A management approach to securing geospatial information systems

Steven Woodhouse, Jason Howarth, and David Tien

Abstract—Geographic information has and will always play a vital role in the complex process of human progress. Traditionally, this information in the form of maps has been the source of both knowledge and power, providing the details from which the decisions that defined national boundaries and economic empires were made. Today, through the development of information technologies, we have the ability to produce electronic maps that contain vast amounts of geospatial information.

On 11th September 2001, the world became a different place not only in the United States, but also in nations around the globe. Coupled with the ensuing Bali bombings in Indonesia a year latter and the bombings in the United Kingdom in 2005 a key message is that despite Australia’s relative isolation from the rest of the world, it is vulnerable in terms of its critical infrastructure.

Because all details about this critical infrastructure are stored in geospatial information systems found in both the public (Federal, State & Local) and the private sector, it is imperative that some form of information security is applied to protect these assets. This paper reviews the application of information security in this critical area.

Index Terms— Geospatial information, Information security, Risk management, Security

I. INTRODUCTION

Geospatial information systems (GIS) encompass information about natural resources, the environment, land ownership and use, transport, communications, utility services, demography and socio-economic factors, in fact any information that can be related to location. The location can be identified by a number of means, such as land parcel, local government area, electorate, postcode, town, line or point.

Using mapping, surveying, aerial photography, remote sensing, global positioning technologies and satellite imagery unique databases of geospatial information about the world we live in are compiled. Through the use of advanced technologies and skills, these unique databases can be merged with other sources of expert knowledge to produce the most comprehensive picture of our environment ever created. As [1] states “Sometimes the visual language of GIS allows us to communicate without saying a single word, which is the essence of effective communication”.

Access to this knowledge gives us the ability to manage our current environment and plan our future environment. It also has the potential to provide our enemies with more information about our critical infrastructure than they have ever been able to obtain. The power and potential of this geospatial information is only limited by the imagination.

The development and implementation of an Information Security Management System (ISMS) to protect this geospatial information would seem the most logical step. The ISMS would define and describe the security measures needed to protect the geospatial information system based on regulatory compliance and the organisation’s own risk appetite.

The key theme of this paper is a review of the current literature in the planning and management of information security, in particular, Information Security Management Systems (ISMS) in the context of geospatial information systems.

The paper is divided into six sections with section one being this introduction. Section two reviews the basic objectives of information security. Section three reviews and describes the risk management process. Section four reviews risk perception. Section five reviews the need for holistic and proactive management of information security. Finally, section six summarises the current view of Information Security Management System’s and suggests directions for further research.

II. INFORMATION SECURITY OBJECTIVES

Information is the life blood of all modern organisations. The purpose of information security is to protect valuable assets, such as geospatial information, hardware, software and people. Through the evaluation, selection and application of appropriate controls, information security helps organisations meet their business objectives or mission by protecting its physical and financial assets, reputation, legal position, employees, and other tangible and intangible assets [2].

Information security should support the business objectives or mission of the organisation, it must be cost effective, must be holistic, and fit into the organisation’s culture seamlessly. Holistic information security should integrate technology, people and processes.

The aim of planning, designing and implementing security in and around geospatial information systems is to ensure not only the confidentiality and integrity of the information produced, stored and used but also the continued availability of both the geospatial information and supporting infrastructure [2]-[6].

The C.I.A triad represents the basic, industry accepted, principles of information security. It is widely agreed [23]: [29]; et al. that these three concepts broadly represent the many
other aspects of information security on which most practitioners focus their efforts. The prime focus of information security, as depicted in Fig 1 below, is maintaining a balanced Confidentiality Integrity Availability (C.I.A) triad.

Fig 1. C.I.A triad

Confidentiality of information is the practice of preventing unauthorised disclosure of information, or ensuring that information is accessible only to those authorized to have access.

Integrity is the process of ensuring the security and trustworthiness of systems, data and geospatial information so that it can be used to make business decisions. Integrity dictates that changes to an entity can only be made in a specified manner, and by specified people or processes. Accuracy and authenticity of geospatial information must be guaranteed.

Availability of geospatial information is the concept of accurate and timely access to the organisation’s information systems and dependant business processes when required.

It is contended in [23] that the classic triad of “C.I.A” is inadequate to describe the requirements of information security for the modern enterprise. A new information security framework to express, in relevant language, the means for information owners, designers, builders and users the requirements to protect the information is required. This new framework would consist of six security elements – availability, utility, integrity, authenticity, confidentiality, and possession – to replace the C.I.A foundation [23].

The reliance by every organisation, both public and private, upon information technology has increased dramatically as technology has developed and evolved. Over the past two decades in particular, the nature of computing has changed significantly, becoming an integral part of business processes.

Geospatial information has developed into a strategic asset, and the computerised information systems have become strategic tools for both organisations and government [4]-[5]; [7]; [10]. Geospatial information is now critical to business operations and decision making activities, allowing organisations to survive and grow in competitive and tough economic environments, and governments to provide services and infrastructure to their constituents. Unfortunately, these critical geospatial information systems are being exposed to greater security risks as organisations push their technological resources to the limit in their desire to achieve more in less time.

As discussed at great depth in [11] “the world is an increasingly dangerous place and maybe more so today than ever before” and “they [risk assessors] are faced with a greater number of threats than ever before and the potential for more sophisticated attacks against corporate assets”. As organisations have evolved management has applied the sophistication of new technology without due regard to the shortcomings and risks inherent in its application. Advances in technology, especially the Internet, have allowed organisations to expand rapidly by utilizing e-business. Unfortunately, the development of security tools has lagged behind and as e-business and Internet applications continue to grow it has become more difficult to protect organisational assets [20].

Organisational strategies have changed, and businesses have altered their organisational structures, management structures and work patterns in order to leverage technology to its greatest advantage. Trends such as downsizing, outsourcing, process re-engineering, distributed architecture, client/server and e-business all include the aim of making the organisation leaner and more efficient. Originally, mainframes were kept in well secured computer rooms and users could connect only from approved locations over static point-to-point connections. Then personal computers and LANs rocked the security boat, the use of the Internet and e-business threatened to sink it [20]. Now, management of organisations need to recognise and acknowledge the risks associated with these technologically-based solutions and implement systems to mitigate the risks.

III. RISK MANAGEMENT

An effective risk management process is an important core component of a successful ISMS. The principal goal of an organisation’s risk management process should be to protect the organisation and its ability to perform its stated mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organisation.

The risks of abuse increases as systems and processes become more distributed and decentralised. Unfortunately, basic security procedures are often overlooked in the redesign of the work environment, or the importance of security is rated lower that the perceived needs of other factors. The changing structure of organisations also has direct implications for security.

One of the key functions of IT managers, CIO (Chief Information Officer), CTO (Chief Technology Officer), CISO (Chief Information Security Officer), is loss avoidance. As discussed in [12] it is asserted that IT managers should strive for loss avoidance “…. by managing risk intelligently to reduce the likelihood of trouble in the IT sector and reduce the costs of coping with trouble” [12].

The Australian Standard, HB 231:2004 Information security risk management guidelines [13], defines threats, assets, vulnerabilities and security risks as follows:

**Threats**: A threat has the potential to cause an unwanted incident that may result in harm to a system or organisation and its assets. This harm can occur from a direct or an indirect attack on an organisation’s information. Threats can originate from accidental or deliberate sources or events.
Denial of Service
Theft
Interruption & Disclosure
Fabrication
Destruction
Modification
Threat

Threats are actions or circumstances affecting information systems assets (computer hardware, software, data, people and buildings) that have the potential to cause loss. Loss can result from processes of modification, erasure, interceptions, fabrication, destruction, damage, theft, leakage, interruption and denial of service. These occurrences come from both intentional and unintentional actions.

Intentional actions include fraud, theft, hacking, viruses, unauthorized access, industrial espionage, sabotage, etc, while unintentional actions include "acts of God" such as earthquakes, fire, flooding, storms, etc and accidents such as burst water pipes, motor vehicle / aircraft / train wrecks, etc.

The table below details the processes causing loss as a result of intentional and unintentional acts

Table 1: Processes causing loss

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modification</td>
<td>Can occur to stored data, transmissions, software and hardware. Modification can occur due to human error, “acts of God”, fraud, hacking, etc.</td>
</tr>
<tr>
<td>Destruction</td>
<td>Affects hardware, software, data, transmissions and documents. This can be caused by human error, sabotage, hacking, accidents, “acts of God”, viruses, etc.</td>
</tr>
<tr>
<td>Fabrication</td>
<td>Applies to data, transmissions and documents. The main sources are industrial espionage, sabotage, hacking and fraud.</td>
</tr>
<tr>
<td>Disclosure</td>
<td>Occurs from leakage of data. This can be caused by the interception of transmissions, unauthorized access, industrial espionage, hacking, spy ware, etc.</td>
</tr>
<tr>
<td>Interruption &amp; Denial of Service</td>
<td>Can affect hardware, software and data. Usually caused by hacking, viruses, accidents, “acts of God”, human error, industrial espionage, etc.</td>
</tr>
<tr>
<td>Theft</td>
<td>Of hardware, software, data and other resources can occur through acts of hacking, spy ware, stealing of physical property, copyright infringement, industrial espionage, etc.</td>
</tr>
</tbody>
</table>

In order to manage these threats effectively, an organisation’s management must understand the character of the threat, the value of the asset and the possible outcomes these threats pose to the organisation’s geospatial information asset. This information is usually gathered during a threat and risk assessment carried out using a generic risk management process such as AS/NZS 4360:2004 or other models such as CRAMM, FIRM, SARA & SPRINT, COBRA or OCTAVE [3]; [11].

No organisation can develop effective information security measures unless it has a clear understanding of what it is trying to protect itself from. In this context a threat can be defined as “…any potential source of harm to the reliability or integrity of the IT system…” [14].

Threats to information systems originate with people. It is proposed in [5] that these people fall into five groups. These groups are:
- criminals (thieves, fraudsters, organized crime);
- malefactors (hackers, vandals, terrorists, cyber-warriors, some ex-employees and other disgruntled or vengeful individuals);
- spies (commercial and governmental);
- undesirables (scam artists, spammers, ‘ethical’ hackers and nerds); and
- the incompetent, or the simply unaware (staff, contractors, customers and other third parties).

One of the indicators of the level of effective security management is the rate of computer-related crime and abuse. Computer crime is defined by the Australian Institute of Criminology as “…offences in which a computer is the object of the offence or the tool for its commission” [21]. Generally a number of different terms are sometimes used interchangeably to describe crimes committed using computers.

It is extremely difficult, if not impossible, to estimate the true extent of losses suffered by organisations due to computer crime, electronic attack and computer access misuse and abuse. Most computer-related crimes probably go undetected [15].

The United States 2004 CSI/FBI Computer Crime & Security Survey put the total losses from 57% of its respondents at $16 million, and went on to say “If these results are typical of other Australian public and private sector organisations, the figure [$16 million] represents only a small fraction of total losses due to computer crime, electronic attack and computer access misuse and abuse in Australia during the survey period”. The United States 2004 CSI/FBI Computer Crime & Security Survey put the total losses from 54% of its respondents at $141 million down from $201 million in 2003.

The Australian 2004 Computer Crime & Security Survey also reported that 49% of respondents suffered one or more electronic attacks in the last 12 months, up from 42% in 2003. Two percent of respondents reported they didn’t know if they had experienced any electronic attacks, down from 4% in 2003.
The rate of abuse occurrence appears to be similar over the past decade. While the majority of electronic attacks in Australia are sourced externally to the organisation [22], the highest risk of successful computer abuse comes from employees within the organisation [2]. Employees within an organisation have detailed knowledge of procedures, where assets are held and how, if at all, they are protected. The Computer Security Institute (CSI) in San Francisco, USA, estimates that between 60% - 80% of all network misuse is perpetrated by people inside the organisation [2].

The proposition of internal threat is certainly supported by investigations and surveys into computer crime over the past decade in particular. In the Office of Strategic Crime Assessments (1997) Computer Crime and Security Survey, the largest category of perpetrator was ‘insiders’. This survey goes on to report that 87% of those that had experienced incidents identified a source internal to their organisation, while 61% of those that experienced an incidence identified a source external to their organisation. The Australian Computer Crime & Security Survey [22] reported static levels of internally sourced attacks over the past three years. In 2003 36% of those that had experienced incidents identified a source internal to their organisation, it was 36% again in 2004 while in 2005 37% of those that had experienced incidents identified a source internal to their organisation.

The picture outside Australia is a little different. According to the CSI/FBI Computer Crime and Security Survey [16] 66% of those that had experienced incidents identified a source internal to their organisation, while the Information Security Industry Survey conducted in 2000 revealed that insiders still pose a more serious security threat to an organisation than outsiders. There also appears to be a high percentage of cases where an organisation has detected a computer crime, but is unable to identify the perpetrators responsible. These figures clearly indicate that the current security measures being implemented in organisations are inadequate.

IV. RAISED SECURITY CONSCIOUSNESS

A major need for effective information security arises from the poor state of security and low awareness levels within organisations. There is a need for increased security awareness in all stakeholders and users at all levels. It is claimed that [24] “A successful security awareness programme may help change the actual mindset and behaviour of people toward security”. Awareness is one key to protecting an organisations geospatial information assets [25]. Practice has shown that when education programmes have been conducted and employees understand protective measures and why they have been implemented, rates of abuse are reduced and employees become more aware of security issues [24]-[26].

Any discussion of risk reveals there is no shared common concept. Questions usually asked are: “what risk? who’s risk? perception of risk?, risk attitude, risk behavior?” [8]. In this context it is all of this so it is appropriate to clarify the meaning of significant words, particularly ‘risk’ and ‘uncertainty’. Risk perception is the subjective judgment that people make about the characteristics and severity of a risk. The word “risk” is most commonly used in reference to natural hazards or threats to the environment, personal circumstances (health, insurance, investments, etc), society (terrorism, economic performance, food safety etc), and business (corporate governance, strategy, business continuity, etc).

Yet there is still no broad consensus on the meaning of this term. The national and international standards and guidelines used for this paper attempt to describe risk, but there are many different definitions and underlying concepts in these documents. There is also a huge variation in the general literature, reflecting the lack of agreement on the basic definition of risk. Even among risk practitioners in the various professional bodies such as ISACA there is an ongoing debate about a definitive definition for the term ‘risk’.

There used to be a common belief that security and technical systems concepts are too complex to be understood by non-IT staff. It was suggested that this belief may have emerged from the inability of IT people to explain concepts in non-technical terms. The belief now is, people make the difference to information security and training on the ethical, legal and security aspects of IT resource usage should be ongoing at all levels within the organisation [27]-[28]. Security awareness training must not only be conducted for isolated groups of employees, but for every employee at every level of the organisation. “With proper training and education, people can even become the most effective layer in an organisations defences” [24].

People will react to different aspects of the content and structure of risk messages. A poorly constructed risk message will not be able to function as adequate communication and may confuse them rather than promoting the desired response. A major component of the risk problem is human behaviour. Preventable system failure inevitably stems from human action [9], when the people involved in the design, operation of a system fail to perceive some set of conditions that might arise and cause the security of the system to be compromised. People adjust their risk-taking behaviour towards their ‘comfortable’ level of risk (i.e. their ‘secure’ level of risk)

Given that perception is influenced by non-epistemological factors and that this is an irreducible condition, it seems that the prospects for the systematic elimination of risk are exceedingly poor [9]. The implications for an ISMS is risk cannot be managed effectively by simply implementing hardware and software controls. The core design of the ISMS needs to change by focusing more on changing attitudes and human behaviour.

V. HOLISTIC AND PROACTIVE MANAGEMENT

The need for a more holistic and proactive approach to planning and managing information security is a paramount consideration for organisations wishing to implement an effective ISMS. The call for a more holistic approach continues to come from numerous sources [7]; [12]; [17] and is becoming more pressing as technology advances and e-business becomes common place.

Security measures need to be implemented to protect geospatial information systems and ensure their integrity, confidentiality and continued availability. Unless the security strategy and implementation is appropriately aligned with
organisational goals its effectiveness will be limited [7]. Information security mechanisms must be pertinent to the organisation’s objectives and activities, and their integration is necessary to ensure security is effective and appropriate.

Information security is not an IT problem, it is a business problem and is different to IT security. Information Security is a broad term covering all forms of information, including paper files and telephone conversations as well as computerized information systems. It also includes physical elements, such as physical access to an organisation’s premises.

In contrast, IT security concentrates on the control of information in an electronic medium. It focuses on information technology, and includes data, computers and networks. As a result of this difference the team implementing an ISMS should include all levels of management and information owners, not just IT staff.

A holistic view requires a comprehensive, top-down, organisation-wide perspective to planning security. Such a view does not happen by accident, it requires full and active involvement from many levels and activities within the organisation [17]. In [18] it comments “We need to focus on demonstrably important, practical risk management measures, not on prophylaxis for theoretically interesting but rare or nonexistent risks”. A holistic perspective will ensure a consistent, structured, and effective security solution is applied and isolated point solutions are avoided. Information security should not be considered only in terms of technology, but must be treated in holistic terms, as social systems in which technology is only one element.

Proactive management requires planning and the implementation of proactive security measures before problems arise, rather than waiting until a security violation has occurred. To achieve this, an organisation’s senior management must be aware of its security risks, understand how solutions can be applied in the context of organisational goals and be prepared to invest resources to ensure these proactive actions. This also requires an active distribution of responsibility for the security of information by stakeholders and ownership by stakeholders of that responsibility [19]. In order to achieve this, effective communication about the business risks that result from inappropriately designed, implemented or omitted technology risks is paramount. Security and risk mitigation must be embedded into the organisational culture to ensure all employees are automatically mindful of security issues in their planning, managing and operational activities.

VI. DISCUSSION AND CONCLUSION

The reliance upon geospatial information systems to produce accurate and timely information for decision making is increasing. However, the rate of technological advancement for the use and deployment of these geospatial information systems is much faster than the development of means to ensure the integrity, confidentiality, and continued availability of these information systems. Although management of organisations are becoming more aware of security issues, the rate of computer-related crime and abuse remains relatively high.

Awareness of security risks are reported to be low in studies carried out over the past few years. These studies also indicate that security measures implemented within organisations to protect information are generally poor. Responsibility for security is assigned on an ad-hoc basis, if at all, and information owners, custodians and users are not held responsible for the security of the information they hold and use. The planning and management of information security appears to be poor in most organisations.

These issues would indicate a need for a more comprehensive or holistic view of information security and its management, a proactive approach to the security of information assets and programmes to raise the awareness of security issues. In short, an ISMS should be established to successfully secure the geospatial information assets of an organisation. A well defined and implemented ISMS addresses a wide spectrum of issues during the planning, management and monitoring of information security within an organisation.

Further research into how risk messages are framed and delivered, and the risk perception by individuals within an organisation might help find a correlation between how a person collects and interprets information presented to them and their risk taking behavior. This research should identify how the design of the ISMS may need to change by focusing more on changing attitudes and human behavior.

REFERENCES

[8] Coleman, L, Why managers and companies take risks, Physica-Verlag, Germany, 2006
[17] IT Governance Institute, IT Alignment: Who is in charge?, IT Governance Institute, USA, 2005