A Strategic Framework for Managing Internet Security

Elena Sitnikova  
School of I.T. and Mathematical Science  
University of South Australia  
Adelaide, Australia  
Elena.Sitnikova@UniSA.edu.au

Mehdi Asgarkhani  
Department of Computing  
CPIT  
Christchurch, New Zealand  
Mehdi.Asgarkhani@CPIT.ac.nz

Abstract—The internet which was originally developed as an open distributed system has since evolved to become a key platform for connectivity of businesses and communities. Today, the internet is used for transferring critical information amongst strategic approach in security management of critical information amongst corporations 

Today, information is being stored and accessed globally through a wide range of Internet access technologies. Consequently, today, vulnerabilities and risks to the Internet are equally relevant to systems that are integrated within corporate networks. Cloud Computing solutions, Supervisory Control and Data Acquisition (SCADA) systems and the Bring Your Own Device (BYOD) approach adopted by some organizations are examples of complexity of managing Internet security today. These systems are not only vulnerable to own system specific issues but also threatened by other Internet-related vulnerabilities. Whilst numerous previous studies have identified the need for managing Internet security, there remains a need for a comprehensive approach in security management of the Internet and sensitive Industrial Control Systems (ICS) integrated systems. This paper examines research on Internet security using a risk management approach. It presents an overview of key issues and recommends a management framework for secure Internet access.


I. INTRODUCTION

The internet in its original form was designed to be an open and distributed environment where security and mutual mistrust was not a primary concern. Today, the internet has developed into a global network with access available to almost anyone. As a consequence, cyber security has become a critical issue. Information is a critical asset for many companies and is part of the core business for many corporations [14]. Given the integration of critical strategic systems such as SCADA systems and complex Cloud Computing solutions, Internet and information security management has become a critical issue worldwide. In addition to cases highlighted above, some organizations in recent years have adopted an approach (Bring Your Own Device – BYOD) that allows employees connect own devices (such as tablets, laptops and mobile phones) to corporate networks. This approach significantly increases the risk to corporate networks and internet security. More specifically, there are significant risks in allowing devices that are not standard devices with approved/tested installed images (portfolio of software) to access a corporate network.

Today, information is being stored and accessed globally leading to threats by cyber-security risks - such as hacking, viruses, worms and phishing – to name but a few. Most organisations recognise the necessity to continuously monitor and improve their internal security procedures using security governance processes. At the same time, they invest in the full range of internet security software options. However, lack of experienced security personnel often leads to incorrect policy configurations creating vulnerabilities [R10]. Vulnerabilities have existed for a long time; however, systems with weaknesses continue to arrive and get installed [10] and worsen the security problem. The responsibility for many of these vulnerabilities must be directed towards the companies who are too keen to release fundamentally unsecure software with a ‘patch later’ attitude [10].

The profiles of cyber-criminals can vary significantly, a shy introvert, a smart professional, an organised gang with significant funding to employ smart hackers, government funded groups who have access to state-of-the-art equipment. Their motivations are equally diverse and can include financial gain, revenge, political, ego and curiosity. Whatever the reason, the results can be devastating for individuals and/or organisations who are at the receiving end of an attack. Attacks are not limited to outside attacks. That is to say, organisations including those who make use of complex technology solutions (e.g. SCADA and Cloud Computing) must ensure that they put in place sufficient security controls to resist attacks from all possible sources. Motivated by factors mentioned above, this paper investigates broader Internet security and information security concerns. In analysis of key issues and vulnerabilities and in recommending a framework for minimizing security risks, this paper follows a broad risk management model and considers the following factors:

- Analysis of broader vulnerabilities related to the Internet
- Investigation of causes and sources of threats, the likelihood of threats from specific sources and risk implications (significance)
• Recommending mitigation plans and a framework for security management

In presenting the paper, cases (examples) of complex systems that are integrated into corporate networks are deployed to emphasize the importance of managing Internet security. Sections 2 to 5 in this paper elaborate on cases of complex systems which are connected to the Internet via integration into corporate networks. Their vulnerabilities are outlined before recommending a framework for managing Internet security and protection of attached corporate systems (section 6). Discussions presented in this paper are the outcome of preliminary investigations with the aim of developing a risk and security management model (hypothesis) for further validation in later stages of this investigation. The methodology for this stage of study has been mainly focused on review of previous literature and analysis of a number of case studies related to cyber security issues and concerns.

II. INCREASED COMPLEXITY OF INTERNET SECURITY: INFRASTRUCTURE AND IT ARCHITECTURE MANAGEMENT SYSTEMS

This section of the paper presents two examples of increased complexity in Internet security by outlining basic principles of Cloud Computing and SCADA systems.

The concept of Cloud Computing emerged in the fourth quarter of 2007 [5] as a joint project between IBM and Google. It is defined (by National Institute of Standards and Technology - NIST) as “a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Cloud computing provides large amount of resources for developing and deploying applications and services. The cloud computing paradigm is an attractive model to upgrade, extend or replace many of the services hosted by the traditional data center. Privacy and integrity are some of the biggest concerns in the implementation and use of cloud computing services. Cloud computing services operate via connection to corporate networks and the Internet. The introduction of this service has meant an increased sensitivity in managing cyber and Internet security.

SCADA systems are generally used to automate complex processes where human interference to collect data in assessing overall performance of a system is not possible. Cases of SCADA in managing electricity generation and distribution or in managing water resources are examples of SCADA as strategic technology system with benefits that reach beyond an organization or one community. Traditionally, SCADA was seen as being a technical engineering tool to automate complex processes. However, soon it was realized that what SCADA systems achieve benefit not only engineers but also decision makers within organizations. It moved from being an engineering solution to be become as a key corporate system. SCADA operations are complex as they involve diverse group of people. Becoming aware of the role of each group and the ways in which groups complement each other’s skills is a critical aspect of successful operation of SCADA. The diversity of groups of people and cultures involved can also lead to risks in operational issues including cyber and information security. Today, SCADA is not only connected to internal network within organisation, but also to the Internet. Therefore, SCADA is exposed to cyber security risks discussed earlier - similar to any other system connected to the Internet.

Overall SCADA provides authorities with control capabilities such as:

• Accessing quantitative measurements of important processes
• Detecting and correcting errors in a timely fashion – as soon as they are detected
• Measuring trends in the ways in which a system functions over time
• Detecting and addressing critical issues and bottlenecks and other inefficiencies
• Controlling complex and sophisticated processes without need for specialist human resources

Those capabilities mentioned above are provided by combination of functions which are in turn supported by various components of SCADA. They include four key functions: data acquisition; networked data communication; data presentation and control. These functions are performed by various SCADA components such as sensors and control relays; remote telemetry units (RTUs); SCADA master unit and the communication network. Another key component of SCADA is the Human Machine Interface (HMI) or (MMI) – Man Machine Interface. As outlined above, SCADA systems have numerous components performing sensitive tasks communicating critical information via corporate networks and the Internet. Consequently, there are significant potential security risks to these systems via Internet vulnerabilities.

III. ANALYSIS OF MOST COMMON VULNERABILITIES AND SOURCES OF THREATS

In previous sections the added complexity of Internet security management was discussed. It was outlined that addition of ICSs and complex Cloud Computing solutions introduce further complexities to information and Internet security management. What’s more, the adoption of BYOD by organizations and allowing remote access to corporate networks have resulted in other layers of risks to managing Internet security.

In this section, before presenting an analysis of Internet and corporate networks vulnerabilities, information management and information security issues are briefly discussed.

In recent years, much of the growing investment on IT systems has been in technology solutions. However, organizations are also required to comply with legal and regulatory requirements to ensure both the quality and security of data and information – resulting in an increase in cost of compliance. The investment on compliance is a clear indication of the reality of risks of operating within the cyberspace and importance of information security.
Internet security breaches have serious implications. Smith (2001) reported that an Australian man was sent to prison in October 2001 for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel. Janelle Bryant of the Australian Environmental Protection Agency reported that “Marine life died, the creek water turned black and the stench was unbearable for residents.” The hacker made 46 attempts to take control of the sewage system during 2000 [22], [24].

In another incident in 2003 the SQLSlammer worm hit the Internet and managed to infect 90 percent of its 75,000 victims within 10 minutes. The worm managed to breach the network of Ohio’s Davis-Besse nuclear power plant – via a contractor of the company. Slammer then crashed the power plant’s computerized display panel and a monitoring system (Poulsen, 2003). The plant was not in use at the time as it had been shut down months earlier; however, the corporate network suffered significant performance issues.

The two incidents presented above highlight the importance of not only Internet security but also protecting complex infrastructure management systems that are connected to the Internet. They demonstrate the impact of breaches in network and Internet security. However, it should be noted that it is not in every company’s interest to acknowledge attacks on their sensitive systems. That is to say there are cases of Internet security failures that have not been discussed in the public domain [16].

As mentioned earlier, the Internet was originally designed to be open without concerns for security. Therefore, as expected, the architecture has vulnerabilities which attackers can exploit.

These (vulnerabilities) can include:

- **Connectivity and resource sharing**: the Internet is an open network designed for information sharing accessible globally via a routable IP address.
- **Authentication, integrity and traceability**: As there is no inherent authentication in place, IP spoofing where false information is injected into IP packets can be possible.
- **Internet Security**: There are numerous insecure unpatched systems connected to the Internet.
- **Intelligence and resources asymmetry**: it appears that almost all the ‘Intelligence’ of the Internet resides at the end hosts - attackers can quickly overwhelm the end hosts.
- **Lack of centralised control on Internet** – due to the global nature of the Internet, there is no overall central authority responsible for network security.
- **Broadcast concept for data communication** - the broadcast concept implies that other computers should ignore data not destined for them, but they can be modified to listen and even change information in data streams.

Adyinka (2008) suggests that some of the more common Internet attack methods used by cybercriminals can include: Viruses, Trojans and Worms, System and Boot Record Infectors, Eavesdropping, Hacking, IP Spoofing Attacks, Denial of Service, Email Bombing and Spawning, Phishing and Man-in-the-middle attacks.

Numerous studies and reports have attempted to assess the cost of cybercrime to organizations. According to the 2012 Norton Cybercrime Report the global rate of direct cybercrime losses rose to $110 billion in 2012. The report highlights that almost 1.5 million people around the world are affected by cybercrime on a day to day basis. The report suggests that nearly half (46%) of the adult on-line population has experienced some kind of cybercrime. Ponemon Institute’s Cybercrime Report presents in details the results of a study of views of business leaders and IT professionals located in five countries (United States, United Kingdom, Germany, Hong Kong and Brazil) regarding the effects and cost of cybercrime on business. The overall indication is of rising cybercrime activities [18]. In a report on UK businesses it was determined that human error was the cause of breaches with the largest indirect financial losses [19]. What’s more, the Information Security Breach Impact report indicated that 82% of organisations had experienced staff related incidents [R10]

Aslanoglu and Tekir (2013) suggest that in 21st century the concept of war has experienced a major paradigm shift. They argue that today, the battle ground is cyberspace and contemporary weapons are continuously renovated viruses, worms, Trojans, denial-of-service and botnets – to name but a few. What’s more, they claim that the strategy of cyberwar is to damage core attributes of information security resorting to propaganda, espionage or destruction of critical infrastructures.

They continue to demonstrate cases of cyberwar including Estonia cyberwar and Georgia cyberwar. Estonia attack is the first known public cyberwar. It brought the country’s IT infrastructure to a halt even though Estonia was one of the most developed countries in Europe with ubiquitous use of information and communication technologies in various fields and industries. The Georgian cyberwar had commenced before Russian invasion into Georgia. The method of these attacks primarily included defacement of public websites (e.g. the National Bank) and Denial of Service attacks against government sites, important media sites and financial institutions [3].

Critical infrastructure control systems (SCADA) have been historically perceived as being safe and efficient - due to their total isolation from external (and un-trusted) networks. Therefore, there has been a high degree of dependency on legacy ICSs [23]. However, as these systems begin to integrate into new communications and networking technologies, we observe both negative and positive implications. On the positive side, the migration into new infrastructures and integration into modern networks empowers organizations to benefit from more efficient methods of communication, more robustness, secure data, quicker time to market and interoperability. At the same time, deploying legacy systems into the modern computing environment can introduce a raft of cyber related vulnerabilities and risks [20] – since these legacy
systems were never designed to be risk-proof against mobile and Internet networks. The interconnection of old (legacy) SCADA systems to the Internet, corporate networks, telephone lines, computer networks and wireless systems has created opportunities for potential attacks. For instance, creating opportunities for terrorists, hobbyist hackers, disgruntled employees and other groups to get access to critical infrastructures (e.g. power grids) and cause considerable damage [R23]. What’s more, with SCADA systems, for the time being, bolted-on (rather than more reliable embedded solutions) security is likely to be seen as the only practical way to tackle the critical security management concern. This further complicates the overall management of Internet security – as it concerns these systems.

Systems and technologies (including software and applications) have often been seen as the core source of security breaches and compromises. However, recent studies in technology management [1] clarify that procedural and human factors can be equally important sources of breaches. Nicholson et al (2012) suggest that between 1982 through to 2000 SCADA attacks were 70 percent internal – mostly related to disgruntled employees and mistakes). The rest (30%) represented external sources – such as hackers and cyber terrorists). On the other hand, Eric Byres presented a different pattern that between 2001 through 2003 70 percent of compromises were external and 30 percent were internal. Nicholson et al (2012) outlines that “it is unlikely that the number of internal attacks had lowered in any way; simply that the number of external attacks had risen so much as to cause these figures.” Regardless, the statistics presented above demonstrate that internal sources of compromises are to be treated seriously as they represent a significant proportion of breaches.

Considering issues related to new trends in using the Internet and network services such as Cloud Computing, from a technical perspective, the majority of security risks associated with cloud computing are already present in traditional networks and data centers. However, the majority of problems are not inherently technical or directly related to Internet vulnerabilities. They are instead related to implicit need to trust external parties to maintain critical information and provide critical IT services. A key approach is compliance with standards and service level agreements to minimize risks.

After presenting an overview of potential vulnerabilities, some of the most common sources of attack initiators are:

- Bot network operators – They are hackers who instead of breaking into systems take over several systems to coordinate attacks.

- Terrorists - Amongst the most concerning sources of attacks is terrorism [16].

- State Sponsored Hackers - Currently, the extent of attacks conducted by these kinds of attackers seems to have been minimal. However, state hackers should be considered to be one of the most dangerous threats to Internet security and critical systems attached to the Internet – simply due to easy access to resources including financial means.

- Criminal groups (organized crime hackers) – Organised crime is motivated by money and hence holding companies to ransom by attacking their corporate networks and in particular their critical systems such as SCADA via the Internet.

- Insider attacks (Disgruntled employees) - Disgruntled employees are reported by Blau (2004) to be the most common internal source of security breaches.

- Hobbyists - Hobbyists are often driven by curiosity or seeking popularity and can cause significant damage to infrastructure if insufficient safeguards are in place.

- Hacktivists - Activist hackers or “Hacktivists” can also cause security risks to Internet security. Attacks based on political reasoning and motivation has been cited in a number of government website defacements [9].

- Unskilled key personnel - IT personnel who are authorized to access critical components of networks but are not possess necessary technical skills and are unaware of processes.

The Internet and systems that rely on the Internet for connectivity may not necessarily be under attack from all sources mentioned above at the same time. What’s more, some of the sources mentioned above are more likely to be the cause of security breaches than others – depending on the type of industry and networks involved. In taking a risk management framework to mitigate risks, it is important that the likelihood of being under attack from various sources is analyzed and taken into consideration.

IV. A RISK MANAGEMENT APPROACH FOR MANAGING SCADA SYSTEMS SECURITY

Previous studies [16] have highlighted that any private or public sector organization with a network that is connected to the Internet is exposed to cybersecurity risks. The risks can be of catastrophic magnitude if a critical system (e.g. SCADA for managing a national power grid) is integrated into the company’s network.

Some of the risks involved include brand damage, loss of revenue, share price reduction and in severe cases and most importantly loss of life. Robles, Choi, Cho, Kim, Park, & Lee (n.d, p.18) classify threats to critical infrastructure into three categories as natural threats, human-caused, and accidental or technical. However, in this paper a broader (strategic) classification is taken into consideration in order to develop a security and risk management framework.

A review of vulnerabilities and sources of risks shows that they can be put in (related to) three main categories:

- Technology – Systems hardware and software

- People – who work with and/or manage corporate networks and systems - including those who set policies and processes

- Governance, Frameworks and Processes – which govern use of systems by people
A. Technology

In general, most solutions and approaches for security management were focussed on system solutions. Solutions outlines in this section relate to broader Internet security management. In this section relate both to broader Internet security and more specific SCADA systems’ security.

- Penetration testing - These tools and solutions are used to help security professionals to perform tests on networks and connected systems. Penetration testing is done to assess security against risks and exploits that are known to the community of security management professionals. For instance, SCADA systems specific modules for penetration testing include Nessus, Metasploit, Core IMPACT and Immunity CANVAS [16]. The drawback of this technique is that it effective against known risks only.

- Honeynets - Honeynets [21] are simulation models of systems (e.g. ICSs) that can be put in place to distract hackers from targeting the real system.

- Simulated Attacks (War games) - Similar to penetration testing, this technique can be used to assess vulnerability of network integrated systems. Richard Clark (once cyberspace security advisor to the U.S. President) claimed that mock intrusion scenarios “have always, always succeeded” [16].

- Access Control – Discretionary Access Control (DAC) and Mandatory Access Control (MAC) are two different approaches. Commercial systems use DAC in which the resource owner determines who can gain access. The MAC system decides itself who can gain access to the particular resource, much like a security guard.

- Cryptographic Systems – this involves encrypting data with a unique key.

- Firewalls – designed to block unwanted traffic either in to or out of a private network.

- Intrusion Detection Systems (IDS) – an IDS system can be hardware or software based and is designed to monitor the network to look for signs of an attack

- Anti-Malware Software and Scanners – these are software based and designed to seek out and destroy malware

- Internet Protocol Security (IPsec) – provides fundamental security at the IP layer of the TCP/IP protocol. It is a point-to-point protocol within which one side encrypts and the other decrypts using one or more shared keys [1] and [15].

- Secure Socket Layer (SSL) – this is a suite of protocols designed to use key exchange, authentication and encryption to create a secure channel for transmission of data.

- Honey Pots – these are decoy servers or systems designed to gather information regarding an attacker or intruder attempting to gain access into your system.

- Sandboxing - enables captured potentially malicious code to be executed in a safe and controlled environment.

- Black Listing - is a network administration practice used to prevent the execution of undesirable programs.

- White Listing – is similar to black-listing, but this time a simple list of authorised programs is maintained.

Some companies offer specific system solutions. For instance, companies such as Tofino offer security solutions that are specific to SCADA and control networks [15], [16]. On the other hand, companies such as Digital Bond develop tools that can be used in more general IT and corporate network situations.

B. People

Systems and networks are run by people. Systems and technology related security measures alone cannot guarantee secured operation of systems. Regardless of robustness of design and reliability of protecting solutions, people related issues can compromise systems.

People are frequently seen as the weakest link in cyber security - [2], [7], and [16]. Greene (2008) argues that social engineering is a method that has a history of success where systems have been compromised by exploiting humans. Slay and Miller (2007) suggest that only the deployment of optimum mix of technological solutions and human best practices can ensure security of systems and networks – including SCADA [7].

Some of the people related issues that can potentially create an environment where security is compromised include:

- Lack of understanding and awareness of implications of security compromises

- A relaxed culture where system reliability is not taken seriously

- Lack of training for admin staff so they can understand functions and risk implications

- Lack of management training to be aware of value of security and cost of being exposed to risks to their businesses

- Shortage of suitably trained and skilled technical staff who manage the operations of the system

- An environment where teamwork is not encouraged – for instance, different groups such as engineers, IT workers and admin workers due to different work culture and personalities run the risk of not working together towards a shared objective.

- Cultural differences in multicultural environments where culture crashes may also result in teams not working together towards shared outcomes.
People who work with networks associated systems can be put into three main categories: technical staff (engineers and IT personnel), admin staff and management.

Engineers and IT personnel need to be equipped with skills necessary to maintain and operate the technical aspects of systems. At the same time, technical skills alone are not sufficient to operate corporate networks effectively. Technical staff need to operate within an environment where importance of security is understood and supported by all groups alike. Occasionally there are confusions on categories and specifications of needed technical skills. Standards (e.g. SFIA – www.sfia.org.uk) where skills categories are clearly outlined can be useful tools for ensuring needed technical skills as specified by standards are available. Certification by recognized industry trainers can be another tool to ensure staff are trained adequately and possess standard technical skills needed to operate systems. Today, regulatory agencies place more responsibility on organisations to provide evidence and formal documentation that operators and supporting teams have the necessary skills needed to safely and effectively manage and maintain their networks and ICSs. For instance, organisations such as the Gas Certification Institute (GCI), Telvent and the Information Assurance certification Review Board (IACRB) offer training and certification to professionals seeking SCADA recognized training.

Admin staff generally operate non-technical functions of networks. However, general admin skills are not sufficient to be a successful operator within complex systems. Admin staff need specific training to be aware of broader issues related to the systems they are working with – including awareness of security risks, implications and processes.

Management teams, including both corporate and strategy level technical managers are responsible for delivery of outcomes as expected by organizations and communities. Managing organizations and complex systems requires not only an understanding of broad technical issues but also an awareness of business and financial parameters. The key function of management in organizations where complex networks and critical systems operate is governance. Governance in this case refers to processes that ensure both selection and deployment of systems and operations of chosen systems are managed effectively. Most of issues related to management, governance and processes are discussed in the next section.

C. Governance Strategies and Processes

IT governance is essential to ensure that the use of IT is aligned with strategic objectives of the organisation. Risk management is an integral part of IT governance. This is to ensure that risks (as outlined in previous sections) are adequately addressed to minimise potential threats to the organisation.

Effective governance of operational aspects can often be achieved via putting in place standardized processes to be followed by all groups of people working on networks and interconnected systems that are integrated within networks. Standardized processes can often be more effective if they are based on industry standards. Some of the industry standards that are applicable to both managing network and Internet security were discussed by Susanto (2011) who suggested that the top five standards are being ISO 27001, BS 7799, PCIDSS, ITIL and COBIT.

Some of the most commonly practiced standards are:

- **ISO27001** – This standard looks at the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving documented Information Security Management Systems (ISMS) within an organisation.

- **BS7799** - This standard concentrates on the implementation of ISMS and also incorporates the Plan-Do-Check-Act (PDCA) system and aligns with the ISO 9000 quality standard.

- **PCIDSS** - The Payment Card Industry Data Security Standard (PCIDSS) is an internally adopted standard defined by the Payment Card Industry Security Standards Council. It was created to help organisation process credit card transactions and prevent credit card fraud by implementing strict data controls.

- **ITIL** - The Information Technology Infrastructure Library (ITIL) is a set of concepts and practices relating to Information Technology Services Management, IT development and IT operations.

- **COBIT** - Control Objectives for Information and Technology was created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute. It is described as a set of practices (framework) for IT management. COBIT has 5 main areas; strategic alignment, value delivery, resource management, risk management and performance management [13].

- **ISO27002:2007/ISO17799:2005** – ISO27001 was discussed earlier as an information security management standard. The ISO27002 series builds on the old ISO17799 standard which in turn built on the old British standard BS7799 (discussed earlier (IT Governance, 2011)).

- **ANSI/ISA-99.02.01-2009** - In 2008 NIST released a comprehensive guidance on securing SCADA systems in the special paper 800-82, Guide to Industrial Control Systems (ICS) Security. This document addresses issues ranging from an outline of SCADA systems, security program development and technical controls and network architecture.

- **ITSEAG Generic SCADA Risk Management Framework for Australian Critical Infrastructure [8].**

- **TISN Critical Infrastructure Resilience Strategy [6].**

With regards to ICSs integrated into corporate networks and the Internet, ISO standards address issues that cover various aspects of effective management of SCADA systems – including: organization of information security; asset management; human resources security; physical and environmental security; communications and operations.
management; access control; information systems acquisition, development & maintenance; information security incident management; business continuity management and compliance.

The emergence of cyber terrorism domain means that a new group of potential attackers on computer and telecommunication technologies may be added to traditional criminals threatening IT infrastructure. Ontologies provide another common framework to share conceptual models. By using an ontology, the internal and external environment of a field can be captured in conjunction with the relationship between these environments. These people propose that an ontology can be used to identify and capture the content and boundaries in the field of cyber-terrorism. The role of the ontology will be to provide a better structure and depiction of relationships, interactions and influencing factors as suggested by Noy and McGuiness (2001) [26].

V. A STRATEGY MODEL FOR MANAGING INTERNET SECURITY: A CORPORATE NETWORK MANAGEMENT PERSPECTIVE

It was noted earlier that the use of Information Systems has spread beyond companies and businesses to customers and suppliers. Information systems facilitate improving business processes and therefore achieving productivity which can either directly or indirectly benefit customers. The spread of systems to customers and suppliers via network connectivity and Internet solutions increases the vulnerability of systems within organizations. Information Security Management Systems (ISMS) have presented companies with solutions to avoid security risks. Some of the techniques to mitigate Internet security risks were outlined in the previous section. At the same time, Norman and Yasin (2013) suggest that these solutions are often based on common practices and current understanding of information security needs. Consequently they may not necessarily offer optimum solutions. The latest security survey by PWC (Norman and Yasin, 2013) indicated that 33% of respondents did not report any security incidents. However, there was an increase in reported security incidents from 3% in 2010 to 8% in 2011. The survey results also showed that IT personnel’s confidence in readiness of business to confront information security risks had dropped from 76% in 2010 to 72% in 2011. The decrease in confidence seemed to be justified given that only 40% of respondents believed they used effective security management solutions while the rest of participants seemed to have been still busy determining the best security management strategies.

The study by Norman and Yasin (2013) suggests that effectiveness or success of security management systems was attributed to three key elements [17]:

- **Technology characteristics**: security infrastructure and tools & support mechanisms
- **Organization structure**: type of industry, size of business, top management attitude/support, formalization and resources available
- **Environment**: Governance, enforcement and market structure

<table>
<thead>
<tr>
<th>TABLE I. SCADA SYSTEMS SECURITY MANAGEMENT FRAMEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Elements of Internet Security Management</strong></td>
</tr>
<tr>
<td><strong>Systems and Technology</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

| **People (Technical staff)** | System specific training – understanding specific system issues |
| | Teamwork training |
| | Training on cultural and role issues |
| | Security training |
| | Standards and best practices guidance |
| | Certification and compliance |
| **People (Admin staff)** | System specific training – understanding specific system issues |
| | Teamwork training |
| | Training on cultural and role issues |
| **People (managers)** | Business awareness of value of securing their system |
| | Understanding security incidents and their |
| | Business implications; |
| | Impact on environment and community |
| | Championing standards, governance and processes |
| **Management, governance and processes** | Addressing policy and process issues: Information management policies, Information access strategies |
| | Clearly defining roles and responsibilities |
| | Defining and documenting information management strategies |
| | Preferably, implementing what is listed above via adopting industry standards such as: ISO27001, BS7799, PCI-DSS, ITIL, |
| | Participating in industry specific forums to share knowledge and learn |
| | Ontologies as a common framework to share conceptual models of security management |

In broadening discussions presented by Norman and Yasin (2013) on effectiveness, overall, effectiveness can be achieved by deploying a strategic framework where all three key aspects
of Internet security management are taken into consideration. Putting together all prevention and mitigation measures discussed in the previous section, the framework (model) outlined in table 1 is a recommended approach for managing security by minimizing risks and by giving consideration to the three key elements of security management discussed in this section.

This framework is presented as a checklist for risk management. It outlines possible course of action to be considered as related to every aspect of a strategic security management.

It should be noted that the framework presented above is the outcome of this stage of the study. It is recommended that this model be examined for further validation through investigations at a later stage of the project.

VI. CONCLUSIONS

This paper addressed a topic that can best fit into the body of knowledge characterized as broader Internet security management and governance of the Internet and the cyberspace. Cloud computing, ICs (e.g. SCADA) and BYOD approaches were used to highlight the increasing importance of managing Internet security within existing complex and sophisticated networks.

Overall, the objective of the paper was to develop a framework that highlights solutions (at management, policy and strategy level) for managing Internet security as it relates to various components of systems (people, processes and systems).

This paper took a risk management framework methodology. More specifically, based on review of cases and previous studies, this paper discussed broader information management and Internet security issues followed by assessing risks and vulnerabilities were analysed (both types and potential initiators of threats) before prevention and mitigation plans were investigated.

The paper identified that vulnerabilities and tools for attacks to include: Viruses, Trojans & Worms, System & Boot Record Infectors, Eavesdropping, Hacking, IP Spoofing Attacks, Denial of Service, Email Bombing & Spamming, Phishing and Man-in-the-middle attacks.

The initiators or sources of attacks could fall into any of the following categories: Bot network operators, Terrorists, State Sponsored Hackers, Criminal groups (organized crime hackers), Insider attacks (Disgruntled employees), Hobbyists, Hacktivists and Unskilled key personnel.

The paper suggested that based on analysis of risks, threats and initiators of attacks, an effective Internet security management framework must consider various elements that contribute to operations of a system. They are: technology, people and processes. More specifically, it was recommended that technology solutions alone cannot guarantee secure and reliable operations. There is a need for a holistic and strategic approach that considers technology alongside other factors – an approach that addresses the “people, technology, policies” triangle. It was recommended that the proposed model be further examined and validated in future studies.

REFERENCES


