ISSUES OF PROFESSIONALISM CONCERNING THE
ETHICAL HACKING OF LAW FIRMS

Georg A. Thomas, MMgmt(InfoTech), GradCertMgmt(InfoTech),
BInfoTech(SysAdm), MACS Snr CP (Cyber Security)

This thesis is presented for the degree of Doctor of Information
Technology at Charles Sturt University

May, 2020

School of Computing & Mathematics
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>ii</td>
</tr>
<tr>
<td>Statement of Original Authorship</td>
<td>v</td>
</tr>
<tr>
<td>Acknowledgement of Assistance</td>
<td>vi</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>vii</td>
</tr>
<tr>
<td>Publications Resulting from the Research</td>
<td>viii</td>
</tr>
<tr>
<td>Glossary</td>
<td>ix</td>
</tr>
<tr>
<td>Abstract</td>
<td>xi</td>
</tr>
<tr>
<td>List of Figures</td>
<td>xii</td>
</tr>
<tr>
<td>List of Tables</td>
<td>xiii</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>xiv</td>
</tr>
<tr>
<td>Chapter 1: Introduction <strong>Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td>1.1 Purpose</td>
<td>2</td>
</tr>
<tr>
<td>1.1.1 Ethical Hacking as an Emerging Profession</td>
<td>3</td>
</tr>
<tr>
<td>1.1.2 Problem Statement</td>
<td>4</td>
</tr>
<tr>
<td>1.2 Research Questions</td>
<td>6</td>
</tr>
<tr>
<td>1.3 Current Strategies</td>
<td>7</td>
</tr>
<tr>
<td>1.4 Chapter Summary</td>
<td>7</td>
</tr>
<tr>
<td>Chapter 2: Literature Review <strong>Literature Review</strong></td>
<td>9</td>
</tr>
<tr>
<td>2.1 Identification</td>
<td>9</td>
</tr>
<tr>
<td>2.1.1 Screening and Eligibility</td>
<td>11</td>
</tr>
<tr>
<td>2.1.2 Included Articles</td>
<td>12</td>
</tr>
<tr>
<td>2.1.2.1 What is Professionalism?</td>
<td>15</td>
</tr>
<tr>
<td>2.1.2.2 Emerging Professions</td>
<td>17</td>
</tr>
<tr>
<td>2.1.2.3 What is a Hacker?</td>
<td>19</td>
</tr>
<tr>
<td>2.1.2.4 Ethical Hacking Strategies and Methodologies</td>
<td>21</td>
</tr>
<tr>
<td>2.1.2.5 Threats and Risks</td>
<td>24</td>
</tr>
<tr>
<td>2.1.2.6 Need for Ethical Hacking</td>
<td>27</td>
</tr>
<tr>
<td>2.1.2.7 White Hats and Implied Trust</td>
<td>29</td>
</tr>
<tr>
<td>2.1.2.8 The Importance of Professionalism</td>
<td>30</td>
</tr>
<tr>
<td>2.1.2.9 Certification for White Hats</td>
<td>31</td>
</tr>
<tr>
<td>2.1.2.10 Codes of Conduct for White Hats</td>
<td>33</td>
</tr>
<tr>
<td>2.1.2.11 Becoming an Ethical Hacker</td>
<td>34</td>
</tr>
<tr>
<td>2.1.2.12 Ethical Hacking in Academia</td>
<td>35</td>
</tr>
<tr>
<td>2.1.2.13 Ethical Implications of Ethical Hacking</td>
<td>36</td>
</tr>
<tr>
<td>2.1.2.14 Frameworks and Standards</td>
<td>39</td>
</tr>
<tr>
<td>2.1.2.15 Law Firms</td>
<td>42</td>
</tr>
<tr>
<td>2.1.2.16 Application to Law Firms</td>
<td>43</td>
</tr>
<tr>
<td>2.1.2.17 Regulation and Legislation</td>
<td>47</td>
</tr>
<tr>
<td>2.1.3 Significance of Research</td>
<td>50</td>
</tr>
<tr>
<td>2.2 Chapter Summary</td>
<td>52</td>
</tr>
<tr>
<td>Chapter 3: Methodology <strong>Methodology</strong></td>
<td>54</td>
</tr>
<tr>
<td>3.1 Methodology Choice</td>
<td>54</td>
</tr>
<tr>
<td>3.1.1 Qualitative v. Quantitative</td>
<td>54</td>
</tr>
<tr>
<td>3.1.1.1 Qualitative Approach</td>
<td>55</td>
</tr>
</tbody>
</table>
3.1.1.2 Methodological Implications ....................................... 57
3.1.2 Sampling ................................................................... 58
3.1.2.1 Sample Size ......................................................... 58
3.1.2.2 Sampling Method .................................................. 59
3.1.3 Data Gathering .......................................................... 60
3.1.3.1 Interviews .......................................................... 61
3.1.3.2 Observations ......................................................... 61
3.1.3.3 Existing Frameworks and Standards ......................... 61
3.1.4 Data Recording .......................................................... 62
3.1.4.1 Preliminary Review of Interviews ............................ 63
3.1.5 Data Storage and Security ........................................... 63
3.2 Research Scope ............................................................. 64
3.2.1.1 Limitations .......................................................... 64
3.2.1.2 Questioning ......................................................... 64
3.3 Chapter Summary .......................................................... 66
Chapter 4: Findings and Results ........................................... 68
4.1 Interviews .................................................................... 68
4.2 Observations ............................................................... 71
4.2.1 Participant Diversity ................................................... 71
4.2.1.1 Legal Professionals .............................................. 73
4.2.1.2 Cybersecurity Professionals ................................. 74
4.2.1.3 Law Firm Cybersecurity Staff .............................. 74
4.2.2 Analysis .................................................................. 75
4.2.2.1 Coding of Data .................................................... 76
4.2.2.2 Confidentiality of Information .............................. 80
4.2.2.3 Ethical Obligations of Legal Professionals .......... 82
4.2.2.4 Ethical Obligation of Ethical Hackers .................. 85
4.2.2.5 Professional Standards ........................................ 86
4.2.2.5.1 Continual Professional Development ............... 88
4.2.2.5.2 Competence Considerations ............................ 89
4.2.2.5.3 Regulating the Profession ............................... 90
4.2.2.6 Issues with Regulation ....................................... 92
4.2.2.6.1 Licensing ....................................................... 94
4.2.2.7 Conflicts of Interest ............................................. 94
4.2.2.7.1 Conflicts due to Information Access ............... 95
4.2.2.7.2 Cross-practice Ethics ................................... 96
4.2.2.8 The Onboarding Process ................................... 96
4.2.2.8.1 Importance of Due Diligence ......................... 96
4.2.2.8.2 Scoping of Engagements ............................... 98
4.2.2.9 Contrast Between Australia and the United States of America .................................................. 99
4.3 Values-based Analysis ..................................................... 101
4.3.1 Trust and Trustworthiness ....................................... 101
4.3.2 Reputation ............................................................... 104
4.4 Chapter Summary .......................................................... 105
Chapter 5: Discussion .......................................................... 106
5.1 Issues of Professionalism ................................................. 106
5.1.1 Due Diligence: Is a Single Check Sufficient? .............. 108
Statement of Original Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, 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.

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 the normal conditions established by the Executive Director, Division of Library Services or nominee, for the care, loan and reproduction of theses.

Signature: [Signature]

Name: Georg Thomas

Date: 11 June, 2020
Acknowledgement of Assistance

Capstone Editing provided copyediting and proofreading services, according to the guidelines laid out in the university-endorsed national ‘Guidelines for Editing Research Theses’.
I am thankful to many people for their support and guidance throughout this journey. First, I would like to thank my supervisors: Professor Oliver Burmeister and Dr. Gregory Low. Your guidance, encouragement and assistance with my research were invaluable and I am forever grateful for the wisdom imparted to me.

I am also very thankful to my wife Alana and son Logan. You motivated me to keep going and provided me with the love and support that I needed over the years. I would also like to thank my parents for giving me the drive to succeed and making me believe that I was capable of anything.

Finally, to all the research participants that took time out of their busy schedules to speak with me—I cannot thank you enough. Without your wisdom and experience, this research thesis would simply not exist.
Publications Resulting from the Research


Glossary

**BitLocker**: a proprietary encryption program developed by Microsoft to protect saved information on computer systems.

**Dark Web**: online content that is not indexed by conventional search engines (e.g., Google, Yahoo and Bing). The content is accessible using a special browser called The Onion Router.

**Encryption**: the process of encoding data or information into an unreadable format. Encryption is designed to ensure that only authorised parties, who possess the ‘key’ to reverse the encryption, have access to the information.

**Ethical hacking**: for the purposes of this research, ethical hacking refers to conducting tests against internal and external computer systems, applications, and infrastructure, wireless networks, physical testing (gaining access to premises) and social engineering, to test security controls and identify any weaknesses and potential avenues for disclosure of confidential information. It is sometimes referred to as ‘white hat hacking’.

**Hacking**: obtaining unauthorised access to a computer system, generally achieved by exploiting a weakness.

**Law firm**: for the purposes of this research, an organisation that provides legal advice, either operating as a law firm or an in-house legal department at an organisation or institution and holds legally privileged, confidential or sensitive information.

**Non-disclosure agreement**: a legally binding agreement between two parties that is designed to protect the confidentiality of information and knowledge.
Penetration testing: a component of ethical hacking that focuses on testing the security controls of specific network systems. Penetration testing may be conducted by a penetration tester or ethical hacker.

Rules of engagement: a document developed to provide the rules and conditions for conducting an engagement.

SHA256 Hash: a signature generated using complex mathematical calculations. The signature is designed to be used to validate the integrity of the information and ensure it has not been tampered with.

Statement of work: a document developed to describe the work required to undertake a project. This may include specific activities, deliverables, timelines and costs.
Abstract

This thesis explores issues of professionalism and ethical considerations relating to performing ethical hacking engagements for law firms. Cybersecurity has become a focus area for many organisations, due to the vast volume of information in the world and the ease of connectivity and sharing made possible by technologies such as the internet.

Law firms possess vast amounts of confidential and sensitive information; law firm clients expect that this information is privileged and will remain confidential. To maintain an appropriate level of confidentiality, law firms must ensure that their cybersecurity controls are adequate to protect the information they hold.

One aspect of a strong cybersecurity program is ensuring compliance and effectiveness of the controls that are implemented. The role of an ethical hacker is often used to test compliance and effectiveness by identifying vulnerabilities and validating an organisation’s security controls.

Previous research has explored issues around ethical hacking and the implications of teaching this subject within an academic curriculum. Much literature has discussed the exact nature of ethical hacking and what is involved in typical ethical hacking engagements. Due to the role played by an ethical hacker within an organisation, potential access to confidential information held by the law firms and the obligations of legal professionals to protect clients’ information, issues relating to ethics and professionalism require further research.
List of Figures

Figure 1. PRIMSA Methodology Stages (Moher et al., 2009) ..................9
Figure 2. Cyber Kill Chain® (Lockheed Martin, 2014) .......................24
Figure 3. Participants by Location .................................................72
Figure 4. Participants by Job Type and Experience ............................73
Figure 5. Participants by Gender .....................................................75
Figure 6. Grouped Findings .............................................................80
Figure 7. Confidentiality Concern by Participant Type .......................81
Figure 8. Discussed Professional Standards for Ethical Hackers ..........87
# List of Tables

Table 1. Initial Search Queries .................................................................11
Table 2. Number of Articles per Category .................................................14
Table 3. Research Participant Types .........................................................68
Table 4. Themes and Categories ................................................................77
Table 5. Summary of Common Security Frameworks and Standards 117
Table 6. Controls that Address Areas of Concern ......................................123
Table 7. Ethical Hacking Framework .........................................................132
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABA</td>
<td>American Bar Association</td>
</tr>
<tr>
<td>ACIS</td>
<td>Australasian Conference on Information Systems</td>
</tr>
<tr>
<td>ACM</td>
<td>Association for Computing Machinery</td>
</tr>
<tr>
<td>ACP</td>
<td>Australian Council of Professions</td>
</tr>
<tr>
<td>ACS</td>
<td>Australian Computer Society</td>
</tr>
<tr>
<td>ACSC</td>
<td>Australian Cyber Security Centre</td>
</tr>
<tr>
<td>APRA</td>
<td>Australian Prudential Regulation Authority</td>
</tr>
<tr>
<td>ASD</td>
<td>Australian Signals Directorate</td>
</tr>
<tr>
<td>ASIC</td>
<td>Australian Securities and Investments Commission</td>
</tr>
<tr>
<td>CBA</td>
<td>Commonwealth Bank of Australia</td>
</tr>
<tr>
<td>CEH</td>
<td>Certified Ethical Hacker</td>
</tr>
<tr>
<td>CEPIS</td>
<td>Council of European Professional Informatics Societies</td>
</tr>
<tr>
<td>CISM</td>
<td>Certified Information Security Manager</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>CISSP</td>
<td>Certified Information Systems Security Professional</td>
</tr>
<tr>
<td>CPA</td>
<td>Certified Practising Accountants</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>CPD</td>
<td>Continuing professional development</td>
</tr>
<tr>
<td>CREST</td>
<td>Council of Registered Ethical Security Testers</td>
</tr>
<tr>
<td>CSA</td>
<td>Cyber Security Agency</td>
</tr>
<tr>
<td>CSC</td>
<td>Critical Security Controls</td>
</tr>
<tr>
<td>CSF</td>
<td>Cyber Security Framework</td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerability and Exposures</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of service</td>
</tr>
<tr>
<td>FFIEC</td>
<td>Federal Financial Institutions Examination Council</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>HREC</td>
<td>Human Research Ethics Committee</td>
</tr>
<tr>
<td>ICT</td>
<td>Information, communications and technology</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IRAP</td>
<td>InfoSec Registered Assessors Program</td>
</tr>
<tr>
<td>IS</td>
<td>Information systems</td>
</tr>
<tr>
<td>ISACA</td>
<td>International Systems Assurance and Controls Association</td>
</tr>
<tr>
<td>ISM</td>
<td>Information Security Manual</td>
</tr>
<tr>
<td>ISMS</td>
<td>Information security management system</td>
</tr>
<tr>
<td>IT</td>
<td>Information technology</td>
</tr>
</tbody>
</table>
**JICES** | Journal of Information, Communication and Ethics in Society
---|---
**LCA** | Law Council of Australia
**NAO** | National Audit Office
**NDA** | Non-disclosure agreement
**NDB** | Notifiable Data Breaches
**NIST** | National Institute of Standards and Technology
**NYDFS** | New York Department of Financial Services
**OAPC** | Office of the Australian Privacy Commission
**PII** | Personally identifiable information
**PIPEDA** | Personal Information Protection and Electronic Documents Act
**PRISMA** | Preferred Reporting Items for Systematic Reviews and Meta-Analyses
**RoE** | Rules of engagement
**SANS** | SysAdmin, Audit, Network and Security
**SFIA** | Skills Framework for the Information Age
**UK** | United Kingdom
**UNSW** | University of New South Wales
Chapter 1: Introduction

Currently, information and cybersecurity are topics of high importance for many organisations. A dramatic increase in the number of significant data breaches has occurred over the past decade; consequently, legislation and regulation have been introduced that focus on such issues. Subsequently, company board members across the globe are turning their attention to cybersecurity and cyber risk, to ensure the ongoing security of information, particularly information that is sensitive or confidential, and managing cyber-related risks effectively.

There are many required components of an effective information security program; one key component is conducting a thorough review of an organisation’s environment to determine the security posture and identify any potential risks and vulnerabilities. One aspect of this review typically involves engaging the services of a security professional who is skilled in testing the effectiveness of security controls, also known as an ‘ethical hacker’ to conduct such an assessment.

Law firms hold a significant quantity of sensitive and confidential information, particularly client information. Examples of such information include trust account information, information about mergers and acquisitions, tax information, intellectual property, information about criminal cases and other kinds of commercially sensitive information. Such information may be subject to misuse; unauthorised disclosure thereof may have catastrophic consequences. Therefore, law firms must ensure the implementation of adequate information security safeguards and proper validation to protect the information they hold.

This thesis focuses on issues of professionalism in ethical hacking, as these relate to law firms. The study primarily focused on legal and cybersecurity professionals in Australia but also included participants
from the United States of America (USA). The inclusion of participants from the USA allowed for both comparison of cultural differences and investigation of whether there existed any significant variation between the two countries’ maturity of laws and cyber resilience.

1.1 Purpose

The purpose of this study was to identify issues of professionalism and ethical issues as they relate to the ethical hacking of law firms and to recommend ways to reduce or mitigate such issues where they are seen as high risk. Mitigation may be achieved through the development of a framework or professional code of conduct or ethics for ethical hackers.

Professionalism can be defined as the ethics, morals, conduct, skills and other qualities that are required of a professional as part of his or her profession; therefore, it forms a key aspect of conducting business. Parsons (2005) has demonstrated that professionalism plays a key role in modern society; fundamentally, it helps to ensure the stability of normative social order in a capitalist economy (Evetts, 2003, p. 400). Gotterbarn, the former chair of the Association for Computing Machinery (ACM) stated that professional ethics concerns the values that guide a professional (McDermid, 2008). Although this statement is largely focused on information, communications and technology (ICT), this definition of ethics can be applied to any profession.

Ethical hacking is a form of security testing that involves the engagement of a consultant, known as an ethical hacker or a penetration tester, by an organisation to attempt to gain access to the organisation’s computer systems (or their physical premises) to gain access to information. Penetration testing generally focuses on discovering vulnerabilities and flaws of specific systems, whereas ethical hacking is broader, involving not only the skills used by a penetration tester to target specific systems but other hacking skills (Infosec
Issues of Professionalism Concerning the Ethical Hacking of Law Firms

Georg A. Thomas

Institute, 2019). The information gained by the tester is generally considered sensitive and may include (but is not limited to) usernames and passwords, financial information, strategic documents, intellectual property, critical infrastructure and other system controls and personal and client information. The primary purpose of ethical hacking is to validate the current security controls of an organisation to determine if there are any vulnerabilities that require addressing before they are exploited either by an attacker or by accidental disclosure.

Recently, there has also been an increase in legislative and regulatory requirements that emphasise cybersecurity. This will inevitably result in more mature security programs that include ethical hacking as a key component to validate their effectiveness. This increase in ethical hacking engagement, in combination with the sensitivity of information, means that further research is required to improve the role of ethical hackers and reduce any risks such as unauthorised disclosure or misuse of sensitive information.

1.1.1 Ethical Hacking as an Emerging Profession

The use of ethical hacking as a method for testing the security controls of an organisation has been present for over nearly sixty years; “ethical hacking has been a professional pursuit since the 1960’s when the U.S. military and other organizations began using “red teams” or “penetration testers” to attempt computer security breaches, and thereby help in identifying and mitigating vulnerabilities” (Slayton, 2018, p147). Yet, ethical hacking has not yet been formally recognised as its own profession. When compared to other similar professions, such as ICT, the first computers were developed during the 1940’s (McCartney, 1999) and the Australian Computer Society (ACS) was only admitted to Professions Australia in January 2000 (Ridge, n.d.; Weckert, Lucas & Selgelid, 2013). This demonstrates a lag of approximately 60 years from when the field first appeared to when then formal recognition as a
profession occurred. Using ethical hacking as an example, if a similar timeline is followed and based on the identified literature and arguments in this section and later in this thesis, ethical hacking is recognised as an emerging profession.

As previously stated, the recognition of ICT as a profession is relatively recent, compared with other established professions with ACS gaining admission to Professions Australia in January 2000 (Ridge, n.d.; Weckert, Lucas & Selgelid, 2013). However, an occupation such as software engineering had already achieved professional recognition and, over several years, evolved to form its own discipline (despite being a subset of computer engineering). As a standalone profession, software engineering obtained an approved code of ethics by the Institute of Electrical and Electronics Engineers (IEEE) Computer Society and the ACM (Gotterbarn, Miller & Rogerson, 1999), which is a key component of profession recognition, which will will be discussed in further detail in Emerging Professions within the literature review.

Much like computer engineering, some individual disciplines of ICT have become recognised as their own professions. Ethical hacking is viewed as an emerging profession and is a discipline of either the ICT or the cyber security profession, both of which are recognised as professions. In Chapter 2, I further discuss how a ‘profession’ may be defined and how these criteria apply to ethical hacking to make it an emerging profession.

1.1.2 Problem Statement

As an emerging profession, much like ICT, which was only recognised as a profession less than two decades ago, ethical hacking has no mandatory or uniform code of ethics. The ethical hacker role provides a significant contribution towards ensuring the security of private and sensitive information, which has become increasingly important in the
current corporate landscape. Factors such as increased legislative and regulatory requirements related to cybersecurity, potential impacts on reputation and significant penalties are influencing the necessity to not only conduct effective tests but also ensure that no adverse consequences arise. Law firms, in particular, handle vast quantities of sensitive and confidential information that may be used in a variety of ways: merger and acquisition transactions, organisation restructures, intellectual property matters, criminal matters and even matters impacting national security. Therefore, it is paramount to ensure appropriate protection and handling of information. Such information is often only disclosed on a need-to-know basis; disclosure to a third party, such as an ethical hacker, may present a concern, particularly if misuse or inappropriate handling of that information were to occur.

Lawyers have specific obligations to their clients—one key such obligation is legal professional privilege; this is, therefore, a key consideration in ethical hacking. Finally, lawyers rely on cybersecurity professionals (e.g., ethical hackers) to be experts in their field because their skills typically fall outside standard lawyer expertise. There is a level of implied trust in the ethical hacker; therefore, it is crucial that the ethical hacker maintains ethical conduct and professionalism.

It would be beneficial to ensure that the ethical hacking specialisation matures and gains recognition as a standalone profession and to ensure ethical conduct and adequate knowledge of professionals in the field. Therefore, it would be useful to develop a mandatory, uniformed code of ethics (or code of conduct), issued by a governing body or some other form of regulatory compliance. The importance of ethical hacking and its recognition as a standalone profession and the usefulness of a mandatory, uniformed code is reflected in my research, as follows.
1.2 Research Questions

As is discussed in further detail in Chapter 2, this study focused on the following research questions:

1) Are there ethical issues and issues of professionalism related to conducting ethical hacking engagements at law firms?
2) Should (and can) a framework be developed for law firms that allows them to conduct better due diligence when engaging ethical hackers and reduce the risks to the firm and their clients?
3) Would a code of conduct add value to the ethical hacking profession?

The first question was designed to identify any professionalism issues, of which lawyers and security professionals were aware, that could result from ethical hacking engagements.

Following the identification of significant professionalism issues, there arises a question of how to address such. Frameworks are commonly used to provide structure and guidance—such an approach could be useful in addressing identified professionalism issues by providing specific guidance that is applicable to the obligations and needs of law firms and legal professionals.

The framework approach could be used as a method for vetting ethical hackers—a preventative method. An alternative option would be a code or policy approach, which could be used to complement a framework approach. For this reason, this study aimed to identify whether a code of conduct would add value to the ethical hacking profession. Although this research focuses on the use of ethical hacking services for law firms, such a code would have wider uses and applicability beyond the legal context.
1.3 Current Strategies

Current strategies used by law firms to engage professionals such as ethical hackers tend to be inconsistent. Many firms rely on contracts and specific contractual obligations to mitigate risk, such as a non-disclosure agreement (NDA), a statement of work and, in some instances, a signed rules of engagement (RoE) (Stefinko, Piskozub & Banakh, 2016). Often, the latter is a document provided by the organisation performing the testing rather than by the law firm; further, not all ethical hacking organisations provide such a document. It is not common practice for a client organisation (not solely law firms) to conduct a background or credit check on the ethical hackers performing work for them. Rather, the organisation providing the service is usually relied on to undertake these checks prior to employment and supply adequate and appropriate vetted ethical hackers.

1.4 Chapter Summary

This chapter has defined the purpose of the research and the problem that this study aimed to address. Ethical hacking, like many ICT-related professions, is a relatively new profession that lacks a uniform or mandatory code of ethics or conduct. Ethical hackers possess the skills and knowledge to gain access to sensitive and confidential information. Law firms hold vast quantities of confidential and sensitive information that must be protected. There exist several legislative and regulatory requirements for certain types of information to be protected, including significant penalties for noncompliance.

Consequently, ethical hackers are engaged by law firms to test their security. A level of implied trust is required by this process. Further, legal professionals would likely not possess the skills to adequately vet a security professional. It is crucial to identify the issues associated with
ethical hacking for legal firms and to find a solution to mitigate any potential risks.

Chapter 2 presents the literature review, which was conducted by analysing existing literature from academic journals and publications.
Chapter 2: Literature Review

Qualitative analysis of current literature and research in the area of ethics and ethical hacking was undertaken to obtain a snapshot of how widely the area had already been researched. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Moher, Liberati, Tetzlaff, Altman & The PRISMA Group, 2009) method was used for this study (see Figure 1).

Figure 1. PRISMA Methodology Stages (Moher et al., 2009)

Multiple possible methods exist for conducting a systematic literature review; to avoid bias, an established, formalised and widely adopted method was used. PRISMA is a well-known protocol for conducting systemic reviews of research and avoiding bias (Knobloch, Yoon & Vogt, 2011). Although PRISMA is typically used in the evaluation of randomised trials, its uses extend to conducting reviews of other kinds of research. Rather than developing a new method for review and evaluation of existing literature, this study used PRISMA because it is an already developed and mature method used by the research community to improve the reporting of systematic reviews (Tao et al., 2011).

2.1 Identification

The identification stage comprised an exhaustive search of Google Scholar and other journal databases. ProQuest (Information Technology), EBSCO Host, ACM Digital Library and IEEE Xplore were searched for research relating to ethics and professionalism in ethical hacking, penetration testing and hacking. There is little existing literature related to ethics and professionalism on ethical hacking; therefore,
common issues of professionalism within ICT were also identified to determine the significance of the topic as it applies to ICT professionals more broadly. Results were retrieved and abstracts reviewed to determine relevance.

Initially, a limited number of base keywords were selected. These keywords were limited to prevent influencing the results; however, they also needed to be specific enough to ensure relevant results. In addition to the base keywords, synonyms were used to ensure the capture of data in which an alternative word was used. Because this paper focuses on issues of professionalism within law firms, specifically with regard to ethical hacking, the initial selection of these papers was performed by searching for ‘ethical hacking’, ‘professionalism’, ‘white hat hacking’, ‘hacking’, ‘ethics’ and ‘penetration testing’. These keywords were chosen because they were more likely to produce results. Subsequently, the terms ‘law firm’, ‘legal firm’ and ‘law’ were added to refine the results to specific literature pertaining to law firms.

An ‘AND’ operator was used to link ‘professionalism’ to ‘ethical hacking’ and ‘OR’ operators were used to include the alternative terms. An example search is as follows:

('professionalism' OR 'ethics') AND ('ethical hacking' OR 'hacking' OR 'penetration testing' OR 'white hat hacking') AND ('law firm' OR 'legal firm' OR 'law')

The search queries were formatted to the appropriate input for the relevant search engine or journal database search, as shown in Table 1.
Table 1. Initial Search Queries

<table>
<thead>
<tr>
<th>Engine</th>
<th>Search query</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Scholar</td>
<td>(‘professionalism’ OR ‘ethics’) AND (‘ethical hacking’ OR ‘hacking’ OR ‘penetration testing’ OR ‘white hat hacking’)</td>
</tr>
<tr>
<td></td>
<td>(‘law firm’ or ‘legal firm’) and (‘ethical hacking’ or ‘hacking’ or ‘penetration testing’ OR ‘white hat hacking’)</td>
</tr>
<tr>
<td></td>
<td>‘law’ and (‘ethical hacking’ or ‘hacking’ or ‘penetration testing’ OR ‘white hat hacking’)</td>
</tr>
<tr>
<td>ACM Digital Library</td>
<td>‘query’: {(professionalism, ethics ethical hacking, hacking, penetration testing, white hat hacking)}</td>
</tr>
<tr>
<td></td>
<td>‘query’: {(professionalism, ethics ethical hacking, hacking, penetration testing, white hat hacking, law firms, legal firms, law)}</td>
</tr>
<tr>
<td>EBSCOHost</td>
<td>professionalism OR ethics AND ethical hacking OR hacking OR penetration testing OR white hat hacking</td>
</tr>
<tr>
<td>IEEE Xplore</td>
<td>(professionalism OR ethics) AND (ethical hacking OR hacking OR penetration testing OR white hat hacking)</td>
</tr>
<tr>
<td></td>
<td>(professionalism OR ethics) AND (ethical hacking OR hacking OR penetration testing OR white hat hacking) AND (law OR law firm OR legal firm)</td>
</tr>
<tr>
<td>ProQuest</td>
<td>all(professionalism) OR all(ethics) AND all(ethical hacking) OR all(hacking) OR all(penetration testing) OR all(white hat hacking)</td>
</tr>
<tr>
<td>(Computing)</td>
<td>all(professionalism) OR all(ethics) AND all(ethical hacking) OR all(hacking) OR all(penetration testing) OR all(white hat hacking)</td>
</tr>
<tr>
<td></td>
<td>all(professionalism) OR all(ethics) AND all(ethical hacking) OR all(hacking) OR all(penetration testing) OR all(white hat hacking) AND all(law) OR all(law firm) OR all(legal firm)</td>
</tr>
</tbody>
</table>

2.1.1 Screening and Eligibility

Each journal database and search engine was searched using the relevant search query outlined in Table 1. A two-stage screening
Issues of Professionalism Concerning the Ethical Hacking of Law Firms

Georg A. Thomas

process was undertaken with the collected literature. Initially, articles were selected based on their titles and abstracts. Some articles were removed because it was clear from the titles and abstracts that they were not relevant to the research (e.g., the term ‘white hat’ may have returned articles regarded to manufacturing ‘white hat’ clothing items.). Next, any duplicate articles were excluded. A duplicate article generally occurred when multiple journal databases returned the same result. Articles that were determined to be plagiarised were also excluded. For example, three articles were determined to be identical, but by different authors. The earliest published version of the article was retained and the others discarded.

Only articles with an available full-text version were deemed eligible for this study. Articles without an available full-text version, such as those that were not accessible via Charles Sturt University’s library access or only provided abstracts or citations, were deemed ineligible and omitted. In some cases, searching yielded thousands of results; however, the review of the results was discontinued when the results were no longer of relevance based on a subjective review of the title and abstract. Search results sets of each database showed diminishing relevancy in all cases as more results were reviewed.

2.1.2 Included Articles

The Google Scholar searches returned 33,400 results; the most relevant, according to Google’s search engine, were listed first. Only those results that met the eligibility criteria were included. Adding the ‘law’, ‘legal firm’ and ‘law firm’ keywords to the search returned no additional results, indicating that little or no research has been undertaken in this area.

The ACM Digital Library search resulted in 120,350 results, including some duplicates of items found in the Google Scholar results. Only the
first 31 papers met the eligibility criteria. Adding ‘law’, ‘legal firm’ and ‘law firm’ keywords to the search query increased the results to 128,038; however, this reduced the number of relevant results to 28, because many of the legal-specific results that increased the dataset size were irrelevant.

The EBSCO Host library returned 5,155 results; however, only six of these articles were eligible for inclusion based on the criteria. IEEE Xplor returned only two results, both of which were relevant to ethical hacking; however, neither addressed law firms specifically.

ProQuest returned 3,913 results, of which 35 were eligible. However, many of these had already been identified by previous searches of Google Scholar. Adding the legal terms expanded the search results to 11,700; however, these results were not specific to ethical hacking and, therefore, subsequently excluded.

The current research indicates that most existing research focuses on ethical hacking strategies and methodologies, the how-to of ethical hacking, definitions of ethical hacking and why it is required in a general context. Although some papers discussed ethical issues, these were found to be largely focused on academic institutions.

Each accepted paper was read, analysed and categorised into one of five categories (derived from the content), as shown in Table 2. Articles returned by multiple databases were only recorded once—this resulted in a total of 54 unique articles.
Table 2. Number of Articles per Category

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Articles</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is a hacker?</td>
<td>Content defines what ethical hacking is, including types of ethical hackers (e.g., black, grey or white).</td>
<td>11</td>
</tr>
<tr>
<td>Ethical hacking strategies and methodologies</td>
<td>Content describes hacking strategies, such as the different phases (reconnaissance/information gathering, exploitation). Also covered are types of exploits and potential targets (e.g., Structured Query Language injection, Cross Site Request Forgery, social engineering).</td>
<td>20</td>
</tr>
<tr>
<td>Threats and risks</td>
<td>Content describes risks and threats related to conducting ethical hacking or the absence of ethical hacking (e.g., disruption of service or perception issues).</td>
<td>8</td>
</tr>
<tr>
<td>Need for ethical hacking</td>
<td>Content describes why ethical hacking is an important part of a modern information security defence strategy.</td>
<td>10</td>
</tr>
<tr>
<td>Ethical issues</td>
<td>Content investigates ethical issues and implications for ethical hacking, including ethical issues related to ethical hackers.</td>
<td>5</td>
</tr>
<tr>
<td>Law firms and ethical issues</td>
<td>Content investigates ethical issues and implications for ethical hacking in the context of law firms.</td>
<td>0</td>
</tr>
</tbody>
</table>

Although many issues arise from the articles described in Table 2, only those pertinent to the development of the research questions for this study are detailed below.

In addition to identifying existing literature related to ethical hacking, law firms and issues of professionalism and ethics related to such hacking, the review also identified literature that defined professionalism. Professionalism is a widely researched topic—the aim of identifying
related literature was to form a definition of professionalism to be used in this research.

The following sections analyse the categories identified in the literature review (see Table 2) in more depth.

2.1.2.1 What is Professionalism?

The Australian Council of Professions (ACP) has defined a profession as follows:

A Profession is a disciplined group of individuals who adhere to ethical standards and who hold themselves out as, and are accepted by the public as possessing special knowledge and skills in a widely recognised body of learning derived from research, education and training at a high level, and who are prepared to apply this knowledge and exercise these skills in the interest of others. It is inherent in the definition of a Profession that a code of ethics governs the activities of each Profession. Such codes require behaviour and practice beyond the personal moral obligations of an individual. They define and demand high standards of behaviour in respect to the services provided to the public and in dealing with professional colleagues. Further, these codes are enforced by the Profession and are acknowledged and accepted by the community. (Australian Council of Professions [ACP], 2018).

As previously stated, professionalism can be described as comprising the ethics, morals, conduct, skills or other qualities that are required of a professional as part of their profession. The Council of European Professional Informatics Societies (CEPIS) Taskforce defined professionals as requiring six common characteristics: knowledge, quality, experience, ethics, accountability and earning a living through their practice (Council of European Professional Informatics Societies [CEPIS] Taskforce, 2010). Alternatively, Dal Pont (2017) defined a profession to have three core considerations: special skills and learning, a primary goal of public service and autonomy or self-regulation. Morrell (2003) also provided a similar definition, but with more emphasis on
public recognition of the professional. In addition to the specific skills, knowledge and education possessed by a professional, Morrell stated that the professional is recognised by the public as possessing authority, independent of influence and disciplined by a professional association.

Regardless of the specific definition selected, ethical hackers meet these characteristics and considerations as part of their profession in the following ways.

**Knowledge, special skills and learnings.** Ethical hackers must possess skills in testing and validating the security of organisations and their systems. Unlike many other professions, such as lawyers and doctors, they do not require formal academic qualifications. Although it is not a requirement, often ethical hackers will have completed a degree in a discipline related to information systems (IS) or cybersecurity; they may also hold one or more industry certifications.

**Quality.** High-quality tests and reports are critical to ensure a satisfactory outcome for clients. Ethical hackers must not only use the skills they may have learned through education and certification but also continually develop those skills to ensure these are up-to-date. Therefore, ethical hackers must self-regulate to ensure high-quality work.

**Experience.** To be an effective ethical hacker, extensive experience is required. The level or depth of skills required is generally not able to be taught in a classroom or through a course. Every environment is different, often involving varying technologies, controls and complexities; therefore, to successfully conduct an engagement, an ethical hacker will often need to leverage vulnerabilities across different systems that will vary from engagement to engagement.
Ethics. As suggested by the name, ethics are critical to the role of an ethical hacker. An ethical hacker often performs duties that could easily be unethical in the wrong context—their skills could be used for unethical purposes. The ethical hacker must possess excellent ethics and morals (Coleman, 2012). This requirement demonstrates the relevance of the public service as a primary goal requirement (Council of Registered Ethical Security Testers [CREST], 2016). Ultimately, an ethical hacker’s goal is to protect the public; typically, this is done via testing the security of systems that supply services to customers on behalf of their clients and identifying vulnerabilities in systems that may be reported back to the vendor.

Accountability. An ethical hacker is accountable for the quality of their work—they are responsible for the tests they conduct and the effectiveness of these tests. An ethical hacker will typically be accountable to the consulting firm they work for, who is then accountable to the client.

Earns a living. Ethical hackers are paid to perform assessments. The profession of ethical hacking can be fairly lucrative: the average US salary is US$71,331 (Infosec Institute, 2018) and Australian salaries range up to A$200,000 (Pauli, 2011).

2.1.2.2 Emerging Professions

Although not yet formalised as a profession, ethical hackers meet all the criteria of a professional according to the ACP and CEPIS. The claim that an occupation had professional status has been met with some criticism (Clarke, 2017). According to Greenwood (1957) and Wilensky (1964) professional work required long and expansive education and training, performing of a public service, decision making that is guided by a professional ethics or code of conduct, special relations of trust with clients, managers and employers, and being altruistic motivated by
universalistic values (p44, p137). Ethical hackers satisfy nearly all the abovementioned criteria, except the lack of a mandatory and unified code of conduct; that is not to say that one does not exist as is discussed in further detail in Codes of Conduct for White Hats below.

According to the Professional Standards Council, in order to become a profession, in order to become a profession, there are three elements; formation of peak bodies at National level, building and maintaining close working relationships between those professional bodies and government, and to raise the standard of induction and reach given competency standards (Bourdieu, 1979; McEwen & Trede, 2014). Using ICT as an example, the Australian Computer Society is the peak National body working closely with government. In order to become a professional member of the ACS members need to meet certain skills and experience requirements as well as commit to abide by the ACS code of ethics and code of practice (Australian Computer Society, n.d.). Comparing this to ethical hackers, bodies like CREST as discussed in Regulating the Profession provide a similar function. Like the ACS (and other professional bodies such as the IEEE Computer society), CREST utilises the Skills Framework for the Information Age (SFIA), which defines core competencies as professional standards in order to meet the requirements to obtain certification. CREST also works with many governments and regulators and has a mandatory code of conduct that ethical hackers who join CREST must commit to (CREST, 2020).

Of interest is that cyber security has already become a recognised profession. The ACS Cyber Security Taskforce was formed to provide recommendations to the Australian Government on the development of Australian Professional Standards to help identify cyber expertise (Slay & Austin, 2018). In September 2017, the ACS announced the availability of a cybersecurity specialisation, which recognises cybersecurity as its own discipline and is available to ACS professional members who meet certain requirements. To be recognised as an ACS Certified
Professional with the cybersecurity specialisation, it is a requirement to demonstrate capabilities that meet level five or higher in four out of eleven listed disciplines, one of which is penetration testing (Australian Computer Society, n.d.).

Although there may be an assumption that the role of an ethical hacker is part of the ICT profession, this is not entirely the case. As identified, penetration testing is one of the disciplines that is included as part of the ACS’s cyber security specialism, but this is only one of the skills that an ethical hacker requires. As will be discussed in Ethical Hacking Strategies and Methodologies, ethical hackers require additional skills in addition to penetration testing, such as those required to conduct physical infiltrations and social engineering tests. These additional disciplines, which fall outside the scope of ICT, help to identify the need for ethical hacking to be its own profession, as codes that have been written for ICT professional members do not cover all the requirements for ethical hackers and the duties of an ethical hacker fall outside the scope of ICT.

As ethical hacking as an occupation matures and organisations such as CREST continue to become the recognised governing body for ethical hackers, ethical hacking will move from an emerging profession, to a formal profession.

2.1.2.3 What is a Hacker?

It is crucial to define the exact role of a hacker. The term ‘hacker’ was coined in the 1960s by Melbourne Institute of Technology programmers to describe someone who had the ability to understand and manipulate technology (Thomas, Burmeister & Low, 2018, p. 113). Traditionally, hackers were people that tinkered with electronic systems; today, a hacker is someone who breaks into systems with malicious intent (Farsole, Kashikar & Zunzunwala, 2010, p. 12). Hackers are generally categorised into five types: black hat, grey hat, white hat, suicide
hackers and script kiddies (Graves, 2010 p. 8). Each type of hacker is motivated by different goals and outcomes (Rezazadehsaber, 2015, p. 7). These types of hackers are explored in further detail below:

**Black hat hackers.** A black hat hacker, also known as a ‘cracker’, is a highly skilled hacker with malicious intent. This type of hacker usually hacks for personal or financial gain. They operate outside the law and do not have authorisation to access the systems they attempt to penetrate. Often, black hat hackers are part of organised crime syndicates.

**Grey hat hackers.** Grey hat hackers fall between black and white hat hackers. Unlike a black hat hacker, who attacks systems for their own gain, grey hat hackers often attack systems for a cause. Examples include hacktivism groups such as Anonymous and state-sponsored hacking groups, who hack for the benefit of their country, such as in the interest of maintaining national security. Like black hat hackers, grey hats do not obtain permission to attack the systems they attempt to penetrate; however, their motives place them in this ‘grey’ area.

**White hat hackers.** White hat hackers are cybersecurity professionals who are engaged by organisations and institutions to test their security. Armed with the same tools and techniques as black and grey hat hackers, white hat hackers (also called ‘ethical hackers’ and ‘penetration testers’) attempt to penetrate their client’s systems and infrastructure to identify any vulnerabilities. Ethical hackers are the individuals that form the focus of this thesis.

**Suicide hackers.** The suicide hacker is a particularly dangerous type of hacker. This type of hacker (like a black hat hacker) has malicious motives. However, they are also unconcerned with the consequences of their actions and are typically motivated by a radical belief system that
may be political or religious. In many respects, they resemble suicide bombers; however, their target is computer systems.

**Script kiddies.** A script kiddie is an unskilled hacker. They may be either malicious or mischievous; however, they only possess basic knowledge of hacking and limited skills. Often, they are still in school and between the ages of 14 to 16 years old (Barber, 2001). The lack of knowledge and skills is dangerous because this inexperience with the tools and techniques they are using can cause significant damage to the systems they are attempting to hack.

### 2.1.2.4 Ethical Hacking Strategies and Methodologies

Much literature has discussed different types of ethical hacking, strategies and methodologies. Depending on the type of engagement, an ethical hacker will typically undertake one or more of these strategies and follow a specific methodology. Strategies describe the type of tests that are carried out or targets. These tests are often, but not always, computer system or technical focused. The strategies are broadly categorised and explained as follows:

**Network penetration testing.** This is the most common type of penetration test (Berger & Jones, 2016). This type of test is used to identify vulnerabilities in network systems, whether they are externally facing (e.g., on the internet), internal networks (e.g., corporate local area networks) or wireless networks. Generally, this type of penetration test uncovers network misconfigurations; the initial identification of vulnerabilities is often performed using automated vulnerability scanning software (Russ, Weil, Eissler, Dibar & Manrique, 2013).

**Client-side penetration testing.** This type of testing involves testing applications and software that reside on a client system. Examples of client-side applications include email clients, browsers and word-
processing applications (Russ et al., 2013). Often, this type of testing is incorporated into network penetration testing and utilises automated scanning tools to identify vulnerable client-side applications.

**Web application penetration testing.** Web applications are applications that are delivered through a web browser, as opposed to a traditional desktop application. This type of application allows for ease of deployment and overcomes many difficulties associated with traditional desktop applications, such as centralised management, ease of wide-scale updates and compatibility with individual systems.

The (in)security of web applications is a significant roadblock to universal acceptance of the technology (Huang, Yu, Hang, Tsai, Lee & Kuo, 2004). Web application tests aim to identify vulnerabilities in web applications.

Web applications can be difficult to test because there are a significant number of runtime interactions that connect to various components (Huang, Huang, Lin & Tsai, 2003; Prokhorenko, Choo & Ashman, 2016).

**Social engineering.** Social engineering focuses on manipulation of people, rather than technology. However, technology may be used as a tool to perform manipulation. Examples of techniques that fall within social engineering are the various forms of ‘phishing’ (e.g., phishing, spear-phishing, whaling, smishing and vishing) and physical security testing.

Phishing is used to trick a person into carrying out a task or providing private information such as usernames, password or financial information to the hacker. Phishing is carried out using fraudulent email messages and is often opportunistic—the attack is sent, somewhat indiscriminately, to many people at once, with the aim of catching anyone. If the attack is targeted, it is known as spear-phishing; when
senior people are targeted (e.g., executives), it is known as whaling. There are also some less common variations—attacks carried out using mobile text messages are known as smishing and those using a telephone call are known as vishing.

Ethical hacking does not always involve testing the security of computer systems. Testing physical security, such as gaining access to secured areas (e.g., computing facilities and private offices) to obtain confidential documents and other assets, may also be needed. Physical security testing attempts to circumvent locks, badge readers and other physical security controls (Scarfone, Souppaya, Cody & Orebaugh, 2008). Techniques include tailgating, which involves following an authorised person into a secured area, and even lock picking. Once an ethical hacker gains access to a secured area, they are often able to connect to the network using a physical network cable and connect devices, such as rogue access points (Scarfone et al., 2008). Another common technique is dumpster diving, which involves looking through bins to find confidential information.

In addition to the strategies outlined above, there also exist several hacking methodologies. Methodologies provide a way of ‘doing things’, and may comprise a series of steps, even if completion of every step is not required in all cases. The most well-known of these is the Cyber Kill Chain®, developed by Lockheed Martin (see Figure 2).
Berger and Jones (2016) described a similar methodology specifically for ethical hacking. The phases of this methodology involve footprinting, scanning, enumeration, system hacking, escalation of privilege, covering tracks and planting backdoors. This resembles the methodology outlined in the EC-Council Certified Ethical Hacker (CEH) guide, which involves reconnaissance, scanning, gaining access, maintaining access and covering tracks (Graves, 2010). These methodologies are each quite similar, exhibiting only minor differences.

2.1.2.5 Threats and Risks

There exist various threats and risks related to ethical hacking. These can be broken into three broad categories: technical testing risks, social engineering risks and information disclosure.
Technical testing, such as network penetration testing, client-side penetration testing and web application penetration testing, carries risks. Risks that relate to technical testing include, denial of service (DoS) and destruction or corruption of data.

Information disclosure is a possible risk with any type of testing (not just technical testing). There is a significant risk that an ethical hacker may gain access to confidential or sensitive information. This is particularly crucial in the legal profession, which will be explored further in the discussion of issues of confidentiality and legal privilege.

DoS results when a system is no longer available for legitimate use. Although ethical hackers do not commonly carry out DoS attacks unless specifically testing for a DoS mitigation control, a DoS scenario may occur if the ethical hacker's work results in the instability or outage of a system or service.

Depending on the criticality of a system, this could have a significant impact on an organisation. On average, Australian lawyers bill between A$300 and A$500 per hour (Lawyers and Legal Services Australia, 2016). With a mid-sized firm of approximately 250 lawyers, a worst-case outage to a critical system (e.g., a document management system, where lawyers store and retrieve their work) could result in lost productivity up to the value of A$125,000 for every hour the system is down.

Destruction or corruption of data may also result from ethical hacking. Although destruction and corruption typically occur when malicious attackers infiltrate systems—as seen with the Distribute IT attack in 2012 (Connolly & Gardner, 2015)—these outcomes are also possible during a penetration test, particularly if the hacker does not have sufficient skills or knowledge to conduct the test successfully.
Social engineering threats and risks are perhaps the most sensitive because they often relate to individuals and may cause devastating consequences. Several ethical issues have been raised regarding the use of social engineering, particularly phishing, a common technique used in penetration testing. Several reported cases around the globe have reported attempted suicides by people who had fallen for phishing scams. One Australian case involved a woman who attempted suicide after falling victim to a phishing scam and losing A$300,000 (Cross, Smith & Richards, 2014; Mandell, 2013). A similar 2016 case in India involved a woman who committed suicide after falling for a phishing scam and losing money (Kumarl, 2016). A British man had also committed suicide after falling victim to an online money-laundering scam (Atkins & Huang, 2013; BBC News, 2004) highlighting psychological consequences that can result from falling victim to social engineering. In each of these cases, social engineering would have contributed to these dire consequences; however, ultimately, the central motivation for suicide was more likely significant financial losses.

A 2012 British Royal Family incident provides an example that is more relevant to the kinds of social engineering engagements conducted in organisations (Mouton, Malan, Leenen & Venter, 2014). A radio station tricked a nurse into divulging private information about a member of the royal family, who was staying in the hospital, as part of a prank call. Shortly after, the nurse committed suicide.

In all but one of these cases, the motives were malicious, as opposed to the kind of test that would be conducted by an ethical hacker. One study, however, discussed the importance of debriefing after conducting a social media test. This debrief is designed to return the target to their original emotional state. For example, due to being tricked into divulging sensitive information (as part of the test), a target could be left feeling inadequate, sad or depressed (Mouton et al., 2014).
Law is a high-stress profession and, although it is difficult to obtain precise data, various sources indicate that lawyers have a high rate of depression (Rothstein, 2007). Several studies have examined depression and substance abuse within the legal community (Langford, 2004). For example, Allan (1997) has discussed issues of substance abuse and depression among lawyers in the USA, suggesting that some states have an occurrence of substance use as high as 79 per cent.

High rates of depression and other issues may put lawyers in a higher risk category for negative psychological impact; contributing to mental health issues must be avoided. Lawyers deal with highly sensitive information that, if accidentally disclosed, could contribute to negative states of mind.

2.1.2.6 Need for Ethical Hacking

The demand for cybersecurity professionals that are skilled in attacking and compromising networks is ever-increasing (Simpson, Backman & Corley, 2010). This type of cyber-security professional understands, on a deep technical level, how not only computer systems but also people work. They are able to manipulate technology and people to find weaknesses. To test people, processes and controls to ensure that they are secure, this specialist occupation, known as an ethical hacker, must conduct an assessment. Many organisations understand the importance of this role—some government departments even train their staff in such techniques. The US government has provided training for the Pentagon network administrator in ethical hacking techniques, to furnish them with the skills to be both defensive and offensive in keeping the Pentagon network safe and the sensitive information therein safe (Lynn III, 2010).

Like the Pentagon, law firms hold significant quantities of high-value, sensitive information that may be subject to misuse. For this reason, law firms need to hire ethical hackers; however, it is likely not feasible to
engage one on a full-time basis or train existing staff in the required skills. Therefore, many firms utilise ethical hackers from consulting firms to conduct their assessments as needed. There is a clear need for ethical hacking to take place as part of an effective security program; however, there currently exists a skills gap within the ethical hacking profession.

According to the 2016 Telstra Cyber Security Whitepaper, 40.4 per cent of surveyed organisations in Australia and 46.8 per cent of organisations in Asia demonstrate a skills gap regarding cyber risk assessments (Telstra, 2016, p. 43). Additionally, the 2016 Verizon Data Breach Investigations Report identified that over 80 per cent of breaches have originated outside organisations, as opposed to human error and insider threats. Most breaches were the result of hacking; further, a steady increase in hacking, malware and social-based attacks had been observed since 2008 (Verizon, 2016, p. 7). Due to the skills gap and the rise in breaches, it stands to reason that an increase in the number of new professionals who specialise in ethical hacking is required. According to the US National Audit Office (NAO), this gap may take up to 20 years to address (Caldwell, 2013).

Although hacking, by nature, is largely thought of as a technology-oriented discipline, there are many instances in which hacking involves non-technological techniques. Technology is designed to facilitate easy use and, in turn, removes many barriers; for example, the internet mitigates the barrier of distance. A hacker may potentially be located remotely, not requiring physical access to target systems. However, other techniques (e.g., social engineering, dumpster diving and tailgating) do not necessarily rely on technology. Therefore, hacking is an emerging profession that requires skills above and beyond technical skills; therefore, it may be difficult to find a hacker with the full required skillset.
Hacking motivations depend on the moral character of the hacker—
moral character ultimately determines whether he or she conducts him
or herself ethically. However, it is also possible that someone in
possession of what society consider good morals may be influenced or
that their values may become skewed. The skewing of these morals
may have several significant consequences; given the significance of
the hacking field in today’s world and, in most cases, the sensitivity of
the information being handled, it is crucial to understand these issues.

Hacking is traditionally thought of as a technical occupation—a
significant number of ‘hacks’ affect technology-oriented systems.
Consequently, some of the research on professionals in ICT also
applies to ethical hackers. Therefore, it is necessary to identify this
research and determine its applicability to ethical hackers. Research
related to ethics and professionalism in ethical hacking, penetration
testing and hacking was identified through Google Scholar, ProQuest
(Information Technology), EBSCO Host, ACM Digital Library and IEEE
Xplore.

**2.1.2.7 White Hats and Implied Trust**

Hacking is a complex role that requires a high degree of technical skill
and knowledge; this may create an impression that ethical hackers are
elite and that it is preferable to allow them to ‘get on with their job’ rather
than attempting to understand what they do. Hacking involves creativity
and the ability to think outside the box (Wilbanks, 2008, p. 65). In a
discussion related to ICT professionals, Gotterbarn explained that
superior technical knowledge puts the ICT professional in an
advantageous position, in which the other party depends on them to
carry out their request and must, therefore, trust them (n.d., para 6). An
ethical hacker effectively has free rein to an organisation’s network to
find any exploitable security vulnerability: ‘during an evaluation, the
ethical hacker often holds the “keys to the company”, and, therefore,
must be trusted to exercise tight control over any information about a
target that could be misused' (Palmer, 2001).

It would be impractical for every person who engages an ethical hacker
to fully understand how ethical hacking works. It may be difficult or even
impossible to evaluate a professional's service from the outside; further,
a certain belief that the person can perform their job is also required
(Fabian, 2009, p. 54). An ethical hacker is also ethically and
contractually bound to abide by the requirements of the customer; therefore, they require the skills to ensure that they do not provide a
false sense of security (Xynos, Sutherland, Read, Everitt & Blyth, 2010).
Due to this complexity, the ethical hacker must be given a certain level
of implied trust. This may be likened to the trust that a patient has in
their physician or a client in their lawyer. In this instance, an ethical
hacker (or any security professional) is trusted to act in the best
interests of the organisation.

2.1.2.8 The Importance of Professionalism

Professionalism is fundamental for ICT professionals and ethical
hackers alike, particularly as many ICT professionals end up working in
the security field. In professional circles, trust and professionalism have
always been interconnected (Evetts, 2006, p. 515). There must be a
level of trust between the professionals and the people that rely on
them. Trust between an employee and their leader(s) has been
demonstrated to have a positive effect on organisational outcomes.
However, trust is not limited to the relationship between an employee
and their leader; it may also relate to a collective, such as a group of
people (Hassan, Toylan, Semercioz & Aksel, 2012, p. 34). Such a group
could comprise ethical hackers, ICT professionals, security consultants
or an organisation itself. Trust may be conceptualised as the belief of
one person that another party upon whom the individual is dependent
will act in his or her interests (Tutzauer, n.d., p. 5). As previously
discussed, the nature of information typically handled or accessed by an ethical hacker may be sensitive. Therefore, a hacker should be trustworthy, an expert in their field and aware of when they should stop before causing damage (Saleem, 2006, p. 202).

A survey conducted in the United Kingdom (UK) by Cyber-Ark Software found that one-third of IT personnel misused their privileges by searching the corporate network for confidential information, including salary information, personal information, board minutes and personal emails (Logistik News, 2008, p. 24). Because many security professionals have previously been, or may still be, ICT professionals, this issue is certainly relevant to the present study. Further, analysis conducted by the US Identity Theft Resource Center found that 16 per cent of data breaches were due to inappropriately secured portable media loss, 15.4 per cent were by insiders and 11 per cent were accidental (Data Leaks Result from Malicious Intent, 2011, p. 20). Some evidence has suggested that information technology (IT) controls such as monitoring and alerting assisted in deterring such behaviour; however, this evidence proved to be ultimately inconclusive.

It is also worth noting that, when a penetration test is conducted against an organisation, IT controls are often disabled. These tests are often aggressive and require days to complete, as opposed to the months that some hacks require; therefore, it is expected that sensor controls will be triggered and alerts generated. This window, in which no alerts are generated, provides an opportune time for malicious behaviour—this further highlights the importance of ensuring the appropriate conduct of ethical hackers.

2.1.2.9 Certification for White Hats

There are several security-oriented certifications available; however, there is no requirement for an individual to obtain these certifications to
work as an ethical hacker. Even in organisations that provide various kinds of hacking, penetration testing and security professional qualifications, training and certification are not mandatory. Such organisations include the International Council of Electronic Commerce Consultants (EC-Council), who certify individuals that have passed the required exams and possess the requisite experience as a CEH or Licensed Penetration Tester; the Global Information Assurance Certification, who provide training and certification for their Penetration Tester (GPEN) certification and the Council of Registered Ethical Security Testers (CREST), who aim to assure the skills of security professionals. However, many talented ethical hackers simply never obtain certification (Conran, 2014, p. 42).

Various experts have suggested that criminal background checks and professional certification might protect against students with malicious intent (He, Kshirsagar, Nwala & Li, 2019; Logan & Clarkson, 2005; Pashel, 2006). Although this could form part of a solution, many certifications (particularly those that are widely recognised) have relevant work experience requirements that must be verified before they can be issued. This affects not only students but also professionals from other disciplines such as ICT entering the field. For example, the Certified Information Systems Security Professional (CISSP) certification requires a minimum of five years’ work experience in two of the domains described in their body of knowledge (International Information System Security Certification Consortium, n.d.); the Certified Information Security Manager (CISM) certification requires five years of security-related experience, with a minimum of three in a management capacity (International Systems Assurance and Controls Association, n.d.) and the CEH certification requires two years of security experience, which may be waived via completing the official training (EC-Council, n.d.). Where courses allow certification within only a short period of training
(e.g., a week), the effectiveness of ethics training requires examination, along with whether an appropriate skill level has been attained.

### 2.1.2.10 Codes of Conduct for White Hats

Much like professions in ICT, ethical hacking is relatively new. It is an ‘immature’ discipline—currently, there exists no mandatory or unified code of ethics for this emerging profession. The absence of such a code of ethics, which must be adhered to and entails consequences for violations, increases the risk of a variety of inappropriate behaviours, including misrepresentation, taking credit for the work of others, privacy and confidentiality issues and failure to comply with laws (Oz, 1992). Many of the security-related certification bodies, such as the International Systems Assurance and Controls Association (ISACA), International Information System Security Certification Consortium (ISC²), SysAdmin, Audit, Network and Security (SANS) Institute, EC-Council and, more recently, the ACS (with the release of the Cyber Security specialisation), have a code of ethics or conduct. However, because there is no mandatory requirement to belong to one of these governing bodies, there is no way to enforce ethical hackers to abide by such a code. Licensing is also not generally a requirement for ICT professionals (Fabian, 2009, p. 54); this is also true for ethical hacking professionals. Some countries, such as Singapore, have considered implementing such a licensing requirement; however, this is not widely practised (Cyber Security Agency [CSA] Singapore, 2018). An ethical hacker may well behave ethically; however, it remains up to the individual to know what the boundaries are, without any specific guidance, based solely on their own moral compass and beliefs. In the event of an ethical breach, not only is it difficult to definitively state that a breach of ethics occurred (due to lack of formal definition), but there may also be no stated consequences unless the law has been broken. In some instances, these potential issues can be somewhat mitigated by a contractual agreement between the ethical hacker and the
organisation engaging the ethical hacker; such an agreement would typically limit liability.

Ethical hacking meets the requirements of a profession based on the CEPIS and Dal Pont definitions (as described earlier); however, the definition set forth by the ACP requires that a code of ethics governs each profession. By this definition, not all ethical hackers at this time would be considered professionals, given the voluntary nature of an ethical code currently required by ethical hackers.

2.1.2.11 Becoming an Ethical Hacker

Some ethical hackers may be self-taught or have undertaken professional courses and certifications (e.g., the CEH or GPEN) to augment their existing skillsets and break into the field. Competence is one key factor to consider when engaging the service of an ethical hacker. Hackers at different points in their career may have different levels of competence; a recent graduate may not have real-world professional experience, or experience within their job or day-to-day life, which may affect their confidence. This leads to varying levels of performance (Smith, 2004, p. 34). Further, the human factor – issues attributed to common human behaviour (and associated issues) play a key role in IT (Siponen, 2000, p. 256; Moody, Siponen & Pahnila, 2018).

Ethical hacking techniques can be taught; however, due to the complexity and varying nature of each environment, there subsequently exists a high level of variability when conducting penetration tests that an ethical hacker must adapt to. A ethical hacker must also be aware of stakeholders’ values; these may vary depending on laws, cultural factors and beliefs (Thomas, Duessel & Meier, 2017). Therefore, ethical hacking is not likely to be conducted in a prescriptive manner; ethical hackers must possess the ability to identify weaknesses and understand different scenarios and strategies to exploit them and conduct a
thorough test. This requires a great deal of experience. There exists an
industry belief that hackers are ‘born rather than made’ and that,
although tools can be taught, these likely do not provide the appropriate
mindset (Caldwell, 2011, p. 11).

2.1.2.12 Ethical Hacking in Academia

Formal training in ethical hacking is now offered by many academic
institutions: ‘they [students] learn how to think and act like a hacker
along with learning many tricks of the trade’ (Poteat, 2005, p. 229).
Offerings like SEC.EDU, which is a collaboration between the
Commonwealth Bank of Australia (CBA) and the University of New
South Wales (UNSW), provide publicly available courses to address the
industry shortage of cybersecurity professionals (Da Silva, 2015, para
3). More recently, Box Hill Institute has opened a new centre in Training
Cyber Security Operations to help address the critical cyber skills
shortage (Box Hill Institute, 2018). It is unsurprising that the ethical
implications of teaching ethical hacking forms an area for growing, albeit
still scarce, research. It is now necessary to teach ethical hacking as
part of computer security course curriculums (Trabelsi & Alketbi, 2013,
p. 285). Additionally, organisations such as ISACA have developed
specific cyber offerings, such as their CSX training and certification.
These are directed at academics and professionals starting out in the
cyber world and generally have a much lower cost entry point than
traditional security training.

Current research addresses ethical concerns surrounding teaching
ethical hacking in educational institutions. Students must be taught
ethical hacking techniques to combat criminal hackers (Saleem, 2006).
Courses that teach ethical hacking often have a hands-on component
that aims to teach students how to attack systems. Teaching ethical
hacking techniques is vital to produce competent cybersecurity
professionals (Trabelsi & Alketbi, 2013). One concern is that students
may use their new skills in inappropriate or irresponsible ways, such as conducting illegal or malicious activities. This concern has been confirmed by instances in which an increase in unethical use of skills against the university firewall has occurred following teaching such skills (Trabelsi & McCoey, 2016, p. 3). However, this unethical use does not necessarily indicate malicious intent; although Trabelsi and McCoey (2016) reported that 88 per cent of study respondents admitted to unethical use of their skills, 72 per cent of these reported non-malicious intent. Often, hacking is performed innocently (e.g., for fun) by students who simply want to learn (Radziwill, Romano, Shorter & Benton, 2015, p. 12). However, in some cases, students learning hacking do possess ill intent; for example, some students subsequently stole exam papers from professors’ computers. In this instance, students made the moral assessment that such behaviour was acceptable because they were not causing harm to others (Xu, Hu & Zhang, 2013, Radziwill et al., 2015).

Another contributing factor to the unethical use of hacking skills is the maturity level of the individual; immaturity may result in single impulsive acts. Teaching self-restraint and how to exercise good judgement can be difficult, particularly for younger students (Cook, Conti & Raymond, 2012). Adequate training in ethics and the law, as well as proper modelling by a mentor, may be one means to address unethical or illegal use of hacking skills taught in academic contexts (Pashel, 2006, p. 199).

2.1.2.13 Ethical Implications of Ethical Hacking

The engagement of an ethical hacker by an organisation typically relies on the organisation’s need for a professional in the field (Thomas et al., 2018b). Several articles have discussed the ethical implications of ethical hacking; however, these generally focus on academics. Jamil and Khan (2011) have discussed issues arising from teaching students to hack without knowing their true intentions, including how the outcome of these teachings could result in both negative and positive student
behaviour. Although there has been some discussion of ethics in ethical hacking, this has mainly focused on the outcome of teaching ethical hacking, as opposed to those who are already ethical hackers and have been practising for some time. The existing discussion also does not account for self-taught ethical hackers, ethical hackers that have transitioned from black hat hacking and those that do not possess the adequate competency level to be professional ethical hackers. Brodkin (2009) has discussed some issues that arise when ethical hackers have transitioned from black hat hackers—such individuals are generally characterised as grey hat hackers. He discussed the legal implications of ethical hacking, suggesting that because ethical hackers study criminal activity, some activities undertaken by them cannot be distinguished from the crimes themselves (Brodkin, 2009). Ultimately, ethical hackers are motivated by finding weaknesses and related solutions to improve the overall security posture of an organisation (Rezazadehsaber, 2015, p. 8).

As previously mentioned, existing research in this area has focused on the ethics around teaching hacking techniques to students. Radziwill, Romano, Shorter and Benton (2015) have discussed how teaching students to hack may result in them stumbling into black hat hacking and, therefore, facing legal consequences. This issue largely results from students not having developed their own abilities in ethical reasoning (Radziwill et. al., 2015). Pashel (2006) has highlighted the importance of ensuring that students understand the ramifications of potentially illegal behaviour. Crucially, student expulsions and convictions due to hacking activities are increasing (Cox, 2013; Pike, 2013, p. 67; Schwartz, 2012).

There remains a need for increased numbers of information security professionals, particularly those that can conduct penetration tests against organisations. A 2016 McAfee report by Intel Security (Intel Security, 2016) highlighted the deficit of cybersecurity talent, particularly
hacking experts. Eighty-two per cent of respondents identified a shortage: ‘teaching ethical hacking techniques has become a vital component of programs that aim to produce competent information security professionals’ (Brutus & Locasto, 2010; Damon, Dale, Land, Mache, & Weiss, 2012; Dornseif, Gärtner, Holz, & Mink, 2005; Ledin, 2011; Mink & Freiling, 2006; Trabelsi, 2011; Trabelsi & Al Ketbi, 2013; Trabelsi & McCoey, 2016; Trabelsi et al., 2013; Yuan & Zhong, 2008).

The McAfee report identified that national hacking competitions were effective in identifying and developing hacking talent; three in five respondents believed these types of events play a key role (Intel Security, 2016, p. 13). This is confirmed by various studies (see Carlin, Manson & Zhu, 2008; Conklin, 2005; Pike, 2013, p. 71; White, Williams & Harrison, 2010). Pike, however, focused on the role of these competitions in reducing potential criminal activity by students involved in ethical hacking training (2013, p. 71). These types of events, such as the annual Defcon conference held annually in Las Vegas, Nevada, and various global B-Sides conferences, attract security professionals and enthusiasts from across the world. Such events are open to everybody and likely attended by inexperienced, experienced, white hat, grey hat and black hat hackers, who network, teach each other skills and form friendships. However, one plausible and unintended consequence of such scenarios is that an ethical hacker could be influenced by a malicious hacker.

Many hackers are computer professionals with a keen interest in the field, who simply want access to information and computing resources to learn (Denning, 1996, p. 4). The same skills and knowledge used by computing professionals can form the foundation for hacking; however, at what point does an ICT professional become a hacker, whether black, grey or white hat? Hackers frequently discuss freedom and liberty (Coleman & Golub, 2008, p. 257). In this context, unethical hackers are referenced; however, because such computer professionals may be
black, grey or white hat hackers, it is possible for the lines between these types to become blurred and issues of professionalism to occur.

Another key point is that ethical hacking generally involves aspects outside ICT. Other vectors, such as social engineering, have additional implications. One common type of social engineering testing is a phishing campaign. These types of attacks attempt to exploit the ‘human factor’ by duping unsuspecting people into providing sensitive information about themselves or their employer. There may be unintended psychological implications of conducting such tests—an ethical hacker must be mindful of such consequences. The previous examples of people attempting or committing suicide following falling for phishing or other scams were related to malicious acts. However, there may still be unintended psychological consequences arising from a poorly executed test or the failure to conduct a test professionally. Because these tests are generally conducted without potential targets’ (usually employees) knowledge of testing and involve a failure to consider the welfare of these potential targets, negative consequences are possible.

2.1.2.14 Frameworks and Standards

Increasingly, hacking frameworks and standards are being adopted across the globe, with many organisations turning to already developed, standardised and recognised approaches to information and cybersecurity. There exist several standards and frameworks that organisations can leverage, depending on what they want to achieve. Some commonly used examples are detailed below.

ISO/IEC27001:2013. This standard, provided by the International Organization for Standardization (ISO) is a globally recognised information security management system (ISMS) standard that aims to assist organisations to manage asset security, including financial and
intellectual property and employee information (International Organization for Standardization [ISO], n.d.). Due to widespread recognition, this is one of the more commonly adopted standards. ISO/IEC27001 is also a standard that an organisation can be certified against, which provides global recognition and assurance to those organisations doing business with them. The Joint Accreditation System of Australia and New Zealand (JAS-ANZ) reports 558 organisations in the region that hold ISO/IEC27001:2013 certification (Joint Accreditation System of Australia and New Zealand, 2019). Within the ISO/IEC27001 ISMS, there is a mandatory requirement to evaluate the performance of the ISMS: ‘the organisation shall evaluate the information security performance and effectiveness of the information security management system’ (ISO, 2013a, p. 7).

ISO/IEC27002 (the supporting practice around implementing controls for ISO/IEC27001) requires the independent review of information security, including technical compliance review:

The organisation’s approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant change occurs. (ISO, 2013b, p. 77)

Although neither requirement explicitly mandates the use of an ethical hacker to conduct such reviews and validation, ethical hackers can be (and are) used to fulfil them.

**Australian Government Information Security Manual.** The Australian Cyber Security Centre (ACSC) and the Australian Signals Directorate (ASD) have released a manual intended to help organisations protect IS from cyber threats (Australian Cyber Security Centre [ACSC], 2019). The manual, known as the Australian Government Information Security Manual (ISM), is used within government contexts but has also been
Issues of Professionalism Concerning the Ethical Hacking of Law Firms

Georg A. Thomas

made available for use by any organisation. Certification against the ISM is achieved by implementing the controls and subsequent assessment by an approved assessor who belongs to the InfoSec Registered Assessors Program (IRAP).

ISM security control 0911 states that organisations should conduct penetration tests to validate the effectiveness of their controls. Further, those conducting the tests should possess adequate skills: ‘vulnerability assessments and penetration tests are conducted by suitably skilled personnel before a system is deployed, after a significant change to a system, and at least annually or as specified by the system owner’ (ACSC, 2019).

Adoption of the ISM in Australia is increasing. As the requirement for the ISM to be implemented within government departments increases, so does the subsequent requirement for suppliers of services to the government to be compliant with the ISM.

**National Institute of Standards and Technology Cyber Security Framework.** The National Institute of Standards and Technology (NIST) is responsible for the establishment of technology-related standards and guidelines in the USA (National Institute of Standards and Technology, 2017). In 2014, NIST released a Cyber Security Framework (CSF) that consists of five categories; identify, protect, detect, respond and recover. Although not explicitly identified, penetration testing can be used as a tool to address areas within the framework on multiple levels. Ethical hackers can help address three of these categories by identifying cyber risk areas and testing the detection and response capabilities of the organisation.

The CSF is the most well-known and adopted NIST standard, supporting publications such as SP800-115 (Technical Guide for
Information Security Testing and Assessment), which provides guidance on penetration testing are often leveraged when adopting the CSF.

**CIS Critical Security Controls (CSC).** The previously identified frameworks can appear overwhelming to many organisations due to their size. ISO/IEC27001:2013, along with ISO/IEC27002, contains 114 controls and the ISM contains over 700. The CIS has provided the CSC: the top 20 prioritised controls to stop today’s most pervasive and dangerous attacks (SysAdmin, Audit, Network and Security Institute, 2019). In the current version of the CIS CSC (version 7), conducting penetration testing are included in control 20. The intent of this control is to test the strength of an organisation’s security defences through simulating an attack (Center for Internet Security, 2018).

In each of the abovementioned standards and frameworks, there is a requirement to both test and validate the security of the organisation. In many cases, this is not prescriptive; however, the use of an ethical hacker may assist in achieving compliance.

The following section provides some discussion of law firms today—it is crucial to understand the requirements and operation of legal professionals.

### 2.1.2.15 Law Firms

In 2014, 12,483 private law firms were operating in Australia, 76.1 per cent (9,504) of which are sole practitioner firms (Law Society of New South Wales, 2014, p. 18). Such firms are unlikely to have a cybersecurity program in place or to engage the services of an ethical hacker. The remaining 23.9 per cent (2,979) of firms have 2 or more partners. The American Bar Association (ABA) Lawyer Demographics report for 2015 identified 47,562 law firms operating in the US in 2005
(American Bar Association [ABA], 2015). Of these firms, 49 per cent were reported to be sole practitioner firms.

Internal issues, such as those affecting firm employees, and external issues, such as those affecting firm clients, will be researched as part of this study. Rule 1.3 of the ABA Model Rules of Professional Conduct states that ‘a lawyer shall act with reasonable diligence and promptness in representing a client’ (ABA, n.d.). The 2015 Legal Profession Uniform Law Australian Solicitors’ Conduct Rules state that a solicitor must ‘act in the best interests of a client in any matter in which the solicitor represents the client; and deliver legal services competently, diligently and as promptly as reasonably possible’ (Legal Services Council, 2015).

Diligence is defined as ‘the attention and care legally expected or required of a person (as party to a contract)’ (“diligence”, n.d.). Like any modern business, law firms have embraced technology in conducting day-to-day affairs, with firms spending between 2 and 6.99 per cent of revenue on technology and 53 per cent of firms increasing their technology budgets in 2016, as compared to 2015 (International Legal Technology Association [ILTA] & InsideLegal, 2016, p. 4). This same survey demonstrated that 59 per cent of firms are purchasing security assessment or penetration testing services (ILTA & InsideLegal, 2016, p. 1). Firms are reliant on the use of technology to deliver services and must be diligent in providing these services, which includes the use of third parties, such as security professionals that may provide and audit such services. The International Legal Technology Association (2017) reported that larger firms (e.g., more than 150 attorneys) are more concerned with security than their smaller counterparts.

2.1.2.16 Application to Law Firms

As identified previously, the ABA and 2015 Legal Profession Uniform Law Australian Solicitors’ Conduct Rules both have requirements
relating to diligence in the provision of services to clients. A search for research relating to law firms, ethical hacking and related synonyms returned no results, indicating that this is a relatively unresearched area.

The regulations introduced by many of the regulatory bodies that relate to third parties demonstrate the significance of this area. Apart from in-house counsel, lawyers (and, subsequently, law firms) are third-party providers that provide services to their clients and are governed by these regulations. Although no explicit regulations pertaining to cybersecurity have been identified for law firms specifically (other than diligence requirements), many regulations apply to law firms’ clients and their third parties.

The New York Department of Financial Services (NYDFS) introduced regulations in 2017 that require financial services and insurance companies to conduct thorough third-party due diligence as part of their formal cybersecurity program (New York Department of Financial Services [NYDFS], 2016, p. 7). These regulations also require companies to conduct penetration testing and vulnerability assessments. Likewise, the Federal Financial Institutions Examination Council (FFIEC) has requirements relating to the security of outsourced (third-party) providers. This includes that third parties comply with legal and regulatory requirements of the entity bound by the regulations (Federal Financial Institutions Examination Council, n.d., para 4). In Australia, the ASD has provided guidance on information security controls, such as maintaining awareness of software vulnerabilities, testing access controls and dealing with cybersecurity incidents (Australian Signals Directorate [ASD], 2016, p. 44). These controls can each be addressed by conducting penetration-testing exercises. On 22 February 2018, the Australian Notifiable Data Breaches (NDB) scheme came into effect, which requires certain data breaches to be reported (Office of the Australian Information Commissioner, 2018). Previously,
there was no obligation for organisations in Australia to disclose when a breach that contained personal information of individuals had occurred.

Similarly, New York introduced the ‘New York State Information Security Breach and Notification Act’ in 2005 (New York State Attorney General, n.d.). These types of laws or schemes will likely raise awareness of cybersecurity; therefore, law firms will be under increased scrutiny to ensure they can address the security concerns of their clients and comply with any regulations that are applicable not only to them but also to their clients. Relevant legislation and regulations are discussed in more detail in Regulation and Legislation.

Currently, little research has been conducted in the area of ethical hacking and law firms. Some research has considered law-related matters and hacking, but not within law firms specifically; certainly, none of these discussed professionalism issues. One article has stated that the law itself is ineffective in preventing a deliberate attack; therefore, it is crucial to think like an attacker, advocating the use of ethical hackers (Bono, Rubin, Stubblefield & Green, 2006, p. 41). One other article has discussed offensive security (hacking hackers), highlighting how the laws governing offensive security are vague (Network World, 2013). In December 2016, media articles were published that highlight how Australia’s law firms are prime targets for cyber attacks and the ABA 2016 Tech report, reported that 26 per cent of the largest firms (over 500 lawyers) had reported some type of breach (ABA, 2016). Firms in the US and globally have already been highlighted as targets by the media. A few high-profile examples are given below.

In 2016, two New York–based law firms (Cravath, Swaine & Moore and Weil, Gotshal & Manges) were attacked by hackers: confidential information was extracted and used to make over US$4 million in illegal stock trades (Randazzo, 2016). Although they were eventually caught,
the hackers were able to effectively commit insider trading, based on the information they obtained.

In 2016, a Panama-based law firm (Mossack Fonseca) was hacked, resulting in the leak of over 11 million documents (British Broadcasting Corporation, 2016). This hack resulted in investigations of the rich and powerful, based on the information leaked, which will likely result in financial and reputation impact to the firm.

In 2017, a leak occurred that is known as the Paradise Papers: the Paradise Papers contained information about the offshore financial secrets of the world’s elite (Garside, 2017; Palan, 2017). Appleby, the law firm from which the information originated, stated that it had been the victim of a cyber attack in the preceding year (Hodgson, 2017).

However, not all law firm cyber attacks result in stolen or misused confidential information. DLA Piper was the victim of a ransomware attack, which led to destruction and corruption of data (Roberts, 2017). Ransomware is a form of malicious software (malware) that encrypts a user’s files and holds the decryption key until the ransom is paid by the victim (Scaife, Carter, Traynor & Butler, 2016).

Unlike Distribute IT, who ultimately went out of business, DLA Piper were able to recover following several weeks of system rebuilding. The ransomware in this case (NotPetya) was related to a Microsoft Windows software vulnerability that was not remediated and was able to spread across their global network.

To help protect law firms, the Law Council of Australia (LCA) launched an information initiative in 2017: Cyber Precedent (Doran, 2016). Cyber Precedent is designed to provide resources, specifically for law firms, on how to protect the sensitive information they hold (Law Council of Australia [LCA], n.d.). Such a resource highlights the duty of lawyers to
maintain the confidentiality of their clients’ information. This guidance from the LCA refers to the ASD guidance, which includes penetration testing as one of its strategies for helping to mitigate cyber attacks (ASD, 2014).

2.1.2.17 Regulation and Legislation

An increase in regulation and legislation has been observed across the world, with many countries, jurisdictions and governing bodies implementing regulation or legislation in some form. These generally focus on privacy and the rights of individuals’ information and data, as opposed to prescriptive requirements for ethical hacking or penetration testing. Although privacy laws can be dated back to the 15th century and the idea of breach of confidentiality to the early 20th century (Solove, 2006), it has only been in the last decade that significant increases in such laws, as they relate to digital privacy, have been observed.

These laws focus on privacy issues and it is important, to take such regulation and legislation into account when engaging the services of an ethical hacker. To protect the privacy and rights of individuals’ data, appropriate safeguards need to be in place. It is also possible that information could be misused, even if an engagement to test the safeguards was in good faith. This may have several implications when it comes to conducting tests, especially in certain jurisdictions, such as the European Union.

The following is a summary of some recent regulations and legislations that have been introduced or amended.

NDB Scheme (Australia). On 22 February 2018, the NDB scheme was enacted, which requires covered entities in Australia to report any breach that may result in serious harm to individuals. Organisations may face fines of up to A$2.1 million if they fail to comply with the act (Office
of the Australian Information Commissioner [OAIC], 2018a). The latest report provided by the OAIC reported 550 eligible breaches; 57 per cent of these were the result of malicious or criminal activity. The legal, accounting and management services industry sector reported the third-highest number of breaches (OAIC, 2018b, p. 13). If a law firm holds significant amounts of personal information and meets other eligibility tests, it may be required to comply with the scheme.

**General Data Protection Regulation (2016/679) (European Union).** On 25 May 2018, the General Data Protection Regulation (GDPR) came into effect in the European Union. The GDPR superseded the existing Directive 95/46/EC that had been in place since 1995 (Thomas, 2018). Of all current regulations and legislation, the GDPR is the most stringent. For example, where Australia’s NDB Scheme requires investigation within 30 days and notification as soon as practicable (as does Canada’s Personal Information Protection and Electronic Documents Act [PIPEDA] and the Philippines Data Privacy Act), the GDPR requires notification within 72 hours. Other key aspects of the GDPR include ‘the right to be forgotten’; where an EU person can request that the personal information an organisation stores of them must be deleted if it is no longer used for its intended purpose, and its ability to provide protections across jurisdictions, despite being an EU regulation.

**Data Privacy Act of 2012 (Philippines).** One of the earliest specific regulations introduced is the 2012 Data Privacy Act in the Philippines. Like the Australian and Canadian acts, this act requires that the National Privacy Commission and affected data subjects be notified if personal sensitive information or other information that may be used to commit identity fraud or real risk of serious harm is acquired by an unauthorised person (Wall, 2017).
**Digital Privacy Act (2015) (Canada).** Canada’s data breach disclosure requirement, known as PIPEDA, came into effect on 1 November 2018 (Ling, 2018). Like the Australian NDB Scheme, the Canadian legislation is an amendment to an already existing act—the Digital Privacy Act of 2015 (Thomas, Burmeister & Low, 2019). The requirements are also similar to the Australian legislation in that they require affected individuals and the Canadian Office of the Privacy Commissioner to be notified in the event of a breach of personal information that may result in a ‘real risk of significant harm’ (Government of Canada, 2018).

**NYDFS Cyber Security Regulation (New York, USA).** At the time of writing, the USA does not have a uniform law or regulation; however, some states (e.g., New York, California and Colorado) have enacted various laws and regulations. For example, the California Consumer Privacy Act is designed to protect the personal information of residents of California (Ghosh, 2018).

The NYDFS Cyber Security (23 NYCRR Part 500) regulation, which came into effect on 1 March 2017, is of special interest. It has explicit requirements for organisations to conduct penetration testing:

> The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity’s Risk Assessment, designed to assess the effectiveness of the Covered Entity’s cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. (NYDFS, n.d.)

Although this regulation is specific to entities covered by the NYDFS (i.e., financial services and insurance organisations within New York state), similar regulations could be extended to other industries and jurisdictions in the future.
2.1.3 Significance of Research

This section summarises and highlights the significance of existing research. Cybersecurity is a growing field, due to the growing use of and reliance on technology. With the identified shortages in the cybersecurity field, simple economics would predict that prices (or salaries demanded) are likely to increase. This increase will attract more people into cybersecurity careers, either as new graduates or as professionals changing careers.

As identified, most of the existing literature on ethical hacking focuses on methodologies, strategies, definitions of ethical hacking and why such hacking is required. Some literature also highlights the skills gap and how this is being addressed via teaching ethical hacking. From an ethical view, nearly all the literature that addresses ethical issues has focused on teaching ethical hacking skills to students rather than professionals that are already in the industry or moving into the industry from other related professions (e.g., ICT).

Therefore, the existing research does not adequately address issues of professionalism and ethics. Ethical hacking and cybersecurity is an emerging field and much of the existing research focuses on defining what ethical hacking is, why it is needed and how it is conducted. Some of the literature identifies that ethical hackers are more likely to encounter sensitive and confidential information because they will be engaged to test the security of organisations who hold such information.

To mitigate the risk of cybersecurity incidents, governments and other regulatory bodies have implemented, or are in the process of implementing, laws and regulations that must be complied with such as the NDB Scheme and the EU GDPR discussed in Regulation and Legislation. In addition to privacy laws, there are several regulatory requirements in certain jurisdictions such as the NYDFS Cyber Security
regulation, the Health Insurance Portability and Accountability Act of 1996, known as HIPAA, which include requirements intended to help mitigate cybersecurity risk.

Currently, many of these requirements affect law firms, either directly or through third-party relationships with covered entities, and many have requirements around information handling and significant penalties for failure to comply. For example, a breach of the GDPR could result in penalties of up to €20 million or 4 per cent of revenue (European Commission, n.d.) and a breach of the Australian Privacy Act (NDB Scheme) in penalties up to A$2.1 million (Office of the Australian Information Commissioner, 2018).

With the increased focus on cybersecurity around the globe, liability for cyber-security related incidents is becoming increasingly important. Civil penalties could result for company directors in the event they are found to be in breach of their duty of care regarding the information they hold (Allens Linklaters, 2017), not to mention any reputational and subsequent financial consequences.

Legal firms store and handle vast amounts of confidential and sensitive client information, unauthorised access to which could be catastrophic, potentially resulting in financial or reputational damage to clients and the firm. This has been emphasised by recent articles in the media about Australian law firms being prime targets for cyber attacks. Various breaches that have occurred further highlight the importance of ensuring that law firms are safeguarded; ethical hackers may play a key role in ensuring this security.

With over 60,000 law firms in Australia and the USA, cybersecurity is certainly an area of growing concern. The combination of the growing threat, confidentiality of information, the increase in professionals entering the ethical hacking field and stringent laws and regulations that
have been or will be introduced highlights the importance of this area of research. The current gaps, as identified above, should be addressed through further research.

2.2 Chapter Summary

In this chapter, the methodology (PRISMA) used to identify existing literature was covered. The methods used to identify existing literature through journal databases were explained and various areas of literature explored.

The literature defined professionalism, emerging professions, the nature of an ethical hacker, ethical hacking strategies and methodologies, threats and risks, the need for ethical hacking and the application(s) to law firms, regulation and legislation.

Defining professionalism leveraged definitions from various bodies including the ACP and the CEPIS Taskforce. Requirements such as knowledge, quality, experience, ethics, accountability and income were detailed.

Analysis of emerging professions and how they become professions, identified how ethical hacking is an emerging profession and compared ethical hacking to ICT, demonstrating the similarities between the two and how the definition of a profession by the Australian Council of Professions, the Council of European Professional Informatics Societies, and the Professional Standards Council are met.

Five different types of hackers were identified. The first type was the black hat hacker, whose motives are malicious, often for personal or financial gain. The second type is the grey hat hacker, who also often operate illegally. However, their motives are not personal or financial gain; they may operate under the direction of a nation-state or for a
cause. White hat or ethical hackers hack for ‘good’; they are engaged by organisations to find and report on vulnerabilities. Suicide hackers are not concerned with getting caught and are often destructive. Script kiddies are inexperienced hackers, often teenagers causing mischief.

The literature review identified different types of penetration tests and social engineering tests are used by ethical hackers, including network penetration testing, client-side penetration testing, web application penetration testing, phishing and social engineering.

Key risks associated with conducting ethical hacking included information disclosure, DoS (where systems become unavailable) and destruction or corruption of data. Some of the psychological risks associated with social engineering were also explored.

The need for ethical hacking was identified, as well as issues relating to the white hat skills gap and implied trust. Academic institutions are offering more cybersecurity degrees; however, concerns exist around the misuse of skills taught, due to the immature ethical conduct of students. It is difficult for a non-security professional to evaluate the skills of an ethical hacker; therefore, there is a level of necessary implied trust. This highlighted the importance of professionalism; however, there is a lack of mandatory codes of conduct and ethics. Although certification, including a code of ethics, is available, it is typically not mandatory.

Some examples of law firm breaches and legislation and regulation were also identified. These examples highlight the importance of identifying security vulnerabilities within law firms. These concerns, the importance of the role of the ethical hacker and potentially related issues highlight the significance of the research.
Chapter 3: Methodology

It is critical to select an appropriate research methodology for gathering and interpreting data. This process comprises identifying a series of steps and actions to conduct the research effectively (Kothari, 2004). The research presented in this thesis occurred in two phases: 1) data collection and 2) data analysis. A qualitative approach, based on interpretivism, was used. The selection process and justification of each chosen method is detailed below.

3.1 Methodology Choice

In selecting the methodology, various factors were considered. These are discussed in detail below.

3.1.1 Qualitative v. Quantitative

For this study, a qualitative approach was more appropriate than a quantitative approach because the study is exploratory and intended to investigate a topic with little to no prior research. According to Creswell (2009), quantitative research provides a means for testing objective theories, via the measurement and analysis of collected data. Therefore, this kind of approach is better suited to research that requires the testing of hypothetical generalisations (Hoepfl, 1997). As seen in the preceding chapter, there is little to no identified research in the area of ethical hacking and law firms. Therefore, it is difficult to make generalisations and develop hypotheses; rather, this study was exploratory and aimed to generate insight into the issues surrounding ethical hacking within law firms. For these reasons, a quantitative approach was inappropriate; instead, a qualitative method was selected. When addressing human or social problems, such as this one, qualitative research may be used effectively to explore and understand the relevant issues (Creswell, 2009).
3.1.1.1 Qualitative Approach

The constructivism method was selected because this research aims to illuminate issues of professionalism via interpretation of the elements of the study. An interpretive, constructivist research method is based on our knowledge of reality as a social construction of human factors (Walsham, 1995). Characteristics of interpretive research include naturalistic enquiry; study of the phenomena within its natural setting; the researcher as instrument; the researcher as embedded within the context they are studying and, therefore, being required to use their observational skills, trust with participants and ability to extract information; interpretive analysis and, finally, that interpretation must happen through the eyes of the participants (Lumen Learning, n.d.).

Walsham has explained the use of interpretivism as a response to Preston’s (1991) argument that information systems (IS) researchers must critically examine the underlying assumptions and theories that shape our current understanding of the field. The validity of such an approach faced some criticism as it there were concerns with issues of subjectivity; however, it has become a widely accepted approach, with publishers welcoming works that are qualitative and interpretive, as opposed to a strict focus on quantitative methods and hypothesis testing (DeSanctis, 1993, Walsham, 1995). This type of approach relies on the interpretation of research data by the researcher; therefore, it is subject to the experience and biases of the researcher. The validity of the researcher and the nature of potential biases is elucidated later in this chapter.

Alternatives to constructivism were also considered, such as ethnography, grounded theory and the case study method. However, following careful consideration, these approaches were eliminated (as explained below).
Ethnography involves the researcher being an observational participant for a prolonged period (Creswell, 2009). Boyle (1994) described ethnography as a series of observations focused on a group of people who share something in common; in this research, this group would include lawyers and ethical hackers. An ethnographical approach was ruled out for the following reasons: 1) observational participation for a prolonged period was not feasible due to time commitments (of participants and the researcher) and geographical restrictions (as participants were located across Australian and the USA) and 2) although the researcher has previously been employed as an ethical hacker and currently works in a law firm, the perspective of lawyers was central to the research—this requirement meant that gathering data from practising lawyers was necessary.

Grounded theory was also excluded due to some specific implications of using such an approach. Issues may arise around deciding the appropriateness of concluding research in grounded theory, particularly because this occurs largely at the discretion of the researcher (Glasser & Strauss, 2009). That is, once the researcher is confident that the research and theory are reasonably accurate, the research may be concluded, even in cases where research could be continued and further developed. Grounded theory has been described as ‘nice stories’ by some scholars and its credibility discounted (Urquhart, 2012; Sikolia, Biros, Mason & Weiser, 2013). Grounded theory is based on real-world actualities; data are often collected through interviews and then analysed to discover key concepts (Allan, 2003; Glaser & Strauss, 1967). Grounded theory may have formed a valid method for the research; however, because this research makes use of the extensive professional experience of the researcher, a constructivist method is a more suitable option in this case.

The case study method presented another potentially suitable method; however, it entails the issue of generalisability, which is a cause for
concern in case study research (Gibbert, Ruigrok & Wicki, 2008). Generalisability refers to the applicability of the research to other settings (given the small-n problem) (Gerring, 2007; Hägg & Hedlund 1979; Hillebrand, Kok & Biemans, 2001; Mohr, 1985; Sharp, 1998; Steinmetz, 2004; Stoecker, 1991; Tsang, 2014). This study considered multiple law firms and ethical hackers across multiple geographic locations, as opposed to a single firm; therefore, this method was not appropriate.

Narrative and phenomenological approaches were also unsuitable for this research. Narrative research involves studying the lives of individuals (Creswell, 2009, p. 13). Therefore, because this study focused on professionalism issues, as they relate to law firms (or organisations), as opposed to individuals, this approach was ruled out. Phenomenological research, which involves prolonged studies across different subjects to identify essences of human experience (Creswell, 2009), was also deemed inappropriate in the context of this research.

3.1.1.2 Methodological Implications

One key issue with a constructivist, interpretivism-based approach is the ability of the researcher to interpret the research. Kapoulas and Mitic (2012) have stated that data can be hard to find, hard to define and may be incomplete. The answers themselves are not contained within the data but in the data’s descriptive and explanatory powers (Gummesson, 2005; Kapoulas & Mitic, 2012). This leads to issues of validity, reliability and generalisability (Kelliher, 2011).

Constructivism, as a subset of interpretive research, was used in this study; the researcher was active in making and structuring the knowledge (Spivey, 1996). Constructivism entails some key implications, which were addressed throughout the research. From an ethical standpoint, there are implications around safeguarding
confidentiality, consent, protecting privacy, guarding against harm, trust and deception (Lincoln & Guba, 2013). Many of these concerns were addressed through the implementation of strong controls and approval of the research by the Human Research Ethics Committee (HREC). Anonymity and full transparency were also practised to ensure trust and reduce the risk of deception.

3.1.2 Sampling

Two methods of obtaining data samples were used in this study. The first was the purposive sampling method, used to select participants for interviews. Participants were partners and employees of law firms and other firms that consult law firms in the ethical hacking field. The second was periodic sampling, in the form of diarised notes taken by the researcher. This occurred as part of observing day-to-day activities related to ethical hacking and legal firms. Further detail is given in the below sections.

3.1.2.1 Sample Size

Creswell suggested that 20–30 samples are sufficient to fully develop a model, depending on the specific study (2007, p. 67). Charmaz (2006) has suggested that a smaller study, as opposed to a broader study, may achieve saturation quicker. During the course of this study, it was identified that saturation of data began occurring at approximately 20 interviews. This is likely due to the relatively small size of the legal industry, compared to other industries, and the fairly consistent and uniformed obligations placed upon legal professionals. Due to Charmaz’s suggestion that a minimum of 25 interviews be conducted, a further eight interviews (which formed the remainder of the consenting participant pool) were conducted. The additional eight interviews ensured that saturation was achieved and indicated whether new data was obtained and further research needed.
3.1.2.2 Sampling Method

The primary method of data collection was participant interviews. The research pertains to professionalism issues in ethical hacking (as it relates to law firms); therefore, the sampling method required that participants were relevant to the study. To gain maximally valuable data, it was necessary to select participants from these fields. Purposive sampling was used because it is intended to produce a sample that can be assumed to represent the population (Lavrakas, 2008) and to ensure that maximal value was gained from the data. To gain a dataset that closely represented the population, various criteria were used.

Participants were either legal professionals (or employees of a law firm) or security professionals. These two types of participants were the most appropriate because this research focuses on ethical hacking of law firms. Participants held a variety of job roles. Law firm participants were either partners or employees of law firms who were direct decision-makers, owners, management or personnel subject to the services of an ethical hacker, either directly or indirectly (they stored or accessed information or a system that an ethical hacker may test or gain access to). Also included in the study were consultants and management-level personnel that provide ethical hacking services or occupy security advisory positions that consult law firms. These participants included personnel at varying levels, such as technical, non-technical and management positions.

Participants occupied varying job levels. By selecting participants at varying job levels, data were obtained about participants’ experiences and knowledge at different stages of their careers. For example, more senior professionals would typically have more responsibility than those early in their careers.
Participants from Australia and the USA were selected for this study. The purpose of considering this international context was to gain insight into cultural, legal and regulatory variances and how these might affect the data. These countries were selected as they are perceived to sit at two different maturity levels, from both cybersecurity and legal system perspectives. The US legal system is approximately 40 years older than the Australian system and is generally more complex because laws often vary from state to state. The Federal Judiciary Act was signed into law on 24 September 1789 by President George Washington (Warren, 1923). Australian laws, by contrast, date to 1828, when the Australian Courts Act came into effect, ensuring that English laws could be enacted in the two Australian colonies at that time—New South Wales and Van Diemen’s Land (now known as Tasmania) (Castles, 1963).

Some potential issues arise from the use of purposive sampling—the most common of these is bias. To address this concern, data were collected from a broad range of interview participants, geographies and organisation types. Participants were from different organisations across Australia and the USA, possessed different levels of seniority and experience in their career and were different genders. The researcher’s experience played a key role in participant selection. Further details about the researcher are provided in Appendix I.

### 3.1.3 Data Gathering

The methods used to gather data were interviews and observation—two common methods of interpretivism. An understanding of the key issues was obtained from the initial review of the data. Next, analysis of the collected data was able to begin, while additional interviews were also conducted. This allowed the identification of any variances that occurred, either between different types of participants or across borders, and allowed in-depth exploration of how these issues affected law firms.
3.1.3.1 Interviews

Intensive interviews were conducted either face-to-face, via Skype, or telephone call. Participants’ demographics and interview questions are described in the following sections. Permission from each participant was obtained using the ‘Participant Consent Form’, approved by the HREC (provided in Error! Reference source not found.). In addition to the consent form, an information sheet (found in Appendix H) provided details of the research project, how data would be handled and how a complaint could be lodged if required.

3.1.3.2 Observations

Due to the paucity of research on this topic, observation provides an effective way to understand the behaviours of people working in this field. For this study, the information security functions of a law firm were observed by the researcher to see how they interact with ethical hackers during a typical engagement. This included the steps and measures taken to begin, operate and conclude an engagement. Ethical hackers were observed to see how they conduct their assessments, in addition to any interactions before they are hired, such as the interview process. Creswell (2009) noted that observations are useful for identifying unusual aspects and topics that may be uncomfortable for participants (Creswell, 2009, p. 179). Observations of interest obtained through the course of day-to-day professional experience were recorded in a journal with the date of the observation.

3.1.3.3 Existing Frameworks and Standards

There exist various well-known and widely adopted frameworks and standards. Standards such as ISO/IEC 27001:2013 and the NIST CSF (as identified in Section 2.1.3.13) likely contain controls that could be used to develop a more tailored and specific framework for conducting due diligence for ethical hacking professionals.
In developing the proposed framework, existing frameworks and standards were reviewed and appropriate controls included.

### 3.1.4 Data Recording

Data collected through interviews were recorded using three main tools:

- Pamela Call Recorder for Skype interviews
- Phillips Dictation iPhone app for in-person interviews
- TapeACall iPhone app for conventional PSTN/mobile phone calls.

All participants were notified prior to the commencement of call recording and permission was formally obtained as part of the consent process. A record of each interview was saved into the Interview Master sheet (see Appendix C), which contains the following high-level information:

- Date—the date the interview took place
- Country—the location of the participant being interviewed (either Australia or the USA)
- Experience—the level of the participant (e.g., lawyer, partner, ethical hacker, security director)
- Gender—the gender of the participant
- Type—whether the participant was from a law firm/legal department or an ethical hacking/security company
- Reference to the recording—the name used to link the recording to the line item in the Interview Master sheet
- Authorisation—whether a consent form had been sent and received (the sheet was used for tracking prior to interviews, all interviews were conducted with consent)
- Checksum—the SHA256 hash of the audio recording to ensure integrity.
3.1.4.1 Preliminary Review of Interviews

Upon the conclusion of the interviews, a preliminary review process was undertaken to ensure interviews did not contain any identifying information. Identifying information included:

- interviewee names
- names of others
- company names.

If identifying information was disclosed, the specific identifying information was redacted by removing the audio data directly within the waveform in that particular part of the original file, resulting in a short silence. The file’s signatures were then hashed, recorded in the Interview Master sheet and sent to the transcribing company for processing.

Data collected through observations followed an observational protocol: either a paper system divided into two-column sections (one for the observation and one for any detail) or the Day One application. Day One records the date of the observation, the narrative and the location of the observation.

3.1.5 Data Storage and Security

Collected data were anonymised and secured. Generic demographic information, such as position (e.g., partner, lawyer, ethical hacker or director), the interview target (e.g., legal firm or consulting firm), gender and country, was maintained. To ensure confidentiality and integrity, the collected data were stored on a BitLocker encrypted drive protected with a strong password (in line with industry best practices). The data are constantly backed-up to a zero-knowledge, cloud-based encrypted drive (SpiderOak). Hashes of the data were maintained to retain integrity. Only authorised personnel (the primary researcher and supervisors)
have access to the data, as described in the participant information sheet.

3.2 Research Scope

This research focused on issues of professionalism (professional ethics) relating to the ethical hacking of law firms. This includes ethical considerations and obligations that lawyers have to their clients and those of ethical hackers who conduct engagements with legal clients. The study aimed to identify if the use of a regulatory approach or (at a minimum) a mandatory and uniform code of conduct will add value to the ethical hacking profession.

The scope of the research participants and, subsequently, research data are limited to legal firms and security consulting firms in Australia and the USA. To ensure diversity among the samples, law firms and consulting firms that offer ethical hacking or penetration testing services of different sizes were included; further, within these firms, participants of varying experience, job roles, seniority and gender were included.

3.2.1.1 Limitations

Some limitations of the research were identified. For example, participants from the USA were often more difficult to involve due to time zone variations, the inability to conduct interviews in person and general reluctance to discuss sensitive topics.

3.2.1.2 Questioning

Creswell (2009) recommended the use of one or two central questions, with no more than five to seven sub-questions, in qualitative research (p. 129). This method is intended to narrow the focus of the study, but allow for questioning. Initially, the research included two central questions that aimed to gather data specifically about the views, opinions and ethical
concerns that surround ethical hacking. The second question, which varied depending on the audience (law firm v. consulting firm), concerned whether lawyers were aware of such services being used (for law firm participants) or ethical hacker behaviours and processes (for ethical hacking participants).

During the initial interviews, it became apparent that some additional areas required exploration. These additional areas offered to address potential solutions to ethical issues in the cybersecurity field. The first was the implementation of regulation for ethical hacking. As lawyers themselves are subject to governing rules that are required to practise, this was unsurprising. The second was continuing education for ethical hackers and related ethical issues.

To conduct this research, four out of the five core research questions were asked of interview participants (depending on the type of research participant). The following questions formed the basis of the interview process:

1) When it comes to conducting penetration testing, or ethical hacking of law firms, are there any ethical considerations or issues of professionalism that come to mind?
   a) If issues are identified, do they relate to:
      i) The organisation in delivering services to the client?
      ii) The ethical hacker in providing services to the legal firm?

2) This question was only asked of law firm participants
   To your knowledge, has your firm ever engaged the services of an ethical hacker to conduct penetration testing?
   a) If you have:
i) Was appropriate due diligence conducted?

ii) What type of testing was conducted?

3) *This question was only asked of consulting firm participants*

When conducting penetration testing against law firms, have you ever been able to or had access to client confidential information?

a) If you have, did:

i) You immediately alert the client to the fact?

ii) Take any of the information as evidence?

4) What is your opinion on the regulation of ethical hacking and do you think it will benefit or hinder the profession?

5) Security is a field that can change on a daily basis. To help ensure an ethical hacker conducts a thorough test, they need to practise continual professional development. There are multiple ways that this could occur: reading articles, tinkering with software, participating in forums or attending conferences. Given the type of information an ethical hacker would be looking for, are there any issues that can be identified?

It is important to limit the response bias encountered in interviews. Therefore, the questions were worded in such a way that bias is limited. They were not: ambiguous, too complicated, filled with jargon or not loaded in such a way that they encourage a particular response. Additionally, participants were anonymised (as described in Section 3.1.5).

### 3.3 Chapter Summary

This chapter described the research methodology used for this study. Due to the paucity of research in the area of professionalism issues
concerning ethical hacking law firms, exploration is necessary and qualitative research was selected as the most appropriate methodology.

A constructivist approach was selected due to the need to interpret elements of the collected data to identify issues of professionalism that might exist. Other potentially suitable methods, such as grounded theory and case study, were excluded. Grounded theory was excluded primarily because a constructivist approach that uses interpretivism was more suitable as it relied on the experience of the researcher. The case study method was excluded because the research did not focus on a single firm.

Interpretivism relies on the ability of the researcher to interpret the data. The researcher’s nearly two decades of professional experience addressed this concern. There were also some issues related to disclosure of information, because some of it may be considered sensitive. Approval to conduct the research was obtained through the HREC and strict security protocols were followed. Bias formed another concern; this was addressed through the diversity of interview participants (e.g., experience, type of participant, gender and location) and ensuring that questions were not ambiguous or leading in any way.

The primary method for gathering data was interviews; however, observations were also recorded during the researcher’s professional experience.
Chapter 4: Findings and Results

Upon concluding the research, the results were divided into different categories. The first was observations made from the participant data, such as sample size, type of participant and various participant characteristics, such as position and experience, country and gender. The second category was analysis of the data, as it related to the research questions on professionalism, ethics and ethical hacking of law firms. This process of analysis separated the data into key themes and categories within those themes.

4.1 Interviews

Interviews were conducted with 28 legal, ethical hacking and cybersecurity professionals in Australia and the USA. The interviews were conducted between December 2017 and November 2018. Table 3 shows the breakdown of the interview participants. In selecting research participants, professionals that held senior roles were preferred. Senior participants were identified as those that held job titles such as Manager, Director, or C-level titles such as Chief Information Security Officer (CISO) at law firm business services and consulting firms or legal practitioners at the Partner, Special Counsel, or Senior Associate level. Participants in these roles were more likely to contribute to the research, due to their experience and knowledge of both the industry and, in the context of legal professionals, the law.

<table>
<thead>
<tr>
<th>Type</th>
<th>Position</th>
<th>Number of participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law firm</td>
<td>Information security</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 3. Research Participant Types
Other reasons for seniority preference include observations by the researcher of many law firms over a long career. Legal firms do not typically have dedicated information security teams like those seen in other industries (e.g., financial services). Often, a senior IT team member is responsible for security (this is especially prevalent in smaller law firms) or the firm completely outsources its security requirements to an external services provider (e.g., a consulting firm). Chapter 2 discussed the issue of the skills gap; for example, the Telstra (2016) report found that over 40.4 per cent of respondents in Australia and 46.8 per cent in Asia reported a skills gap. Further, the NAO stated that such a gap could take 20 years to address (Caldwell, 2013). This gap is currently being addressed through an increased focus on cybersecurity in academia, aiming to encourage and develop students to choose cybersecurity as a career. Such offerings include the previously mentioned SEC.EDU offering by CBA and UNSW or the Training Cyber Security Operations Centre at Box Hill Institute. The other common approach involves IT and other professionals moving their specialisation to cybersecurity (either fully or partly) through self-education, training and professional certifications. As the introduction of cybersecurity
degrees is relatively recent, cybersecurity professionals often emerge from a shift in careers; consequently, these professionals are often appointed to more senior roles.

From a legal practitioner perspective, senior lawyers were typically more accessible and more willing to be interviewed. Professional services environments typically have higher billable target requirements for personnel that are less senior. Additionally, those legal staff at associate and lawyer level were reluctant to be interviewed as they believed they were not able to contribute to the topic, given their lack of sufficient experience in the area.
4.2 Observations

The primary researcher also made various observations before, during and after ethical hacking engagements. These were kept in a journal, together with other reflections made during the data-gathering and progressive analysis stages of the research. This journal also forms part of the body of documents analysed and discussed in the following chapter.

4.2.1 Participant Diversity

In addition to the experience level differences described in the previous section, several observations were made during the recruitment process of interview participants. It was generally more difficult to obtain participants from the USA. Based on interactions, this was largely due to participants being time-poor and challenges caused by time zone variations. US participants also tended to be more conservative and were reluctant to be interviewed (despite the anonymity of the interviews). These factors often resulted in interviews remaining unconfirmed or being cancelled. As shown in Figure 3, there were eight participants from the United States; the remaining 21 were from Australia.
Figure 3. Participants by Location

Figure 4 shows that 64.3 per cent of the interviews were undertaken by professionals with more than 10 years’ experience and the remaining 35.7 per cent by those with less than 10 years’ experience. The selection process was conducted primarily through the primary researcher’s professional network of professionals across Australia and the USA and their wider connections. Participants were either directly contacted due to their job roles and the roles’ suitability for the research criteria or through requests for research participants or referrals. Only those participants that met the criteria were selected for interview. The bias towards experienced professionals is best explained by the belief that the participant had value to contribute because they had more professional experience and knowledge to share. The development of ethical knowledge is created by transforming experiences (Kimball, 2018; Kolb, 1984, p. 38, Pelsma & Borgers, 1986, p. 313). As a professional progresses through their career, their day-to-day work and interactions will likely increase their knowledge and experience. They will also be required to make more decisions and, as they become more senior, those decisions may affect more people. Consequently, they will have an increased level of experience in ethical decision-making.
The participants can be divided into three distinct groups: legal professionals (39.3 per cent), cybersecurity professionals (35.7 per cent) and law firm information/cybersecurity staff (25 per cent).

4.2.1.1 **Legal Professionals**

Of the participants classified as legal professionals, 72.7 per cent were considered senior. They held titles such as Partner, Shareholder, Special Counsel or Senior Associate. These four titles are common across nearly all law firms; this is why they were selected for this study. Deviations from these titles are uncommon in either Australia or the USA. Once a lawyer has approximately six years’ experience (although this may occur earlier), they are often promoted to the level of Senior Associate (Donahue, 2015). From the Senior Associate level, a lawyer may then be promoted to one of the higher levels, such as Special Counsel or Partner. A partner may be either salaried or an equity partner (i.e., they have some ownership of the firm) and is responsible for running their practice. In some firms that are based on partner structure, such as those that are incorporated as a company (e.g., Pty.)
Ltd. in Australia or PC for professional corporations in the USA), a partner may be referred to as a shareholder.

4.2.1.2 Cybersecurity Professionals

Of the participants classified as cyber security professionals, 60 per cent were considered to be senior. These possessed experience greater than 10 years and held titles such as CISO, Director, Manager, Penetration Tester or Senior Consultant. These titles were often fairly generic, which is common in professional services. Typically, those that did not hold a Chief, Director or Manager title were responsible for delivery of services. Those that did hold Chief, Director and Manager titles were generally responsible for managing teams of consultants, commercial agreements and the setting up of engagements.

4.2.1.3 Law Firm Cybersecurity Staff

Of the participants classified as law firm cybersecurity staff, 75 per cent were considered to be senior. They held Manager, Director or Chief titles and possessed over 10 years’ experience. Because many law firms do not have specific information security teams or dedicated resources, it was not uncommon for security responsibility to fall within the IT department. This resulted in personnel such as the IT Manager, IT Director or Chief Information Officer being interviewed.

Figure 5 shows that 24 of 29 interview participants were male. There are very few female hackers—the profession is male-dominated (Adam, 2005, p. 130). Therefore, the total number of female security professionals represented in the study is very low. In the field of law, there is an almost balanced ratio of male to female lawyers (Victorian Legal Services Board, 2018). Additionally, women account for 18 per cent of students who earn an undergraduate degree in computer and
information sciences and 26 per cent of professional computing occupations in the USA (Jung, Clark, Patterson & Pence, 2017, p. 26). This is consistent with the dominance of male participants in the research sample.

![Figure 5. Participants by Gender](image)

4.2.2 Analysis

Data analysis formed a continuing process throughout the research, even while additional data was being collected (Charmaz, 2006, p. 5). An iterative approach was used, in which the data and analysis are continually intermeshed; this had a direct bearing on determining when the research would end. As each step of data collection and analysis occurred, the theory was further developed.

As a first step, the process of coding was performed. This involved naming and labelling segments of data to categorise, summarise and account for them (Charmaz, 2006, p. 43). From this point, the researcher identified any themes that were present, how they interrelated and then interpreted these themes.
4.2.2.1 Coding of Data

Each data sample (e.g., observation notes or transcribed interview) was loaded into NVivo. As each sample was reviewed, categories emerged and were used to created nodes. Initially, 23 categories were created (detail of the coding process can be found in Appendix D) and then categorised into six main themes and twelve categories within those themes (see Table 4).
Table 4. Themes and Categories

<table>
<thead>
<tr>
<th>Themes</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality of information</td>
<td>Ethical obligations of legal professionals</td>
</tr>
<tr>
<td></td>
<td>Ethical obligations of ethical hackers</td>
</tr>
<tr>
<td>Professional standards</td>
<td>Continuing professional development</td>
</tr>
<tr>
<td></td>
<td>Competence considerations</td>
</tr>
<tr>
<td></td>
<td>Regulating ethical hacking</td>
</tr>
<tr>
<td></td>
<td>Licensing requirements</td>
</tr>
<tr>
<td>Conflicts of interest</td>
<td>Conflicts due to information access</td>
</tr>
<tr>
<td></td>
<td>Cross-practice conflicts</td>
</tr>
<tr>
<td>Onboarding process</td>
<td>Due diligence</td>
</tr>
<tr>
<td></td>
<td>Scoping of engagement</td>
</tr>
<tr>
<td>Differences between Australia</td>
<td>Legislation and regulation</td>
</tr>
<tr>
<td>and the United States of America</td>
<td>Privilege requirements</td>
</tr>
<tr>
<td>Values-based findings</td>
<td>Trust</td>
</tr>
<tr>
<td></td>
<td>Reputation</td>
</tr>
</tbody>
</table>

Confidentiality of information. Confidentiality can be defined as ‘preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information’ (McCallister, 2010). Law firms handle vast amounts of such information and are subject to legal professional privilege requirements;
therefore, it is not unexpected that this would emerge as a key category. Within this category, the key identified themes centred on the ethical obligations of both lawyers and ethical hackers around confidentiality and ensuring that confidentiality is maintained.

**Professional standards.** Both lawyers and ethical hackers are considered experts in their respective fields; as highlighted in Chapter 2, professionalism is of high importance for this research field. Findings that were best aligned with the category of professional standards were prevalent in the research data. Professional standards are a set of rules and guidelines prescribing how a professional should conduct themselves within their profession. Within this category, identified themes included requirements about the significance of an ethical hackers’ competence and how continuing professional development, regulation and licensing may assist to ensure this.

**Conflicts of interest.** According to the Australian Public Service Commission, conflicts of interest occur in the presence of influential factors that fall outside of those that are relevant (2019). Due to the nature of the information handled by law firms and the possibility of its misuse (e.g., through insider trading), identifying and addressing potential conflicts of interest is of high importance.

**Onboarding Process.** Another key category involved the process used to onboard ethical hackers at the commencement of an engagement. This process is designed to help ensure that all the correct agreements, validations and other rules are in place before allowing the professional access to the systems. This includes engagement letters, NDAs and background checking.

**Differences between Australia and the United States of America.** The study aimed to identify key differences between Australia and the
USA; therefore, this is a key category. Key identified themes related to legislation and regulation and the requirements of legal professionals.

**Values-based findings.** Several outliers were also identified, including a small number of values-based findings that were related to interpersonal trust and reputation. These values apply to multiple categories, which highlights the significance of these outliers and the resulting need to include them.

Although these findings were outliers within the dataset, they are significant due to the weight that they carry. When considering professionalism and professional ethics, the significance of these values cannot be understated. For example, to promote a profession, a culture of trust in the profession and among individuals must exist. Simply attempting to control unethical behaviour using codes, legislation or other regulations may not be successful (Brien, 1998). Likewise, a relationship between trust and reputation has been identified, in which both values may influence the experiences of people and that a good reputation is valued (Holste & Fields, 2010). These areas are discussed in further detail later in this thesis.

Key themes identified by the study are grouped below in Figure 5. Confidentiality was a key finding, identified in every interview. Other key findings related to the process of ensuring that engagements had the right controls in place and other items relating to due diligence and scoping, as well as profession-related controls such as regulation, oversight and standards.
Each category in Table 4 is explored in further detail in the following sections.

4.2.2.2 Confidentiality of Information

Maintenance of the confidentiality of client information was identified as the most frequent and important requirement. Sixty-seven per cent of research participants highlighted confidentiality as a key consideration when engaging the services of a penetration tester. Of all participants, legal professionals were the most concerned with confidentiality; 90 per cent of legal professional participants highlighted the concern (see Figure 7).
The emphasis of confidentiality by legal professionals is unsurprising because law firms are trusted by their clients to handle potentially highly sensitive information and have an ethical obligation to protect that information. One Australian lawyer stated that ‘we need to ensure that client confidences are maintained because that’s one of the real primary reasons why clients come to a law firm. They have an expectation of absolute confidence in relation to their confidential information.’

The protection of information a law firm holds is critical, but could also have negative consequences. Allowing an ethical hacker to gain access to sensitive information could have serious implications for maintaining privilege; however, clients also expect that firms have appropriate security systems that require independent validation. Although independent validation has not yet been prescriptively defined, it is common practice that services such as conducting a penetration test or attempting to ‘hack’ the firm are utilised. One Australian lawyer stated that ‘clients need to have absolute faith when they engage a lawyer that the flow of their information remains private and is protected’.

Figure 7. Confidentiality Concern by Participant Type
In relation to the confidentiality of information, two ethical perspectives must be considered: the ethical obligation of legal professionals and the ethical obligations of ethical hackers. These two perspectives are explored further in the sections below.

4.2.2.3 Ethical Obligations of Legal Professionals

Lawyers have an ethical obligation to their clients that requires them to maintain the confidentiality of their information. Legal professional bodies in all states of Australia (except for Tasmania) have adopted ‘codes of professional conduct’ (Dal Pont, 2017, p. 24). This adoption is relatively recent, however, commencing in the late twentieth century. Although these codes previously existed in many states, they were not always uniform and, as noted, not all states adopted them. In 2011, the LCA promulgated the Australian Solicitors’ Conduct Rules: a set of professional obligations and ethical requirements for all Australian solicitors (LCA, 2018).

By contrast, the ABA first adopted its ethical code in 1908. This was named the ‘1908 Canons of Professional Ethics’ and was later superseded by the ‘Model Code of Professional Responsibility’ in 1969 and the ‘ABA Model Rules of Professional Conduct’ in 1983 (ABA, 2018).

Both countries’ codes include requirements relating to the confidentiality of information. The ABA rules, for example, require that:

A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorised disclosure of, or unauthorised access to, information relating to the representation of a client. (Rule 1.6(c), ABA, n.d.)

The Australian equivalent of the ABA rule is more detailed, yet still requires confidentiality be maintained in relation to client privileged information:
A solicitor must not disclose any information which is confidential to a client and acquired by the solicitor during the client’s engagement to any person who is not: a solicitor who is a partner, principal, director or employee of the solicitor’s law practice; or a barrister or an employee of, or person otherwise engaged by, the solicitors law practice or by an associated entity for the purposes of delivering or administering legal services in relation to the client. (LCA, 2018)

Compared to the confidentiality requirements of the ABA rules, the Australian rules appear to allow greater flexibility regarding to whom information may be disclosed.

Beyond confidentiality rules, there are ethical requirements for a lawyer to act in the best interests of the client; this requirement is broad and requires more detailed discussion. The current de facto standard for addressing this requirement is the implementation of contractual control, such as an NDA. Such agreements are designed to prevent the other party from disclosing information; a breach of the agreement would likely result in legal ramifications and, potentially, reputation damage. Lawyers are also required to undertake ethics training, which includes requirements regarding how client information is handled and may include the requirement to notify their clients if a particular client’s data are accessed by a third party. Should an ethical hacker gain access to client data as part of the engagement, there may be considerations related to notifying the client.

*We have a duty of confidentiality to our clients. Now that is managed in some ways through reciprocal confidentiality agreements that are imposed upon pen-testers. But I think there is always an inherent uneasiness about the potential that a pen-tester may access some client’s information. (Partner, Law Firm, Australia)*

It was also clear from the data that legal professionals rely on their internal operational teams (e.g., information security or IT team) to handle the organisational security, including the engagement, due
diligence and oversight of ethical hacking and penetration testing engagements. Legal professionals are not generally aware if this type of testing takes place, or of the process and what is involved. Often, best practice procedures and processes are inconsistently followed, which may result in increased risk.

Further, in some cases, the sensitivity of information is not fully understood. This has been observed by personnel at all levels within legal firms, both legal and non-legal professionals. This lack of understanding is often, but not always, more prevalent in junior staff. The task of engaging and managing ethical hackers is often delegated to operational staff; therefore, there may be an increased risk that sufficient controls and processes have not been initiated.

_The impression that I got, particularly from junior staff, but even some very experienced staff, was that they didn’t understand—until it was pointed out to them—how important data was in terms of client information, personally identifiable information, transactional records, and business strategies. This type of information generally sits inside the document management systems of law firms._ (Director and lawyer, consulting firm, Australia)

Often, because the tasks of maintaining security and managing information falls to the internal operation teams, there may be no delineation between firm information and client information: 'law firms tend to forget at least on a business side that a lot of the data we hold is not our data [and] we’re holding it on trust for our clients' (Lawyer, USA).

This may have significant consequences for both the firm and the clients that the data relate to. The risk of confidential or proprietary information being exposed could have significant reputational and financial consequences.
4.2.2.4 Ethical Obligation of Ethical Hackers

Ethical hackers have an obligation to ensure that the use of any information gained through the course of an engagement is ethical. As part of an ethical hacking engagement, evidence of a successful breach is often taken as proof of a successful outcome for the tester. This evidence is useful in ensuring the integrity of the report, particularly if a finding is disputed.

We have occasions where the client will dispute something that we may have found so we need evidence that we actually did find that. So, every single time we list a vulnerability on a report, there has to be factual evidence to support that. So, if it was ever challenged, we have the evidence to prove that was in the system. (Ethical hacker, Australia)

Any information captured as evidence of a successful test objective would generally not contain sensitive client data; however, it may contain other sensitive operational information, including information on the vulnerabilities and steps to reproduce and exploit any identified vulnerability. This collection and use of evidence can be connected to the significance of the values-based findings, in which both trust and reputation are key. There must be trust in the ethical hacker, including a belief that they will behave ethically and handle the information they obtain accordingly. From the interviews with ethical hacking and consulting professionals, it was identified that information of a sensitive nature would be securely stored and is generally destroyed shortly after the conclusion of the engagement. Further, any reports containing the information are only retained for a finite period before being destroyed.

As one director pointed out, ‘some organisations want us to keep their reports on our file exchange, our web-based file exchange thing because it’s convenient for them. And that’s against our policy. We just don’t do it’ (Director, consulting firm, Australia).
Another key point is that non-legal professionals, such as ethical hackers and IT professionals, do not generally comply with the regulations required by legal professional associations, such as the Legal Services Board or Bar Association:

*I think that an IT person is not governed by the Bar Association’s Code of Conduct and it’s not necessarily that they shouldn’t be, but there’s no process for it. Every non-attorney is not going to review the entire Code of Ethics for the relevant state’s Bar Association, or for that matter, necessarily understand what it means.* (Security Director, law firm, United States)

This gap means that the requirements of legal professionals, including confidentiality, do not necessarily extend to the professionals that may gain access to confidential and privileged information.

The ethical standards available from various certification and professional bodies provide requirements regarding dealing with confidentiality; for example, CREST requires that: no information about clients is to be disclosed to any third parties, all information is adequately safeguarded to preserve confidentiality, professionals maintain their competencies and professionals act ethically and comply with all applicable laws and regulations (CREST, 2016). Similarly, the EC-Council Code of Ethics requires that professionals: keep information they gain during their engagements as private and confidential, use their skills to protect the intellectual property of others and are competent and honest (EC-Council, 2018). In Australia, the ACS Code of Ethics requires that professionals be honest, competent and maintain a level of professionalism that enhances the integrity of the ACS and its members.

### 4.2.2.5 Professional Standards

Professions such as lawyer, doctor and accountant have formal professional standards bodies; membership of these is mandatory for practice. For relatively new professions such as cybersecurity (or ICT in
general), while there are associated professional standards bodies, membership is not required to practise. As in the ACS example above, a professional standard body generally has a code of ethics or conduct that must be adhered to—this is a requirement for continual professional development. The requirement for continual professional development in the field of ethical hacking raises some questions regarding both the need for such a requirement and also the methods and implications for obtaining knowledge and further developing skills. Of the research participants, 50 per cent of ethical hackers and consultants, 70 per cent of legal professionals and 75 per cent of law firm security personnel discussed professional standards for ethical hackers (see Figure 8).

![Bar chart showing discussed professional standards for ethical hackers](image)

**Figure 8. Discussed Professional Standards for Ethical Hackers**

Enforcing professional standards would be most likely to affect ethical hackers and potentially provide a hindrance; therefore, it was expected that this group would be less likely to raise it, compared to the other two groups who have more to gain from such regulation. However, many of the ethical hacking research participants saw professional standards and regulation as generally positive. Although the research does not directly provide much detail as to why this is the case, it is notable that the professionals interviewed are perceived as leading experts from
highly reputable organisations. One theory is that such professionals are advocates for the profession and would regard such regulation as assisting to mature and improve the profession. Another theory is that such regulation could assist in identifying rogue and incompetent ethical hackers, who are detrimental to the profession.

4.2.2.5.1 Continual Professional Development

Often, continual professional development forms part of professional standards. Continual professional development is crucial for ethical hackers. For an ethical hacker to remain at the top of their field and stay abreast of the latest threats and vulnerabilities, they must continue learning. There are multiple potential sources for learning, including reading; conducting lab exercises where a professional configures systems in their own private environment and then attempts to hack into them; attending conferences (e.g., Blackhat, RSA and Defcon) or participating on dark web forums and downloading malware and exploits from the dark web.

I think penetration testers would need to spend some time on the dark web to see what’s out there and also to brush up on their skills and stay on top of the ever-changing field. (Cybersecurity Professional, law firm)

Penetration testers must employ varied and diverse methods for obtaining information about the threat landscape; for a tester to remain at the top of their field and be effective, they must continually research what threats are out there and develop their skills. To elucidate this point, some context regarding the changing threat landscape will prove useful. In 2018, 16,555 vulnerabilities were identified and added to the Common Vulnerability and Exposures (CVE®) list, a well-known industry source of vulnerabilities (MITRE Corporation, 2019).

You need to know where the new exploits are, you can’t effectively run a pen test if you don’t know how the systems are
going to be exploited, and with the rapid pace of change [in cyber security] - reading a book that was written nine months ago and published three weeks ago, is essentially pointless. The threat landscape changes so quickly. (Director, consulting firm, Australia)

There may be ethical implications and considerations related to such practices, particularly those that involve communicating on the dark web or associating with malicious hackers. In some cases, legal boundaries may even come into question.

*I think it really comes down to the individual’s ethics and values, and I think someone who is or has good ethics, won’t be affected by some of the things they find on the dark web*  
(Cybersecurity professional, law firm)

Another key discussion point identified the potential need for a framework or guidance when continuing professional development might require the use of questionable methods, such as attending hacking conferences and using the dark web. Providing some sort of oversight and guidance may assist to reduce the risk that unethical behaviour may occur as the result of such activities. However, competence issues may arise if ethical hackers are not given enough freedom to effectively gain the knowledge that they need due to overly stringent guidance. Similarly, oversight might prove ineffective without some sort of auditing component.

4.2.2.5.2 Competence Considerations

Another key area for discussion was competence. Due to the ever-changing nature of cybersecurity, ethical hackers must be competent in conducting engagements. An ethical hacker needs to have a baseline level of knowledge and competence to ensure that the tester not only provides a minimum level of testing but does not create any adverse effects. An inexperienced tester could cause an outage during the
engagement, which may create significant negative consequences, particularly in environments that require high levels of system uptime.

*It is possible that an inadvertent denial of service results. But, I mean, it'd depend on the skill of the penetration tester. (Chief Information Officer, law firm, USA)*

Another key consideration was the value of certification and how this relates to competence. Different certifications have different reputations within the industry; some certifications are held in higher regard and provide greater levels of credibility. Many of the ethical hacking firms included in this study held similar certifications, which they believed were more valuable and resulted in a more skilled and competent professional and, subsequently, a better quality of work.

*Some firms will talk about how they’re CREST-certified and all their pen-testers have this certification and it’s all very formalised. On the other hand, there’s particular certifications you can get that aren’t as credible; you tick a box and [they’re] multiple choice. The more difficult certifications require the pen tester to actually conduct hacks within 48 hours, or capture the flag—these kinds of things. (Director, Cybersecurity firm, Australia)*

### 4.2.2.5.3 Regulating the Profession

The topic of regulating ethical hacking was discussed in several instances; views varied as to whether regulation would advance or hinder the profession. Both clients and ethical hacking firms provided arguments both for and against regulation. Most regulatory standards are inherently inefficient; they are often only optimal for the average firm, due to less knowledge and incentive for those that create the requirements (Scholz, 1984, p. 392). Key benefits of regulating ethical hacking include mandating a minimum standard that all professionals must abide by. Regulation would also allow better enforcement action and subsequent consequences, such as financial penalties and
removing the right to practise—these could be used to discourage unethical behaviour.

By chartering and coming together as a regulated professional organisation, you can explore whether things like insurance, standards, and discipline are mandatory. Effectively like doctors and lawyers, which is to say that you are not entitled to practice without this certification. (Partner, Australia)

Conversely, the implementation of regulatory requirements may have several disadvantages; these will be explored in further detail in the next section. Ethical hackers (and hackers in general) often break the rules. For an ethical hacker to perform their job effectively, they must work outside customary bounds. They think ‘outside of the box’ to determine how a system works and then identify how to break those rules to manipulate the system they are testing.

For this reason, they may struggle to adhere to regulatory rules, particularly if these impede how they work effectively. Another concern is that compliance with regulatory requirements may suggest that an ethical hacker is competent when they are, in fact, not. This may occur if regulatory requirements are insufficient, often a result of requirements being developed by those that lack the required knowledge.

The costs and requirements associated with regulatory compliance are also an important consideration. For smaller cyber security firms such as start-ups and boutique firms, in particular, this could result in less innovation due to the inability to afford the regulatory requirements. Regulation may also increase the cost of conducting tests, thereby discouraging organisations from engaging ethical hacking professionals, in turn resulting in increased risk.

In the absence of regulation, organisations such as CREST (which originated in the UK but has launched chapters around the world) have been established to provide a level of assurance that security staff are
competent and qualified in conducting security work including penetration testing (Thomas et al., 2018).

*I think as an industry, hackers may need to look into being recognised as a profession for the purposes of obtaining [appropriate] insurance. Solicitors, accountants, doctors for example, each through our various societies have a limited liability scheme. (Partner, law firm, Australia)*

### 4.2.2.6 Issues with Regulation

Although there are many advantages to taking a more regulatory approach to ethical hacking, several concerns were also identified; these could result in regulation being ineffective or cause negative outcomes for the broader profession. Concerns relating to the cost of regulatory compliance was raised by several participants, particularly how those costs would affect smaller and start-up firms. Further, there were concerns that the cost of such compliance requirements would inevitably force up the price of cybersecurity services, resulting in decreased engagement of such services:

*Cybersecurity is expensive enough as it is, I know how difficult it is for many IT managers and CIOs to secure the funding to get ongoing penetration testing and security checks done, so adding another ten or fifteen per cent to cover mandatory compliance may result in smaller organisations ceasing to exist, and larger organisations simply charging more. (Director, consulting firm, Australia)*

Technology is always evolving and changing; innovation and evolution are required in the ethical hacking field to ensure effective assessment of systems. In 2017, 15,038 new vulnerabilities were identified; further, the first half of 2018 has seen a 27 per cent rise in new vulnerabilities (Hackney, 2018). Innovation often originates in start-up organisations; despite reduced capital, the entrepreneurial model proves to be a good vehicle for the development of breakthrough innovations (Freeman & Engel, 2007, p. 94). An additional burden of compliance (and associated
costs) may deter start-up organisations, particularly those that are not well-funded; therefore, innovation within the profession may be stunted:

> In my opinion, if you force everyone down that regulation path – there is a cost involved. For example, CREST is not cheap to an organisation like ours...For a smaller company to do that, if you were to force them to regulate or something similar to that, that's just raised the bar for them to provide boutique services per se. (Director, cybersecurity firm, Australia)

Participants also raised concerns about who was responsible for creating specific regulatory requirements and professional standards. Recent events in Australia’s financial services sector such as the Financial Services Royal Commission (Royal Commission, 2018), for example, have cast some doubt on the effectiveness of regulation:

> There are two main issues I can see with regulation; firstly, the compliance, who's doing the checking, and more importantly, who’s responsible for that checking? As we saw with APRA [Australian Prudential Regulation Authority] and ASIC [Australian Securities and Investments Commission], you can have all the rules in the world, but if someone isn't enforcing them, then they're essentially pointless. (Senior Consultant, consulting firm, Australia)

Finally, the difficulty of regulatory compliance may form another issue:

> My concern though, is that if you put that [regulation] in place and have in effect, a system where you can’t work as a pen tester without being a member of SANS or ACIS or something like that, and have to go through the CPD [continuing professional development] requirements, then you’re going to dissuade people. (Director, consulting firm, Australia)

The study identified that law firms were generally in favour of regulating ethical hackers, believing that appropriate regulation would have positive effects, assist to advance the profession and help reduce the risks associated with engaging ethical hackers. Ethical hacking and consulting firms also viewed regulation as a potentially positive step; however, some highlighted several issues around ensuring that
regulation was appropriate, would not create a significant burden and would allow ethical hackers to continue effectively operating.

4.2.2.6.1 Licensing

Questions around licensing, as opposed to specific regulation, were also raised. Licensing would generally apply to individual ethical hackers but could also apply to ethical hacking firms. For example, Singapore has proposed a bill that would require cybersecurity providers of penetration testing services (and security operations centre services) to be licensed (CSA Singapore, 2018). Such licensing was comparable to that of law enforcement and their ability to perform certain activities (e.g. exceeding the speed limit) in order enforce the law.

As previously discussed, continual professional development is key to ensuring that adequate skill levels are held by ethical hackers; however, such development may also have disadvantages, particularly if it leverages controversial resources such as the dark web.

4.2.2.7 Conflicts of Interest

Issues arising from conflicts of interest were identified by 22 per cent of research participants. Although this is a relatively small proportion, conflict of interest remains a significant issue for legal practice. Further, it was clear from the research that this area had not been (but should be) given much thought in the context of third-party engagement.

The two areas of conflict that arose from the interviews were related to the access of information obtained through the course of a penetration testing or ethical hacking engagement and providing advice when the consulting organisation is not truly vendor-agnostic. Ensuring the absence of conflicts of interest is crucial for ensuring independence and avoiding bias and unethical use of information:
It’s one of those things, the rules around conflict are such that if there is – well, I mean, the rules aren’t hard and fast, and that’s part of the problem – but the issue comes, it’s that nebulous concept, if people might reasonably perceive that there is a bias or a potential for bias, then you’re conflicted. (Director, consulting firm, Australia)

4.2.2.7.1 Conflicts due to Information Access

As previously established, ethical hackers may gain access to potentially sensitive information. Such access generally demonstrates a successful outcome for the testers; however, this kind of information may also be subject to inappropriate use. Law firms deal with many matters that are subject to conflicts, such as merger and acquisition transactions. Another consideration relates to information that is subject to legal privilege and held by two opposing firms. It is possible that the same ethical hacker could be engaged to test both organisations and may gain access to information on both sides, generating a conflict of interest.

When a legal or accounting professional works on a new issue, they are generally subject to conflict-checking to ensure that no conflicts of interest exist:

You have to choose your tester carefully. For example, if you have an accounting firm that does penetration testing and they penetration test a law firm and come across data which is relevant to one of their [other] matters, then you have a potential information barrier breach. (Senior Management, law firm, Australia)

Although conflict-checking is commonplace in legal and accounting firms (including those that provide cybersecurity and ethical hacking services), such as the ‘Big Four’ (the four largest professional services firms in the world), conflict-checking is not typically practised by most ethical hacking organisations: ‘I don’t think we ever had a conversation about
conflicts, both internally when I was in-house, and now, as an external consultant’ (Director, consulting firm, Australia).

4.2.2.7.2 Cross-practice Ethics

Another potential conflict is related to cross-practice. It is often the case that ethical hackers are employed by firms that perform services aside from ethical hacking. Often, these firms engage in other practice areas and related vendor partnerships that supply products and services to their client base. It makes commercial sense to do so as these other practice areas provide additional revenue streams, while still remaining under the broad banner of ‘cybersecurity’, however, this creates another potential conflict. ‘Are they [ethical hackers] identifying those areas of risk purely because they can solve the problem through a partnership they have, or is it a genuine risk that you [the client] have as an organisation?’ (Cybersecurity professional, law firm, USA).

One general observation is that ethical hackers within consulting organisations are separate from those consultants that sell and implement products and services, which may address a direct conflict of interest.

4.2.2.8 The Onboarding Process

The procedures that are carried out when engaging the services of an ethical hacker, known as the ‘onboarding process’, were identified as the most stringent form of risk management at present.

4.2.2.8.1 Importance of Due Diligence

Due diligence was highlighted as a crucial practice when engaging any party, not just ethical hackers. However, because ethical hackers can potentially access highly sensitive data, appropriate due diligence is critical: ‘there’s an expectation that in the same way that a law firm has
vetted all of its lawyers that a cybersecurity company has done a ridiculous amount of background checking on their staff’ (Director, consulting firm, Australia).

In discussions with legal professionals, all respondents believed that adequate due diligence was undertaken when engaging ethical hackers; however, they were not familiar with the process or compliance with such checking. The task of conducting due diligence was generally delegated to others in the organisation, typically the IT department or information security department.

The expected process of conducting due diligence included gathering client references (of the consulting organisation) and conducting background checks on individuals. Although conducting criminal and financial (e.g., credit report) checks undoubtedly has merit, such practices were generally not typical when engaging a consultant. Further, the practice of conducting due diligence checks was inconsistent, not only between organisations but within the same organisation over multiple engagements with different parties.

Several participants indicated an assumption that background checks and other due diligence activities were undertaken by the party being engaged (e.g., the ethical hacking company):

There’s an expectation that, in the same way that a law firm has vetted all of its lawyers, that a cyber security company has done a ridiculous amount of background checking on their staff. (Consultant, Australia)

If they have been employed by an organisation to test you would think that they have adequate agreements in place that would apply to whoever is testing and prevent them from doing something outside of the bounds of whatever has been agreed to. (Lawyer, Australia)
It was observed that the larger firms are more likely to conduct thorough due diligence. This is not unexpected, because larger firms typically have greater resources and more formalised processes, including the formation of committees and bodies that are dedicated to risk management. ‘We don’t do anything without a million checks on service providers. It (engaging an ethical hacking firm) would’ve gone to a specific subcommittee and it would have gone to the board. There definitely would have been a review process’ (Partner, law firm, USA [1500+ attorneys]).

4.2.2.8.2 Scoping of Engagements

One key consideration when conducting an ethical hacking engagement is ensuring appropriate scope of engagement. Understanding where critical data and systems reside assists in reducing the inherent risk of conducting such tests. Although many firms know where their resides (e.g., in repositories such as document management systems, email mailboxes, archiving stores and even in filing cabinets in physical paper form), they may not know the exact nature of the data or be able to easily identify it.

*Pen-testers themselves were very conscious of not having an impact on the system, but I think where issues came was that, I think the firms themselves, sometimes don’t know where their data sits, particularly for smaller and mid-tier firms, and particularly firms that have merged, there can be repositories of data that people just aren’t aware of.* (Director, consulting firm, Australia)

Another issue that arose from interviews relates to the effectiveness of a test when some information or systems are not included as part of the engagement’s scope. It may make sense to scope out data that have specific requirements around confidentiality, such as highly sensitive matters. However, if these have special controls, or if the out-of-scope item is an entire system, this may result in an inadequately thorough
test, because that control cannot be adequately tested or that particular system assessed for any vulnerabilities. ‘When engaging penetration testers, a process that includes scoping is important to potentially scope out highly confidential information’ (Director [lawyer], Australia).

Scoping does, however, reduce risk by helping to ensure confidentiality of data and minimise possible disruptions. For example, some systems may be sensitive to attack, even something as simple as a port-scan. Such systems might subsequently go offline if assessed, causing business disruption. Being able to specify which systems can be tested and when may help to mitigate this risk: ‘you can identify a system as critical. You could specify to hit this [system] on a Saturday or maybe do it after hours. Perhaps a more targeted penetration testing rather than just guessing and hitting an entire network’ (Lawyer, Australia).

In many cases, the client may not be aware of what should be in or out of scope; therefore, they rely on the ethical hacker (or consulting firm providing the services) to help scope the engagement. This requires the consultant to understand the client’s environment and how law firms operate. This knowledge will assist in defining the scope through asking specific and relevant scoping questions. Several interview participants expressed that they were unaware of where all critical data reside within their network.

4.2.2.9 Contrast Between Australia and the United States of America

The findings indicate both similarities and differences between professionals in Australia and the USA. From a legal professional perspective, client confidentiality was the primary concern for all interview participants from the USA. Differences largely related to the due diligence process and variations in legislation across borders. Screening of consultants was typically more stringent in the USA, with
client firms (in addition to the employer) often requiring background checks of individual ethical hackers and, potentially, also drug tests—this was not highlighted as a requirement in Australia.

We check the company that does our penetration testing and our vulnerability assessments, that person [the ethical hacker] gets vetted, has a background check and then before they can do any work on our systems, they have to sign the non-disclosure agreement and our proxy statements. They also have to agree to, and comply with all of our security policies. (Security Director, law firm, USA)

From a variation of legislation perspective, although the duty of confidentiality is universal, ethics rules may vary from state to state; each state has its own bar exam that must be passed in order to practise in that state:

You take different bar exams in different states and the ethics rules vary from state to state as well as the ethical obligations. They have these legal ethics opinions that the state bar offers to attorneys to be able to give guidance about what the rules mean, and so those can vary also state by state. (Lawyer, USA)

This variation highlights the importance of ethical hackers needing to be fully informed of different rules if they practise in different jurisdictions. Although it is less likely that an ethical hacker would conduct tests across international borders, conducting tests across national borders within the same country is plausible. Knowledge of multi-jurisdictional legislation and regulation was raised by Australian participants; however, this was emphasised more by US participants: ‘an ethical hacking company would want to be certain that they are in compliance with those ethics rules and conducting the hacking in the way that would be in compliance with every state’s ethical rules’ (Lawyer, USA). As in Australia, the requirement for an agreement (e.g., an NDA) to be entered into prior to the engagement of an ethical hacker was highlighted as either an expectation or a requirement.
In many respects, US requirements resemble Australian requirements. However, US legal firms are more stringent in their vetting of external parties and legislation is more complex and varied. According to the ABA (2018), conducting background checks is common practice in organisations; this is unsurprising due to increased emphasis on supplier security in the USA. Both Australia and the USA require agreements to be executed that protect the interests of the firm (e.g., an NDA). Both countries are also primarily concerned with ensuring that legal privilege and client confidentiality of data are maintained.

4.3 Values-based Analysis

Values are a core set of beliefs and principles that stem from an individual’s culture (Burmeister & Kreps, 2018). Analysis of the collected data revealed a relationship between the data and values: more specifically, the values held by each party within the ‘chain’ of ethical hacking. The identified parties in the chain are:

- the lawyer
- internal law firm staff (e.g., IT or Security Department)
- the client (of the lawyer/law firm)
- the ethical hacker.

Although this list is not exhaustive, some key values were identified as part of the research. These values are organisation-focused, either within organisations or in relation to engaging outside organisations. These core values are listed below and then explored in further detail as they relate to each party:

- trust and trustworthiness
- reputation.

4.3.1 Trust and Trustworthiness
Studies have demonstrated that trust plays a significant role in daily life; professionally, there is high significance placed on interpersonal trust within organisations (Qi & Chau, 2013). In modern organisations, with the prevalence of technology, a new perspective on trust arises. Therefore, it is crucial to understand both the nature and significance of trust. As previously described, Tutzauer (n.d.) has conceptualised trust as the belief of one individual that another party upon whom the individual is dependent will act in his or her interests. This definition is key for this study because trust emerged as an important value among all parties.

*We have a committee of the board, which is a representative selection of the partnership that manages risk, and has our head of IT and head of security reporting into it, managing the process of both the selection and implementation of things like pen-testers. As a partner that's not directly exposed to the process, I'm confident that there is a management structure in place, which is doing a job to make sure that there is some rigour applied in this space.* (Partner, law firm, Australia)

Although lawyers are experts in the field of law, they likely do not possess cybersecurity knowledge. For this reason, they trust their operational IS or IT teams to manage risks and act in their best interests. From an internal law firm staff perspective, the IT and IS staff must trust the ethical hacker to perform their job effectively and not to misuse their skills. They must trust lawyers to assist them in scoping engagements, including the exclusion of any data that should not be included in the engagement.

From the client perspective (although clients were not included as part of the research), interviews with legal professionals highlighted two key client values based on their expectations when dealing with a law firm. Both values centred on trust: trust that they have an engaged an expert (a lawyer) to help them and trust that their information is appropriately
handled and, where appropriate, subject to legal professional privilege and will remain confidential.

*Every state has rules regarding confidentiality of information and that’s to preserve the attorney–client privilege. It’s fiercely guarded because the idea is that you want your clients to be forthcoming with you. We want to instil trust and confidence in our clients and our relationships so it’s an ethical obligation to protect that attorney–client privilege.* (Lawyer, USA)

In these examples, there exists implied trust. As part of the trust process, Li, Rong and Thatcher (2012) have highlighted a willingness by one party to be vulnerable to another party. Examples of this include the lawyer trusting their IS or IT department to keep client data secure, the client trusting lawyers to protect their information and the IS or IT department trusting the ethical hacker to conduct an adequate and ethical engagement. These are all prime examples of a vulnerable party being willing to allow the other party to carry out their task as required, irrespective of the ability to monitor or control them (Li, Rong & Thatcher, 2012).

Implied trust requires trustworthiness. Hardin (2002) has pointed out that much of the literature on trust actually relates more closely to trustworthiness. For example, for a client to trust a lawyer, the lawyer must be trustworthy. Likewise, law firm security personnel must be trustworthy for the lawyer to trust them and an ethical hacker must be trustworthy for the law firm security personnel to trust them: ‘Only trusted penetration testers should be allowed to penetrate organisations with lots of confidential and sensitive data’ (Information Security, law firm, Australia).

Each party in the chain must be trustworthy; they will then be trusted to perform their respective duties. There is little literature that explores what makes a person trustworthy; however, professional competence, taking responsibility and organisation responsibility have been identified
as key attributes (Nishishiba & Ritchie, 2000). Once again, these attributes highlight a link between trustworthiness and those factors that help to reinforce certain attributes, such as professional codes of ethics and conduct, in addition to formal professional associations.

### 4.3.2 Reputation

Reputation is another key value that emerged from the research. Reputation related to the ethical hacking organisation, rather than individual ethical hackers themselves. Reputation is generally described as belief or opinion about another; in the case of ethical hacking organisations, this largely consisted of the reputation that the organisation possessed in the marketplace. Factors that played a role in the formation of reputation included whether the organisation was a well-established player in the market with a solid track record; which processes they perform as an organisation (e.g., conducting thorough checks and employing solid methodologies) and how these have been conducted; how many engagements they have conducted and the nature of the outcomes.

You want to ensure that they’re a recognised and trusted body that you’re working with and that there is a set standard contractual agreement put down in terms of non-disclosure. You always look for those kinds of points when you’re dealing with the providers that you’re seeking to do the testing with. (IT Director, law firm, USA)

Recently when we engaged them at our firm we made sure they were pre-certified, we made sure they were a reputable company, we made sure that the people that were testing had been with the firm for a while and they themselves were also certified. (Security Manager, law firm, Australia)

A key factor in determining reputation was the opinion of peer firms, particularly whether those firms viewed the ethical hacking firm positively and were willing to recommend them: ‘I would want some sort of references from others that they’ve done’ (Consultant, USA).
Research has identified a relationship between trust and reputation, whether trust is a consequence of good reputation (Keh & Xie, 2009) or reputation is a consequence of trust (Fatma, Rahman & Kahn, 2015; Yoon, Gürhan-Canli & Schwarz, 2006). Further, ethical behaviour by an organisation contributes to its brand valuation (Holt, Quelch & Taylor, 2004).

4.4 Chapter Summary

This chapter has presented the research findings. Twenty-eight interviews were conducted, in addition to data collection through day-to-day observations. The research participants comprised legal professionals, IS and IT (who were responsible for information security) professionals and ethical hacking and cybersecurity consulting professionals, from both Australia and the USA.

Six main themes and fourteen categories were identified from the data. These themes were: confidentiality of information, professional standards, issues with regulation, conflicts of interest, the onboarding process and differences between Australia and the USA.
Chapter 5: Discussion

This chapter will discuss the research findings in the context of the existing literature identified in Chapter 2. The purpose of this discussion is to answer the research questions and address the problem statement outlined in Chapter 1.

5.1 Issues of Professionalism

The first research question focused on ethics and professionalism. It is clear that confidentiality of information is the primary concern for legal firms. This is not to say that integrity and availability of information is not a concern, rather than confidentiality is perceived to carry the most risk in terms of financial and reputational consequences. Although this is common for most organisations, emphasis in this context is given to the confidentiality of client information that is held under legal privilege, the disclosure of which may have consequences that extend beyond the firm itself. For example, the disclosure of information related to a merger and acquisition transaction could affect the transaction and result in fraudulent activity, as seen in the hacking of Cravath, Swaine and Moore and Weil, Gotshal and Manges (Randazzo, 2016). Although this example involves activity conducted by malicious hackers, it illustrates some potential consequences of the disclosure of sensitive information.

For the legal professionals who participated in this research, confidentiality is a critical requirement that is mandated by the respective professional bodies in each jurisdiction: the LCA and the ABA. Despite variations in laws across each state, the ABA provides some consistent requirements.

There are no similar requirements for ethical hackers; therefore, there exist concerns regarding how legal privilege would extend to third
parties who are likely to gain access to privileged or sensitive information. Further, in the event of such disclosure, the obligations of the ethical hacker and the law firm are unclear. For example, as discussed in Chapter 2, there have been significant regulatory and legislative changes across the globe that relate to the privacy of individuals (Thomas, Burmeister & Low, 2019). In the context of regulations and laws that require notification to affected individuals in the event of exposure of their information and the potential for significant penalties (OAIC, 2018a), the requirements around how such data are handled are critical. Further, these requirements must extend to anyone who may gain access to the data. This relates to those attributes of professionalism focused on ethics (CEPIS Taskforce, 2010). An ethical hacker must possess the necessary ethical and moral attributes to ensure any handling of privileged and sensitive information is appropriate.

The EU GDPR differentiates between a data controller and a data processor (EUR-Lex, 2016). The controller determines the purpose and means of processing personal data (often the organisation to which the individual provided their personal information), whereas the processor ‘processes’ the personal data on behalf of the controller. It is possible that the controller and processor are the same; however, personal data are often provided to third parties—in these cases, the controller must ensure that protections are in place to protect this data, as required by the GDPR (Kolah, 2018). Therefore, ethical hackers must be aware of legislation and regulation requirements and possess the necessary skills and knowledge to ensure that their clients (the law firms) do not breach those requirements. Once again, the significance of professionalism (and some of the specific attributes identified in Chapter 2) is highlighted.

Although Chapter 2 focused on specific knowledge, special skills and learnings within professionalism, current research has identified that
these attributes were more technically focused (e.g., the ability to validate and test the security of systems) (Berger & Jones, 2016). The research data in this study revealed the need for an ethical hacker to not only possess such technical skills but also be familiar with laws and regulations. However, this is not typically a core focus of an ethical hacker’s skillset.

For this reason, the importance of appropriate onboarding has been emphasised. The onboarding process takes place prior to commencement of the engagement and aims to conduct vetting and provide ground rules. Generally, any contracts or agreements are made at this time. The most common type of agreement in use is the NDA (Bechtsoudis & Slavos, 2012); however, as identified, there are several issues with such agreements. The first is that such an agreement requires all parties to uphold the agreement and address the accountability component of professionalism. However, the party that signs the NDA is not necessarily the person who will conduct the engagement. Second, there often exists an assumption (on the part of the organisation consuming the services) that each professional who will work on the engagement has undergone adequate vetting by their employer. Although this does occur in many cases, it does not always occur. The study highlighted two key areas of importance within onboarding: due diligence and scoping.

5.1.1 Due Diligence: Is a Single Check Sufficient?

Although the criticality of due diligence was highlighted, the actual practice of conducting due diligence checks on individuals engaged to conduct assessments was not consistently enforced, particularly in Australia. US firms are generally more thorough in their approach to risk management; firms require background checks of all personnel, including external consultants as well as employees. Further, where screening is conducted by an employer (e.g., police checks, credit
checks and, in some instances, drug screening), these are often not repeated beyond initial employment. Conducting a single check at a particular point in time may be ineffective, because it is based on the assumption that the particular individual will never commit a crime, encounter financial troubles or take illicit drugs in the future (Brody, 2010). In the context of ethical hackers, possible concerns relate to issues such as hacking conference attendance or dark web research, which may entail a risk of malicious influence, much like in university hacking courses (Trabelsi & McCoey, 2016). Many such risks may be mitigated, to some extent, by using standardised approaches, such as the frameworks and standards described in Chapter 2. For example, ISO/IEC27001, the Australian Government ISM and the NIST CSF all incorporate controls that may assist to address some of these issues. This includes requirements around background and supplier screening, which were highlighted as key by participants: ‘there’s an expectation that, in the same way that a law firm has vetted all of its lawyers, that a cybersecurity company has done a ridiculous amount of background checking on their staff’ (Consultant, Australia).

One challenge involved in utilising such standards and frameworks is that this may require significant time, effort, resources and ongoing compliance requirements. One approach could be to take the relevant controls from these frameworks that address relevant risk areas and produce a new specific framework. This approach is discussed later in this chapter.

5.1.2 Scoping of Engagements: What Data are Possessed?

Chapter 2 discussed some technical threats and risks associated with conducting penetration testing and ethical hacking. To address such risks, engagement scoping is commonly used to define authorised targets (Engebretson, 2013). However, the scope may not be sufficiently detailed; often, it only covers the type of test to be performed and what
(or who) will be tested. As highlighted in Chapter 4, it is crucial to ensure that a clear scope is developed and documented:

*If they have been employed by an organisation to test, you would think that they have adequate agreements in place that would apply to whoever is testing and prevent them from doing something outside of the bounds of whatever has been agreed to. (Lawyer, Australia)*

Common scoping questions may include:

- **Type of test(s)**–
  - External (internet-facing systems) test
  - Internal (corporate network) test
  - Wireless test or application test
  - Social engineering (e.g., a phishing campaign)
  - Physical test (e.g., gaining access to specific premises)

- **Test target(s)**–
  - IP addresses
  - Email domain
  - Corporate website address
  - Specific people or groups
  - Wireless network IDs

- **Broad exclusions**–
  - Specific systems (particularly those viewed as unstable)
  - Specific people or groups
  - Specific buildings or locations.
However, further detail regarding what should be scoped out is often lacking. While problematic systems are often scoped out to reduce risk of availability or stability issues (e.g., the broad exclusion identified above), there is generally only limited scoping out of specific data. This may occur because many firms do not know data specifics, including where data reside or the type of data:

*I think where issues occur is that sometimes firms don’t know where their data sits, particularly for smaller and mid-tier firms, and particularly firms that have merged. There can be repositories of data that people just aren’t aware of and sometimes it’s highly confidential. (Director [lawyer], consulting firm)*

For example, a firm’s document management system may be in-scope, but there exists a highly confidential matter that resides within that system—this should be, but is not, scoped out.

Obligations of legal privilege, along with regulatory and legislative requirements, highlight the criticality of knowing the data held by a firm, including its location, and determining whether it should be explicitly excluded from the scope of the engagement.

### 5.1.3 Professional Standards: Are Guard Rails Required?

As with any other kind of practitioner, there exists a need for continuing professional development in ethical hacking (Nolan, Owen, Curran & Venables, 2000). However, the rate of change generally experienced in the ethical hacking and cybersecurity fields is significantly higher than in most other fields (MITRE Corporation, 2019). With new technologies constantly being developed, increased uptake of technology capabilities by all organisations and the volume of new vulnerabilities that are discovered every year, it is crucial to ensure up-to-date skills and knowledge.
Many professional organisations have specific teams that are responsible for learning and development; however, there is no clear guidance or structure on obtaining continuing development for ethical hackers—often, this comes in the form of self-education (Lakhani & Wolf, 2005). Some ethical hackers are self-taught; this is a fairly common method of continuous learning and development. Significantly, this leads to research, potentially conducted on the dark web or at hacking conferences and meetings:

*Any time you talk about the dark web, you’re on that borderline in my opinion, of whether you’re doing stuff ethically, even if it’s for the sake of research, you’re doing stuff that isn’t really deemed as professional, in my opinion. I, for one, have no interest in going into the dark web, and while a lot of that fascinates me in terms of what people are trying to do and the tactics that they’re trying to use, [it] just seems to me that it’s an area that you don’t want to be operating in because it’s borderline unethical.* (Senior Security Consultant [ethical hacker], USA)

The dark web contains significant volumes of illegal and questionable material, individuals and groups (Mörch et al., 2018). While there is likely value in obtaining knowledge an information from the dark web, the associated risks associated must be managed, especially in the absence of clear guidance, ‘guard rails’ or oversight. Ethical hackers (and hackers in general) are often described as ‘outside of the box’ thinkers; therefore, they may not wish to be bound by rules. However, a set of guidelines attached to a formal qualification or requirement may help reduce risks to not only firms engaging ethical hackers, but also the ethical hackers themselves.

### 5.1.4 Conflict of Interest: A Perspective on Independence

The research identified several key perspectives on conflicts of interest, including professional conflicts, personal conflicts and cross-practice conflicts. The need for an ethical hacker, or any consultant providing
advice (particularly audit advice), to remain independent is critical. Independence is a fundamental principle of auditing; confidence in the value of an auditor’s findings is dependent on this independence (Certified Practising Accountants [CPA] Australia, 2013; Firth, 1980). It is crucial to explore such conflicts in further detail, considering when conflict may occur and how to determine the course of action to be taken to minimise conflict. Conflicts of interests also fall within the realms of professionalism and ethics, as discussed in Chapter 2.

Professional conflicts may occur when an ethical is simultaneously working on two engagements that conflict with one another. Several scenarios may result in this type of conflict, for example:

- Law Firm A holds sensitive information about Client A.
- Law Firm B holds sensitive information about Client B.
- Client A and Client B are involved in a transaction (e.g., litigation matter).
- Law Firm A and Law Firm B have engaged Ethical Hacker X to conduct a test of their systems.

This type of conflict could result in an ethical hacker obtaining information that could be subject to misuse by the ethical hacker or anyone else that has access to both sets of information.

Personal conflicts occur when an engagement that an ethical hacker is working on conflicts with any personal interests. One example of a personal conflict is:

- Law Firm A holds sensitive information about Client A.
- Ethical Hacker X has an interest in Client A.
This type of conflict could result in misuse of information (e.g., fraudulent share trading) or access to sensitive information that is pertinent to a case in which the individual or a related individual is involved.

The third category is cross-practice conflict, in which the ethical hacker is employed by a firm that provides other services that might address remediation efforts. An example of cross-practice conflict is:

- Ethical Hacker X works for Consulting Firm A.
- Consulting Firm A provides security solutions, such as selling and installing firewalls.

This type of conflict could result in biases during the conduct of ethical hacking engagements. Although this is often considered to be a value-added offering, in which a single provider may provide a number of solutions, this could also arguably contradict the independence of the assessment.

Independence plays a key role in the auditing field. As described in Chapter 2, ethical hacking refers to cybersecurity professionals who test and validate (e.g., audit) the security controls of an organisation; therefore, it is clear that independence plays a key role in audit activities such as ethical hacking. The kinds of conflicts described above may have serious consequences, such as fraud and bias. These conflicts have not previously received the required attention; while many professions, such as law (LCA, 2018) and accounting (CPA Australia, 2013), require independence and management of conflicts of interest, this is not widely practised or researched in the ethical hacking field. For these reasons, it is necessary to consider what level of oversight is required to minimise the risk of conflict and implement a level of guidance and assurance to address this.
5.1.5 Contrast Between Australia and the United States of America

Two key differences were identified between Australia and the USA, in terms of the engagement of ethical hacking services: the importance of cross-jurisdictional knowledge and the pre-engagement vetting of the ethical hacker.

One key difference between the Australian and US legal systems is the variations in legislation and regulatory requirements across each state (Cornell Law School, n.d.a). There exist both federal laws and laws that only apply in certain states. The US Computer Fraud and Abuse Act is a federal law that prohibits certain activities relating to computer systems, such as unauthorised access to computer systems to obtain information (e.g., financial data), carrying out fraudulent activity using computer systems and causing damage or disruption (Cornell Law School, n.d.b).

Some laws, such as California’s new privacy act, are state-based. The 2018 California Consumer Privacy Act provides increased rights for Californian residents regarding how their personal information is collected and used (Ghosh, 2018). An ethical hacker would need to be aware of any legislation and regulation with which they may be required to comply. This increases the knowledge requirement of ethical hackers that work across different jurisdictions.

5.2 Do Issues of Professionalism Exist?

Professionalism, as defined previously, has some key requirements, including that the professional is bound by a code of ethics, has special knowledge that is applied in the interest of others and is accountable to a governing body. Based on these requirements, various potential issues arise from the research contained in this study.
5.2.1 Developing a Framework: A Consistent Approach to Risk Management

The research questions investigated the potential need for a framework to conduct better due diligence and reduce the risks to law firms and their clients when engaging ethical hackers. As this study progressed, the need for such a framework that ensures, for example, due diligence tasks, scoping and other steps to help reduce risk became increasingly evident.

*There’s an expectation that in the same way that a law firm has vetted all of its lawyers that a cyber security company has done a ridiculous amount of background checking on their staff.* (Director, consulting firm)

*We don’t do anything without a million checks on service providers. It (engaging an ethical hacking firm) would’ve gone to a specific subcommittee and it would have gone to the Board. There definitely would have been a review process.* (Partner, law firm, USA [1500+ attorneys])

*When engaging penetration testers, a process that includes scoping is important to potentially scope out highly confidential information.* (Director [lawyer], Australia)

*We check the company that does our penetration testing and our vulnerability assessments, that person [the ethical hacker] gets vetted, has a background check and then before they can do any work on our systems, they have to sign the non-disclosure agreement and our proxy statements. They also have to agree to, and comply with all of our security policies.* (Security Director, law firm, USA)

To assist in reducing the risk to a law firm (and potentially other organisations) when engaging an ethical hacker, there are several requirements that warrant consideration. To address these requirements on a consistent basis, there is merit to be found in developing a framework for use by law firms. This framework should account for key areas, related to all stages of engagement, identified by this study. A proposed framework, named the Ethical Hacking Framework for Law
Issues of Professionalism Concerning the Ethical Hacking of Law Firms

Georg A. Thomas

Firms (EHF), is provided in Section 5.2. It is divided into the following control groups (stages):

- Prior to Engagement (PE)
- During Engagement (DE)
- After Engagement (AE)
- Engagement Review (ER).

There are 16 controls within the framework.

A framework is generally neither prescriptive nor intended as an instruction manual. Rather, a framework provides some structure that may be followed, based on the needs of the organisation adopting the framework. The EHF includes guidance for each control to help provide context and guide decisions.

5.2.1.1 Included Controls

To develop the proposed framework, the relevant controls needed to be determined. Two key sources were used to do this: data obtained from the present study and existing standards and frameworks (as shown in Table 5). Opinions regarding the quality of different frameworks and standards vary widely among industry security professionals. Factors such as geographic region, organisation and client requirements, cost factors and ease of implementation influence which framework or standard is chosen. Further, many of these standards and frameworks also overlap to some degree.

<table>
<thead>
<tr>
<th>Framework</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC27001:2013</td>
<td>ISO/IEC27001:2013 is an information security management system (ISMS)</td>
</tr>
<tr>
<td>Framework</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ISO/IEC27001:2013</td>
<td>from the International Organization for Standardization. It comprises 114 controls, in 14 clauses, with 35 control groups (International Organization for Standardization, n.d.). ISO/IEC27001:2013 is a global standard, with wide adoption across the globe. Organisations in the United States of America (USA) and Australia continue to adopt this standard as part of their information security and risk management programs.</td>
</tr>
<tr>
<td>NIST Cybersecurity Framework</td>
<td>The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was first published in 2014 by NIST in the USA. The NIST CSF consists of standards, guidelines and best practices and aims to manage cyber-related risk (National Institute of Standards and Technology [NIST], n.d.). The NIST CSF comprises five core functions, 23 categories and 108 controls. Although it is a USA-</td>
</tr>
<tr>
<td>Framework</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>based framework, many organisations outside of the USA (including those in Australia) have adopted the framework because it is easy to understand and pragmatic.</td>
</tr>
<tr>
<td>NIST SP 800-53</td>
<td>In 2005, NIST published special publication 800-53. NIST SP 800-53 (Security Controls and Assessment Procedures for Federal Information Systems and Organisations) provides a catalogue of security and privacy controls. This catalogue is designed to protect US federal information systems and organisations from hostile threats, natural disasters, structural errors, human errors and privacy risks (NIST, 2017). Like all NIST publications, the goal is primarily the protection of US government information systems; however, the frameworks are publicly available and adopted by many organisations outside of government.</td>
</tr>
<tr>
<td>Framework</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Australian Government Information Security Manual (ISM)</td>
<td>Much like the US NIST frameworks, the Australian Signals Directorate (ASD) produces the Australian Government ISM. The ISM aims to help protect information and systems from cyber threats (Australian Cyber Security Centre, 2019). Like the ISMS, it is primarily intended for government systems, or those organisations that handle government information, but is freely available to the public and adopted by other organisations. The ACSC ISM includes over 800 controls that are applicable according to different classification levels (e.g., Official, Protected, Secret, Top Secret). Many Australian organisations seek to comply with the ISM and obtain InfoSec Registered Assessors Program (IRAP) certification. IRAP certification requires an organisation to meet the controls of the ISM, based on the classification of information they</td>
</tr>
</tbody>
</table>
The research data identified the key areas that must be addressed when engaging and using the services of an ethical hacker; the existing standards and frameworks provide controls that may address those areas. It was crucial to determine which standards and frameworks would provide the most appropriate controls; to achieve this, the most widely adopted standards and frameworks were selected. This selection occurred through a qualitative analysis of each framework or standard, based on the experience of the researcher, with a focus on those used in Australia and the USA.

Limiting the scope of the frameworks to those used in Australia and the USA is beneficial because organisations will not only already be familiar with those frameworks but may also have incorporated some controls into their business processes.

### 5.2.1.2 Standards and Frameworks Addressing Identified Areas

The study identified controls from these common standards and frameworks that may assist in addressing the identified key areas. The following controls were taken from the selected frameworks to address areas relating to confidentiality, professional standards, conflicts of interest and onboarding, as identified from the research data of this thesis. Table 6 provides a description of each area and the relevant selected controls from each framework or standard.
### Table 6. Controls that Address Areas of Concern

<table>
<thead>
<tr>
<th>Area</th>
<th>Control(s)</th>
</tr>
</thead>
</table>
| Confidentiality of information | • ISO/IEC27001 A8  
                         | • ISO/IEC27001 A15  
                         | • ISO/IEC27001 A18  
                         | • NIST ID.SC-3  
                         | • NIST ID.SC-4  
                         | • NIST DE.CM-6  
                         | • NIST PR.AT-3  
                         | • NIST PR.DS-5  
                         | • NIST 800-53 AU-13  
                         | • ISM 0805  
                         | • ISM 0141  
                         | • ISM 0435  
                         | • ISM 0072  |
| Professional standards      | • ISO/IEC27001 A7  
                         | • NIST 800-53 PS-3  
                         | • NIST 800-53 PS-7  |
| Conflicts of interest       | • ISO/IEC27001 A7  
                         | • NIST PR.IP-11  
                         | • NIST 800-53 PS-3  
                         | • NIST 800-53 PS-7  
                         | • ISM 0434  |
| Onboarding process          | • ISO/IEC27001 A7  
                         | • ISO/IEC27001 A8  
                         | • ISO/IEC27001 A15  
                         | • NIST ID.AM-6  
                         | • NIST PR.AT-3  
                         | • NIST ID.SC-3  
                         | • NIST 800-53 PS-3  
<pre><code>                     | • NIST 800-53 PS-4  |
</code></pre>
<table>
<thead>
<tr>
<th>Area</th>
<th>Control(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• NIST 800-53 PS-7</td>
</tr>
<tr>
<td></td>
<td>• NIST 800-53 RA-3</td>
</tr>
<tr>
<td></td>
<td>• NIST 800-53 CA-5</td>
</tr>
<tr>
<td></td>
<td>• ISM 1531</td>
</tr>
<tr>
<td></td>
<td>• ISM 0434</td>
</tr>
<tr>
<td></td>
<td>• ISM 0435</td>
</tr>
</tbody>
</table>

Each control, and its corresponding description (identified in Table 6), is discussed below. It is worth noting that some controls address multiple areas and may be repeated.

5.2.1.2.1 ISO/IEC27001:2013

The controls contained within ISO/IEC27001:2013 that best meet the needs identified within the research are:

**Annex Item 7—Human Resource Security.** All controls are applicable and include checks before employment/engagement, terms and conditions, requirements during employment/engagement and requirements at the termination of employment/engagement.

**Annex Item 8—Asset Management.**

- Control 8.2—Information Classification and its related sub-controls are necessary to properly identify the scope of the engagement.
- Control 8.3—Media Handling and its related sub-controls are necessary to ensure any media used as part of the engagement that may contain sensitive or confidential information is secure and properly destroyed at the conclusion of the engagement.
Annex Item 15—Supplier relationships. All controls are applicable and include security requirements between the ethical hacking firm and the law firm, monitoring and review of the service and handling of any identified security weaknesses or incidents.

Annex Item 18—Compliance. All controls are applicable and include compliance of any contractual and legal requirements, such as the protection of personally identifiable information (PII).

5.2.1.2.2 National Institute of Standards for Technology Cybersecurity Framework

The controls contained within the NIST CSF (NIST, 2018) that best meet the needs identified within the research are:

ID.AM—Asset Management.

- Control ID.AM-6—Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g. suppliers, customers and partners) are established.
- Control ID.BE-1—The organisation’s role in the supply chain is identified and communicated.
- Control ID.GV-2—Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
- Control ID.GV-3—Legal and regulatory requirements regarding cyber security, including privacy and civil liberty obligations, are understood and managed.
- Control ID.RA-4 Potential business impacts and likelihoods are identified.
- Control Group ID.SC—this group emphasises various controls, given below.
o Control ID.SC-3—Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organisation’s cybersecurity program and Cyber Supply Chain Risk Management Plan.

o Control ID.SC-4—Suppliers and third-party partners are routinely assessed using audits, test results or other forms of evaluations to confirm they are meeting their contractual obligations.

- Control PR.AT-3—Third-party stakeholders (e.g. suppliers, customers and partners) understand their roles and responsibilities.
- Control PR.DS-5—Protections against data leaks are implemented.
- Control PR.IP-6—Data are destroyed according to policy.
- Control PR.IP-11—Cybersecurity is included in human resource practices (e.g. deprovisioning and personnel screening).
- Control DE.CM-6—External service provider activity is monitored to detect potential cybersecurity events.

5.2.1.2.3 National Institute of Standards for Technology Special Publication 800-53

The controls contained within the NIST Special Publication 800-53 (NIST, 2018) that best meet the needs identified within the research are:

- AU—Audit and Accountability
  - AU-2—Audit Events
  - AU-6—Audit Review, Analysis and Reporting
5.2.1.2.4 Australian Government Information Security Manual

The Australian Government ISM includes several relevant controls. These controls are divided into groups and are applicable based on the classification of the information they are designed to protect (e.g., Official, Official (Sensitive), Protected, Secret or Top Secret) and whether they are mandatory (e.g., identified by SHOULD [S] or MUST [M]). The controls contained with ISM (ASD, 2016) that best meet the needs identified in the research are as follows:

- AU-9—Protection of Audit Information
- AU-10—Non-repudiation
- AU-13—Monitoring for Information Disclosure

- CA—Security Assessment and Authorisation
  - CA-1—Security Assessment and Authorisation Policies and Procedures
  - CA-2—Security Assessments
  - CA-5—Plan of Action and Milestones
  - CA-6—Security Authorisation
  - CA-7—Continuous Monitoring
  - CA-8—Penetration Testing

- PS—Personnel Security
  - PS-3—Personnel Screening
  - PS-4—Personnel Termination
  - PS-7—Third Party Personnel Security

- RA—Risk Assessment
  - RA-3—Risk Assessment
• Conducting Security Assessments
  o 1531 (S)—Prior to the beginning of a security assessment, a test plan is developed by assessors in consultation with the system owner.
  o 0805 (M)—During a security assessment, the system is reviewed by assessors to determine whether security controls in the Statement of Applicability (SOA) are appropriate, have been implemented and are operating effectively.
  o 1140 (M)—At the conclusion of a security assessment, a security assessment report is produced that outlines the effectiveness of the implementation of security controls, the system’s strengths and weaknesses, any recommended remediation activities and an assessment of security risks associated with the operation of the system.

• Reporting cyber security incidents
  o 0141 (M)—When organisations use outsourced IT or cloud services, their service providers report all cybersecurity incidents to the organisation’s CISO (or one of their delegates), as soon as possible after they occur or are discovered.

• IT and cloud services
  o 0873 (M)—If using an outsourced IT service, or cloud service not listed on the ACSC’s Certified Cloud Services
List, a service provider whose systems are located in Australia is used.

- 0072 (M)—Any security controls associated with the protection of information entrusted to a service provider are documented in contract provisions, a memorandum of understanding or an equivalent formal agreement between parties.

- 1451 (S)—When entering into a contractual arrangement for outsourced IT or cloud services, contractual ownership over an organisation’s data are explicitly retained.

- 1452 (S)—A review of suppliers, including their country of origin, is performed before obtaining software, hardware or services to assess the potential increase to an organisation's security risk profile.

- **Personnel Security—Access to systems and their resources**
  - 0434 (M)—Personnel undergo appropriate employment screening and, where necessary, hold an appropriate security clearance, before being granted access to systems.
  - 0435 (M)—All personnel receive any necessary briefings before being granted access to systems.
  - 0430 (M)—Access to systems, applications and information is removed or suspended on the same day a
user no longer has a legitimate business requirement for access.

- System Monitoring—Event logging and auditing
  - 0580 (M)—An event logging strategy is developed and implemented covering events to be logged, logging facilities to be used, event log retention periods and how event logs will be protected.

5.2.1.3 Proposing a Framework

Based on the identified need for a framework and the controls from established standards and frameworks that have been identified as potentially addressing a significant proportion of the identified areas of concern from the research, a new framework (the EHF) was developed by the primary researcher. This framework may be used in mitigating the risks associated with engaging ethical hackers to conduct ethical hacking and penetration testing engagements against law firms. It is worth noting that the final control (ER-1 Engagement Review) was not part of any existing framework; however, based on the primary researcher’s professional experience, review (including lessons learned) is a common risk management technique that assists to secure future successes and avoid potential failures reoccurring (Trevino & Anantatmula, 2008).

The next section contains the proposed draft EHF.

5.3 Ethical Hacking Framework for Law Firms

5.3.1 Purpose

To reduce the risks experienced by law firms, a framework was developed to guide the use of ethical hacking or penetration testing of
Issues of Professionalism Concerning the Ethical Hacking of Law Firms

Georg A. Thomas

law firms. This framework provides guidance on engaging and conducting ethical hacking and penetration testing engagements end-to-end. The framework covers areas such as due diligence, scoping of the engagement and oversight. It is based on industry research and the collection of data from legal practitioners at all levels, law firm security, risk personnel and ethical hackers and consultants. It is divided into four control groups or stages that represent the lifecycle of the engagement:

- Prior to Engagement (PE)
- During Engagement (DE)
- After Engagement (AE)
- Engagement Review (ER).

5.3.1.1 Ethical Hacking Framework Control Groups (Stages)

Table 7 identifies and describes the EHF controls and provides guidance on how controls may be implemented.
<table>
<thead>
<tr>
<th>Stage</th>
<th>Control</th>
<th>Description</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>PE</td>
<td>PE1 Screening</td>
<td>Personnel that will work on the engagement have been appropriately background screened.</td>
<td>Background-screening has taken place by a qualified entity (e.g., a background-screening agency) appointed by the law firm. The screening process should include police checks, credit checks and drug tests. Where engagements run for extended periods, repeat checking should be considered.</td>
</tr>
<tr>
<td>PE</td>
<td>PE2 Conflicts</td>
<td>Personnel that will be working on the engagement have been conflict-checked to ensure that no conflicts of interest exist.</td>
<td>Conflict checks have been conducted to ensure that personnel working on the engagement have no interests that may conflict with the information to which they may gain access. This could include, but is not limited to, information that relates to shareholdings, relatives and other clients and matters. For example, if another client of the ethical hacker has information held by the law firm, this would be considered a conflict.</td>
</tr>
<tr>
<td>PE</td>
<td>PE3 Skills and Competence</td>
<td>Personnel that will work on the engagement have had</td>
<td>Reference-checking and, where possible, a practical assessment should be conducted to validate the skills</td>
</tr>
<tr>
<td>Stage</td>
<td>Control</td>
<td>Description</td>
<td>Guidance</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>their skills verified to ensure they can adequately conduct the engagement.</td>
<td>of the ethical hacker. A practical assessment should be conducted by an assessor with a reasonable technical knowledge level.</td>
</tr>
<tr>
<td>PE</td>
<td>PE4 Licensing and Qualifications</td>
<td>Personnel that will work on the engagement carry appropriate certifications and licensing.</td>
<td>Ethical hackers will hold appropriate qualifications/certification/licence from a well-known body. Qualifications must be appropriate for the type of work that will be carried out. For example, individuals that only carry qualifications that include web application testing should not conduct network tests.</td>
</tr>
<tr>
<td>PE</td>
<td>PE5 Contractual Obligations</td>
<td>Appropriate contractual obligations are implemented.</td>
<td>Agreements, such as NDAs, are created. Such an agreement must extend to the ethical hacker and any party that may come into contact with firm data. Other contractual items that should be considered include the right to audit and consent for the ethical hacker to test; further, the agreement should be supported by a scoping document, such as an RoE document (see PE7).</td>
</tr>
<tr>
<td>Stage</td>
<td>Control</td>
<td>Description</td>
<td>Guidance</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>PE</td>
<td>PE6 Code of Conduct</td>
<td>Personnel that will work on the engagement have adopted a code of conduct or ethics by which they will abide.</td>
<td>A code of conduct or ethics from a well-known professional organisation is adopted by the ethical hacker, who will provide confirmation that they will abide by the nominated code.</td>
</tr>
<tr>
<td>PE</td>
<td>PE7 Engagement Scope</td>
<td>The engagement must be appropriately scoped.</td>
<td>Thorough scoping of the engagement must take place. In addition to specific systems, locations and IP addresses, specific information pertaining to data scoping should be included. This includes, as required, determining whether any specific matters (e.g., those considered to be highly sensitive or personally identifiable information [PII]) should be excluded from the testing. Requirements regarding notification (in the event of identified vulnerabilities or system disruption) should be agreed upon. All scoping requirements should be documented and signed off by the law firm, the ethical hacker and an authorised representative of the ethical hacking firm.</td>
</tr>
<tr>
<td>Stage</td>
<td>Control</td>
<td>Description</td>
<td>Guidance</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PE</td>
<td>PE8 Security Requirements</td>
<td>Agree upon security requirements for storage and handling of information.</td>
<td>Security requirements should be agreed upon in writing. This includes requirements regarding the storage and access of any obtained information, who has access to the information and any retention and destruction requirements. Any information should be protected using a multilayered approach.</td>
</tr>
<tr>
<td>PE</td>
<td>PE9 Compliance Requirements</td>
<td>Personnel that will work on the engagement are aware of any applicable legislative or regulatory requirements.</td>
<td>Any applicable legislative or regulatory requirements (e.g., specific jurisdictional laws) will be identified and compliance enforced.</td>
</tr>
<tr>
<td>DE</td>
<td>DE1 Status Meetings</td>
<td>Conduct regular meetings to ensure compliance with scope and any requirements from control group PE.</td>
<td>Regular meetings with the ethical hacker should be conducted. Compliance with requirements from the PE control should be reviewed to ensure there is no deviation from these.</td>
</tr>
<tr>
<td>DE</td>
<td>DE2 Auditing</td>
<td>Regularly check audit logs to ensure compliance with the scope.</td>
<td>Audit controls should be in place for sensitive information. These controls should be regularly reviewed and audited to ensure that the engagement is conducted within the defined scope.</td>
</tr>
<tr>
<td>Stage</td>
<td>Control</td>
<td>Description</td>
<td>Guidance</td>
</tr>
<tr>
<td>-------</td>
<td>-----------</td>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DE</td>
<td>DE3 Conflicts</td>
<td>Perform regular follow-up conflict checks to identify any new conflicts.</td>
<td>Periodic conflict checks should be conducted to ensure that no new conflicts occur. This is particularly important over longer engagements or when a new client or matter is introduced that could cause significant risk.</td>
</tr>
<tr>
<td>DE</td>
<td>DE4 Scope Validation</td>
<td>Continually validate the scope to ensure that any new items that should be out of scope are scoped out.</td>
<td>When any significant clients or matters are introduced (or any other significant changes occur), the scope should be revalidated to ensure that it remains appropriate. Should any high-risk items appear, the scope should be changed to exclude such items.</td>
</tr>
<tr>
<td>AE</td>
<td>AE1 Data Destruction</td>
<td>Upon conclusion of the engagement, any data retained by the ethical hacker (or their organisation) is adequately destroyed.</td>
<td>When no longer required, all data held outside the firm should be destroyed, in accordance with best practice data destruction procedures or with the firms’ data destruction or disposal policy. Certification of destruction should be supplied in writing.</td>
</tr>
<tr>
<td>AE</td>
<td>AE2 Security Remediation</td>
<td>Where feasible, remediation is commenced and any</td>
<td>Easy-to-remediate items should be addressed as soon as possible. At a minimum, any credentials that</td>
</tr>
<tr>
<td>Stage</td>
<td>Control</td>
<td>Description</td>
<td>Guidance</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>AE</td>
<td>AE3</td>
<td>compromised credentials are reset.</td>
<td>were compromised by the ethical hacker should be reset immediately.</td>
</tr>
<tr>
<td></td>
<td>Engagement Sign-off</td>
<td>Upon conclusion of the engagement, sign-off is required by the law firm, the ethical hacker and the ethical hacking organisation.</td>
<td>A document should be executed to acknowledge formal sign-off. This includes reinforcing confidentiality and non-disclosure requirements and ensuring any equipment, tools or changes (such as disabling alerts) or creating tester accounts have been removed from the environment.</td>
</tr>
<tr>
<td>ER</td>
<td>ER1</td>
<td>The engagement is reviewed to determine whether improvements have been made or lessons learned.</td>
<td>A debrief meeting should take place to discuss the engagement, highlight any lessons learned and identify any improvements.</td>
</tr>
</tbody>
</table>
### 5.3.1.2 Ethical Hacking Framework Stages Matrix

The following matrix contains the EHF controls and brief descriptions; it may be used to track the completion of each stage of the framework. It also contains references to frameworks and standards that were leveraged in its development.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
<th>☑</th>
<th>Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>PE1 Screening</td>
<td>Personnel that will work on the engagement have been appropriately background screened.</td>
<td></td>
<td>ISO/IEC27001 A7&lt;br&gt;NIST PR.IP-11&lt;br&gt;NIST SP800-53&lt;br&gt;PS-3/7&lt;br&gt;ISM 0434</td>
</tr>
<tr>
<td>PE2 Conflicts</td>
<td>Personnel that will work on the engagement have been conflict-checked to ensure no conflicts of interest exist.</td>
<td></td>
<td>ISO/IEC27001 A7&lt;br&gt;NIST PR.IP-11&lt;br&gt;NIST SP800-53&lt;br&gt;PS-3/7&lt;br&gt;ISM 0434</td>
</tr>
<tr>
<td>PE3 Skills &amp; Competence</td>
<td>Personnel that will work on the engagement have had their skills verified to ensure they can adequately conduct the engagement.</td>
<td></td>
<td>ISO/IEC27001 A7&lt;br&gt;NIST PR.IP-11&lt;br&gt;NIST SP800-53&lt;br&gt;PS-3/7&lt;br&gt;ISM 0434</td>
</tr>
<tr>
<td>PE4 Licensing &amp; Qualifications</td>
<td>Personnel that will work on the engagement carry appropriate certifications and licensing.</td>
<td></td>
<td>ISO/IEC27001 A7&lt;br&gt;NIST PR.IP-11&lt;br&gt;NIST SP800-53&lt;br&gt;PS-3&lt;br&gt;ISM 0434</td>
</tr>
<tr>
<td>PE5 Contractual Obligations</td>
<td>Appropriate contractual obligations are implemented.</td>
<td></td>
<td>ISO/IEC27001 A15&lt;br&gt;NIST ID.SC-13</td>
</tr>
<tr>
<td>PE6 Code of Conduct</td>
<td>Personnel that will work on the engagement have adopted a code of conduct or ethics by which they will abide.</td>
<td></td>
<td>NIST SP800-53&lt;br&gt;PS-7</td>
</tr>
<tr>
<td>PE7 Engagement Scope</td>
<td>The engagement must be appropriately scoped.</td>
<td></td>
<td>NIST SP800-53&lt;br&gt;CA-5&lt;br&gt;NIST SP800-53&lt;br&gt;RA-3&lt;br&gt;ISM 1531</td>
</tr>
<tr>
<td>Control</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE8 Security Requirements</td>
<td>Security requirements for storage and handling of information are agreed upon.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE9 Compliance Requirements</td>
<td>Personnel that will work on the engagement are aware of applicable legislative or regulatory requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE1 Status Meetings</td>
<td>Conduct regular meetings to ensure compliance with the scope and any requirements from control group PE.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE2 Auditing</td>
<td>Regularly check audit logs to ensure compliance with the scope.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE3 Conflicts</td>
<td>Perform regular follow-up conflict checks to identify any new conflicts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE4 Scope Validation</td>
<td>Continually validate the scope to ensure any new items that should be out of scope are scoped out.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AE1 Data Destruction</td>
<td>Upon conclusion of the engagement, any data retained by the ethical hacker (or their organisation) is adequately destroyed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AE2 Security Remediation</td>
<td>Where feasible, remediation is commenced and any compromised credentials are reset.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AE3 Engagement Sign-off</td>
<td>Upon conclusion of the engagement, sign-off by the law firm, the ethical hacker and the ethical hacking organisation should occur.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ER1 Engagement Review</td>
<td>An engagement debrief should be conducted to identify any improvements and lessons learned.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.4 Mandating a Code of Conduct

The second research question aimed to identify whether a code of conduct would add value to the ethical hacking profession. As previously discussed, there exist issues of professionalism in the ethical hacking field. Although many of these are mitigated through practice or controls, these controls are decided by the professionals themselves. A tester may belong to an organisation (e.g., CREST, EC-Council or the ACS) and, therefore, must abide by a code of conduct or ethics; however, such membership is voluntary and not a mandated requirement for an ethical hacker.

Unlike the legal profession, ethical hacking does not entail uniformed or mandatory requirements. Although professional standards do exist for ethical hackers, adherence to these depends on the desires of the individual professional. However, for an ethical hacker to be considered a true professional (according to the ACP), they must adhere to ethical standards; possess special knowledge and skills derived from research, education and training; use these skills in the interests of others and abide by a code of ethics that governs the activities of the profession (beyond the normal, personal morals and ethics of the individual) (ACP, 2018).

This requirement is true of all well-established professions (e.g., lawyers, doctors and accountants); for ethical hacking to be considered a true profession, these requirements must also apply. A 2017 special issue of the Journal of Information, Communication and Ethics in Society (JICES) focused on professional ethics in ICT (Rogerson, 2017).
It included articles on the value of creating a global code for ICT (Burmeister, 2017), IT professionalism from the perspective of CEPIS (Brady, 2017) and general professional ethics in the information age (Gotterbarn & Miller, 2017); however, no articles addressed ethical hacking. It is worthy of note that all existing ethical hacking or security professional codes (of ethics or conduct) identify the body that issues and governs the code and suggests that it applies to only members of those bodies. This is implied through the titles of these codes, such as the ‘(ISC)$^2$ Code of Ethics’ and ‘ACS Code of Ethics’, and statements such as: ‘ISACA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders’ (International Systems Assurance and Controls Association [ISACA], 2019).

The intention is that members of those specific organisations comply with these codes; however, such codes do not refer to the broader profession, including those that are not members of a specific professional organisation. Therefore, such codes may be beneficial for those wishing to adopt a code of ethics, but who do not belong to a specific organisation.

Establishing broader applicability and developing an ‘Ethical Hackers Code of Conduct’, much like the Australian Solicitors’ Conduct Rules, may encourage more ethical hackers to adopt such codes. Alternatively, it would be beneficial to either form a new professional body or create a requirement to belong to an existing one. Such a body would ensure that an appropriate code of conduct (and ethics) is available, some level of insurance is held and provide requirements regarding minimum levels of competence and certification. Such a body could also enforce licensing requirements. Members who do not comply with professional rules could be disciplined or, in the worst case, expelled; this may assist in discouraging negative or damaging behaviours within the profession.
5.5 Chapter Summary

This chapter has discussed the research findings and how these relate to the research questions. Due diligence was discussed, including whether it is sufficient to conduct a single check (typically during the hiring process). The discussion of engagement scoping covered issues such as whether lawyers, who are ultimately responsible for their client’s data, are aware of how data are handled (as part of ethical hacking engagements) and, if necessary, scoped out. Various ethical and professionalism issues were also identified. Professional standards were analysed, including a discussion of professional conduct, particularly in areas that are considered questionable or ‘grey’, such as accessing the dark web to obtain intelligence. Conflicts of interest were also discussed, including not only the conflicts that might occur if an ethical hacker works on an engagement that conflicts with their interests but also potential conflicts in situations where organisations who offer ethical hacking services also provide remediation services. Key differences between Australia and the USA were discussed. Legislative and regulatory requirements demonstrated key differences, particularly in the USA, where variation often occurs across state borders. The final section of the chapter addressed issues of professionalism and the development of a framework for providing a consistent approach to managing ethical hackers before, during and following engagements. Finally, the potential benefits of a mandatory code of conduct were discussed, including an analysis of some existing professional bodies that have provided such codes and comparison of these with mandatory, uniformed codes (e.g., the ABA or the LCA).
Chapter 6: Conclusion

6.1 Summary of Previous Chapters

The previous chapters of this thesis have identified the existing literature in the field, factors that influence the importance of and requirement for adequate cybersecurity within law firms and the ways in which ethical hacking may assist in ensuring a law firm’s security. Professional requirements of lawyers were also identified, such as those provided by legal professional bodies. The interview data were analysed and discussed, key themes were extracted and investigated in further detail and a proposed framework for use when engaging an ethical hacker was developed.

Chapter 1 identified the purpose of the research and its relevance to the modern world. It detailed the increase in cyber threats, the demand for ethical hacking and the absence of a uniformed or mandatory code of conduct for ethical hacking. Chapter 1 identified the following research questions:

1) Are there ethical issues and issues of professionalism related to conducting ethical hacking engagements at law firms?
2) Should (and can) a framework be developed for law firms that allows them to conduct better due diligence when engaging ethical hackers and reduce the risks to the firm and their clients?
1) Would a code of conduct add value to the ethical hacking profession?

Chapter 2 reviewed the existing literature and identified relevant gaps. Key areas reviewed include the nature of both professionals and hackers, ethical hacking strategies and methods, potential threats and risks, why ethical hacking is needed, implied trust, certification, codes of conduct, the pathway to becoming an ethical hacker and any relevant
implications of ethical hacking. Cybersecurity standards and frameworks are also reviewed, in addition to regulation and legislation, the reasons for which cybersecurity is crucial in the context of law firms and, therefore, why ethical hackers are required to address cybersecurity in law firms.

Ethical hacking is not yet considered a profession, but it is considered an emerging profession. To be considered a professional, as defined by the requirements provided by various bodies, including the ACP, CEPIS, and the PSC, relevant criteria were identified and compared that of other professions, such as ICT and similarities identified to support ethical hacking as an emerging profession. The professional must possess knowledge and special skills, ensure quality, possess experience, conduct themselves ethically, be accountable and earn a living from the profession. As professionals, these requirements would apply to anyone in the ethical hacking profession; however, there currently exists no mandatory requirement or oversight. While most ethical hackers meet these criteria, some may not. Although ethical hackers undoubtedly possess specialist skills and knowledge, they may not receive the same professional recognition received by other professions. The reliance on an ethical hacker’s skills and ethics to ensure the security of information is of critical importance. Some systems tested by ethical hackers are considered to be highly sensitive, such as the systems of information held by law firms or critical infrastructure systems such as power, gas and water systems. Increasing regulatory and legislative requirements (e.g., the GDPR and NDB scheme) further highlight the importance of adequate and effective testing and conduct by ethical hackers.

Chapter 3 described the study methodology, selection justification and sampling information. A constructivist approach was selected as the best approach for exploratory research. Data were gathered via participant interviews and observations made by the researcher through the course of professional duties.
Chapters 4 and 5 identified and discussed the key findings from the interviews, particularly how these relate to the problem statement and research questions. This discussion included a proposed draft framework for the engagement of ethical hackers.

6.2 Conclusion of the Research

Ethical hacking is not currently a mandatory requirement of broader cyber related legislation and regulation, however, will likely be included in future regulation as part of a cyber-defence strategy. This type of approach has already been observed in some industries, such as the NYDFS Cyber Regulation; therefore, it is plausible that this requirement will become more widespread.

Law firms hold vast amounts of sensitive information and lawyers are entrusted to ensure the security of that information, with an expectation of legal professional privilege. In addition to legal professional privilege, there exists a risk of inadvertent access to personal information and subject to enforcement actions (e.g. penalties) of ever-increasing privacy laws (EUR-Lex, 2016).

Through the researcher’s extensive experience working in cyber security and specific work within the legal industry in Australia and the United States, a unique insight has been developed on how cyber security has evolved and matured, and the risks faced by law firms and organisations. For these reasons, the need to conduct further research was identified and the study has both confirmed some of those observed risks from the industry and highlighted additional ones.

This study has identified potential issues relating to ethics and professionalism. These focused on the following key areas: confidentiality, ethical obligations, reputation, knowledge and skills (including how an ethical hacker may go about acquiring and
maintaining them), trust and conflicts of interest. This set of identified issues highlights the need for a uniformed code of conduct to address these issues consistently.

Current controls largely rely on the execution of an NDA; however, this type of agreement is often executed between organisations, rather than individuals, which means that individual ethical hackers may not be fully aware of their obligations. Such an agreement also relies on individuals to do the 'right' thing and not breach the terms of the NDA.

Therefore, additional controls such as the proposed EHF may provide key benefits (as identified in the research questions). This framework includes contractual obligations (as are often currently practised) and additional checks on scoping, due diligence, conflict-checking and oversight. These checks occur before, during and following the engagement to assist in addressing any risks encountered throughout the lifecycle of the engagement. Such a framework may be easily adopted by any organisation wishing to engage an ethical hacker. However, because the framework is currently untested, additional empirical research should be conducted to validate the framework.

Merit may also be found in regulating ethical hacking and formal recognition as a profession. However, as the research identified, care must be taken to ensure that such regulation does not hinder the innovation and ability of ethical hackers to conduct their work and enhance their skills. Regulation could be used to ensure appropriate skill levels, certification and licensing and the formalisation of ethical hacking as a profession could be beneficial to achieving this. As identified, ethical hacking already includes many components of a profession by any definition; extensive education and training, performing a public service, an available code of ethics, a potential governing body that works closely with government, and as identified as critical from the research, special relations of trust. This special relation of trust as
identified from the research, is between those professions, such as lawyers that rely on the services and skills of an ethical hacker. Lawyers as an example rely on ethical hackers to help meet some of their professional obligations as well as have the expectation that an ethical hacker conducts themselves in an ethical, professional manner, and has the appropriate skills to do their job effectively. Although Conran (2014) has stated that many talented hackers remain uncertified, such controls would likely improve the field and provide benefits for the hackers themselves, potentially resulting in higher demand and increased compensation.

Regulation would also require all ethical hackers to adopt an approved code of conduct or ethics—this would add value to the ethical hacking profession. It would also assist in guiding ethical hackers' behaviour, particularly in situations where they may be unsure of the best course of action. The interviews uncovered that it was not uncommon for ethical hackers to be asked to perform questionable or even illegal tasks for clients, such as a client requesting that staff or board members' personal email accounts be tested. Guidance provided by a professional body may be beneficial in assisting with addressing or resolving such requests. This type of organisation could also assist with providing guidance on the use of other information sources (e.g., the dark web), including regarding the appropriateness of different kinds of information, processes and behaviours.

Merit may be found in the requirement for ethical hackers to belong to a professional association and abide by a uniformed code of ethics or conduct. Currently, depending on which criteria are used to define a professional, not all ethical hackers would be considered professionals. Such hackers do not meet the requirements as defined by Morrell (2003), CEPIS (2010), ACP (2018), do not belong to a professional association or do not abide by a specific code of ethics or conduct.
It would be helpful to determine which standard skills and certification an ethical hacker should possess—a professional body could help direct and endorse such a process. Each of the certifications discussed in this thesis has individual merits; however, they focus on different areas. A framework such as the Skills Framework for the Information Age (SFIA) is designed to address the issue of standardising the description of skills (Armstrong, 2009; Herbert, Lewis & De Salas, 2013; von Konsky, Jones & Miller, 2013). This framework could be applied to the IS industry, particularly ethical hacking, to identify which skills are required to competently perform the job. Further, certifications could be mapped to the SFIA framework to provide an easy comparison between different certifications, thereby defining a standard and removing some ambiguity surrounding the skill sets required by various certifications. This would make it easier for decision-makers to determine whether an ethical hacker possessed the appropriate certifications and, therefore, to reduce the risk to the organisation.

To conclude, there exist many areas requiring improvement in the ethical hacking profession and also ways in which law firms may continue to improve their security programs. The engagement of ethical hackers to test their defences will become more prevalent, which will result in potential risks that need to be managed.

Based on the researcher’s extensive professional and academic experience, the study findings are consistent with observations made in a day-to-day professional legal environment. Some key themes of the research (e.g., professionalism concerns) were identified by the researcher prior to commencing the study; the interviews conducted reinforced the existence and critical importance of such issues, particularly in a law firm setting.

It is crucial to provide the appropriate tools to help minimise risks, which could have significant consequences. Lawyers have obligations (as
professionals) to perform their jobs effectively—so, too, do ethical hackers. However, unlike many other professions, ethical hacking does not have a clear set of guidelines. The profession of ethical hacking will continue to grow and play a crucial role in modern society; therefore, one aim should be to raise it to the same maturity level as other professions.

6.3 Future Research Directions Arising from this Study

This study has highlighted the need for a mandatory uniformed code of conduct or ethics for ethical hackers. Although this research has focused on the context of law firms, the issues and application of such a code in other industries outside of legal would warrant further research.

Further development and empirical testing of a framework to manage the risks associated with the engagement of ethical hackers, particularly in environments that hold sensitive information, would be of value to and assist to further the maturity of the profession.

Another potential area of research relates to intelligence gathering, such as the use of questionable resources like the dark web, and whether these are valuable sources when the risks associated with using such sources are weighed against the potential gains.

Finally, defining the standard skills and certification required by an ethical hacker would be beneficial for establishing a baseline of what ethical hacking is and formalisation of ethical hacking as a profession. At present, there are no set standards—the value of each available certification is subjective and dependent on individual opinions.

6.4 Chapter Summary
This chapter began by summarising the previous chapters of this thesis. Next, it discussed the possibility for ethical hacking to be regulated, as seen in some jurisdictions already. The current controls used to manage risk within law firms (and more broadly) when engaging an ethical hacker are discussed, in addition to the potential value of a framework used to assist in further mitigating any risks. Finally, the chapter reinforced the key role played by ethical hackers in our modern connected world and suggested that the research lends itself to broader use cases that could also assist to mature the profession.
References


conference on Information security curriculum development (pp. 44-48).


Issues of Professionalism Concerning the Ethical Hacking of Law Firms

Georg A. Thomas


Thomas G., Low G. & Burmeister O. (2018a) 'Who was that masked man?': System penetrations—friend or foe?. In H. Prunckun (Ed.) *Cyber weaponry: Advanced sciences and technologies for security applications*. Springer, Cham.


U. S. Code (44).

USC § 3542 (b)(1).


Appendices

Appendix A: Data Security and Integrity

Cloud Storage/Backup: SpiderOak [https://www.spideroak.com](https://www.spideroak.com)

Creating and verifying SHA256 hashes: `Get-FileHash -Algorithm SHA256 -Path`

Windows PowerShell

Copyright (C) 2016 Microsoft Corporation. All rights reserved.

```
PS C:\Users\georg> Get-FileHash -Algorithm SHA256 -Path 'C:\Users\SpiderOak Hive\Research\test.txt'
Algorithm Hash Path

--------- ---- ----

SHA256

E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA4959
91B7852B855 C:\Users\georg\Documents\Spid...
```
# Hash Record

<table>
<thead>
<tr>
<th>File Name</th>
<th>Date</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>e.g test.txt</td>
<td>27/11/2016</td>
<td>E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934C</td>
</tr>
<tr>
<td></td>
<td>016</td>
<td>A495991B7852B855</td>
</tr>
</tbody>
</table>
Appendix B: PRISMA 2009 Flow Diagram

Source: Moher et al. (2009).
### Appendix C: Interview Master Record

The following table is an anonymised record of the interviews and the hash value of the original (post anonymised where appropriate) recording.

<table>
<thead>
<tr>
<th>Interview#</th>
<th>Date</th>
<th>Country</th>
<th>Level</th>
<th>Gender</th>
<th>Years Exp</th>
<th>Type</th>
<th>Reference</th>
<th>Auth Sent</th>
<th>Auth Checksum (SHA256)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>06-12-17</td>
<td>Australia</td>
<td>Partner</td>
<td>M</td>
<td>&gt;10</td>
<td>Law Firm</td>
<td>1-061217-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>12-12-17</td>
<td>Australia</td>
<td>IT/Security</td>
<td>M</td>
<td>&gt;10</td>
<td>Law Firm</td>
<td>1-121217-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>03-02-18</td>
<td>United States</td>
<td>Partner</td>
<td>F</td>
<td>&gt;10</td>
<td>Law Firm</td>
<td>1-020218-US</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>4</td>
<td>16-03-18</td>
<td>Australia</td>
<td>IT/Security Staff</td>
<td>M</td>
<td>&lt;10</td>
<td>Law Firm</td>
<td>1-160318-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>5</td>
<td>29-03-18</td>
<td>Australia</td>
<td>IT/Security Management</td>
<td>M</td>
<td>&gt;10</td>
<td>Law Firm</td>
<td>1-290318-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>6</td>
<td>09-04-18</td>
<td>Australia</td>
<td>Lawyer</td>
<td>M</td>
<td>&gt;10</td>
<td>Law Firm</td>
<td>1-090418-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>7</td>
<td>13-06-18</td>
<td>United States</td>
<td>Lawyer</td>
<td>M</td>
<td>&gt;10</td>
<td>Law Firm</td>
<td>1-130618-US</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>8</td>
<td>06-07-18</td>
<td>Australia</td>
<td>Lawyer</td>
<td>M</td>
<td>&gt;10</td>
<td>Law Firm</td>
<td>1-060718-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>9</td>
<td>20-08-18</td>
<td>Australia</td>
<td>Director</td>
<td>M</td>
<td>&gt;10</td>
<td>Consultant</td>
<td>1-200818-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>10</td>
<td>22-10-18</td>
<td>Australia</td>
<td>IT/Security</td>
<td>M</td>
<td>&gt;10</td>
<td>Consultant</td>
<td>1-221018-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>11</td>
<td>25-10-18</td>
<td>Australia</td>
<td>Consultant</td>
<td>M</td>
<td>&gt;10</td>
<td>Consultant</td>
<td>1-251018-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>12</td>
<td>26-10-18</td>
<td>United States</td>
<td>Consultant</td>
<td>M</td>
<td>&gt;10</td>
<td>Consultant</td>
<td>1-261018-US</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>13</td>
<td>29-10-18</td>
<td>Australia</td>
<td>Consultant</td>
<td>M</td>
<td>&lt;10</td>
<td>Consultant</td>
<td>1-291018-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>14</td>
<td>30-10-18</td>
<td>Australia</td>
<td>Lawyer</td>
<td>M</td>
<td>&lt;10</td>
<td>Law Firm</td>
<td>2-301018-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>15</td>
<td>09-11-18</td>
<td>Australia</td>
<td>IT/Security</td>
<td>M</td>
<td>&lt;10</td>
<td>Law Firm</td>
<td>2-091118-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>16</td>
<td>30-10-18</td>
<td>Australia</td>
<td>Consultant</td>
<td>M</td>
<td>&lt;10</td>
<td>Consultant</td>
<td>3-301018-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>17</td>
<td>09-11-18</td>
<td>United States</td>
<td>Consultant</td>
<td>F</td>
<td>&lt;10</td>
<td>Law Firm</td>
<td>1-091118-US</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>18</td>
<td>05-11-18</td>
<td>Australia</td>
<td>Lawyer</td>
<td>M</td>
<td>&lt;10</td>
<td>Law Firm</td>
<td>1-051118-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>19</td>
<td>02-11-18</td>
<td>Australia</td>
<td>IT/Security</td>
<td>M</td>
<td>&lt;10</td>
<td>Law Firm</td>
<td>2-021118-US</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>20</td>
<td>01-11-18</td>
<td>Australia</td>
<td>Consultant</td>
<td>F</td>
<td>&lt;10</td>
<td>Consultant</td>
<td>1-011118-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>21</td>
<td>05-11-18</td>
<td>Australia</td>
<td>Consultant</td>
<td>M</td>
<td>&lt;10</td>
<td>Consultant</td>
<td>2-051118-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>22</td>
<td>02-11-18</td>
<td>Australia</td>
<td>Partner</td>
<td>M</td>
<td>&gt;10</td>
<td>Law Firm</td>
<td>1-021118-AU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>23</td>
<td>31-10-18</td>
<td>United States</td>
<td>Lawyer</td>
<td>M</td>
<td>&gt;10</td>
<td>Law Firm</td>
<td>1-311018-US</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
### Issues of Professionalism Concerning the Ethical Hacking of Law Firms

#### Georg A. Thomas

<table>
<thead>
<tr>
<th>Interview#</th>
<th>Date</th>
<th>Country</th>
<th>Level</th>
<th>Gender</th>
<th>Years Exp.</th>
<th>Type</th>
<th>Reference</th>
<th>Auth Sent</th>
<th>Auth</th>
<th>Checksum (SHA256)</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>09-11-18</td>
<td>Australia</td>
<td>Partner</td>
<td>F</td>
<td>&gt;10</td>
<td>Law Firm</td>
<td>2-091118-AU</td>
<td>Y</td>
<td>Y</td>
<td>B3DC14D0956F9126E57DB85E6595CE7D22A4F06B35FC502E838E31EA</td>
</tr>
<tr>
<td>26</td>
<td>15-11-18</td>
<td>Australia</td>
<td>IT/Security</td>
<td>M</td>
<td>&gt;10</td>
<td>Law Firm</td>
<td>1-151118-AU</td>
<td>Y</td>
<td>Y</td>
<td>15962C7735FF03D41D0370E8CC7EA4523528BB18A0C5B2D2B84A6E6558A9</td>
</tr>
<tr>
<td>27</td>
<td>07-11-18</td>
<td>Australia</td>
<td>Consultant</td>
<td>M</td>
<td>&gt;10</td>
<td>Consultant</td>
<td>1-071118-AU</td>
<td>Y</td>
<td>Y</td>
<td>60118F99907F9785F9D4EDF86F99A84A59016A5DBDFC8F17E114C3A7C199</td>
</tr>
<tr>
<td>28</td>
<td>09-11-18</td>
<td>Australia</td>
<td>Director</td>
<td>M</td>
<td>&gt;10</td>
<td>Consultant</td>
<td>1-091118-AU</td>
<td>Y</td>
<td>Y</td>
<td>262ED420B8F46AE2F4B1F437AC0B85118C5B0D691E06E3311AC2578F338EDDODD</td>
</tr>
</tbody>
</table>
## Appendix D: Coding of Data

<table>
<thead>
<tr>
<th>Categories</th>
<th>Description</th>
<th>Sources</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavioural Ethics</td>
<td>Considerations related to behavioural aspects of ethics</td>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td>Client Requirement</td>
<td>Clients requiring or expecting that firms conduct testing</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Competence</td>
<td>Discussions relating to competence of ethical hackers</td>
<td>13</td>
<td>18</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Considerations regarding maintaining confidentiality</td>
<td>19</td>
<td>27</td>
</tr>
<tr>
<td>Conflict of Interest</td>
<td>Considerations related to conflict of interest scenarios</td>
<td>6</td>
<td>11</td>
</tr>
<tr>
<td>Contractual Obligations</td>
<td>The need for contractual requirements prior to engagement</td>
<td>9</td>
<td>13</td>
</tr>
<tr>
<td>Disclosure of Issues</td>
<td>Disclosure of identified vulnerabilities</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Disruption of Service</td>
<td>Considerations related to ensuring continued operations of the firm</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Due Diligence</td>
<td>Considerations and requirements related to verifying professionals prior to engagement</td>
<td>14</td>
<td>23</td>
</tr>
<tr>
<td>In-House Hackers</td>
<td>Using in-house resources to conduct tests against the firm</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Oversight and Frameworks</td>
<td>Discussions related to the need for oversight or guidance for ethical hackers</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>Need for testing</td>
<td>Discussion regarding the importance of conducting testing</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>Personal Information</td>
<td>Issues related to personal information</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Professional Standards</td>
<td>Discussions related to professional standards for ethical hackers</td>
<td>17</td>
<td>31</td>
</tr>
<tr>
<td>Regulation</td>
<td>Discussions related to regulating the ethical hacking profession</td>
<td>19</td>
<td>26</td>
</tr>
<tr>
<td>Topic</td>
<td>Description</td>
<td>Pages</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>Reputation</td>
<td>Issues related to reputation impact</td>
<td>8 9</td>
<td></td>
</tr>
<tr>
<td>Rogue Professionals</td>
<td>Issues related to rogue professionals</td>
<td>8 10</td>
<td></td>
</tr>
<tr>
<td>Scoping of Engagements</td>
<td>The need to ensure scope is appropriately created and managed during engagements</td>
<td>11 14</td>
<td></td>
</tr>
<tr>
<td>Security of Sensitive Data</td>
<td>Discussions related to security-sensitive data obtained during testing</td>
<td>9 17</td>
<td></td>
</tr>
<tr>
<td>Testing Firms</td>
<td>Awareness of whether a legal professional’s firm has been tested</td>
<td>6 6</td>
<td></td>
</tr>
<tr>
<td>Trust</td>
<td>Issues related to trust</td>
<td>8 11</td>
<td></td>
</tr>
<tr>
<td>Types of Testing</td>
<td>Discussions related to different types of ethical hacking or penetration testing</td>
<td>2 2</td>
<td></td>
</tr>
<tr>
<td>Unethical Use of Information</td>
<td>Issues related to the unethical use of information</td>
<td>4 5</td>
<td></td>
</tr>
</tbody>
</table>
20 November 2017

Mr Georg Thomas
By email: gethomas@csu.edu.au

Dear Mr Thomas,

Thank you for providing additional information in response to a request from the Charles Sturt University Human Research Ethics Committee relating to your research proposal.

The Charles Sturt University Human Research Ethics Committee is constituted and operates in accordance with the National Health and Medical Research Council’s *National Statement on Ethical Conduct in Human Research* (National Statement).

Based on the guidelines in the *National Statement* the Committee has approved your research proposal. Please see below details of your research project:

**Project Title:** Issues of Professionalism concerning Ethical Hacking within Law Firms

**Approved until:** 30 November 2018 (subject to annual progress reports)

**Protocol Number:** H17186 (to be included in all correspondence to the Committee)

**Progress Report due by:** 14 December 2018

You must report to the Committee at least annually, and as soon as possible in relation to the following, by completing the ‘Report on Research Project’ form:

- any serious and/or unexpected adverse events or outcomes which occur associated with the research project that might affect participants, therefore, the ethical acceptability of the project;
- amendments to the research design and/or any changes to the project (Committee approval required);
- extensions to the approval period (Committee approval required); and
- notification of project completion.

This approval constitutes ethical approval in relation to humans only. If your research involves the use of radiation, biochemical materials, chemicals or animals, separate approval is required by the appropriate University Committee.
Please contact the Governance Office on (02) 6338 4628 or ethics@csu.edu.au if you have any queries.

The Committee wishes you well with your research.

Sincerely

Mrs Sue Price
Governance Officer
On Behalf of Associate Professor Catherine Allan
Presiding Officer, HREC

Cc: Dr Oliver Burmeister and Dr Greg Low
22 March 2018

Mr Georg Thomas
Email: gethomas@csu.edu.au

Dear Mr Thomas,

Thank you for providing further information in response to a request from the Charles Sturt University Human Research Ethics Committee relating to your variation request.

The Charles Sturt University Human Research Ethics Committee is constituted and operates in accordance with the National Health and Medical Research Council’s *National Statement on Ethical Conduct in Human Research* (National Statement).

Based on the guidelines in the *National Statement* the Committee has approved your variation request. Please see below details of your approved research project:

**Project Title:** Issues of Professionalism concerning Ethical Hacking within Law Firms  
**Approved until:** 30 November 2018 (subject to annual progress reports being submitted)  
**Protocol Number:** H17186 (to be included in all correspondence to the Committee)  
**Progress Report due by:** 30 November 2018.

You must report to the Committee at least annually, and as soon as possible in relation to the following, by completing the ‘Report on Research Project’ form:

- any serious and/or unexpected adverse events or outcomes which occur associated with the research project that might affect participants, therefore, the ethical acceptability of the project;  
- amendments to the research design and/or any changes to the project (Committee approval required);  
- extensions to the approval period (Committee approval required); and  
- notification of project completion.

This approval constitutes ethical approval in relation to humans only. If your research involves the use of radiation, biochemical materials, chemicals or animals, separate approval is required by the appropriate University Committee.

Please contact the Governance Officer on (02) 6338 4628 or ethics@csu.edu.au if you have any queries.

The Committee wishes you well with your research.

Sincerely,

Mrs Sue Price  
Governance Officer  
on behalf of Associate Professor Catherine Allan  
Presiding Officer, HREC

cc: Dr O Burmeister and Dr G Low
Appendix G: Informed Consent Form

INFORMED CONSENT FORM

Project Title: Issues of Professionalism concerning Ethical Hacking within Law Firms
Researcher: Georg Thomas, Oliver Burmeister, and Gregory Low
Organisations: Charles Sturt University

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: ________________

NOTE: Charles Sturt University’s Human Research Ethics Committee has approved this project. If you have any complaints or reservations about the ethical conduct of this project, you may contact the Committee through the Executive Officer:

The Executive Officer
Human Research Ethics Committee
Tel: (02) 6338 4628
Email: ethics@csu.edu.au
Any issues you raise will be treated in confidence and investigated fully and you will be informed of the outcome.
PARTICIPANT INFORMATION SHEET

Project Title: Issues of Professionalism concerning Ethical Hacking within Law Firms

Principal Researcher: Georg Thomas

Supervisors: Oliver Burmeister and Gregory Low

Organisation: Charles Sturt University

Invitation

You are invited to participate in a research study on issues of professionalism concerning ethical hacking within law firms.

The study is being conducted by Georg Thomas (Doctor of Information Technology student) from the School of Computing and Mathematics at the Charles Sturt University.

Before you decide whether or not you wish to participate in this study, it is important that you understand why the research is being done and what it will involve. Please take the time to read the following information carefully and discuss it with others if you wish.

1. What is the purpose of this study?
   The purpose of this study is to further research on the issues of professionalism surrounding ethical hacking of law firms. This area is not yet researched and it is believed that the importance of these issues is likely to increase as law firms seek to increase their information security programs and engage the services of ethical hackers.

2. Why have I been invited to participate in this study?
   You have been invited to participate in this study because you have been identified as an individual who has relevant experience either working in or with law firms.

3. Will my firm/company be identified if I participate in this study?
   No, all data is anonymous and participants should not disclose the name of the firm or organisation they belong to. In the event that a participant accidentally identifies the name of their firm, it will be redacted from any captured data upon conclusion of the interview.

4. What does the study involve?
   This study involves being interviewed directly or participation in small focus groups by the researcher on their experiences with or as an ethical hacker. It is important to ensure no sensitive/classified or identifying information about the participants employer/organisation is disclosed during the interview. In the event of accidental disclosure, this information will be redacted. Interviews will be recorded and transcribed prior to analysis. Interviews will take place in person or via Skype depending as mutually agreed. A follow up survey may also be requested post-interview. The follow-up questions will be based on data collected during the interviews.
5. **How is ‘personal experience’ defined in the context of the study?**

   Personal experience is defined as the non-proprietary experience and knowledge gained in the course of professional employment and/or education at the participant’s current organisation, previous organisations, or institution. This experience should focus solely on issues related to the study and not include specifics about the participant’s organisation (such as security test results or identified vulnerabilities). In many cases this experience includes knowledge and skills outside of the area of ethical hacking such as how specific industry knowledge may relate to ethical hacking.

6. **Are there risks and benefits to me in taking part in this study?**

   There have been no identified risks of part-taking in this study as all data is anonymised, with the exception of some demographic data (country, level within the organisation/firm, interviewee type (client or provider)).

7. **How is this study being paid for?**

   This study is being funded by the researcher.

8. **Will taking part in this study cost me anything, and will I be paid?**

   There should be no additional costs associated with part-taking in this study. No payment is included as part of this study.

9. **What if I don’t want to take part in this study?**

   Participation in this research is entirely your choice. Only those people who give their informed consent will be included in the project. Whether or not you decide to participate, is your decision and will not disadvantage you.

10. **What if I participate and want to withdraw later?**

    If you do decide to participate you may withdraw from the project at any time without giving a reason and have the option of withdrawing any data (with the exception of data collected as part of a focus group), which identifies you.

11. **How will my confidentiality be protected?**

    Any information collected by the researchers which might identify you (name, email address, telephone number, and region) will be stored securely and only accessed by the researchers unless you consent otherwise, except as required by law. There are limits on assurances of confidentiality as law may subpoena research data/records.

    Research data will be kept encrypted at rest at all times and transmitted in an encrypted format. Data will be backed up to SpiderOak ([www.spideroak.com](http://www.spideroak.com)) a zero-knowledge cloud backup platform, which is only accessible by the researchers.

    Any data that is to be transcribed by persons outside the research team will be anonymised and referenced only by a numeric reference number.

    Any published research will not contain any identifiable references, however, demographic data (country, level within the organisation/firm (legal or corporate staff), interviewee type (client or provider)) may be available as part of the research.

    In the event of illegal behaviour, where specific information is provided, the researcher may be obliged to report the information to law enforcement.
Data will be retained for the duration of the research and then securely destroyed.

12. **What will happen to the information that I give you?**
The information will be included in a thesis for Mr Thomas’ Doctoral Degree.

Individual participants will not be identified in any reports arising from the project.

Any recorded audio from the interviews may be reviewed by the participant and be edited or erased upon request.

Due to the nature of focus groups containing multiple simultaneous participants, focus group recordings cannot be erased.

13. **What should I do if I want to discuss this study further before I decide?**
If you would like further information please contact the researcher Georg Thomas on +61 (within Australia), +1 (within the United States), or via email at gethomas@csu.edu.au

14. **Who should I contact if I have concerns about the conduct of this study?**
The researcher or project supervisors can be contacted at:

Georg Thomas (Principal Researcher/DIT Student)
e. gethomas@csu.edu.au
t. +61 (within Australia)
t. +1 (within the United States)

Oliver Burmeister (Supervisor)
e. oburmeister@csu.edu.au

Gregory Low (Co-Supervisor)
e. greg@greglow.com

Note: Charles Sturt University’s Human Research Ethics Committee has approved this project. If you have any complaints or reservations about the ethical conduct of this project, you may contact the Committee through the Executive Officer:

The Executive Officer
Human Research Ethics Committee

Tel: (02) 6338 4628
Email: ethics@csu.edu.au

Any issues you raise will be treated in confidence and investigated fully and you will be informed of the outcome.

Thank you for considering this invitation.
This information sheet is for you to keep.
Appendix I: About the Researcher

The primary researcher’s interpretation of the data relies on nearly two decades of experience within the industry, working across many different roles, industries and countries. The researcher is recognised as an industry leader and expert, which can be defined as a ‘thorough acquaintance with some area of knowledge together with experience in applying and/or extending that area of knowledge’ (Lincoln & Guba, 2013, p. 56).

The researcher is an IS and risk leader based in Melbourne, Australia. He is the National Security and Risk Manager for a premium independent law firm with over 600 attorneys and 1200 employees. Prior to joining that firm, he was based in New York and held Director and senior management roles for a global consulting firm. In this role, he provided IS-related consulting services, including leading ethical teams, hiring ethical hackers and conducting ethical hacking engagements with law firms across the USA, including many AMLAW100 firms and Fortune 500 companies. He also served as IT Manager for a Melbourne-based law firm from 2008 to 2011. His legal management roles involved being responsible for the procurement and engagement of ethical hacking services.

The researcher holds a number of industry certifications including the Information Systems Audit and Control Association Inc. (ISACA) CISM, the International Information System Security Certification Consortium (ISC)² CISSP, the International Council of Electronic Commerce Consultants (EC-Council) CEH and Certified Chief Information Security Officer (C|CISO) and the Microsoft Certified Systems Engineer with Security specialisation (MCSE(S)). He also received the Microsoft Most Valuable Professional Award in 2014, 2015 and 2016.

He is a Senior Member of the ACS, a Certified Professional with the Cyber Security specialisation (MACS Snr. CP [Cyber Security]) and a member of the ACS Profession Advisory Board National Ethics Committee.
The researcher served on the ISACA New York Board of Directors in 2016 and 2017. ISACA® is a non-profit, independent association that advocates for professionals involved in IS, assurance, risk management and governance.

In addition to his professional pursuits, Georg is a lecturer with IT Masters, lecturing and assisting with the development of curriculum for their Master of Cyber Security course.