CRITICAL INFRASTRUCTURE INFORMATION SECURITY: IMPACTS OF IDENTITY AND RELATED CRIMES

Rodger Jamieson∗ Lesley Land† Stephen Smith‡
Greg Stephens** Donald Winchester††

∗University of New South Wales, r.jamieson@unsw.edu.au
†University of New South Wales, l.land@unsw.edu.au
‡NSW Department of Commerce, Stephen.Smith@commerce.nsw.gov.au
**University of New South Wales, g.stehens@unsw.edu.au
††University of New South Wales, d.winchester@unsw.edu.au

This paper is posted at AIS Electronic Library (AISeL).
http://aisel.aisnet.org/pacis2009/78
CRITICAL INFRASTRUCTURE INFORMATION SECURITY:
IMPACTS OF IDENTITY AND RELATED CRIMES

Rodger Jamieson
Visiting Professor of Information Systems
School of Information Systems, Technology and Management
Australia School of Business, University of New South Wales
ANZAC Parade, Kensington, Sydney, NSW 2052, Australia.
r.jamieson@unsw.edu.au

Lesley Land
Senior Lecturer, School of Information Systems, Technology and Management
Australia School of Business, University of New South Wales
ANZAC Parade, Kensington, Sydney, NSW 2052, Australia.
l.land@unsw.edu.au

Greg Stephens
Senior Lecturer, School of Information Systems, Technology and Management
Australia School of Business, University of New South Wales
ANZAC Parade, Kensington, Sydney, NSW 2052, Australia.
g.stephens@unsw.edu.au

Stephen Smith
Senior Project Officer, Federated Information Exchange
Office of the Government Chief Information Officer, Department of Commerce
Level 21, McKell Building, 2-24 Rawson Place, Sydney, NSW 2000, Australia
Stephen.Smith@commerce.nsw.gov.au

Donald Winchester
Research Fellow, Security, E-Business, Assurance Research (SEAR) Group
School of Information Systems, Technology and Management
Australia School of Business, University of New South Wales
ANZAC Parade, Kensington, Sydney, NSW 2052, Australia.
d.winchester@unsw.edu.au

Abstract

The physical and digital security of a nation’s critical infrastructure is necessary for its citizens, commerce and their public and private owners’ to conduct successful business transactions. A complicating factor towards this security is the multi-jurisdictional nature of some critical infrastructure assets e.g., telecommunications or financial systems. Information systems (IS) and information technology are playing an ever more important role in the security of a nation’s (state, territory, or province’s) critical infrastructure. This longitudinal study investigates public sector critical infrastructure incidents across nine sectors in an Australia state - New South Wales. The New South Wales State Government is the largest by full-time employees in Australia. An action research methodology was employed. Data was collected by online survey, complemented by interviews and secondary data searches. Results were reinforced from independent sources. Our main finding is that NSW State Government IS security incidents against critical infrastructure assets are decreasing in both nominal and relative terms over time as prevention techniques and solutions are increasingly becoming available. However, we must be cautious in making causal inferences or generalising to other organisational situations without further study investigating other exogenous determinants.

Keywords: Critical Infrastructure, IS Security Incidents, Identity Crime, Cyber Crime.
1. INTRODUCTION

Information systems (IS) and information technology (IT) usage and their interoperability are continuing to increase for communities social and economic transacting across the globe. The downside to this is the deviant behaviour of some individuals or groups in the offline or online channels who seek to gain from other legitimate transactions via identity crimes (theft, fraud) and identity related crimes (e.g., terrorism, money laundering, or trafficking). The deviance (or delinquency) is mostly from adults but also from a growing number of juveniles (Pontell and Rosoff, 2009). The perpetrators can go to the extremes of putting the security of a nation’s (or state, territory, province’s) critical infrastructure (information) at risk by breaching, stealing, looting, disrupting, damaging or destroying it (Baskerville and Portugual, 2003; Pontell and Rosoff, 2009). In Australia, “the greatest sources of financial loss for 2006 were due to theft or breach of proprietary or confidential information; computer facilitated financial fraud; and telecommunications fraud” (AusCERT, 2006, p.4). Critical infrastructure can be publicly and/or privately owned and managed and are essential “to the minimum operations of the economy and government” (US Government, 1998, p.1). Critical infrastructure has been defined in legislation and by organisations. Most commonly associated with the term are facilities for:

- electricity generation, transmission and distribution;
- gas production, transport and distribution;
- oil and oil products production, transport and distribution;
- telecommunication;
- water supply (e.g., drinking water, waste water/sewage, stemming of surface water);
- agriculture, food production and distribution;
- heating (e.g., natural gas, fuel oil);
- public health (e.g., hospitals, ambulances);
- transportation systems (e.g., fuel supply, railway network, airports, harbours, shipping);
- financial services (e.g., banking, clearing and settlement); and
- security services (e.g., police, military).

In the United States (US) the Patriot Act (2001) and Section 2 of the Homeland Security Act (2002) define critical infrastructure as those “systems and assets, whether physical or virtual, so vital to the US that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” The US Federal Computer Fraud and Abuse Act (18 U.S.C. S1030) where actual losses exceed US$5,000, as well as other US federal or state laws may be applicable for events against critical infrastructure involving computers or information systems. In addition, the Federal US Identity Theft Enforcement and Restitution Act (2008) now removes the prior US$5,000 threshold effect “for hacking computers and other cybercrime charges against a perpetrator” (Santa Fe, 2009, p.11). Countries which act as intermediaries for outsourcing data centres in the ICT sector should not be overlooked because they are part of the critical ICT infrastructure which may facilitate IS security intrusions. These countries which may include: India, China, Singapore, Malaysia, or Indonesia.

In Australia, there is no unique legislation for critical infrastructure offences against organisations. The two main pieces of legislation that are applicable for the Commonwealth of Australia are the Crimes Act (1914, and amendments) and the Criminal Code Act (1995). There may be some specific legislation which covers particular industries, such as airports or defence infrastructure (e.g., Defence Act, 1903). The Commonwealth Criminal Code Act 1995, Part 10.7 - Computer Offences, legislates against activities (incidents) such as:

- computer intrusions (e.g., malicious hacking);
- unauthorised modification of data, including destruction of data;
- Denial-of-Service (DoS) attacks;
- Distributed Denial of Service (DDoS) attacks using botnets; and
- the creation and distribution of malicious software (e.g., viruses, worms, trojans).
The Australian Federal Attorney-General’s Department describes Critical Infrastructure as (Lundy, 2003, p. 1):

“… those physical facilities and those information technologies and communication networks which would, if destroyed, degraded or rendered unavailable for an extended period, impact on the social or economic well-being of the nation or affect Australia’s ability to conduct national defence and ensure national security.”

Section 2 reviews the critical infrastructure and closely related literature. Section 3 discusses our methodological approach and Section 4 our results. Section 5 observes simulations and Section 6 briefly explains implications and limitations. The last section concludes and suggests future research.

2. LITERATURE REVIEW

There exists at least two distinct strands of critical infrastructure research – security and network management (Bass, 2000; Hale and Brusil, 2007). “Both help prevent, detect, and recover from disruptions whether the disruptions may be, for example, component failures (addressed by the network manager) or malicious acts (addressed by the security manager)” (Hale and Brusil, 2007, p.530). Network evaluation is an important element of critical infrastructure analysis and has been investigated by other disciplines including, mathematicians, statisticians and engineering (Bayrak and Brabowski, 2006). Networks could include for example, closed-circuit television (CCTV) systems, supervisory control and data acquisition (SCADA) systems and remote access solutions. Closely related to and in Australia included within (Rothery, 2005) the security management research of critical infrastructure are the emergency services or response literatures (Chen, 2008; Klashner, and Sabet, 2004; Turoff et al., 2004). Intrusion detection techniques in IS and networks play an important deterrence role in network management (Yue and Çakanyildirim, 2007; Zhu and Premkumar, 2001). Where techniques such as, data mining are used then privacy issues have been raised especially with information or data sharing (known as computer sharing in the US) (Li and Sarkar, 2006). Others have publicly stated that the lack of information sharing has hindered law enforcement efforts (Mitchell, 2008). International evidence of information security enforcement has found displacement effects with deterrence. “US enforcement substantially increases attacks originating from other countries” (Png, Wang and Wang, 2008, p.125).

Baskerville and Portougal (2003, p. 3) posit “terminal defence” and “collective action” as two essential strategies for the protection of critical infrastructures. These strategies can involve preventative measures to improve system security or the exchange of threat and countermeasure information e.g., research and development (Baskerville and Portougal, 2003; Lukasik et al., 1998). Baskerville and Portougal (2003) also discuss two theories for analysing security – probability used as a base for risk analysis and possibility theory. They reject probability theory because it “is not a good basis for security in the case of high-stakes information resources where these resources are subject to attacks upon national infrastructure” (Baskerville and Portougal, 2003, p. 3). They favour possibility theory stating that “persistent well-supported, and highly professional intrusion attacks will have a higher possibility of success … a theoretical framework more suitable for the protection of complex national infrastructures” (Baskerville and Portougal, 2003, p. 3). Similarly, the literature has investigated security guards of critical infrastructure assets (physical) comparing their pay rate to the average US salary, and their powers and training to police (Parfomak, 2004). Weaknesses in the identity processes online and offline have lead to adoption of biometrics as a means to better assure critical infrastructure security (Ryan, 2006). Industry organisations in Australia (AusCERT, 2006) and the US (Richardson, 2008) have collected data from public and private organisations about the extent of their security incidents. In Australia, the surveys have looked at security incidents (among other things), sampling organisations with critical infrastructure from throughout the country. The results were mixed in with other organisations in the analysis (AusCERT, 2006). Penetration simulation

---

1 Gordon and Dion (2008) show definitions of other countries e.g., Canada, Germany, Netherlands and the United Kingdom as well as Australia and the US.
exercises such as Cyber Storm and Cyber Storm II have also been undertaken in a similar vein across several countries including the US and Australia (Australian Government 2008a). A gap in the literature exists regarding security incidents arising from critical infrastructure assets only. We fill this gap by investigating critical infrastructure incidents across nine sectors in the New South Wales (NSW) State Government setting. The main research question to be addressed is what are type and number of security breach incidents occurring across the NSW State Government?

3. METHODOLOGY

Information systems research has an established methodology of using action research to investigate practical research problems (Baskerville and Wood-Harper, 1998; Susman and Evered, 1978). An action research methodology was followed for our data collection as our goal is to determine the change of IS incidents on critical infrastructure assets during our study. We classified 60 agencies into the nine broad Australian Federal Government critical infrastructure asset sectors at the start of the study. Online surveys were used as a medium to collect data for 2001, 2002, 2003, 2004 and 2006 on IS incident intrusions from New South Wales government agencies (see Table 2). A sample of the online survey questions from the survey instrument are exhibited in Table 1 below. This survey was not conducted in 2005 for political reasons - a forthcoming election. Government agency’s IS security managers where tasked as those responsible for completing the online survey questionnaires. The managers were required to answer qualitative and quantitative questions. The survey data was complemented with selected interviews from about 10 of the surveyed critical infrastructure agencies. The duration of the interviews was approximately 90 minutes during which open-ended questions were asked. The number of agencies varied over the study period due to mergers, demergers, closures, or new agencies being created. Data collected from the interviews consisted of notes of issues raised by participants, audio recorded interviews, short surveys and questionnaires relating to security issues. Secondary data from government publications and third party IS security surveys (e.g., AusCERT, 2006) were also used as the basis for analysis in this study. Australian cases of IS security intrusions within many of the nine critical infrastructure sectors were included to illustrate the real implications on targeted organisations and the community.

<table>
<thead>
<tr>
<th>Sample of Questions from Online Survey (Quantitative and Qualitative)</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many information security incidents occurred in calendar year 2006?</td>
</tr>
<tr>
<td>How is the incident count maintained?</td>
</tr>
<tr>
<td>What are the business consequences of an information security incident involving - Loss of financial or material assets by public, government or private sector?</td>
</tr>
<tr>
<td>Does your agency have a current risk assessment, if not when will there be one?</td>
</tr>
<tr>
<td>What is the inherent likelihood of the security incident that would be most likely and significant in causing loss of financial or material assets by public, government or private sector?</td>
</tr>
<tr>
<td>Does the agency use IS security standard AS/NZS 17799.2 or ISO/IEC 27001?</td>
</tr>
<tr>
<td>Approximately how many different pieces of NSW or Commonwealth legislation does your agency have to comply with?</td>
</tr>
</tbody>
</table>

*Table 1. Survey Instrument: Example Questions from Online Survey*

4. RESULTS AND DISCUSSION

In Australia, there are nine defined critical infrastructure sectors; namely, banking and finance, emergency services, energy and utilities, food, health care, IT and communications, mass gatherings, transportation, and water (Choo, Smith and McKusker, 2007, p. 65). Table 2 shows the nine key sectors, examples of services within the sectors and sector-specific government (national) agencies.
Table 2. Summary of Australia’s key critical infrastructure sectors (Choo et al., 2007a, p. 65)

<table>
<thead>
<tr>
<th>Key sectors</th>
<th>Examples of services within the sectors</th>
<th>National government agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking and finance</td>
<td>Banking, securities and investment</td>
<td>Attorney-General’s Department</td>
</tr>
<tr>
<td>Emergency services</td>
<td>Chemical, biological, radiological and nuclear safety, hazardous materials,</td>
<td>Emergency Management Australia, a division of the Attorney-General’s</td>
</tr>
<tr>
<td></td>
<td>search and rescue, and dams</td>
<td>Department</td>
</tr>
<tr>
<td>Energy and utilities</td>
<td>Electrical power, natural gas, oil production, transmission systems, and in</td>
<td>Department of Industry, Tourism and Resources</td>
</tr>
<tr>
<td></td>
<td>future nuclear power production</td>
<td></td>
</tr>
<tr>
<td>Food</td>
<td>Safety, supply and distribution, agriculture and food industry</td>
<td>Department of Agriculture, Fisheries and Forestry</td>
</tr>
<tr>
<td>Health care</td>
<td>Hospitals, health care and blood supply facilities, laboratories and</td>
<td>Department of Health and Ageing</td>
</tr>
<tr>
<td></td>
<td>pharmaceuticals</td>
<td></td>
</tr>
<tr>
<td>Information technology</td>
<td>Telecommunications, broadcasting systems, international submarine cable and</td>
<td>Department of Communications, Information Technology and the Arts</td>
</tr>
<tr>
<td>and communications</td>
<td>postal, software, hardware, and networks/the internet</td>
<td></td>
</tr>
<tr>
<td>Mass gatherings</td>
<td>Built environment, event spaces, and public spaces including key national</td>
<td>Attorney-General’s Department</td>
</tr>
<tr>
<td></td>
<td>sites and monuments</td>
<td></td>
</tr>
<tr>
<td>Transportation</td>
<td>Aviation, maritime and rail</td>
<td>Department of Transport and Regional Services</td>
</tr>
<tr>
<td>Water</td>
<td>Fresh drinking water and wastewater management</td>
<td>Attorney-General’s Department</td>
</tr>
</tbody>
</table>

Table 3 below shows the number of IS security incidents in NSW government agencies across the nine critical infrastructure sectors from 2001 to 2006. A major reason for the high number of total incidents from 2001-2004 compared to 2006 was due to the lack of an IS security standard certification of agencies. However, we must be cautious in making causal inferences or generalising to other organisational contexts without further study investigating other exogenous determinants. The certification process began to take effect in 2006 where a significant number of agencies were certified and became ‘hardened’. Target hardening from a crime perspective tends to force perpetrators to the weakest links in the critical infrastructure asset landscape. The results in Table 3 suggest this was the banking and finance sector. Over time, technology has improved and viruses, hacking, or intrusions have begun to decline because security resources (staff and money) have caught up with the perpetrators (reasons include a better understanding of hacking techniques, training and security exercises like Cyber Storm). Criminals are now focused more on softer targets like individuals or private organisations for identity crimes because they are easier. Also there is less to gain (apart from political) other than kudos from hacking into Government agency’s websites. In NSW, government agencies try and overcome any internal employees creating IS security incidents by having robust security vetting processes in place for all staff, contractors and consultants. Similarly, staff are required to sign off for appropriate usages of internet and email. The IS security incident counts were maintained in a number of different ways by agencies including: manual count from various logs; through management meeting minutes; incident reports; automated counts; and help desk tickets. The agencies also reported that as part of their normal business they had to abide by up to 100 pieces of legislation for the most regulated agency; the average was between 5 and 10 different laws. In addition, agencies were asked if they had risk assessment plans or complied with a
relevant IS security standard. More than half of the agencies had formal risk plans as part of their process to meet compliance targets to a standard. However, only a few agencies were accredited to IS security standard AS/NZS 17799.2 or ISO/IEC 27001. We now briefly discuss the incidents across the sectors focusing on incident data from Table 3 and where possible giving real live case examples and feedback from participant interviews.

### Table 3. NSW Government IS intrusions across Australia's Nine Critical Infrastructure Sectors

<table>
<thead>
<tr>
<th>NSW</th>
<th>Australia's Nine Critical Infrastructure Sectors (number of agencies in parentheses)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Banking &amp; finance</td>
</tr>
<tr>
<td>2001Q4</td>
<td>15 (3)</td>
</tr>
<tr>
<td>2002Q1</td>
<td>21 (4)</td>
</tr>
<tr>
<td>2002Q2</td>
<td>27 (5)</td>
</tr>
<tr>
<td>2002Q3</td>
<td>27 (5)</td>
</tr>
<tr>
<td>2002Q4</td>
<td>22 (5)</td>
</tr>
<tr>
<td>2003Q4</td>
<td>23 (5)</td>
</tr>
<tr>
<td>2004 Q4</td>
<td>24 (5)</td>
</tr>
<tr>
<td>2006Q4</td>
<td>37 (9)</td>
</tr>
</tbody>
</table>

#### 4.1 Banking and Finance

Table 3 shows that the IS security incidents in the banking and finance sectors of the NSW government critical infrastructure assets more than doubled from 2001 to 2006; the reverse trend of the other eight sectors. Generally this number of incidents is seen as very low compared to the huge number of transactions performed by these agencies. The number of agencies in this sector was low compared with emergency services, energy and utilities, health care, mass gathering or transport sectors. Perpetrators may have targeted this sector with more vigour thus increasing the number of recorded incidents, because their rewards were financial and economic as opposed to just kudos.

Internally, many financial institutions individually and through their peak organisational body have initiated an awareness program regarding IS security. An important issue noted by a government organisation was that of when to replace the many legacy systems with ‘one’ updated centralised system. IS security needs to cover physical, personnel, protection, and business continuity planning with disaster recovery program development methodologies as well as ICT. Other effects are customer service interruption, loss of business opportunity and reputation. As an example “the National Australia Bank’s telecommunications system was shut down by a computer virus on 19 September 2001. Telephone, Internet and share trading services at Australia's largest bank were
affected. A spokesperson for the bank would not confirm whether the problems were caused by the World Trade Centre virus, which infected computer systems around the world. A virus called "Nimda", which attacked global networks on the same day, may also have been responsible for closing down the system" (ABIX, 2001, p.1).

4.2 Emergency Services

It is not only banking and finance organisations that are being targeted by identity or cyber crime perpetrators. In 2001 there were nine intrusions. “In the wake of the recent tsunami tragedy in Asia, Australian media covered the story of a website purporting to be collecting donations for the Australian Red Cross, when in fact the charity had never heard of the company behind it” (Fagg, 2009, p. 1). Intrusion attempts to jam or hack into Australia’s emergency 000 telephone service or other routing systems could lead to untold damage. To date there have been no incidents on the 000 telephone service. Critical Infrastructure affects emergency services in two ways:

1. They are usually the 1st responders to a physical attack (response) on Critical Infrastructure and are called to assist in the recovery, and

2. Their equipment can also be under threat from physical and cyber attacks; emergency services are classified by TISN (Trusted Information Sharing Network) as one of the nine Infrastructure Groups. However, their equipment, while just as vulnerable to physical attack as any other physical asset, is usually more resilient to cyber attack because of the operating environment and emergency service’s familiarity with cyber crime. This familiarity stems in particular from law enforcement agencies involvement with emergency services. Emergency service communications equipment and dispatch systems are usually proprietary in nature. This makes it difficult to gain access to the characteristics of their software and to gain access to the source code thus making it a hard target for hackers to attack. Hackers will tend to attack easier targets with more generic operating software. Because of the high risk factor in terms of health and safety and other threats their messaging systems (voice and data) are usually encrypted to a high standard making it even more difficult to attack. This eliminates the possibilities of using listening devices, war driving, or police scanners and radio to eavesdrop because they are not open radio channels. The only way to eavesdrop is with stolen radio equipment although this is becoming more difficult because all equipment is registered and uniquely identified.

4.3 Energy and Utilities

Table 3 shows the number of incidents in this sector was relatively stable although they did decrease by over 20% from 37 in 2001 to 30 in 2006. Electricity comprises power generators and retailers and the main transmission system organisations who own, operate and manage the high voltage power systems, sub-stations and power station switchyards. Key risks are loss of data although not ‘valuable’ to people - the biggest risk is employees (internal, disgruntled employee or contractor). ‘Energy and Utilities’ and the ‘Water’ agencies may also have market trading systems that if hacked, could be very damaging to their overall position; although they do also have manual backup systems.

In July 2006, Faheem Khalid Lodhi was convicted for offences including plotting, in October 2003, to bomb Australia’s national electricity grid in the cause of violent jihad (Wallace 2006). Lodhi was sentenced to 20 years in prison on 23 August 2006 (Regina v Lodhi (2006) NSWSC 691 23 August).

The secondary data sources and literature show that the energy and water (see section 4.9) infrastructure are particularly dependent on Supervisory Control and Data Acquisition Systems (SCADA), Distributed Control Systems (DCS) and other specialised computer control systems. Control systems have been used for years to control power grids, gas and oil distribution pipelines, water treatment and distribution systems and flood control dams, as well as other physical systems. SCADA users are sometimes seen as the ‘weakest link’ in their supply chain. The organisations controlling these large energy infrastructure assets (in Australia and many developed nations) were often government owned but deregulation lead to privatisation of a lot of Australian electricity infrastructure. In NSW most energy assets are still government owned.

4.4 Food
The number of incidents was low which most probably reflects the benefits or harm a perpetrator could inflict on such organisations. A risk identified within this sector by participants was the exchange of confidential information (information within and between organisations). “The more we learn (about IS Security) the more we realise what we don’t know” (Agriculture Participant). Broadband would allow more centralised information across disparate sites. “We have reviewed policies at induction, how to lock computers, what they can and can't do … email viruses - highest risk is viruses. Hacking is not a big threat at present, firewall perpetrators do try and get through though” (Food Authority Participant).

4.5 Health care

The health sector had 14 agencies and was frequently targeted by perpetrators. Legislation, especially the Privacy Act amendments (2001), forced agencies in this sector to pay more attention to IS security. This may have been a major reason for the large decrease in the number of recorded incidents in 2006 compared to 2001 (about a 95% decline). Some hospitals are privately funded but are contracted back to public sector. Health has a risk management framework – a prepared business risk plan. “The need to educate organisations and executives that information systems security is a data owner responsibility…” (Health Service Provider Participant).

Australian Federal Police alleged that “A Medicare employee used his access privileges to hack into a database of deceased persons to claim more than A$300,000 in false Baby Bonus payments”. The man was charged with 23 counts of abuse of public office under Section 142.2, which carries a maximum gaol; term of five years; 23 counts of obtaining advantage by deception under Section 134.2, which has a maximum 10 year gaol term; and two counts of money laundering under Section 400.4 and 400.6 of the Commonwealth Criminal Code Act 1995. The maximum penalty for the money laundering offences is 20 years imprisonment and/or a $132,000 fine” (Dahdah, 2008, p.1).

4.6 Information Technology and Communications (ICT)

There was only one agency grouped into the ICT sector in all surveys. The number of IS security incidents were also low at six in 2001 and throughout the study with none being reported for 2006. This may not be as surprising as it seems with more dedicated IS security managers and staff in this particular agency than the others. They are more aware of IT/IS security issues, tools and solutions.

“A 28-year-old man has pleaded guilty to hacking into the Northern Territory's (of Australia) computer system, deleting the identities of more than 10,000 public servants and shutting down the entire system … causing more than A$1 million of damage. He had just been let go from a company responsible for maintaining the network and used a colleague's log-in details to hack in. He accessed data and then shut down the network at Royal Darwin Hospital, the prison, Supreme Court and Parliament House. He also deleted the network accounts of 10,475 public servants who could not work while it was (being) repaired. The court heard that all of the government servers had to be replaced by specialists” (ABC News, 2009, p. 1).

Prosecuting cyber crimes is made more difficult when the criminal leaders of an operation cannot be readily identified. Internet programs enabling anonymous work online and encryption may obscure these details. However, often court cases can proceed where the ‘middle person’ in the criminal network can be identified and a crime proved, leaving the leaders and real reason for the crime unknown. Computer forensics is becoming an important area to gather vital evidence that is robust enough for the rigours of court procedures eventuating in successful prosecution of perpetrators. Successful court outcomes may act as prevention and deterrence measures.

4.7 Mass gatherings

There were 16 agencies in this sector which was the largest number in the 2001 survey. They were represented by well known tourist attractions such as the Sydney Opera House. This sector also had a
A question posed by a participant was how do you quantify value of protecting artefacts (historic and often one of a kind)? Records of some organisations where there can be mass gathering for example, sports and event grounds are on a central database, which can cause problems if financial transactions are stored. ‘Cultural change [is] required to change perception of ‘red tape’ to ‘helpfulness’. Education in security longer term - newer employees seem quicker to adapt’ (Participant Feedback).

A major risk to the mass gatherings sector is website hackers for example; there was a ‘fake' Sydney Opera House website where some people were actually scammed into ‘purchasing tickets'. Several changes have been made due to terrorism scares overseas at major tourist attractions (e.g., Bali bombings in Indonesia).

4.8 Transportation

The two agencies in this sector in 2001 were ports and rail. The agencies in this sector increased to 10 by 2006. The Sydney Airport is privately owned and was not surveyed. However, aviation is an important area for the transportation sector since September 11, 2001 attacks on US. If a hacker was able to intrude and disable the computer system of an airport control tower the consequences are almost unimaginable. Other risks include; disgruntled employee and proliferation of wireless devices.

4.9 Water

The number of average incidents per agency in the water critical infrastructure sector was relatively high at six in 2001 compared to the other sectors. The following case example in a neighbouring state illustrates the harm that can occur.

Vitek Boden hacked into the Maroochy shire council’s computerised sewerage system, causing hundreds of thousands of litres of raw sewage to flow into a public area at Pacific Paradise, Queensland, Australia. This caused serious environmental harm as a result of an overflow on 26 March 2000 in which marine life died, the creek water turned black and the stench became unbearable for residents. The overflow had placed at risk “the health, the safety and the quality of life of the people” in the surrounding area (EPA and QPWS, 2001, p.6). Since this incident State/Territory Governments in Australia have tried to be more proactive in guarding their water sector assets from IS security breaches, especially their agencies SCADA control systems (see ‘Energy and Utilities’ section 4.3).

5. CYBER-ATTACK SIMULATIONS

To date there have been two well-publicized international cyber-attack simulations - Cyber Storm (6-10 February 2006) and Cyber Storm II (11-14 March 2008). Australia did not participate in Cyber Storm. Cyber Storm II tested the national security of Australia, the US, Canada, the UK and New Zealand. Participants engaged in an international hacking exercise. Cyber Storm II divided participants into attackers and defenders over simulations that tested national responsiveness to cyber-attacks on IT systems and transportation, communications, and chemical infrastructure. The event was lead by the US Department of Homeland Security and supported by more than 100 public, private and international organizations including NSW government agencies. Some of the international organizations involved were the FBI, Microsoft, Verizon, McAfee, Australian Computer Emergency Response Team (AusCERT), Attorney General’s department, the Department of Defense, the Australian Federal Police, and Telstra. The purpose of the exercise was to allow participants to test their incident response and crisis management arrangements under cyber attack.

Within scenarios of both Cyber Storm simulations, various cyberspace channel identity crime methods were played out, such as computer virus attacks, worms, purchase of personnel identity data, and malware distribution. These identity crime methods can result in identity details or personnel information identifiers being fraudulently obtained by identity crime perpetrators (Australian Government 2008a). The Security and Critical Infrastructure division within The Commonwealth
Attorney General’s Department developed and led Australia’s successful participation in the international cyber security exercise, Cyber Storm II, which was held over five days in March 2008. “More than 50 organisations from Australian, State and Territory Governments, the IT industry and private sector members of the Australian Government’s TISN took part in the Australian arm of the exercise. AusCERT provided specific cyber threat information to more than 400 critical infrastructure and other key business organisations to assist them to protect their information and communications technology systems and networks” (Australian Government 2008b, p.130). The list of Cyber Storm II participants highlights a very diverse group of multidisciplinary organisations ranging from governments, banks, telecommunications and industry. The banks particularly are governed by the Basel II Accord where the IS security requirements go beyond basic security concepts of availability, confidentiality and integrity. Governments, like the NSW Government, have tended to adopt a version of the International IS security standard to guard against IS intrusions.

6. IMPLICATION AND LIMITATIONS

Implications from this study for organisations are that target hardening due to increased awareness, training, and resources for prevention solutions reduces IS security incidents on critical infrastructure assets. A limitation of this study was that no private critical infrastructure organisations or other government agencies outside of NSW provided IS security intrusion information for analysis. Our analysis of AusCERT (2006) survey comparisons across time and other publicly available information suggested the trends in our results were comparable. International evidence showed similar trends regarding declining IS security incidents in organisations compared to 2004 or 2007 (Richardson, 2008). Further research should investigate IS security incidents impact on private organizations and needs to understand the reasons behind incidents disclosed.

7. CONCLUSIONS

Internal agents of an organisation seemed to be as big a concern as external intrusion across critical infrastructure sectors; for example, contractors connecting a laptop to an organisations network (i.e., if it had a virus). Often an IS security focus on core ICT components at the expense of proper protection for the whole of the organisation leaves weak links at peripheral organisational sites in a multi-site organisation. Success of IS security in an organisation was due mainly to executive accountability, funding and culture (employees need to have a high regard for IT security). Different levels of security are required for different systems, for example, SCADA in ‘Energy and Utilities’ and ‘Water’ sectors. Consultation with key stakeholders and users is seen as important; for instance, information sharing among organisations targeted by perpetrators is seen as essential for reducing the risk of attack and to improve response to incidents. Organisations both public and private need to be aware of the speed with which sophisticated and organised perpetrators are able to benefit from new and emerging technologies. These case study findings show that the number of IS security incidents against NSW governments critical infrastructure assets have unequivocally declined over time. Reasons for this provided by interviewed participants and from online survey qualitative and quantitative results include; increased resources expended (money and staff), training and awareness programs, and participating in international cyber attack simulation programs. Our contribution is exploratory in nature due to data restrictions with respect to generalising our results to other jurisdictions within Australia, either private or public organisations. We certainly caution generalising our findings to jurisdictions outside of Australia. Future research should investigate both public and private organisations’ critical infrastructure asset IS security intrusions within other Australian and overseas jurisdictions. In addition, qualitative research will be used to identify rationale behind quantitative results and hence develop theory relevant to this area.

References


