear, then management would not support the program and users would not be interested in participating. The security program coordinator must ensure that the program has a specific target and should explain all the steps on how to achieve that target. Before implementing the training and awareness program, the program coordinator should present the roadmap of the program to managers and security professionals.

**Review of information security policy and procedure:** Measuring the security policy concentrates and motivates organisations on particular security processes. The ISP should include in-depth information on how to use control measures for IS (Chew et al., 2008). Security policy should also describe how to deploy security control measures to gain better IS performance. In some organisations, the changes in implemented technology and the organisation’s mission requires an update of the ISP. The review of ISP should be undertaken not only for the current training and awareness purposes, but also for future programs. For example, measuring and reviewing the security policy allows program coordinators to mark topics of the policy which have already been completed so that other topics could be discussed in a future training and awareness program.

**Review of existing and previous information security programs:** Measuring previous IS programs allows the program coordinator to identify and discuss the previous program’s topics, the success factor of the program, the program’s achievement towards the desired target, and the program’s plan for change. If the security program coordinator reviews a previous program and finds that the implemented method was ineffective, then an alternative approach could be applied (Chew et al., 2008). As technology changes, there are changes in security controls and methods of evaluation as well. An alternative way of delivering and communicating the training and awareness content could be applied, measuring current and previous programs. The IS program should also be reviewed as the organisation’s business processes change the security performance of organisations. While implementing new resources, such as training topics, delivery methods and evaluation methods in the security program, they should be compared with previous programs, as well as weighing them against other organisations that have already implemented those measures.

**Cost of the training and awareness program:** Cost is another factor in determining whether the training and awareness program is effective and likely to be continued. The higher the cost, the more effective the program; in many organisations when the budget is low, training and awareness programs are the first casualties. To implement a training and awareness program is not an easy task and requires enormous cost and sometimes there is an extra cost for continuation of the program. The cost of an IS program does not give anotable ROI because its repayment is hidden; it is only determined by measuring the
reduced number of security incidents after the program. Additional funds should be allocated for future programs and for necessary changes in the program.

**Review of training and awareness delivery methodology:** The training and awareness delivery method plays a significant role in the success of the program. Training delivery methods, such as classroom-based, computer-based, group discussion, audio and videos, picture and image descriptions, should be based on participant preference (Kim & Homan, 2012). For example, in classroom-based training participant comfort and refreshments should be considered. To sit in the classroom for long hours and listen to lectures could be boring. Therefore, something exciting should be planned between sessions of the program, such as lectures followed by group discussion, audio-video learning, short breaks and refreshments during the course, and a half-hour break every three to four hours.

**Review of security metrics:** Security metrics should be reviewed on a timely basis because the previously used metrics may not be valid for recent programs (Schroeter, 2014). For example, if the earlier program implemented a manual survey for data collection, then new technology such as SurveyMonkey should be applied to collect the data and give numeric and statistical data. Before implementing the actual training and awareness program, the effectiveness of the program is reviewed through pilot testing (sample testing with a few participants to show managers and security professionals how a training and awareness program works, and the goals and objectives that could be gained before getting final approval for the actual implementation). The latest software that can measure security program effectiveness could be implemented, depending on the allocated budget. Measuring the security metrics ensures that the collected data cannot be modified by the program coordinator or participants, so data reliability and validity are achieved. Measuring the security metrics assists managers and security professionals to see the changes in IS incidents through security audits (Greaux, 2013).

**6.4.4 Review and analysis**

Assessment of the attributes using basic and advanced measurement of the theoretical frameworks is required to review and analyse the security program. The review process, including the assessment reports, and statistical facts and figures, could be implemented either on-site or off-site. The analysis of the reports should be created and published in such a way that is easily understandable and accessible to all users. Usually, security professionals execute the reviewing process in the schedule, but sometimes organisational managers are included, which also assists in decision-making. The reviewing process concludes that either the security program was a success or a failure. If the reviewing process found that the implemented IS program did not achieve the targeted goals and was ineffective, the reviewing team sends the review report with suggestions and feedback so the current program can be updated for future action. The review team could look at the content of the IS program and evaluate it alongside the organisational needs and expectations of the security program. But, if the review found that the IS program was
successful in measuring the effectiveness of the program, there would be a change in the behaviour of users, and there would also be a change in the performance of the IS program.

**Information security behavioural change**

Measuring the behavioural change of users is difficult, but it can be estimated by noting the reduced number of security incidents in an organisation. The increase in knowledge and positive attitude towards IS leads to positive behavioural change, for example, logging off the computer before leaving the office, not sharing the password, attending training programs, and the belief that IS is not only for the organisation but is also for users. Another observation is whether users follow the knowledge and instructions they received during the training and awareness session.

**Information security awareness performance change**

In most of the literature, researchers only focused on changing the performance of users, failing to measure the performance of the security awareness program. Since the IS awareness and training program is a continuous process, if the program is successful in achieving the targeted goals, the program should be reviewed for future issues and challenges for better performance. For example, if the current program focuses on social engineering and phishing attacks, the next program should focus on other types of internal and external security attacks. That is, if the same program is implemented in future, the content should be different from the previous program. Otherwise, participating users get bored because there are no innovative concepts or ideas, and users could skip the program thereby affecting the performance of the program.

**Contribution of proposed research framework**

It is clear from the literature review that while measuring the effectiveness of IS training and awareness program, most researchers only focus on the security-related incidents such as social engineering, password protection and phishing attacks. This research, however, focuses on measuring the effectiveness of an IS training and awareness program differently. This research framework emphasises the importance of ISP in securing organisational IS. This research also draws the attention of organisation management to the need for updating the organisation’s ISP when there is an emergent risk factor in the organisation’s information system. The research framework emphasises the procedure for ongoing monitoring and support for IS programs. Three features need to be considered while designing an IS program—knowledge, attitude and behaviour. The IS program should provide knowledge to end users that encourages a positive attitude regarding the IS and directs behavioural change.

The research framework contributes to measuring the effectiveness of an IS training and awareness program from two different angles—basic measures and advanced measures—which verify the fact that one size does not fit all. The training and awareness program should be different according to the user’s functioning area, and the measuring tools should
also be different. For example, IS training and awareness topics designed for general users could be too easy for IT professionals and would not be useful for them.

While measuring the effectiveness of the IS training and awareness program, the program should not only focus on IT effects on IS, but on how IT affects organisational business processes. For example, if the IS training program is related to the denial-of-service attacks, the training content should not only relate to the technical countermeasures for such attacks but also needs to consider how those kinds of attack affect business processes. The backup policy and business contingency plan, which are the key requirements for business processes, need consideration during the training program.

Several other factors responsible for the training program to be effective are discussed in this research, such as management support and attitude about IS, user’s interest in the IS training program, training delivery methods, and procedures for ongoing support.

Most training programs are designed and measured by behavioural change, rather than educating users about how their irresponsible behaviour jeopardises the organisation’s information system. For example, the training content related to password change should include that the password should be changed every week or every fortnight and a strong password should always be used. The training content also should consider why there is a need for password change, how passwords are made stronger, why passwords should not be shared and written on sticky notes, and how hackers or attackers guess the password.

This research measured the effectiveness of the IS training and awareness program from every angle. The effects were measured through surveys and interviews, user’s experiences about security incidents, numbers of reported incidents, and comparing the efficacy of the existing and previous training programs. These factors all contribute to making this research novel and different.

6.5 Outsourcing the information security program

Outsourcing is defined as the method of contracting or agreement with another company and agencies to execute all the jobs of the organisation’s IS system (Alner, 2006). In other words, it refers to transferring the organisation’s IS risk to third-party agencies that are proficient and have expertise in handling IS solutions. The concept of outsourcing is emerging in most medium-sized Australian organisations. Outsourcing assists organisations implement innovative skills based on innovative technology, which further helps the organisation to concentrate on business activities rather than organisational IS (Colwill, 2006). Outsourcing could be implemented in two ways: onshore or offshore.

Onshore outsourcing is often known as domestic or local outsourcing, where organisations outsource IS solutions to local IS agencies within the country. The reason behind onshore outsourcing is that it gives more guarantees and control because both the organisation and outsourcing agency need to follow the local and national rules and regulations for data and
information protection. Additionally, there would be no issues in communication, a timely delivery process, and risk and fear of losing the data and information are minimal because the outsourcing agencies know the local and national rules and regulations (Buck, 2016).

Offshore outsourcing is often known as global outsourcing because in this process organisations outsource their IT solutions to foreign country companies that are experts in solving problems. The main reason for offshore outsourcing is the cost; it is comparatively cheap (Rowe, 2007). But specific issues and challenges need to be considered before utilising offshore outsourcing. Issues related to offshore outsourcing include ownership and control of the organisation’s data and information, the risk of compromising data and information, and the procedures for data and information protection and disclosure falling under the legislation of the foreign country. Offshore outsourcing is often a difficult task because the variation in time and location requires additional management. Lacity and Rottman (2008) argue that the cost of offshore outsourcing is higher compared to onshore outsourcing. The global recession also pushed many large organisations to offshore outsourcing to save on IT costs.

There is always a significant relationship between outsourcing agencies and organisations because IT and its processes area big concern for management, and they are looking for someone who can look after it so that management can focus on business issues only. Training and educating employees about IS is often costly, and after completing the training and education, there is no guarantee that users remain in the organisation. The change in global IT pushes for additional education and training to implement new technology and is also an additional cost for the organisation. These are some common reasons that force organisations to outsourcing their IT systems.

6.5.1 Is outsourcing friend or foe?

On the friendly side of outsourcing, outsourcing agencies give helpful advice and assure that they handle the organisation’s confidentiality with integrity. They could also provide some examples of how they protect other organisations’ assets and respond when major security incidents occur. The outsourcing agencies could identify the current issues in an organisation’s IS, provide useful advice and solutions, and save organisations time and money. Apart from giving numerous advantages of outsourcing, organisations could be assured that they are getting total IS.

The relationship between organisations and outsourcing agencies depends on how they contract their service levels. On the dark side, sharing organisational data and information could set up more threats and risks compared to an organisation that has data and information on its own network only. Distributing data and information offshore could lead the organisation to potential threats and organisations would be vulnerable to attack (Lacity, Khan, & Willcocks, 2009). For example, the national legislation for protecting data and information in an organisation’s own country could be different to that of outsourcing
countries. Some other factors, such as a change in government and government policy in IS, could affect the outsourcing procedures even though both organisation and outsourcing agency have maintained a service level agreement. The government could not tax offshore outsourcing agencies, which means the organisation could save tax on the IS cost, but there would be some government protocol for the tax system for outsourced products.

6.5.2 Risk of outsourcing the security program
The risk in outsourcing is defined as the possibility of activities that could have a significant impact on an organisation. IS outsourcing focuses on handling the risks by understanding the risks, evaluating and prioritising the risks, and mitigating their effects. While outsourcing the IS program, an organisation should focus on the risks of outsourcing and how to minimise those risks. Bahli and Rivard (2005) conducted experimental studies focusing on particular risks in outsourcing and strategies for managing those risks. Iacovou and Nakatsu’s (2008) studies focused on identifying the risks and risk mitigating strategy related to offshore outsourcing. The most common risks identified by Lacity and Rottman (2008) are poor management, powerless service level agreement, unskilled users, no latest technology and shortage of learning processes. Lacity et al. (2009) agree that before outsourcing an organisational IT system, the organisation needs to be competent in dealing with its IT. In their study, they found that the risks they identified were threatening. Separate research conducted by Lacity and Rottman (2008) focused on a risk-minimising strategy for beginners and professionals, and found that there are specific procedures intended for minimising the risks and enhancing the possibility of outsourcing effectiveness.

6.5.3 Measuring the success of outsourcing
Measurement of an outsourced IS program is determined by the organisation’s strategy (how it affects and determines the outsourcing by measuring the degree of performance) and the role and responsibility of IT (how outsourcing defines IS enhancement). Examples include minimising IS cost and stepping up the degree of service, and other hidden factors (such as outsourcing determined by the allocated funds, the time taken to accomplish the outsourced activity, and quality of the accomplished action). Based on the success factors of outsourcing, researchers have investigated and measured the success of three types of outsourcing IS programs: outsourcing determination, managed by the service level agreement, and similar controls. The outsourcing decision is affected by the quantity of outsourcing, support from management and measuring procedures. The amount of outsourcing is decided by IS costs and the number of IS jobs outsourced. Seddon (2001) introduced the concept of too much, and found that organisations spending more than 80% of their IT cost on outsourcing have a lower success rate compared to organisations paying less than 80%. Management support is another factor indicating success of outsourcing, because participation of management in determining outsourcing resources has a positive influence on the entire success of IS outsourcing. Management participation in contract preparation, reviewing and decision-making helps to maintain the success of the service
level agreement. The corresponding control measures include hidden factors such as trust, information sharing, contract price for IS solutions and requesting bidding or tender costs. To evaluate the control measures, other forms of methodology could be implemented, such as case studies and interviews, because surveys would not be useful in this discipline (Lacity et al., 2009).

Outsourcing business processes means taking over the organisation’s business processes to ensure that the organisation meets business standards in the global market (Davenport, 2005). For example, organisations outsource to human resource agencies to recruit new employees, and to accounting firms for the organisation’s accounts and audits. Business processes in conjunction with IS processes are unique and evolving, with outsourcing having a significant impact because organisations outsource the IS process to help and assist in the organisation’s business processes (Wüllenweber, Beimborn, Weitzel, & König, 2008). Business processes are measured according to standard level, service level agreement, IS cost, quality of the service, and continuous functions (Sullivan, 2004). Tanriverdi, Konana, and Ge (2007) suggest that when there is a secure attachment in business processes and an organisation’s IS processes, onshore outsourcing would be a practical solution compared to offshore outsourcing.

6.5.4 Measuring the effectiveness of outsourcing

Dahlberg and Nyrhinen (2006) implemented an innovative tool for measuring and justifying the effectiveness of outsourcing the IT training and awareness program. The tool is designed to implement multiple surveys, which could be helpful for future research and for IS professionals to establish goals and measure the success of IT outsourcing. The tool evaluates all the benefits of outsourcing, such as technical, economic and social, and combines them with the success factors in the literature, which have been endorsed by professionals. The tool also evaluates the objectives that have been established for outsourcing and attainment of the goals to find out if there is any variation in between the established goals and attained goals. For example, the tool can evaluate the goals of the IT outsourcing service and the goals set by the organisational IT department to establish the difference between the goals of the outsourcing service and the goals of the organisation’s IT department.

Hodosi and Rusu (2013) discuss a critical success factor that assists in measuring the effectiveness of an IT outsourcing program. They suggest that the critical success factor described in the literature on IT outsourcing would not be effective unless there is a critical review is undertaken by the security professionals in the organisation because some success factors might not meet their expectations.

McIvor et.al. (2009) state that while measuring the effectiveness of IT outsourcing, it is essential to analyse and determine factors such as inadequate functioning, the interior and exterior dependency process, identification and measurement of the contract and service
level agreement between two parties, and measuring the tools and equipment that outsourcing service providers implement.

Kadjani (2014) argues that IT outsourcing should be measured on three levels—user, business and total satisfaction—thus proving the significance of the performance of IT outsourcing. IT outsourcing can be measured simply in some of the levels, but in others both parties need to establish the benchmark for measuring effectiveness at the point of setting up the contract. Most outsourcing companies only focus on the outsourcing process and business processes. However, successful outsourcing companies not only emphasise the fulfilment of the contract, they also pay attention to the organisation’s moral and cultural development and are loyal to the service level agreement and key performance indicators (IT Business Edge and Allied Digital Services, 2010).

6.6 Training and awareness partnership program

A partnership describes the mutual connection between two or more organisations or people, or groups performing together for the same goal (Publow, 2010). The partnership could be shaped in the form of intermediate level to advanced level depending upon the shared goal. Some research shows that the procedure of the partnership depends upon accepting the agreement by both parties, provisional, everlasting, changeable or as a standard process. In the standard process partnership, two or more organisations are involved in the learning process for the successful organisation and receive useful and constructive skills helping to attain their aims and ambitions. The regularly changing IS environment and business environment forces organisations to understand the value of IS training and awareness programs to maintain their position in the competitive market. But, due to inadequate and insufficient materials, organisations look for additional materials for training and awareness programs. Materials are provided by external sources, such as security training agencies, education providers and local communities (Paek & Hawley, 2006). If the organisation gets assistance from security training agencies, then it would be more likely to be outsourcing rather than partnering, because in a partnership the main point to note is that the organisation’s level or position needs to be the same or approximately the same. The reason for being at the same level is that they could have identical goals, similar opinions, similar issues and challenges, and thus might need related training and awareness resources (Paek, 2005).

In most of the research, the results of the training and awareness program is used to evaluate the success of the program and compared with other outcomes to measure its effectiveness, but measurement of how external security training agencies impact on its success is limited. Some researchers determine that the success of a training and awareness program is due to partnership with other organisations and sharing the resources among organisations. The effectiveness of partnering IS programs could be evaluated by similar
goals between the organisations, by evaluating the training results in every organisation, and performance of the security program.

Before establishing training and awareness programs among partnership organisations, it is essential to know the current status of the partnering organisations (Kruss & Petersen, 2016), for example, how they implemented the training and awareness program, the strengths and limitations of the program, and the content and resources they executed during the program. After knowing the strengths and limitations of the training program from each organisation, a joint training and awareness framework needs to be designed that can address all recent issues and challenges. For example, one organisation could be experiencing phishing and social engineering attacks, but another could be suffering virus attacks. If they need additional resources, they could buy them, which would be cheap and an example of implementing the concept of sharing is caring or unity is strength. Sharing the knowledge between partner organisations could increase skills, and group meetings provide a platform for discussion of new topics and getting solutions. Partnering the training and awareness program in a standard user interface and interactive program for users could be another effective way of communicating with users (Sterrett, 2015).

6.6.1 Partnering security training and awareness program: friend or foe?

Partnering the IS training and awareness program brings many benefits to organisations. As mentioned earlier, it brings the concept of sharing is caring and unity is strength. By discussing the security issues and challenges with other organisations, organisations could come up with standard solutions on how to mitigate those issues. Organisations could implement those solutions in their training and awareness program or could design a joint training and awareness program that fits every partner organisation and this practice would assist in identifying the unknown and possible risks and threats. Partnering the security training and awareness program allows organisations to compare the resources with other organisations and understand how another organisation’s knowledge and understanding could be implemented in their own organisation to build up user proficiency in handling the organisation’s IS. Additionally, a partnership program would build extensive knowledge and understanding focused on users to identify their needs. Most importantly, partnership programs allow organisations to understand and take advantage of the knowledge and skills of security professionals from another partner organisation, enabling that organisation to bring resources and materials together to develop their security training and awareness program (GMBPlymouth Health Branch, 2018).

However, partnering the IS program has also some limitations. Maintaining the partnership is not an easy task; it includes trust and lots of commitment from all partner organisations. The partnering organisations have to develop the contract and service level agreement, which could be successful temporarily but not permanently. The organisation could fear that sharing training and awareness resources with other organisations who may be their competitors could affect their position in the market because the organisation might think
they are giving their resources to another organisation to allow them to stand next to them. The conflict of ideas and the organisation’s intellectual property could be another issue while developing an IS program with the partnering organisations. The decision to use organisational resources and materials for training and awareness has to go through all partnering organisations because every partnering organisation is liable for damages and costs (Queensland Government, 2018).

6.6.2 Measuring the effectiveness of the partnership program

The IS program partnership could be evaluated in different ways. The partnership security training and awareness program could be isolated from the organisation’s training and awareness program and measured, and the effectiveness of both programs could be compared (Green, 2015). Partnership program effectiveness is determined by how an organisation describes the term effectiveness. For example, one organisation’s intention in a partnership could be to train their users to be aware of different kinds of IS attacks. When users are aware of the different types of IS attacks, then the organisation would consider the partnering program to be active. Another organisation could find the partnering program is useful when the organisation gets a high score during the evaluation process. Partnering organisations could use their own methods for measuring the effectiveness of the program. Comparing the results assists in deciding which approach was useful for the evaluation (Green, 2015). Additionally, if another evaluator who is not from the partnering organisation assesses the effectiveness of the training and awareness program, there would be fairness in the results (Paek, 2005).

Myran, Crum, and Clayton (2010) implemented repeated programs to evaluate the success of a partnership program from various sources and generated a model. The model constitutes four components: implementing expansion approach, balancing theoretical and practical methods, continuing efficient communication, and concentrating on management instruction. Scherer (2009) evaluated the construction of a partnership program and found that it is affected by its characteristics and actions, concluding that the effectiveness of partnership program is not influenced by the number of partnering organisations. Waschak and Kingsley (2006) implemented theoretical and practical approaches with processes to investigate a partnership program. They found that constructional and relationship factors direct the partnership program and that the combination of many organisations can affect measuring the effectiveness of an IT partnerships program. Wildridge, Childs, Cawthra, and Madge (2004) define the term partnership in various ways, and found critical success factors for the success of the IT partnership program. They also analysed various frameworks from the literature and classified the expansion phase of the partnership program and approaches for measuring its effectiveness.

Coppola (2011) and Bodkin (2018) implemented three stages to measure the effectiveness of a partnership program. In the first stage, the measurement process includes how the partnership program is performing, modification to the size and category of the partners,
and aims and objectives of the partnership program. The second stage measures the actions of the organisations in the partnership program and evaluates its success by measuring the user’s knowledge, behaviour and attitude to find innovative concepts for improvement. The third stage measures the sustainability and effectiveness of the partnership program over time and how the partnering organisations work as a team to defend the emerging issues.

Butterfoss (2007) states that measuring the effectiveness of a partnership program is a continuing procedure that assists partner organisations to know their targeted goals and how their goals influence their organisations and their users. He further states that measuring the effectiveness of a partnership program provides continuous and organised information to reinforce the program to enable the application and execution of data to measure the level of change within users. The measuring procedure also needs continuation after the partnership program has achieved its goal to show that the ongoing program supports and attains its objectives.

Caplan, Gomme, Mugabi, and Stott (2007) state that an initial assessment of the partnership program needs to be carried out to give a solid benchmark, and an annual evaluation should be conducted to ensure continued effectiveness and improvement. The time frame between the initial assessment and another assessment depends on the reason for the assessment and the level of improvement required in the partnership program.

6.7 Failure of the training and awareness program

There are many reasons for failure of a training and awareness program, and mostly users get blamed. The security training and awareness program fails when users do not comply with what they learned in the training program or are not provided with sufficient information in the training program (Shellntel, 2016). Most of the literature points towards the users as well. As mentioned earlier, there are many aspects responsible for the success of the training and awareness program, so the question is why users are singled out as the cause of failure of the program. The three elements responsible for failure of training and awareness programs are explained below: management, user, and technical.

6.7.1 Management

Management commitment and encouragement in implementing and continuing IS training and awareness is key to the success of the program (Werlinger, Hawkey, & Beznosov, 2009). Management roles and responsibility include implementing the training program, allocating additional funding for the program, creating the environment for the program, and making resources available. But when management fails to provide these, the security program fails (Aksorn & Hadikusumo, 2008; Whitten & Kayworth, 2010). Ignorance from management in IS and their knowledge about when they cannot coordinate business processes with IS processes leads to failure in the security program (Ma, Schmidt, Herberger, & Pearson, 2009). Apart from not supporting the program, management may not encourage and
motivate their users in the IS program (Winkler, 2016). Examples of lack of encouragement include making the security training program optional rather than mandatory, not encouraging the users to read the organisation’s ISP, not involving users in the training and awareness program, failure to evaluate and monitor the program, and failure to continue training. As mentioned earlier, management should be engaged from the designing phase to the implementation phase. Therefore, management’s inactive support in defining the goals and objectives leads to the failure of the training and awareness program (Winkler & Manke, 2013).

The other reason for the failure of IS program is that management is not successful in setting up any standard benchmarking for the training program (Ghazvini & Shukur, 2017). Lack of knowledge about IS programs, such as what they are, how they work, and what happens when they are not implemented leads to malfunctioning of the security program. Most security programs fail when management does not measure its critical success factor and does not continue the program. Senior management not carrying guardianship of the program leads to failure in managing the IS program and implementing the same training and awareness program for achieving temporary and permanent goals (Tu & Yuan, 2014).

The most important reason for failure is that management fails to measure the behavioural change in users after implementation (O’Bryan, Caraway, Cilli, Chavez, & Lambert, 2005). Organisational management should seek to answer the question about whether the user’s behaviour changed after the training and awareness program leading to a reduction or improvement in the number of security incidents. Further questions include whether the organisation can calculate its ROI, and whether management is aware of the effect of IS on their business processes. When management overlooks those questions, their training and awareness program is not performing as they want and the program is unsuccessful (Paganini, 2015).

Ignorance from management in collecting comments and feedback from users, and failure to act according to the comments, are also reasons for failure of the IS training program (Craig, 2011).

### 6.7.2 User

Users play a critical role in both success and failure of training and awareness programs because success and failure depend upon how users know, understand and implement the program in their workplace. User failure depends upon two factors. First, they do not know what to do unless someone tells them what to/not to do, and second, they know what to do but are not doing it. For example, if users do not know how to report security incidents and what to say, the risk of security attacks increases. When users know how to report but are not reporting, the risk of security attacks increases. The first factor relies on interest and enforcement by management. When users are not interested in training and awareness programs, then the outcomes are unsuccessful because users do not know why the
organisation is implementing the program, how it would be beneficial to them and what potential harm not following procedures would bring.

The second factor relies on the enforcement of security policy and procedures and mandatory participation in the security training and awareness program. Ineffective action from management in enforcing ISP could result in an unsuccessful security program. Inadequate IS user knowledge is one of the most significant factors in program failure (Spitzner, 2018). In most training and awareness programs, users are taught what things users should not be doing, but fail to explain why they should not be doing such things, and also fail to tell users what they need to do (Isquarellc, 2010). Moreover, the training and awareness program fails to explain scenarios based on real-life events.

The skill of the training coordinator in delivering and conveying the message to users also affects failure of the security program because whatever the training coordinator teaches in the session, users follow. If the training coordinator is not qualified, there would be a direct impact on users (Shellntel, 2016). When users are forced to participate in a training and awareness program, and the training content is boring, the user’s performance would be futile. The payment and meal policy also affects the user’s active involvement. For example, if users are paid for the training session and offered a good meal or lunch, users could be interested and actively involved in the training and awareness session. Users prefer to skip unpaid training sessions, and even if they are forced to sit for the course, instead of listening to or reading the content, they scroll down or click to the next page without understanding and just try to finish the end-of-session test.

Highly developed and sophisticated training content could be another reason for the failure of the program because general users are not familiar with IS terms (Ghazvini & Shukur, 2016). Lack of supervision and encouragement to users is another factor for the failure of the training program. The training coordinator can believe that a training session is successful when they see a good score at the end of the test, but fail to monitor how users did the test, for example, copying from a colleague, getting help from a colleague, getting a colleague to do the test on their behalf, or only focusing on the examination. Rather than reading and understanding the training content, some users take pictures of the training materials on the phone without reading, or concentrating only on how to get excellent scores in the test. This kind of practice happens mostly when computer-based training is used. The most important factor to consider is that one training and awareness session does not determine the user’s behavioural change and cannot judge the effectiveness of the training and awareness program. Since every user is different in their learning and understanding, the training content and delivery method could also affect the user’s ability to gain from the education, and if management overlooks the user’s needs, the training and awareness program would be fruitless (Abawajy, 2014). Management needs to conduct such training and awareness programs more frequently, and needs to measure the effectiveness in such a way that users are motivated and encouraged. When the user
believes the IS training and awareness program is for them, the program would be considered successful and productive.

6.7.3 Technical

Software malfunctioning, projector or PowerPoint applications not working correctly during the training session, users unable to hear content during the training session, poor lighting, and a noisy environment are technical factors leading to failure of the training program. Ineffective capability of security professionals in measuring how IS performance influences business performance leads to failure of the security program. When technical countermeasures such as anti-virus, firewalls, and intrusion detection systems are not communicated and taught during the training session, the training session cannot give expected outcomes. Users are not educated and trained about the new technology and users not communicating how they deal with the latest technology shows failure of the program (Durbin, 2014). Ignorance from both security and general managers in implementing additional policy in data management, that is, confidentiality, integrity and availability is another factor (Tu & Yuan, 2014). Not having an appropriate strategy in incident response, backup and a business continuity plan could lead to failure in the training program (Lord, 2017; Spitzner, 2018).

There is no proper way to measure the failure of a security program from the technical point of view, but the fault could be determined by how technology is supporting data and information protection, and how technology is easy to use for users. The practice of implementing the same training program for end users, managers and security professionals could be one reason for program failure (Craig, 2011). The training program not including additional training and education resources for security professionals and managers on new and potential threats and risks and how to mitigate those threats and hazards could lead to the failure of the program. Some well-known security attacks such as social engineering attacks, phishing attacks, scam emails and calls, and other types of security which do not need advanced knowledge should be taught to general users because they are more likely to experience such attacks. Failure to include those attack types in the training program means the training program is not effective. The security training and awareness program also fails from the technical point of view when the designed IS processes are not adequate, and its objectives are not defined (Krigsman, 2008). A training program coordinator who does not have enough knowledge of IS cannot build up sufficient training materials that have a direct impact on the training program (Essays, UK, 2015b). Additionally, training coordinators implementing defective hardware and software in the training program also leads to failure. The shortage of IS professionals in an organisation means no one is available direct the training and awareness program and measure its effectiveness. In such conditions, organisations are more likely to outsource the training program once only, and there would be no continuity because continuity requires additional cost and needs the training coordinator again. The organisation’s culture and politics also play a significant role in an IS program. User attitude on how they manage to change when the organisation
changes its policy and technology also has an impact on IS program (Bada & Sasse, 2014). During the decision-making process, a sole decision of the organisation’s management on organisational security culture changing without consulting IS professionals could lead to failure of the IS program (Mueller-Jacobs, 2012; Paganini, 2015).

6.7.4 Measuring the failure of the information security training and awareness program

The success and failure of any IS training and awareness program is determined by measurement using proper security metrics. The success of the program is determined when the program has a positive influence on changing the behaviour of the user and the organisation’s security performance is improved. But what happens when the security program fails? The IS training and awareness program is considered to have failed when there is no sign of improvement in user behaviour even after the implementation of the IS training and awareness program, the number of security incidents do not decrease, and the organisation’s security and overall performance declines (Bemis, 2015).

If the security program fails, it is necessary to determine the cause. It could be that the content of the program is not relevant, in which case validating the content through the security and management team is critical. A further reason for failure could be inexperience of the training coordinator, or the program was not monitored and continued. In most cases of failure, the organisation focuses on the results of a post-training survey, considering a high score as indicative of success with no need for continuity. In other cases of failure, the training and awareness program goals did not match the organisation’s expectations.

Spitzner (2018) states that having an unclear plan, the training and awareness program being obsolete, and end users and management not being committed to the training and awareness program are the main reasons for the failure of such programs. He further suggests that investing in end users could bring huge ROI, but to achieve that it is essential to get support from managers and decision-makers. Ghazvini and Shukur (2016) state that the complexity of training and awareness content is the main reason for the failure of the program. They also mention that end users lose interest in the program because the content is too professional. They suggest that the program coordinator needs to be aware of the user’s background and design training and awareness content that is easily understood by the user to avoid failure. Bada and Sasse (2014) state that undefined warnings and complex suggestions could lead users to give up the training and awareness session. Threatening messages during the training and awareness session could raise user’s stress level, which could also affect user’s security judgement ability.
6.8 Summary

This chapter measured the effectiveness of the training and awareness program. The intention of such measurement is to focus on the end users, as well as organisational and training program needs. The measuring process was initiated with performance planning, which consisted of estimating the possible actions to achieve success. The measurement procedure consisted of multiple methods, such as measuring the participant’s knowledge about the training and learning satisfaction (tested after the training session) and measuring the participant’s behaviour and effectiveness of the training and awareness program (multiple testing).

The proposed framework for measuring the effectiveness of an IS training and awareness program was discussed. The IS program comprised risk management, information security policy, training and awareness program, and monitoring and continuity. The training and awareness program was measured in terms of participant’s knowledge, attitude and behaviour towards organisational IS. The measuring process included basic measures for general users and advanced measures for managers, security professionals and decision-makers. Basic measures included the user’s knowledge about the organisation’s IS, security policy, and types of IS attacks. Advanced measures included organisational IS and business processes, security process performance and business process performance, and user’s behaviour and management attitude towards organisational IS. While there is no exact procedure for security metrics to measure the effectiveness of the training and awareness program, the metrics should comprise what to measure, how to measure, and when to measure. The reviewing and analysis procedure involved in reporting, description of analysis result through statistical facts and figures and also determines whether the program is success or not. If the program is not successful a detailed report needs to be provided for feedback with suggestions for updating.

This chapter also emphasised the significance of outsourcing and partnering for training and awareness programs, as well as reasons for failure.

Chapter 7 provides the conclusion of the whole thesis.
Chapter 7. Conclusion

This chapter concludes this thesis by reiterating the objectives of the research, outlining the findings and their implications, presenting the limitations of the research and making suggestions for future research.

This research provided a theoretical framework for measuring ISB and ISA through a training and awareness program. A literature review provided an in-depth analysis of end-user ISB before outlining the methodology for data collection for the surveys. The surveys collected data that enabled the development of the framework to measures user knowledge, attitude and behaviour.

The remainder of the thesis concerned the development and implementation of a training and awareness program.

7.1 Objectives

The purpose of the IS training and awareness program is to make sure that every user in an organisation is aware of organisational ISP. Most organisations assume that IS is a technical issue, but this research suggests that IS is not a technical issue anymore and every user is responsible for security incidents in an organisation. The literature review also made it clear that the organisation’s management support and involvement in every step of building the IS program is essential (Heidt & Cardholm, 2008).

An awareness program is necessary for changing the behaviour of end users, but their interest and commitment is also necessary. To motivate and encourage a user’s behavioural change it is necessary to continue a training and awareness program on a scheduled basis and measure it every time it has been deployed. The critical success and failure factors need to be considered when measuring the effectiveness of the program, and should be discussed with the users.

This research aimed to measure the effectiveness of the IS training and awareness framework and minimise the IS risks in an organisation. This research also evaluated the various IS training and awareness methods and their success factors. It also verified that before implementing any training and awareness program it is essential to know what the training goals of the organisation are and what they had already done. This research ensured that the changes happening in organisational business have a direct impact on the information system, which proves that information system is not only a technical issue but is also a business issue. The utilisation of fun and practical scenarios through animated video in training and awareness program presented innovative ideas for the success of the program.
This research also focused on various procedures and stages in measuring the effectiveness of training and awareness program. The primary research question was based on measuring the research framework through a training and awareness program and other methods that were identified in the literature review. The research sub-questions queried whether user behaviour changed or resulted in changes in the organisational IS. Additionally, this research also measured other success factors of the training and awareness program by critically analysing the reasons for the failure of the program.

This research undertook critical analysis in developing, implementing, and measuring the training and awareness program and also found that there are other factors responsible for its success. The research explored how outsourcing and partnership programs affect a training and awareness program.

The critical analysis involved the identification and recognition of organisational threats and potential risk so end users could notify the appropriate person, which was the purpose of the training and awareness program. Additionally, the potential risks the organisation could face by outsourcing IT and partnering the training and awareness program were discussed.

7.2 Findings

This research established the need for measuring a training and awareness program to determine the knowledge, behaviour and attributes of the users. Deciding what to measure, how to measure and when to measure, enables effective measurement and management of the program. The possible risks and threats to organisational IS need to be identified through the risk-management process, with attention to additional risks identified during the analysis of outsourcing and partnership programs.

This section outlines the findings according to the research questions.

7.2.3 Primary research question: How is measuring the information security education training and awareness framework effective in minimising organisational information security incidents?

This research was able to measure the effectiveness of IS training and awareness framework through the basic measurement of the general user’s knowledge of the organisation’s IS, ISP and primary education on different types of IS attacks and the organisation’s general manager’s and IS manager’s understanding of the organisation’s IS and how IS influences the business process were measured through advanced measurement. In the advanced measurement, organisational management knowledge and attitude towards IS discuss and analyse how user behaviour jeopardises the organisation’s entire IS. It also outlines how organisational security process affects the organisational business process, and how outsourcing and partnership program effects in making users aware of IS and change their behaviour. The literature also focuses on how the organisation’s general managers and security managers could work together in achieving the best result for the organisation’s IS
performance and business performance. The measurement process described in this research could be implemented entirely or partially by organisations depending upon their needs because the whole measurement procedure could not fit in some organisations as stated, earlier that none of the security program and measurement process fit every organisation. The difference in the outcomes of first survey and second survey, first survey and third survey, and no major variation in the result of the second survey and third survey results proved and verified that the proposed framework is useful in making users aware of IS. And the user’s awareness brings positive change in their behaviour which ultimately reduces the IS incidents in an organisation.

7.2.2 The first research sub-question: How does employee behaviour affect the overall information security in an organisation?

This research analysed user behaviour through theory and practical considerations based on the literature review. The level of damage caused to an organisation’s IS could indicate a user’s intentional action, and identification of the level of damage should be included in risk management procedures so organisations can prepare necessary countermeasures for prevention and defence. Erratic behaviour from users could also jeopardise organisational IS, such as providing access to the premises to unauthorised users, sharing the password, leaving the computer without logging off, or choosing a password which could be easily guessed. Technical measures cannot detect this kind of practice from users. The only way to get rid of those behaviours is through training and awareness about IS. The user’s action can be measured through security audits, for example, how many intentional security incidents have been reported in the last year. Measuring unintentional security incidents is a little bit tricky, however, as many incidents go unreported due to users fearing losing their jobs.

7.2.3 The second research sub-question: Will employee behaviour be changed after implementing the information security training and awareness program?

This research found that ISA has a positive influence on ISB. The higher the awareness, the more in ISB improves. The literature review verified that ISA is a significant factor in making users aware of organisational ISP and also making users aware of their roles and responsibility. The user’s level of knowledge and behaviour changed after the training and awareness program. For example, users completely stopped sharing their password with their colleagues; users were more aware of phishing and social engineering attacks; users read, understand and exhibited knowledge about the ISP, and also about their roles and responsibilities in protecting organisational assets. The number of overall security incidents dropped from 60% to 7% after the training and awareness program, which proved that a positive change in user behaviour has a positive influence on an organisation’s IS.
7.2.4 The third research question: How is an information security training and awareness framework is evaluated, and its success measured?

The proposed framework used basic measurement techniques for general users and advanced measurement techniques for the managers and security professionals. The proposed framework designed and described an IS program where general information on IS, security policy, risk management and monitoring and continuing procedures were detailed. This framework was used to formulate the content of the training and awareness program that was delivered to users. The metrics in the proposed framework measured the user’s level of understanding based on their knowledge, attitude and behaviour. The survey results based on the proposed framework gave the expected results from the program, which verified that the proposed framework is useful in measuring the training and awareness program.

7.2.5 The fourth research sub-question: How does the age factor affect the training and awareness framework?

The research found that users aged 18 to 35 are more interested in computer-based training and group discussion. As the user’s age increased, their interest in computer-based training decreased, while their interest in classroom-based training increased. No major variation was found between group discussion and group meetings, which proves that group discussion or group meetings are an effective method of training for all age groups. The research found that users from all age group are interested in group meetings and discussion because those formats are a combination of classroom-based training and computer-based training. Group discussion is two-way communication between the users and training coordinator where real IS incidents are discussed, and users are encouraged to give their views and opinions about the incidents. Additionally, the research found that including some fun games helped make group discussion effective.

7.3 Implications of the findings

The finding of this research has two implications: theoretical and practical.

7.3.1 Theoretical

On the theoretical side, this research investigated and reviewed the popular theories on understanding user behaviour. This research measured user knowledge, attitude and behaviour based on what to measure, how to measure and when to measure. This research measured the ROI of an organisation’s IS budget. This research would be beneficial for beginners who are new in the field of IS research and the academic researcher.

7.3.2 Practical

On the practical side, this research proposed a framework for measuring the effectiveness of an IS training and awareness program that could be implemented by organisations. This research also reviewed the supportive role of organisational management and user
involvement in an IS program. This research also examined how an IS training and awareness program influences ISB. The combined role of management along with the security managers and professionals affects users to comply with ISP and build a successful organisational security culture. This research measured the IS program and calculated its success factors. This research found that the first survey and third survey did not have a high difference in their results—users forget training content after a specific interval of time and there is need for continuity of the training program. This outcome has implications for industry researchers as well as security training program coordinators in an organisation.

7.4 Research limitations

Although this research has accomplished its aim, there are some limitations. Since SurveyMonkey was used to conduct the surveys, most participants were from various states of America, so the study was limited to a developed country. This research also exclusively focused on changing user behaviour through a security training and awareness program, but there are other factors that could change user behaviour, and those factors were not included in this research. Since the training and awareness program is related to IS, it only considered the IT discipline.

Additionally, the sample size was limited to 100 people. The survey consisted of maximum 10 questions, and survey responses based on yes, no, and I do not know responses would not be an adequate response for measuring the behaviour of participants. The research was designed to change the behaviour of users by measuring the effectiveness of the training and awareness program, so this research was limited to developing the training materials and content, and measurement was limited to focusing on ISP to change participants’ habits. The author designed the survey questions, which were peer reviewed by the principal supervisor and co-supervisor for approval. The survey could be more effective if there was consultation with security professionals before designing the questions.

Some other areas of IS performance could not be investigated in this research. Participating employees are not always ready to communicate fully about the IS incidents they have experienced. While the effectiveness of IS training and awareness was measured within organisations, it was not measured externally. This research also only investigated the IS professional side, and is further limited to examining the analysis of an existing training and awareness program, establishing other factors for the success of the existing program and implementing strategies for ongoing support. IS is continually changing, and the relevance of the results will possibly change over time.

7.5 Future directions

This research provides numerous perspectives for future research. While this research only used surveys as the method for data collection, future research needs to utilise other methodologies, such as one-to-one interviews and group interviews. This research used the
scenario-based method for training, thus future research should use alternative methods, such as instructor-based, computer-based or group discussion. This research implemented a training and awareness program to raise awareness of users and change their behaviour, but future research could study alternative sources to improve user action. This research focused on how IS performance affects business performance, but future research should focus on how business threats and risks affect the organisation’s security processes. This research implemented an online survey for collecting the responses from the participants, but it does not show how participants responded. For example, did they answer the survey questions themselves or did they get help from others, or did others complete the responses in their behalf? The survey participants were from a developed country, but additional research is required in developing and underdeveloped countries so that the effectiveness of the training and awareness program can be measured across different country types. The sample size was 100 participants, but future research should include more participants. The training and awareness program was implemented only in the IT field, and future research should measure the effectiveness of the training and awareness program in different disciplines. Future research should be carried out on how external vendors play a significant role in maintaining an organisation’s IS. Future research should refer to how another training and awareness program should be implemented to maintain continuity of the program and keeping users refreshed and updated on IS program. This research only discussed on internal users, and how their behaviour affected the organisation’s business and IS performance, further research needs to be carried out on external users and factors that influence an organisation’s IS.
Bibliography


177


177


Olusegun, O. J., & Ithnin, N. B. (2013). People are the answer to security: Establishing a sustainable information security awareness training (ISAT) program in organization. *International Journal of Computer Science and Information Security, 11*(8), 57-64.


Rowe, B. R. (2007, 3 28). *Will outsourcing IT security lead to a higher social level of security?* Retrieved 12 20, 2017, from Repository: https://repository.lib.ncsu.edu/bitstream/handle/1840.16/441/etd.pdf?sequence=1


http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.9412&rep=rep1&type=pdf

http://www.statisticssolutions.com/manova-analysis-paired-sample-t-test/

Statistic Solutions: http://www.statisticssolutions.com/manova-analysis-anova/


Waugh, R. (2013). *The terrifying rise of cyber crime: Your computer is currently being targeted by criminal gangs looking to harvest your personal details and steal your money.* Retrieved 12 26, 2017, from mail online:


http://dspace.ou.nl/bitstream/1820/9497/1/Thesis%20Wissen%20van%20D.pdf


18, 2017, from Information Sheild: https://informationshield.com/five-reasons-why-
security-policies-dont-get-implemented/


effectiveness.pdf


https://brage.bibsys.no/xmlui/bitstream/handle/11250/143974/Peng%20Xiong.pdf?s equence=1


17, 2017, from ECIS 2011 Proceedings:
http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1241&context=ecis2011

policies-and-procedures-why-you-need-them
Appendix 1: Ethics approval

13 July 2016

Mr Roshan Dhakal

School of Computing and Mathematics
Charles Sturt University
WAGGA WAGGA CAMPUS

Dear Mr Dhakal,

Thank you for the additional information forwarded in response to a request from the Faculty of Business, Justice and Behavioural Sciences Human Research Ethics Committee.

The Faculty of Business, Justice and Behavioural Sciences Human Research Ethics Committee has approved your proposal “Information Security Attacks and Security Awareness in an organisation” for a twelve month period from 13 July 2016.

The protocol number issued with respect to this project is 200/2016/10. Please be sure to quote this number when responding to any request made by the Committee.

Please note the following conditions of approval:

- all Consent Forms and Information Sheets are to be printed on CSU letterhead. Students should liaise with their Supervisor to arrange to have these documents printed;
- you must notify the Committee immediately in writing should your research differ in any way from that proposed. Forms are available at http://www.csu.edu.au/research/ethics_safety/human/ehro_managing;
- you must notify the Committee immediately if any serious and or unexpected adverse events or outcomes occur associated with your research, that might affect the participants and therefore ethical acceptability of the project;
- amendments to the research design must be reviewed and approved by the Faculty Human Research Ethics Committee or if no longer minimal risk by the University Human Research Ethics Committee before commencement. Forms are available at the website above;
Appendix 2a: First survey of support group and initial survey of control group

1. How often do management conduct information security education training and awareness to employees?
   a. □ only during induction at the beginning of the job
   b. □ every month
   c. □ twice a year

2. Who is responsible for identifying and managing information security threats in an organization?
   a. □ IT professionals/ Information security staff
   b. □ organization management
   c. □ all employees
   d. □ all of above

3. In your view, what are the major factors that are preventing to achieve the successful information security in your organization?
   a. □ Unclear information security policy and procedure
   b. □ lack of security education training and awareness
   c. □ lack of appropriate technology

4. How organizations deliver training and awareness session?
   a. □ computer based training and awareness
   b. □ monthly meeting
   c. □ posters/ power point slides

5. In your opinion, how management could improve the information security systems in their organization?
   a. □ top management should consult with the employees about the trouble they are facing
   b. □ management should encourage employees to share their ideas and thoughts
   c. □ top management should give strong and consistent support to the security program

6. Do external vendors and contractors can get access to the data and information in your organization?
   a. □ yes but they must be organization’s stakeholders and they must logon through contractors account to get access to information
   b. □ no external vendors and contractors are allowed to access organization’s information
c. it depends on organization information security policy and procedure

7. In your opinion how would you improve more information security in your organization?
   a. implement latest information technology
   b. effectively implement security education training and awareness program
   c. implement both technology and awareness and training program

8. In your organization, do information security staff and IT staff are allowed to make any important decision in relation to information security issues?
   a. yes if it is related to information security
   b. no it has to be approved from management
   c. don’t know

9. Have you noticed in your organization whether or not employees are sharing password?
   a. yes
   b. no
   c. don’t know

10. How often your organization routinely manages information security audits and maintains its records?
    a. everyday
    b. monthly
    c. annually

193
Appendix 2b: Second survey with the scenario

1. The chief information security officer is responsible for implementing overall strategy for the information security awareness and training program, make sure that all the stakeholders know about the information security education training and awareness concepts and notify the outcomes of program’s implementation, make sure that employees are well trained to perform their information security responsibilities as well as real time tracking and efficient reporting procedure are prepared.

Based on the above information which statement is true.
   a. ☐ It is the duty of chief information security officer to set up strategy for information security education training and awareness program.
   b. ☐ It is the duty of chief information security officer to ensure that organization management, employees and contractors should understand the concepts and strategy of information security education training and awareness program.
   c. ☐ It is the duty of chief information security officer to ensure that management, employees and contractors are properly trained while performing their information security tasks and reports the results of the program’s implementation.
   d. ☐ All of above.
   e. ☐ Others, please explain

2. Teaching employees to be aware of an organisation's security requirements can be one of the most effective ways to enhance the company's overall security programme.

Why is it so called?
   a. ☐ It is so called because information security education training and awareness is a cornerstone of many regulations and standards, making employee compliance education not only worthwhile, but essential.
   b. ☐ Teaching employees about information security education training and awareness comes under organization information security policy and procedure.
   c. ☐ Both a and b.
   d. ☐ None of above.
   e. ☐ Others, please explain
3. It is often said that any successful organization must focus on people, processes and technology in equal order. Technology provides automated safeguards and processes to determine the series of actions to be taken to achieve a particular end. But even organizations with strong security practices are still vulnerable to human error. Oftentimes, there is insufficient attention paid to the “people” part of the equation. To stem errors made through social engineering and to raise awareness of the potential caused by carelessness, technology and processes must be combined with employee education.

In your view, how organization should manage people, process and technology to achieve successful information security?

a. [ ] Whatever the process and technology an organization implements, it would not be successful unless employees or users are aware about those technologies such as how to use, what would happen if misused and what should be done if there is faulty in technology?

b. [ ] Organizations should focus only on latest technology and monitor the information security process so that if human error occurred then it could be detected.

c. [ ] While implementing the latest technology in information security process, organization management should educate, trained and aware their employees about those technologies to minimize the risk of human error.

d. [ ] Both a and c.

e. [ ] Others, please explain

4. Some of the organizations experience the information security issues due to indistinct information security policy and procedures. Even the organizations have information security policy and procedures, employees might not be aware of it. Therefore some of the information security issues are unknown for long period even though those incidents occur frequently. This kind of information security issues and incidents occurs because there is no proper information security education training and awareness program. This program is designed to minimize the error occurring from human factor by teaching them about information security, training them about the technology that has been implemented in the organization as well as make them aware of the information system. Beside these, organization also has to implement the latest technology or upgrade the current technology and system because technology is changing day by day and organization cannot rely on the old technology.
In your view, what are the major factors that are preventing to achieve the successful information security in your organization?

a. [ ] Unclear information security policy and procedure
b. [ ] lack of security education training and awareness
c. [ ] lack of appropriate technology
d. [ ] All of above
e. [ ] Others, please explain

5. Information technology security is no more a technical issue but it is a business issue now. It is so called because all the data and information are collected, processed and stored online through internet. So it is not only the duty of information technology department to be responsible in dealing with the information security issues and incidents. Organization management and employees are also responsible for dealing with the information security issues and incidents because they are the one doing online activities with organization data and information. Sometimes organization management could identify the information security threats which are not noticed by organization information technology department and same thing could happen to employees as well. Therefore if organization management and employees notice the information security threats or are the witness of any suspicious behaviour then they have to report to information technology department immediately.

Who is responsible for identifying and managing information security threats in an organization?

a. [ ] IT professionals/ Information security staff
b. [ ] Organization management
c. [ ] Employees
d. [ ] All of above
e. [ ] Others, please explain

6. Training and awareness are two different things but if they are combined together it could be fruitful. **Training** is short-term learning of skills that is specific to an environment such as computer-based and instructor-based training and power point slides during monthly or periodic meeting. Training can be applied immediately after a session. Awareness connects people to the consequences of their actions, creating
a shift in thinking that inspires behaviour change and individuals achieve understanding in their own context such as posters, screen saver, discussion and graphical 3D videos. Awareness is an attribute that can only be attained through the training. For e.g. if organization conducts the training on password handling then organization could make employee aware of it in different ways such as in screen saver displaying the message never share the password, in lunch room or tea room hanging a poster which says change your password frequently, in meeting room hanging a poster saying that always use strong password and do not use organization password for your social networking sites.

How organizations deliver training and awareness session?

a. [ ] Compute based training and awareness
b. [ ] Monthly meeting and discussion
c. [ ] Posters/ power point slides
d. [ ] All of above
e. [ ] Others, please explain

7. Organization management plays a crucial role in establishing a stable relationship within its department and employees. It would be not a good idea for the organization management to focus on one department and disregard the others because it is the centre point of contact for all department and employees. Organization management should give freedom to speak about the problem they are experiences as well as encourage them if they come up with any idea or solution. Organization should not force their employees to follow their decision but also need to listen what the employee think about their decision. In order to achieve successful information security, organization should listen to employees, consult with information technology department and implement information security education training and awareness program.

In your opinion, how management could improve the information security systems in their organization?

a. [ ] Management should consult with the employees about the trouble they are facing and encourage employees to share their ideas and thoughts
b. [ ] Management should consult with information technology department
c. [ ] Management should give strong and consistent support to the security education training and awareness program
d. [ ] Management should implement both latest technology and information security education training and awareness program
e. [ ] Others, please explain
8. An information security audit involves the examination of the practices, procedures, technical controls, personnel, and other resources by a technology team conducts to ensure that the correct and most up-to-date processes and infrastructure are being applied. An audit also includes a series of tests that guarantee that information security meets all expectations and requirements within an organization. During this process, employees are interviewed regarding security roles and other relevant details.

How often your organization routinely manages information security audits and maintains its records?

a. [ ] Monthly  
b. [ ] Quarterly  
c. [ ] Semi annually  
d. [ ] Annually  
e. [ ] Bi annually  
f. [ ] Others, please explain
Appendix 2c: Third survey of support group and final survey of the control group

1. If you noticed any kind of information security incidents in your organization, what would you do?
   - [ ] Immediately notify the mangers
   - [ ] React and respond with the security incidents
   - [ ] Let it go

2. What would be the reasons for the information security incidents in an organization?
   - [ ] Viruses and malicious software
   - [ ] Hackers and crackers
   - [ ] Equipment failure
   - [ ] Employee’s mistakes

3. Is there enough budget and management support on maintaining the information security in an organization?
   - [ ] Yes there is enough budget allocated for information security
   - [ ] No there is no budget allocated for information security
   - [ ] Don’t know

4. What kind of data and information are necessarily needed to be protected in an organization?
   - Critical business data and information
   - Customer data and information
   - All of above

5. How organizations deliver information security training and awareness to employees?
   - [ ] Computer based training
   - [ ] Instructor based training
   - [ ] Group discussion

6. In your view, what are the major factors that are preventing to achieve the successful information security in your organization?
   - [ ] Unclear information security policy and procedure
   - [ ] Lack of security education training and awareness
   - [ ] Lack of appropriate technology
   - [ ] All of above

7. In your opinion how information security in an organization would be improved?
   - [ ] Implement latest information technology
   - [ ] Effectively implement security education training and awareness program
   - [ ] Implement both technology and awareness and training program

8. How often organization routinely should manage information security audits and maintains its records?
9. Who is responsible for identifying and managing information security threats in an organization?
   - IT professionals/ Information security staff
   - Organization management
   - Employees
   - All of above

10. If employees do not comply with the organization information security policy and procedures, what would be the action management can take?
    - Fire or punish employees
    - Train and aware employees and make sure that they understand
    - Investigate the reason why employees are resisting organization's information security policy and procedures
Appendix 3: Consent form

Charles Sturt University

CONSENT FORM

Understanding the Information Security Attacks and measuring the effectiveness of Security Awareness in an organization

Researchers

Mr. Roshan Dhakal, Doctor of Information Technology, Student ID: 11407004

Project Supervisor Project Co Supervisor

Dr. MD Rafiqul Islam Dr. Champake Mendis

I agree to participate in the above research project and give my consent freely.

I understand that the project will be conducted as described in the Information Statement, a copy of which I have retained.

I understand I can withdraw from the project at any time and do not have to give any reason for withdrawing.

I consent to participating in an interview and having it recorded.

I understand that my personal information will remain confidential to the researchers.

I have had the opportunity to have questions answered to my satisfaction.

Print Name:

Signature: Date:
## Appendix 4a: Measuring the effectiveness of training and awareness program (basic measures)

<table>
<thead>
<tr>
<th>Security issues</th>
<th>What to measure</th>
<th>How to measure</th>
<th>When to measure</th>
<th>Who measures</th>
<th>Mitigating strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisational information security</td>
<td>Reported numbers of information security incidents in organisation</td>
<td>Survey or interview</td>
<td>After the training session</td>
<td>Training coordinator/ organisation management</td>
<td>Educating users on organisation’s information security: why we need it? How to maintain or improve security? What happens if fail to do so?</td>
</tr>
<tr>
<td>Information security policy</td>
<td>Users knowledge on security policy</td>
<td>Survey and group discussion</td>
<td>Quarterly</td>
<td>Security professionals</td>
<td>Train and aware users about security policy to ensure users are complying policies</td>
</tr>
<tr>
<td>Phishing attacks</td>
<td>Number of reported phishing emails: by reporting, ignoring or opening it.</td>
<td>Survey and counting the numbers of recent and earlier phishing attacks</td>
<td>Every month</td>
<td>Security professionals</td>
<td>Train and aware users on phishing attacks and include it in security policy</td>
</tr>
<tr>
<td>Social engineering attacks</td>
<td>Number of reported social engineering attacks</td>
<td>Survey measuring the security attitude and behavior of user</td>
<td>Every month</td>
<td>Security professionals/ organisation management</td>
<td>Proper training and awareness on how users unintentional activities lead to vulnerabilities</td>
</tr>
<tr>
<td>Sensitive information</td>
<td>Number of reported</td>
<td>Survey and</td>
<td>Every month</td>
<td>Security professionals</td>
<td>Educating the users on</td>
</tr>
<tr>
<td>Handling sensitive information</td>
<td>Incidents relating to handling classified information</td>
<td>Assessment</td>
<td>Handling sensitive information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------</td>
<td>------------</td>
<td>--------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Password and access control</strong></td>
<td>Number of incidents related to password</td>
<td>Survey and security audits</td>
<td>Every month</td>
<td>Security professionals</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Training users on implementing strong password and not sharing the password</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Securing organisational assets</strong></td>
<td>Number of physical damage to organisational assets or data breaches</td>
<td>Assessment and audits</td>
<td>Weekly</td>
<td>Security professionals/managers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Educate and train users on how to secure organisation's assets</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Appendix 4b: Measuring the effectiveness of training and awareness program (advanced measures)

<table>
<thead>
<tr>
<th>Security issues</th>
<th>What to measure</th>
<th>How to measure</th>
<th>When to measure</th>
<th>Who measures</th>
<th>Mitigating strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management knowledge and attitude towards information security</td>
<td>Management approach to information security</td>
<td>Management assessment</td>
<td>Every month</td>
<td>Training coordinator/senior management</td>
<td>Educating users on organisation’s information security: why we need it? How to maintain or improve security? What happens if fail to do so?</td>
</tr>
<tr>
<td>Users behaviour</td>
<td>Number of reported incidents on users behaviour affecting the organisation’s security</td>
<td>Survey and group discussion</td>
<td>Quarterly</td>
<td>Security professionals</td>
<td>Train and aware users about security policy to ensure users are complying policies</td>
</tr>
<tr>
<td>Organisation security process</td>
<td>Number of reported incidents on organization’s security process</td>
<td>Survey and security assessment</td>
<td>Every month</td>
<td>Security professionals</td>
<td>Train and aware users on how their activities influences on organisation’s security</td>
</tr>
<tr>
<td>Organisation business and security performance</td>
<td>Number of reported incidents on organisation’s business disruption due to security</td>
<td>Security audits and assessment</td>
<td>Every month</td>
<td>Security professionals/organisation management</td>
<td>Proper training and awareness on how users unintentional security activities affects the Organisation business and security performance</td>
</tr>
<tr>
<td>Outsourcing the security performance</td>
<td>Number of reported security incidents relating to outsourcing</td>
<td>Survey and security audits</td>
<td>Every month</td>
<td>Security professionals/managers</td>
<td>Implement backup and providing limiting access to outsource companies</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>-------------</td>
<td>---------------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Overall security performance</td>
<td>Number of information security related incidents</td>
<td>Security assessment and audits</td>
<td>Every month</td>
<td>Security professionals</td>
<td>Train and aware users on organisation’s security especially security professionals</td>
</tr>
<tr>
<td>Securing organisational assets</td>
<td>Number of physical damage to organisational assets or data breaches</td>
<td>Assessment and audits</td>
<td>weekly</td>
<td>Security professionals/managers</td>
<td>Educate and train users on how to secure organisation’s assets</td>
</tr>
</tbody>
</table>