Potential Impact of Information Operations and Possible Countermeasures: Evidence from the Financial Services Sector

Sebastian P. Schroeder, David R. Wilton
Institute of Information and Mathematical Sciences
Massey University Auckland, New Zealand

ABSTRACT

This paper aims at giving a short introduction to Information Operations (IO) and an overview of a one-year Postgraduate IS Security Research Project conducted in New Zealand. The study analyzed the potential risks of IO especially in the Financial Services Sector (FSS), clarified how FSS organizations are prepared for IO, demonstrated how IO threats are addressed within the FSS, and identified weaknesses that require improvement.

1. INTRODUCTION

When trying to define IO there is a danger of defining the concept either too narrowly or too broadly. IO describes activities that involve the use of powerful new tools the Information Age has provided to states, military forces, and even to individuals, to achieve strategic, operational or tactical advantages and objectives. The use of information to shape perception and attitudes as well as modern IT lie at the core of IO (Brosnan, 2001). Due to the fact that they are commonly in use, definitions of the DOD Dictionary of Military and Associated Terms (U.S. Department of Defense, n.d.) will be used:

Information Operations
Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Defensive Information Operations
The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems.

Offensive Information Operations
The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers to archive or promote specific objectives.

Information Warfare
IO conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Seven distinct forms of information warfare (IW) can be identified (Avruch, Narel, & Siegel, 2000): (a) command and control warfare, (b) intelligence-based warfare, (c) electronic warfare, (d) psychological warfare, (e) hacker warfare, (f) economic information warfare, and (g) cyber warfare. Moreover, three IW classes can be defined (Schwartau, 1996):

Class1: Personal Information Warfare
Personal IW is an attack against an individual's electronic privacy. This includes the exposure of digital records and database entries in every place information is stored

Class2: Corporate Information Warfare
Corporate IW describes the war between corporations around the world. This includes disinformation, theft of data, espionage, and data destruction.

Class3: Global Information Warfare
Global IW works against industries, global economical forces or entire countries or states. This includes sneaking in research data of a competitor, theft of secrets, and turning information against its owners.

2. LITERATURE REVIEW

There are many references in the literature to IO and IW. However, most of them have a military background and will only be described very shortly in this paper.

2.1 Critical Infrastructure

Critical infrastructures are those facilities, services and information systems which are so essential that their incapacity or destruction would have a devastating impact on national security, national economy, public health and safety, and the effective functioning of the government. The interconnectivity used by the FSS for customer services and operations poses significant information security risks to computer systems and to the critical operations and infrastructures they support. The dependence of the FSS on other critical infrastructures poses additional risk (Federal Office for Information Security (BSI) Germany, 2004; U.S. Government Accountability Office, 2003).

The United States commenced action on an IO defensive posture by means of 1996 the President's Commission on Critical Infrastructure Protection. Six at-risk sectors were identified: (a) defense and government, (b) information and communications, (c) banking and finance, (d) energy, (e) physical distribution, and (f) vital human services.

2.2 Weaponry and Trends

IO has some advantages over physical methods, because attacks can be conducted remotely, anonymously, and without large budgets (Denning, 1999a). In a very extreme way directed energy weapons, electromagnetic pulse weapons, or destructive microbes can destroy the IT of IO targets. But there are many other IO techniques which will not be examined in detail in this paper, including exploitation, back or trap doors, social engineering, flood attacks, eavesdropping, spoofing, unauthorized access, malicious software, and indirect vulnerabilities.

There are several trends in the FSS that raise new security concerns. Some examples are distributed and mobile computing, the use of the Internet, intranet and Internet portals, voice over IP, and outsourcing.

2.3 Threats and Threat Sources

One major difficulty that distinguishes cyber threats from physical threats is determining who is attacking the system, why, how, and from where. This difficulty stems from the ease with which individuals can hide or disguise their tracks by manipulating logs and directing their attacks through networks in many countries before hitting their target (Cordesman & Cordesman, 2001).

In general, the FSS faces cyber threats similar to those faced by other critical infrastructure sectors, but the potential for monetary gains and economic disruptions may increase its magnetism as a target (U.S. Government Accountability Office, 2003). Three broad IW threat categories can be identified (Alberts, 1996): (a) the vast majority of the threats that occur everyday and do not pose a threat to national security, (b) a small area that represents those threats having national security implications, and (c) threats that may have national security implications and represent a particularly difficult challenge.

Vulnerabilities in themselves and the existence of methodologies to exploit those vulnerabilities do not constitute a threat. A threat arises only when there is a threat source with the intent, capability, and opportunity to carry out an attack (Denning, 1999b). Five main threat sources were identified: criminal groups, insiders, mercenaries, governments and organizations, and terrorists.

2.4 Countermeasures

Protecting an organization's cyber assets is as critical as protecting its physical assets. Computer technology has made enterprises interdependent, which has created incredible opportunities, but has also created some major vulnerabilities (National Center for Technology & Law, 2002). Organizations that are unable to protect their information assets will find their corporate credibility, business relationships, and expensively developed brand and brand image damaged (Calder & Watkins, 2003).

2.4.1 Risk Assessment

In general Risk Assessment (RA) is a part of harm minimization that investigates (a) what you are protecting, (b) what you are protecting against, and (c) how much the protection is worth to you. The goal is to provide some assurance that the cost of countermeasures is commensurate with the risks. Without RA organizations could spend too little or too much (Wilton, 2005).

Several methods for analyzing and managing risks exist. One of them is the CCTA Risk Analysis & Management Method (CRAMM) which is a trade-off between the impact of the risk and the cost of countermeasures. CRAMM provides a staged and disciplined approach embracing technical and non-technical aspects of security (U.K. Office of Government Commerce, n.d.). In addition, RA can be seen as part of Enterprise Risk Management (ERM) defined in the Australian/ New Zealand Standard on Risk Management (AS/NZS 4360). The standard extends traditional risk management (RA: identify, analyze, and evaluate risks; treat risks; monitor and review) with the two tasks of establishing the context and communicate and consult.

2.4.2 Network and Operating System Security

Ten countermeasures to ensure network security can be identified (Bragg, Phodes-Ously, & Strassberg, 2004): (a) secure the physical environment, (b) keep patches updated, (c) use antivirus scanners, (d) use firewalls, (e) secure user accounts, (f) secure the file system, (g) secure applications, (h) back up the system, (i) automate security, and (j) create a computer security defense plan.

But there are always general network security issues remaining. Firewalls, for instance, provide perimeter defense and are generally limited because they only accept or deny packets rather than analyze them. Therefore, intrusion detection and prevention techniques are necessary. Traditional intrusion detection systems (IDS) can be grouped into two categories: misuse IDS that works by rule matching and abnormal IDS that works by statistically computing. Intrusion Prevention Systems (IPS), the advanced version of IDS, have the ability to detect known and unknown attacks and prevent them from being successful. IDS and IPS can be classified by their location, either network-based (NIDS/NIPS) or host-based (HIDS/HIPS).

Deceptive tactics can provide another line of defense. Honeypots and honeynets, systems designed to entrap attackers and collect information about them, are a simple "decoy" deception technique that is increasingly popular. Such a system could be part of "active network defense" that impedes an attacker in more complicated ways (Rowe, 2003).

Operating systems (OS) are one of the most vulnerable components of any application framework. Developers often create strong security controls within an application but have no control over lower-level exploits (Siegel, Sagalow, & Serritella, 2002). Main OS security issues that need to be addressed are (Wilton, 2005): (a) identification and authentication to verify a user's identity, (b) audit to monitor authorized and unauthorized actions, and (c) installation, configuration, and management to ensure continued security status.

Cryptography as a part of cryptology is an essential countermeasure for protecting information on its way through networks as well as when it is stored on clients or servers. But cryptography does not exist in a vacuum. Security involves things people know, relationships between people, and how people relate to machines as well as computers which are complex, unstable, and prone to errors (Schneier, 2000). In addition, cryptography and especially steganography (hiding information within ways that prevent the detection) can be seen as a threat to confidentiality from an organizational perspective due to the ability of unrecognized data ship-off.

2.4.3 Cyber-Risk Insurance

Technical countermeasures cannot completely reduce an organization's risk to security breaches with their associated financial losses. Therefore, organizations turn to insurance to deal with the risk of substantial financial losses that remain after technical countermeasures have been implemented. Although insurance companies do not currently have good actuarial data on which to base cyber-risk insurance rates, a number of companies do offer such polices (Computer Security Institute, 2004).

The optimal model to address IO must combine technology, process, and insurance. This permits organizations to successfully address a range of different risk exposures. A comprehensive policy backed by a specialized insurer with top financial marks and global reach allows organizations to lessen the damage caused by significant IO attacks, and better manage costs related to loss of business and reputation (Siegel et al., 2002).

2.4.4 Security Policy

Historically, enterprises have secured their information assets on an ad hoc basis, generally relying on physical security to avoid compromise. This has the great advantage that physical security is generally well understood and relatively easy to implement. Unfortunately it breaks down when there are non physical paths by which assets may be attacked. The Internet provides a large amount of such paths. A strong information security policy is a foundation for successful and sustainable security outcomes (Paddon, 2000).

A security policy describes the philosophy by which security is managed. The spine of good security policies is risk assessment. Policy must address needs using terms and definitions relevant to the organization. A security policy specifies: (a) who should be allowed access, (b) to what resources, and (c) how this access is regulated. In the end this comes down to a matter of trust: who do we trust enough to allow which type of access to what resources. It is important that security policies are realistic. Otherwise people simply will work around them, to detriment of security (Wilton, 2005).

2.4.5 Information Assurance

Information assurance (IA) stands for IO that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality,

and nonrepudiation (U.S. Department of Defense, n.d.) and is often divided into six different domains (Bass & Robichaux, 2001): (a) human introduced errors, (b) user abuse of authority, power, and policy, (c) system probing or mapping, (d) system probing with malicious hardware and software, (e) system penetration, and (f) subversion of network and device security and control mechanisms.

A practical strategy for achieving IA is called Defense-in-Depth. Its aim is to establish protection across multiple layers and dimensions that will cause an adversary who penetrates or breaks down one barrier to promptly encounter another barrier, and then another, until the attack ends. In addition to incorporating protection mechanisms, organizations need to expect attacks and include attack detection tools and procedures that allow them to react to and recover from these attacks. Defense-in-Depth integrates the three primary elements people, operations, and technology (National Security Agency, n.d.).

From a storage point of view, several techniques developed over the last years to support always-availability, location-independence, ultra reliability, and infinitely scalability. They consist of creating multiple copies of information, migrating the copies between different storage types, managing the consistency of these copies, and replacing the information in one copy with information taken from another (Cummings, 2002).

2.5 Critical Infrastructure Protection

Nearly all industrialized countries have set up, or are setting up, Centers for Critical Infrastructure Protection (CIP) that keep relationships between each other, with law enforcement, intelligence, infrastructure operators, and other diverse instances. The aim is to provide timely and relevant information about arising threats and general IT security issues. As an example, New Zealand's CIP center's functions are divided into three main groups: a 24/7 watch and warn function, an investigation and analysis function, and an outreach and training broking function (Federal Office for Information Security (BSI) Germany, 2004; N.Z. Government Communications Security Bureau, 2001).

3. METHODOLOGY

Interpretive research was performed during the literature review. A range of other research approaches was analyzed prior to the research project. Field experiments, for instance, were identified as a potentially capable technique, but unfortunately it would be very hard to find organizations that are prepared to be experimented on. This approach is also likely to raise ethical and legal issues.

Finally, two research approaches were selected: expert interviews as an argumentative approach and case study to gather practical insights. In order to ensure confidentiality, the names of interviewees and their organizations are not included in this paper.

Expert interviews were identified as a good method for receiving qualitative results in terms of potential risks, likely IO attacks, countermeasures, and weaknesses. Three FSS security consultants from different organizations were asked for their opinion. During the project other people with diverse occupations and backgrounds were asked about particular aspects to adjust and extend the findings.

It was clear that not many people in high positions would want to publicize weaknesses within their organization. Moreover, people with helpful insights normally do not have much time. Fortunately one CIO in a small NZ FSS organization participated in the case study.

4. RESEARCH RESULTS

4.1 Potential Risks

Main risks identified were that sensitive data files or figures could be accessed, deleted, or damaged especially by competitors within the industry. Lack of user awareness in terms of unauthorized access to data, security settings, and threats arising from malicious software pose additional risks. Eavesdropping and espionage activities, even though normally not directly targeted against the FSS, can have an enormous impact on confidentiality and availability. Moreover, the physical infrastructure could be manipulated or attacked.

Customer data disclosure or ship-off is dangerous from a competitive perspective as well as in the sense of indirect vulnerabilities. Malicious insiders are the most dangerous source for this threat. In addition, criminal groups are switching from broadcast to personalized phishing methods utilizing compromised customer data. The risk is even worse due to the fact that customer data are available from many sources, including insurance databases, e-commerce portals, and payment gateways.

Mobile computing can be seen as a big risk for the FSS. Mobile devices contain increasingly confidential corporate, customer or authentication data which can be disclosed, for example, when losing a device or through device and infrastructure vulnerability exploitation. Other trends such as outsourcing, remote connections, portal solutions, and voice over IP raise additional risks.

Many risks, including direct and indirect vulnerabilities, result in negative reputation for FSS organizations. This can be advantageous especially for competitive organizations within the same industry. Back doors and chipping as well as potentially exploitable vulnerabilities in software and hardware generally can be seen as a high risk. Malicious software is another major concern.

Another risk identified through the case study is that, especially at small business levels, management and staff generally seem not to be aware of IO threats and how to minimize or prevent them occurring.

4.2 Likely IO Attacks

Main concerns include social engineering, malicious software, flaws in physical security, poor authentication mechanisms, exploitable vulnerabilities in software and hardware, and insufficient network security. Malicious insiders, either normal employees or mercenaries in the role of an insider, need to be considered as the most dangerous threat source. Attacks often aim at employee and administration accounts resulting in unauthorized access and confidential information ship-off.

Mobile devices might be lost, stolen, or compromised enabling attackers to gain access to corporate networks. Eavesdropping attacks are likely to occur in wide area networks and within corporate networks. Also likely is the exploitation of vulnerabilities in hardware and software by professionals initiated either internally or externally as well as by malicious software. This can result in unauthorized access, infrastructure breakdowns, or privacy breaches.

Social engineering techniques can be seen as one of the most dangerous attacks. On the one hand, they can be directly targeted against the FSS by gathering sensitive information such as customer data, access information, or information about internal structures and weaknesses resulting in unauthorized access and confidential data ship-off. On the other hand, social engineering can be indirectly targeted against the FSS by attacking customers through

phishing or malicious software aiming on credit card details as well as online banking access and transaction information to initiate illegal payments and money transfers. Related to this is identity theft which can go further than illegal payments or money transfers.

Large FSS units are not as vulnerable to flood attacks as small and medium sized organizations. But flood attacks aiming on transactions with back-end systems can be dangerous for the whole FSS. Physical destruction is not very likely and will normally have no significant impact on business continuity. Nevertheless, weaknesses in physical security can be exploited to obtain unauthorized access to critical systems or to place eavesdropping devices.

4.3 Countermeasures

Main countermeasures taken by the FSS to address the identified threats are risk assessment, security policies, access control, physical security, OS security, basic network security, and cryptography. The implementation depends mostly on the size of the organization and the money available for security measures.

Risk assessment is one of the most important countermeasures and is generally conducted formally or informally in the whole FSS. Internal revisions and legal guidelines force FSS organizations to adopt risk assessment techniques. Internally performed studies addressing actual weaknesses and former incidents foster risk identification and management. Security policies based on risk assessment are an essential countermeasure. It is important to make the security policy in integral component of every day business. Some organizations adopt compliance management mechanisms to force their security policy.

FSS organizations implement improved authentication mechanisms, including authentication of customers to Internet services as well as authentication of employees to physical environments and critical systems. Single sign-on solutions are in use in some FSS organizations mainly to counter user indiscretions and to enable portal workplaces. However, nowadays authentication mechanisms are still mostly based on passwords.

Threat awareness seminars and campaigns conducted internally and externally are increasing in quality and quantity. Email functionality within FSS applications allows authenticated communication between organizations and their customers. Personnel security and employee satisfaction are seen as a good measure to prevent insider threats. Moreover, rotating staff through specific areas and not having one person doing the work is a practical way of minimizing FSS fraud and misappropriation.

OS and basic network security are common measures to counter threats arising from remote and local attackers, malicious software, back doors, and exploitable flaws in software and hardware. Updates of spyware and virus signatures as well as key programs with service packs are generally conducted regularly. In several cases IDS, in a few cases IPS, mechanisms are in place. Moreover, some organizations start implementing behavior monitoring and compliance management systems. Vulnerability scans are regularly performed at least in large organizations.

Incident management, mostly performed by large FSS organizations, promises business continuity and disaster recovery in the event of equipment breakdown, power failure, or man-made disasters. Physical security is implemented in most critical areas, but some areas always remain insufficiently protected. An example of this could be the failure to implement rigid identification techniques because security agents have become familiar with the users and do not challenge them to produce identification.

4.4 Weaknesses and Improvements

Backlog demands were identified in IPS and behavior monitoring capabilities, especially to counter threats arising from malicious insiders. Moreover, when basic OS and network security measures fail IPS can prevent several attacks from being successful. IPS can be declared as the predominant choice for intrusion systems in the next couple of years.

Network hardware needs to be equipped with eavesdropping prevention mechanisms. This includes that all network ports need to be able to authenticate connected hosts to prevent malicious hardware. These measures are in place in some large FSS organizations but normally not in small and medium sized business levels. The same is true for vulnerability scans against network infrastructure and critical systems.

Physical security and access control require improvements in some insufficiently secured areas to prevent unauthorized access. As soon as access control mechanisms that provide a mix of what you know, what you have, and what you are, become more widespread, prices will increase and as a result those mechanisms will be affordable in small and medium sized organizations as well, enabling further authentication on top of password mechanisms.

Cryptographic countermeasures need to be implemented within the whole FSS. It is not acceptable that unencrypted protocols, especially for system management, are sometimes still in use. Corporate traffic needs to be encrypted. Incorrect use or implementation need to be foreclosed.

In terms of mobile computing a backlog demand in cryptographic measures enabling end-to-end encryption as well as for data in mobile devices and additional storage mediums was identified. Moreover, secure and resource-friendly authentication mechanisms are strongly required. Remote deletion and device tracking mechanisms should be implemented on mobile devices utilized by FSS staff. Secure device configuration and secure software execution are other essential measure to counter the threats that face current mobile devices.

Awareness seminars and campaigns need to be conducted internally (to employees and security agents) and externally (to customers) on a regular basis. It can be assumed from the case study that there are accumulated needs within in the FSS. Social engineering awareness and personnel security need to be exercised, especially if contractors or other externals are able to access critical systems. Circumstantial security audit needs to be performed even though it can come along with association objections and legal issues. Actually mainly intra-organizational audits are conducted. Little or no attempt has been made to conduct audits or penetration testing on an FSS-wide basis.

Security policy enforcement needs to be practiced. Compliance management should be performed throughout the whole FSS. Threats against customer data need to be countered across the whole FSS, connected sectors, and on the customer side. Internal countermeasures reduce the risk of customer data being compromised, leaving over the risk of exploitable FSS infrastructure and malicious software on the customer side. Information assurance and incident management need to be performed by small and medium sized, in addition to large, organizations to guarantee business continuity and disaster recovery in all FSS levels.

The use of certified hardware and software as well as the use of trusted sources that produce advice on installing software securely need to be ensured in all critical areas.

Critical infrastructure protection efforts need to be coordinated on an industry-wide basis. The FSS as a whole seems not to be aware of IO and the threat it poses and should therefore be addressed at all levels with at least an overview. Patching mechanisms need to be optimized in many cases. This is especially important in FSS organizations with complex application landscapes.

Deceptive tactics should be considered as another line of defense. Honeypots can make it harder for an attacker to identify critical system and can help to identify risk practices performed by insiders and compromised systems within a corporate network. Insurance policies are not considered in most FSS organizations even though they could be an effective measure to absorb financial losses in the event of significant IO attacks.

5. CONCLUSIONS

Main security concerns include social engineering, malicious software, flaws in physical security, poor authentication mechanisms, exploitable vulnerabilities in software and hardware, and insufficient network security. Mobile computing is a seminal trend, but comes along with several backlog demands. The most dangerous threat source was identified as mercenaries in the role of an insider.

Main countermeasures taken by the FSS are risk assessment, security policies, access control, physical security, OS security, basic network security, and cryptography. The implementation depends mostly on the size of the organization and the money available for security measures.

Awareness seminars and campaigns need to be conducted internally and externally on a regular basis. Critical Infrastructure Protection efforts need to be communicated frequently at all FSS levels. This includes a move towards FSS-wide security audits and penetration testing.

Threats against customer data need to be countered across the whole FSS, in connected sectors, and on the customer side. To counter insider threats personnel security and employee satisfaction must be exercised. Incident management needs to be performed on a FSS-wide basis to guarantee business continuity and disaster recovery. Information assurance and security policy compliance management need to be addressed more frequently. Moreover, patching mechanisms need to be optimized in many cases.

Further backlog demands were identified in IPS and behavior monitoring capabilities. Physical security and access control require improvements in some insufficiently secured areas. Cryptographic countermeasures generally need to be implemented within the whole FSS. Deceptive tactics as another line of defense and insurance policies as financial losses absorbers should be considered as potentially good countermeasures.

It is apparent from the above that IO directed against the FSS has the potential to cause significant harm at many levels - individual customer, financial institutions, national and even international. The threats in this area, which are increasing in frequency and sophistication, need to be taken seriously. Formal risk analysis needs to be undertaken and appropriate countermeasures implemented. Identified weaknesses need to be addressed at certain levels.

Limitations

Due to the sensitivity of this research topic it was extremely difficult to find participants for the case study. Fortunately one FSS organization responded. In general, information concerning specific organizational security issues in this area is hard to obtain.

Future research

In future research more case studies should be conducted to get broader insights. Field experiments should be considered as additional approach. As mentioned in 4.4 this needs to be done in addition to intra-organizational security audits and penetration testing. Moreover, it would be interesting to analyze the impact on other sectors in the event of successfully performed IO attacks against the FSS and vice versa.

Acknowledgement

I would like to thank my supervisor and IS Security lecturer Mr. David Wilton for all the help I received during my research project. Without his guidance my report would not have materialized. Special thanks go to the case study participant and the expert interviewees who shared their experience and valuable insights with me. I also wish to thank all those who supported this research project with helpful suggestions, expertise, or information.

REFERENCES

Alberts, D. S. (1996). *Defensive information warfare*: CCRP publication series.

Avruch, K., Narel, J. L., & Siegel, P. C. (2000). *Information campaigns for peace operations*: CCRP publication series.

Bass, T., & Robichaux, R. (2001). *Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations.* Paper presented at the Military Communications Conference, 2001.

Bragg, R., Phodes-Ously, M., & Strassberg, K. (2004). *Network security: the complete reference*. New York: McGraw-Hill.

Brosnan, A. J. (2001). Information operations - what is IO? *Journal of Battlefield Technology, 4*(2), 32-36.

Calder, A., & Watkins, S. (2003). *IT governance: a manager's guide to data security & BS 7799 / ISO 17799* (2nd ed.). London: Kogan Page.

Computer Security Institute. (2004). *CSI/FBI computer crime and security survey.* Retrieved May 08, 2005, from http://www.gocsi.com

Cordesman, A. H., & Cordesman, J. G. (2001). *Cyber-threats, information warfare, and critical infrastructure protection: defending the U.S. homeland*. Westport, Conn.: Praeger.

Cummings, R. (2002). The evolution of information assurance. *Computer, 35*(12), 65-72.

Denning, D. E. (1999a). *Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy*. Retrieved April 11, 2005, from http://www.nautilus.org/gps/info-policy/workshop/papers/denning.html

Denning, D. E. (1999b). *Information warfare and security*. New York: ACM Press.

Federal Office for Information Security (BSI) Germany. (2004). *Critical infrastructure protection (CIP) - a sector-oriented introduction.* Paper presented at the Critical Infrastructure Protection and Civil Emergency Planning Conference, Zurich, Switzerland.

N.Z. Government Communications Security Bureau. (2001). *National information infrastructure protection project final report: towards a centre for critical infrastructure protection.* Retrieved July 28, 2005, from http://www.ccip.govt.nz/about-ccip/ccip-final-report.pdf

National Center for Technology & Law. (2002). *Relevance of the insurance sector to national critical infrastructure protection (CIP Report 1.2).* Retrieved May 06, 2005, from http://cipp.gmu.edu/report

National Security Agency. (n.d.). *Defense in depth: a practical strategy for achieving information assurance in today's highly networked environments.* Retrieved August 11, 2005, from http://www.nsa.gov/snac/support/defenseindepth.pdf

Paddon, M. (2000). *The art of keeping secrets - or aspects of good information security policy.* Paper presented at the AUUG2K Conference, Australian National University, Canberra.

Rowe, N. C. (2003). *Counterplanning deceptions to foil cyber-attack plans.* Paper presented at the Information Assurance Workshop, 2003. Ieee Systems, Man and Cybernetics Society.

Schneier, B. (2000). *Secrets & lies: digital security in a networked world*. New York: Wiley Computer Publishing.

Schwartau, W. (1996). *Chaos on electronic superhighways: information warfare* (2nd ed.). New York: Thunder's Mouth Press.

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-risk management: technical and insurance controls for enterprise-level security. *Information Systems Security, 11*(4), 33-49.

U.K. Office of Government Commerce. (n.d.). *CCTA Risk Analysis & Management Method (CRAMM).* Retrieved May 13, 2005, from http://www.ogc.gov.uk

U.S. Department of Defense. (n.d.). *DOD Dictionary of Military and Associated Terms*. Retrieved May 07, 2005, from http://www.dtic.mil/doctrine/jel/doddict

U.S. Government Accountability Office. (2003). *Critical infrastructure protection: efforts of the financial services sector to address cyber threats*. Retrieved April 11, 2005, from http://www.gao.gov

Wilton, D. R. (2005). *Information systems security (PG seminar)*: Auckland, N.Z.: Massey University.