

Information Operations

Sector-Oriented Analysis of the Potential
Impact and Possible Countermeasures

23c3 Who can you trust?

December 2006, Berlin, Germany

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



Agenda

Introduction

Background

- Critical Infrastructures

- Current Trends

- Threats

- Countermeasures

Methodology

Research Results

- Expert Interviews

 - Threat Sources

 - Current Trends

 - Weaponry

 - Countermeasures

- Case Study

Conclusions



Information Operations

- ... involves much more than computers and computer networks.*
- ... encompasses information in any form and transmitted over any medium.*
- ... covers operations against information content and operations against supporting systems, including hardware, software, and human practices.*
- ... 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.*
- ... raises a mixture of legal and organizational problems due to the pervasive nature of information and reliance on it, the speed of transmission of information, and the diverse spheres.*

Information Operations

Definitions

When trying to define IO there is a danger of defining the concept either too narrowly or too broad. Commonly-in-use definitions:

- **Information Operations (IO)**
Actions taken to affect adversary information and information systems while defending one's own information and information systems.
- **Information Warfare (IW)**
IO conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.
- **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 Operations

Weaponry

- IO has some advantages over physical methods, because attacks can be conducted remotely, anonymously, and without large budgets.
- In a very extreme way directed energy weapons, electromagnetic pulse weapons, or destructive microbes can destroy the IT of a target organization.
- However, there are more common techniques, including:
 - Exploitation
 - Back / trap doors
 - Social engineering
 - Flood attacks
 - Eavesdropping
 - Spoofing
 - Unauthorized access
 - Malicious software
 - Indirect vulnerabilities

Information Warfare

Classes

→ **Class1: Personal Information Warfare**

Attacks against an individual's electronic privacy, including the exposure of digital records and database entries in every place information is stored. In the majority of cases the victims do not notice this kind of intrusion.

→ **Class2: Corporate Information Warfare**

War between corporations around the world, including

- disinformation,
- theft of data,
- espionage, and
- data destruction.

→ **Class3: Global Information Warfare**

War against industries, global economical forces, or entire countries or states, including

- sneaking in research data of competitors,
- theft of secrets, and
- turning information against its owners.

Information Warfare

Forms

- Command and control warfare
- Intelligence-based warfare
- Electronic warfare
- Psychological warfare
- Hacker warfare
- Economic information warfare
- Cyber warfare

Research Questions

- Main research questions of this one-year Postgraduate Infosec Research Project were:
 - What potential risks does IO pose?
 - What kinds of IO are the most likely ones?
 - What measures are adequate to counter IO threats?
 - Where are weaknesses that require improvements?

Agenda

Introduction

Background

- Critical Infrastructures

- Current Trends

- Threats

- Countermeasures

Methodology

Research Results

- Expert Interviews

 - Threat Sources

 - Current Trends

 - Weaponry

 - Countermeasures

- Case Study

Conclusions



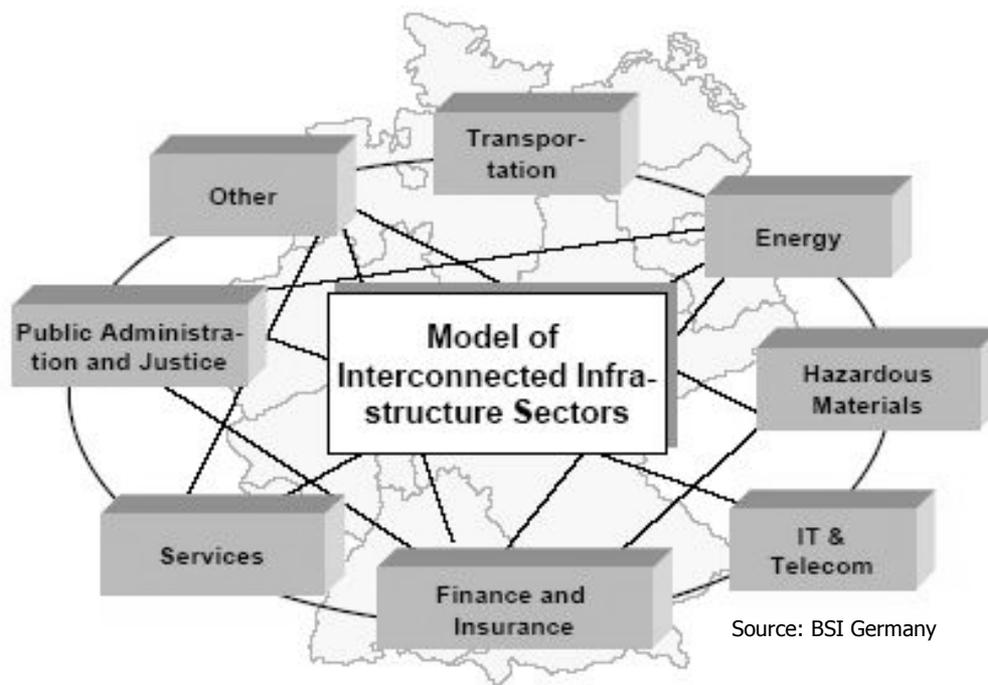
Critical Infrastructures

- 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/or
 - the effective functioning of the government.
- 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:
 - Defense and government
 - Information and communications
 - Banking and finance
 - Energy
 - Physical distribution
 - Vital human services

Critical Infrastructures (2)

- IO against one sector may have an impact on all connected sectors.
- Potential targets in the FSS include payment systems, investment mechanisms, and banking facilities.
- Example of a country with eight interconnected critical infrastructures:
- Example of the scope of banking operations involving money transfers:

- FEDWIRE, operated by the U.S. Federal Reserve Board, processed 108 million transactions in the year 2000, with a total value excess of \$379 trillion.
- If such a system was to be attacked successfully, the consequences for the financial health of several nations would be devastating.



Agenda

Introduction

Background

Critical Infrastructures

Current Trends

Threats

Countermeasures

Methodology

Research Results

Expert Interviews

Threat Sources

Current Trends

Weaponry

Countermeasures

Case Study

Conclusions



Current Trends

→ **Distributed and mobile computing**

- Increasing number of remote access ports on corporate networks.
- Many vulnerabilities due to the general openness of wireless networks.
- Mobile devices generally vulnerable to loss and theft.
- Increasing amount of sensitive and private data on mobile devices.
- Lack of good authenticating, encryption, and basic operating system features in mobile devices.

→ **Outsourcing**

- Organizations need to take appropriate contractual and managerial steps to protect information.
- Outsourcing contract one of the key aspects and must be drafted and analyzed by specialists.

Current Trends (2)

→ Use of the Internet

- No built-in security and no built-in protection for confidential or private information.
- Potential threats to an organization can be multiplied by the number of Internet connections.
- Reasonable approach: simply not to connect or strongly quarantine exposure.
- But commercial and technical pressures are driving most organizations in the opposite direction.

→ Voice over IP (VoIP)

- Potential communication cost savings and complexity reduction.
- But threats like call tracking and eavesdropping are pretty hard to counter.

Current Trends (3)

→ Open source software

- Strongest argument for open source: if everyone can study the source code and experiment with the software, then bugs are likely to be found and fixed.
- But once software becomes large and complex, there may be only a few or no capable motivated people inspecting it.
- There might be attackers who are motivated to spend more time finding bugs or exploitable features than the community of reviewers is.
- Consequently, the important questions are
 - how much effort was spent by capable people in checking and testing the code and
 - whether they tell you everything they find.

Agenda

Introduction

Background

- Critical Infrastructures

- Current Trends

- Threats**

- Countermeasures

Methodology

Research Results

- Expert Interviews

 - Threat Sources

 - Current Trends

 - Weaponry

 - Countermeasures

- Case Study

Conclusions



Threats

- 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 final target.
- Many attacks go undetected or unreported.
- Vulnerabilities in themselves and the existence of methodologies to exploit those vulnerabilities do not constitute a threat to information resources.
- A threat arises only when there is a threat source with the intent, capability, and opportunity to carry out an attack.

Threat Sources

→ **Criminal groups**

- Criminal groups attack information systems for purpose of monetary gain.
- Organized crime as the new frontier for large-scale theft can be expected.

→ **Insiders**

- Most mechanisms are ineffective against misbehavior by legitimate users who perform functions for which they are authorized.
- Many network-based attacks let an attacker masquerade as a legitimate user.

→ **Mercenaries**

- Mercenaries mostly work for payment by gaining commercial advantage for their paymasters by means of internal or external espionage.

→ **Governments and organizations**

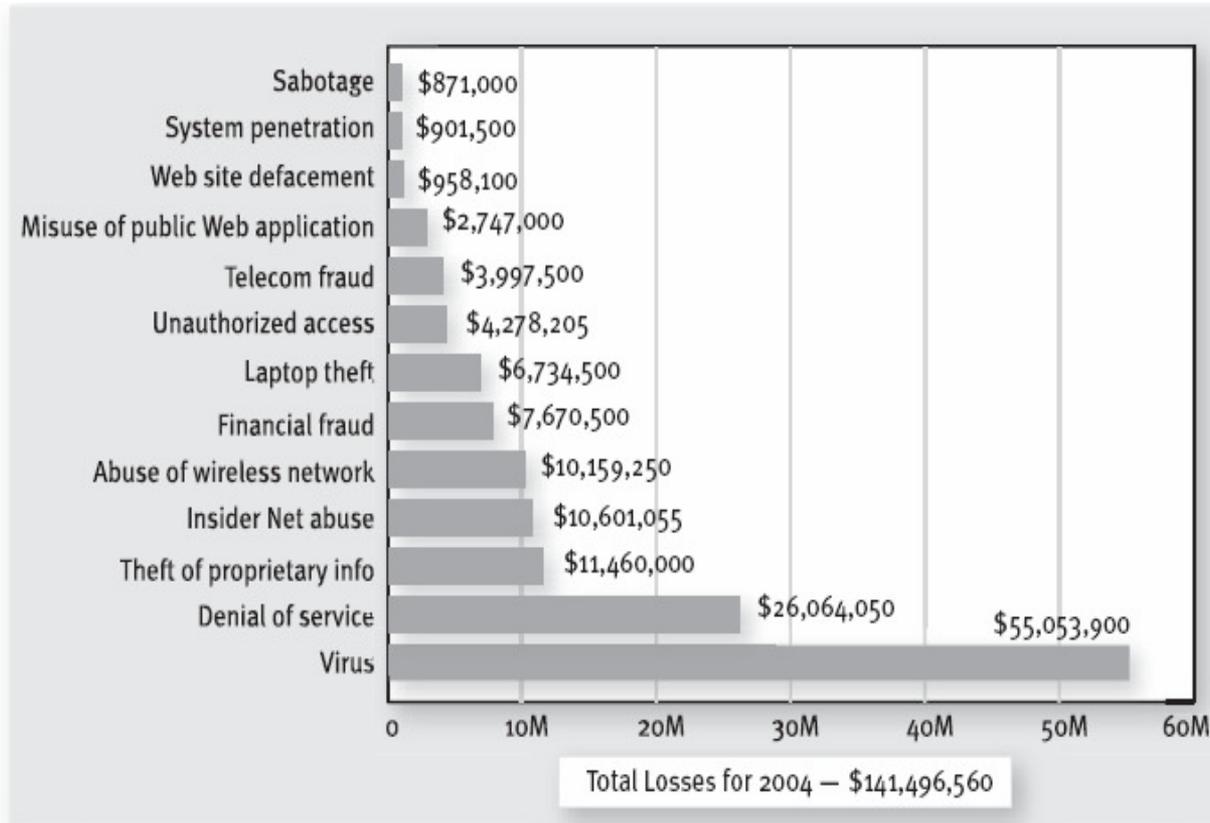
- Some governments and organizations have resorted to industrial and economic espionage to gain unfair advantages over competitors.
- Computer intrusions are increasingly viewed as a powerful instrument for acquiring sensitive government and private sector information.

→ **Terrorists**

- Some terrorist groups tend to switch from their usual methods to the use of the Internet as the major focus of their attack.

Threat Statistics

→ Amount of losses by type:



CSI/FBI 2004 Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

- Most organizations do not yet know that their defenses have already been breached.
- Therefore, statistics are only the tip of the iceberg.

Agenda

Introduction

Background

- Critical Infrastructures

- Current Trends

- Threats

- Countermeasures**

Methodology

Research Results

- Expert Interviews

 - Threat Sources

 - Current Trends

 - Weaponry

 - Countermeasures

- Case Study

Conclusions



Countermeasures

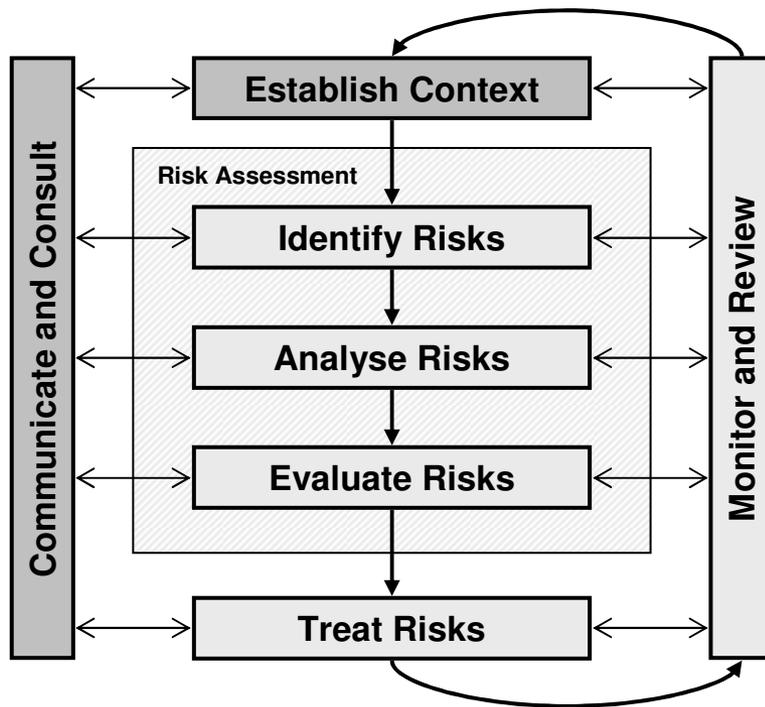
- Organizations that are unable to counter threats to their information assets will find their
 - corporate credibility,
 - business relationships, and
 - expensively developed brand and brand image damaged.
- Security involves
 - processes,
 - preventative technologies,
 - detection and reaction capabilities,
 - an entire forensics system to hunt down and prosecute the guilty,
 - things people know,
 - relationships between people,
 - how people relate to machines, as well as
 - computers which are complex, unstable, and prone to errors.

Risk Assessment

- In general Risk Assessment (RA) is a part of harm minimization that investigates
 - what you are protecting,
 - what you are protecting against, and
 - 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.
- Several methods for analyzing and managing risks exist...

Risk Assessment

Enterprise Risk Management

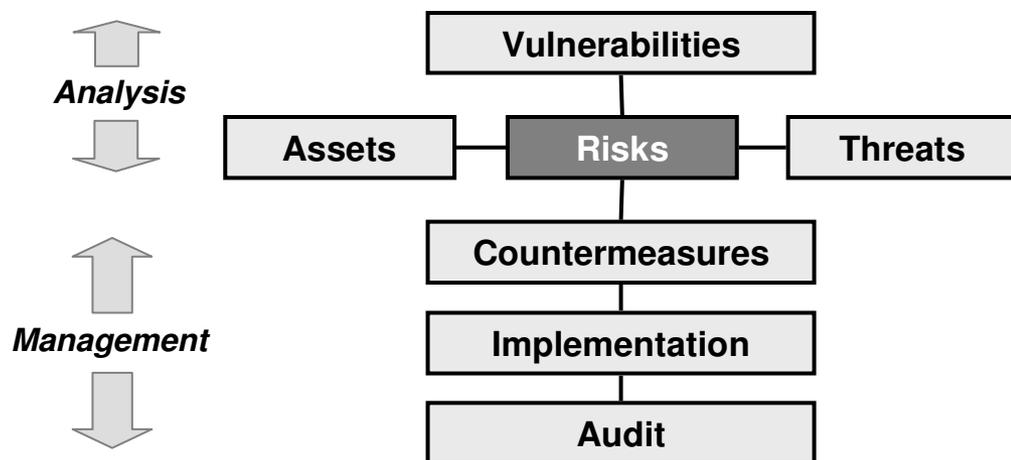


- RA can be seen as part of Enterprise Risk Management (ERM) as defined in the Australian/ New Zealand Standard on Risk Management AS/NZS 4360.
- The standard extends traditional risk management with the two tasks of
 - establishing the context and
 - communicate and consult.
- ERM is an iterative process of continuous improvement that needs to be embedded into existing practices and/or business processes.

Risk Assessment

CCTA Risk Analysis & Management Method

- CCTA Risk Analysis & Management Method (CRAMM) is a trade-off between the impact of the risk and the costs of countermeasures.
- The method is a staged and disciplined approach embracing technical and non-technical aspects of security and should be used...
 - during the system development process,
 - throughout the operational lifecycle of the system, and
 - whenever any alteration including enhancements is made.



Identify and value the physical, software, data and location assets that make up the information system.

Identify the possibility of the problem occurrence and calculate the level of the underlying or actual risks.

Use countermeasures of risks determined and compare them against the security level in order to identify if the risks are sufficiently great to justify the installation of a particular countermeasure.

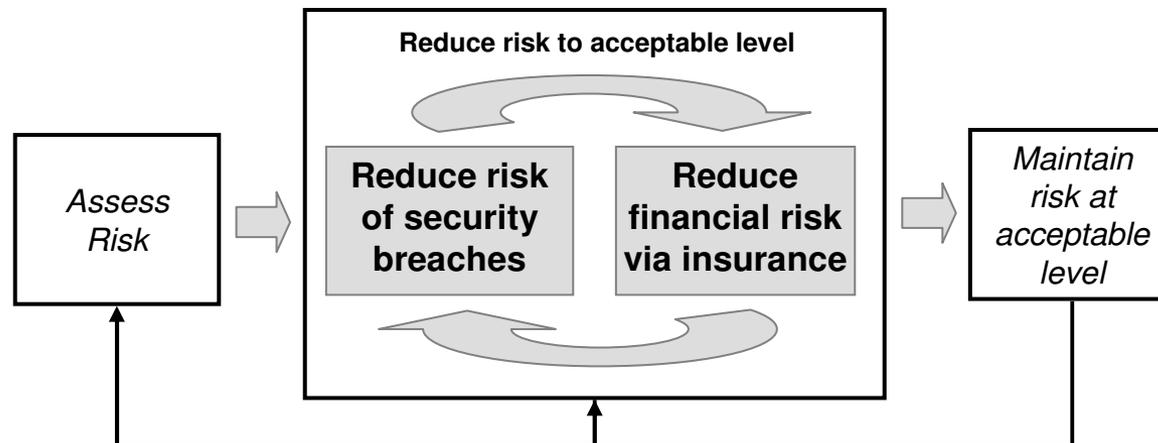
Cyber-Risk Insurance

- Technical countermeasures cannot completely reduce an organization's risk to security breaches.
- Therefore, more and more organizations turn to insurance to deal with the risk of substantial financial losses that remains after technical countermeasures have been implemented.
- A number of companies do offer such policies.
- As important as finding the right product is finding the right insurer.
- Key criteria are
 - financial strength,
 - experience, and
 - claims philosophy.

Cyber-Risk Insurance

Generic Framework

- A generic framework for using insurance helping to manage information security risks demonstrates that a trade-off between
 - the amount that should be spent on countermeasures and
 - the amount that should be spent on insurance exists.



Security Policy

- A information security policy describes the philosophy by which security is managed.
- The spine of good security policies is risk assessment.
- A security policy specifies
 - who should be allowed access,
 - to what resources, and
 - 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 and that they address needs using terms and definitions relevant to the organization.
- Otherwise people simply will work around them, to detriment of security.

OS and Network Security

- Countermeasures to ensure OS and network security are:
 - Secure the physical environment
 - Secure user accounts
 - Secure the file system and applications
 - Keep patches updated
 - Use malicious software detection mechanisms
 - Back up the system
 - Use firewalls (perimeter defense)
 - Implement intrusion detection (IDS) and prevention (IPS) capabilities
 - Audit to monitor authorized and unauthorized actions
 - Encrypt information
 - on its way through networks and
 - when it is stored on clients or servers
 - Automate security
 - Create a computer security defense plan

Network Security

Intrusion Detection and Prevention

- Today the use of tunneling and encryption means to put more content out of the reach of perimeter control.
- But when network traffic increases, IDS are extremely challenging to understand and manage due to an increasing number of generated alerts.
- Intrusion Prevention Systems (IPS) are either network-based (NIPS) or host-based (HIPS), active, in-line devices that
 - can detect anomalies in the regular routine of network traffic by comparing it in real time to a set of rules that represents permissible or harmful behavior and
 - then stop the possibly malicious activity by
 - dropping attack packets or
 - disconnecting connections before reaching the target host.
- But... even though IPS will prevent attacks, some might slip through.

Network Security

Deceptive Tactics

- 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.
- But... honeypots are a relatively passive deception that is easy to recognize via packet sniffer and file system inspection.
- A real computer system that serves real needs is more likely to fool an attacker.
- Such a system could be part of active network defense, defense that impedes an attacker in more complicated ways.

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.
- 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.
- 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.

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 as well as
 - with law enforcement,
 - intelligence,
 - infrastructure owners / 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:
 - 24/7 watch and warn function
 - Investigation and analysis function
 - Outreach and training broking function

Agenda

Introduction

Background

- Critical Infrastructures

- Current Trends

- Threats

- Countermeasures

Methodology

Research Results

- Expert Interviews

 - Threat Sources

 - Current Trends

 - Weaponry

 - Countermeasures

- Case Study

Conclusions



Methodology

- Expert interviews were selected as an argumentative approach.
 - Three FSS security consultants from different organizations were asked for their opinion about main threat sources, actual trends, dangerous IO weapons, and possible countermeasures.
 - During the project other people with diverse occupations and backgrounds were asked about particular aspects to adjust and extend the findings.
- Case study was selected to gather practical insights.
 - It was clear that not many people in high positions would want to publicize weaknesses within their organization and people with helpful insights normally do not have much time.
 - Fortunately one CIO in a small NZ FSS organization participated in the case study.
- Field experiments were identified as another 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.
- In order to ensure confidentiality, the names of interviewees and their organizations are not included in the presentation.

Agenda

Introduction

Background

Critical Infrastructures

Current Trends

Threats

Countermeasures

Methodology

Research Results

Expert Interviews

Threat Sources

Current Trends

Weaponry

Countermeasures

Case Study

Conclusions



Threat Sources

Espionage and Terrorists

- Foreign organizations and governments, including the intelligence community, are already equipped with or actually establishing industrial and economic espionage capabilities.
- Even though attacks from those sources typically aim on other targets it is obvious that the FSS handles sensitive information, especially from a privacy perspective.
- Threats arising from those sources are currently not usually considered, even though the impact especially on confidentiality and availability can be immense in times of crisis.
- Attacks performed by terrorists aim on the destruction of infrastructure.
- Business continuity can generally be guaranteed in the event of such an attack. But when an attack is successfully accomplished it might result in:
 - Public attention leading to fear within the population
 - Indirect consideration of terrorist's political, ideological, or social intentions
 - Negative reputation for FSS organizations

Threat Sources

Criminal Groups

- Criminal groups generally attack the weakest link - the customer - for purpose of monetary gain.
- They are dangerous for the FSS in sense of indirect vulnerabilities, especially through phishing or malicious software.
- Those methods aim on gathering sensitive data such as authentication information and transaction numbers which enable an attacker to perform money transfers.
- The methods of this threat source are getting better and better: Phishing emails, for example, are no longer simple broadcasts; they are personalized and well targeted.
- Organizations in the FSS are reacting through, for example, improved authentication methods as well as social engineering consciousness.
- Unfortunately, customers - especially older generations - are still not sufficiently aware about those threats and often easy to deceive.
- However, indirect vulnerabilities are not directly IO related and will therefore not be exhaustively discussed.

Threat Sources

Mercenaries and Insiders

- IO attacks performed by insiders can generally be seen as a very dangerous threat source.
- Mercenaries can act remotely or masquerade as insiders utilizing compromised employee or administration accounts.
- The risk of insider attacks worsens when mercenaries are employed by an organization in the FSS so that they can act as legitimized insiders.

Threat Sources

Essence

- Criminal groups, foreign organizations, governments, and terrorists - even though each of them can be dangerous by themselves - are likely to hire mercenaries or to develop professional in-house capabilities for IO attacks.
- The main threat source can therefore be declared as mercenaries in the role of an insider:



Agenda

Introduction

Background

- Critical Infrastructures

- Current Trends

- Threats

- Countermeasures

Methodology

Research Results

- Expert Interviews

 - Threat Sources

 - Current Trends**

 - Weaponry

 - Countermeasures

- Case Study

Conclusions



Current Trends

Outsourcing

- Outsourcing is a very controversial trend.
- It might enhance the general security of an organization due to better transparency in terms of costs and security aims.
- Moreover, security policies become an integral part of the contract whereas security policy compliance conducted internally sometimes does not produce the expected outcome.
- On the other hand, major concerns include
 - implementation and technology failure risks,
 - loss of intellectual history,
 - more complex business continuity planning, and
 - from a concentration perspective – a lack of control and a systemic risk to the industry as a whole.

Current Trends

Open Source

- Open source software was mostly seen as a positive influence on security.
- Open source products are seen to be more secure than closed source software
 - not only because of the possibility to verify the source code of applications and OS features on critical systems,
 - but also because of the possibility to enhance open source products by further development.
- One interviewee mentioned that in some cases the basic authentication module was enhanced by including smart card capabilities on top of the basic password authentication.
- The same possibility exists for biometric authentication mechanisms as well.

Current Trends

Use of the Internet and Mobile Computing

- The use of the Internet is essential
 - to provide customer services as well as
 - to perform transactions and collaboration between institutions within the same industry and connected sectors.
- Unfortunately, most of the attacks come from the Internet which makes it necessary to have sufficient countermeasures in place.
- Moreover, the increasing adoption of remote connections can be dangerous especially if devices are compromised or connected to the Internet and the corporate network at the same time.
- In this constellation there is a substantial risk that malicious software can spread especially if no network security measures are in place to counter threats arising from such devices.
- One interviewee mentioned that a large FSS organization directly connects its remote workplaces per dial-up to the corporate network.
- Voice over IP as well as portal workplace solutions are increasingly adopted and will raise further security issues.

Current Trends

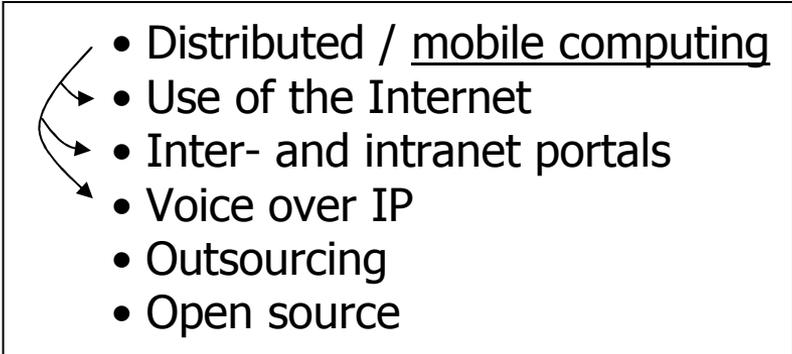
Use of the Internet and Mobile Computing (2)

- Implementation flaws in short-range links such as Bluetooth can result in large quantities of confidential data loss when attacks are directed, for example, against mobile devices in a large FSS building utilizing remote attack methods.
- Such an attack can be performed from farther distances utilizing special equipment.
- M-payment mechanisms are still not secure enough to face the trust issues of customers.
- Several e-commerce payment methods exist but they cannot be well adapted to the m-payment context due to unique wireless network vulnerabilities and general constraints of mobile devices.
- Location-based services (LBS) raise further concern, especially from a privacy perspective.

Current Trends

Essence

- Mobile computing is seen as the most important trend but also as the trend with the most security issues.
- Concerns include
 - user identification,
 - secure storage,
 - secure data communication,
 - tamper-resistant implementations,
 - secure software execution,
 - secure network access, and
 - secure content.
- This affects
 - device security,
 - network and session security, as well as
 - application and payment security.

- 
- Distributed / mobile computing
 - Use of the Internet
 - Inter- and intranet portals
 - Voice over IP
 - Outsourcing
 - Open source

Agenda

Introduction

Background

- Critical Infrastructures

- Current Trends

- Threats

- Countermeasures

Methodology

Research Results

- Expert Interviews

 - Threat Sources

 - Current Trends

 - Weaponry**

 - Countermeasures

- Case Study

Conclusions



Weaponry

Espionage and Flood Attacks

- Espionage capabilities enable foreign organizations and governments all over the world to eavesdrop communication links, mainly wide area networks.
- This threat is especially dangerous because of poor threat awareness as well as the broad adoption of mobile computing where sensitive data is often transferred insecurely due to computational constraints or configuration flaws.
- Flood attacks can be dangerous in two ways:
 - Firstly, if an organization is not equipped with redundant high-speed connectivity, availability can be attacked quite easily utilizing, for example, zombie networks.
 - Secondly, and this concerns all FSS organizations, flood attacks could be targeted against back end systems by small front end requests which trigger complex back end transactions.

Weaponry

Eavesdropping

- The vulnerability level of eavesdropping depends very much on the size of the organization.
- In many organizations it is likely that some network traffic remains unencrypted.
- Moreover, budget constraints can lead to
 - an unsatisfactorily secured physical environment,
 - weak critical network zone encapsulation (logical and physically), and
 - deficient audit and incident response capabilities.
- Access points placed by malicious insiders within a corporate network could remain undetected at least in small or medium sized institutions.
- An attacker could also start a well targeted eavesdropping attack by, for example, placing a mobile computing device with eavesdropping capabilities inside the network or between the network and a specific host.
- While communicating per UMTS with the managing instance, such an attack might remain undetected in large corporations as well.
- In addition, some cryptographic mechanisms are often insecurely implemented enabling an attacker to break end-to-end encryption.

Weaponry

Back Doors and Malicious Software

- The main focus lies mostly on back doors in software.
- Possible back doors in hardware (chipping) are not often recognized even though they can be very dangerous, especially in network or security-related hardware.
- Statistics confirm that malicious software can be identified as one of the most dangerous weapons.
- The main question is how fast systems are patched so that exploitable components are not vulnerable anymore.
- Successful malicious software attacks (individual or general targeted) can have an enormous impact especially on availability and confidentiality.
- They could also result in indirect vulnerabilities like
 - compromised customer authentication data through phishing or Trojan horses as well as
 - negative reputation in the event of a successful attack.

Weaponry

Unauthorized Access

- Password authentication is not appropriate, especially on critical systems.
- Passwords are still handled inappropriately or given away to colleagues.
- Single sign-on solutions based on passwords have weaknesses as well.
- An extension with smart card capabilities increases security, but this enhancement is obviously useless when, for example, employees leave their smart cards in the card reader during their lunch break.
- Biometric mechanisms are still not highly developed enough to solve those problems.
- In addition, costs for mature authentication mechanisms are often seen as too high by FSS management, particularly in small and medium sized organizations.

Weaponry

Mobile Attacks and Social Engineering

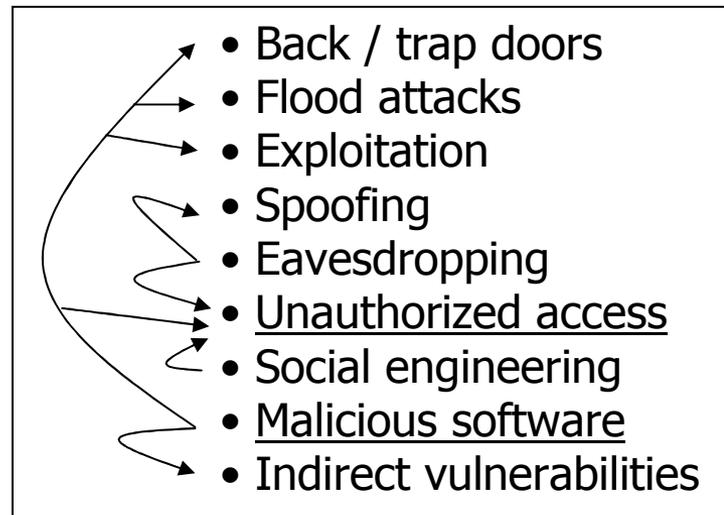
- Mobile computing comes along with an important issue from an attacker's viewpoint:
 - Users of wireless devices can go online and offline easily.
 - That makes it difficult to trace back attackers to a fixed geographic point.
 - Therefore attacks over mobile communication systems might become the preferred method in the future.

- Social engineering is seen as one of the most effective methods to gather authentication information or sensitive information about internal structures through aggregation of publicly available data or insider deception.
- One interviewee mentioned the possibility to trick security agents when, for example, external specialists or contractors are known by security agents.
- They might still get access to an organization even though they are not involved into projects anymore.
- Awareness seminars address social engineering amongst other issues, but circumstantial audit is not possible in most cases due to staff association objections and legal issues.

Weaponry

Essence

- Unauthorized access and malicious software were identified as the most dangerous IO weapons.
- They require special attention to decrease the likelihood of successful conducted IO attacks against the FSS.



Agenda

Introduction

Background

- Critical Infrastructures

- Current Trends

- Threats

- Countermeasures

Methodology

Research Results

- Expert Interviews

 - Threat Sources

 - Current Trends

 - Weaponry

 - Countermeasures**

- Case Study

Conclusions



Countermeasures

- Many countermeasures are currently available.
- In large FSS institutions a lot of money is allocated for countermeasures, but in small and medium sized organizations the trade-off between potential risk and monetary resources available is very high.
- Countermeasures will mostly be discussed from a large FSS organization perspective.
- Small and medium sized organizations are likely to be more vulnerable to IO attacks than large organizations.
- During the interviews it transpired that most technical countermeasures are already somehow implemented or at least discussed in large FSS organizations.
- Non-technical countermeasures - such as cyber-risk insurance - seem to be not that much recognized in the FSS probably because they still remove only a small number of large risks.

Countermeasures

Network Security

- Firewall rules need to be updated and evaluated on a regular basis to ensure that no vulnerabilities exist through outdated permissions.
- While NIDS capabilities are normally already in place there seems to be a backlog demand in IPS and behavior monitoring capabilities for critical servers and workstations, especially to counter threats arising from malicious insiders.
- All interviewees agreed that simple access logs are not enough.
- But IPS and behavior monitoring require enormous setup and administration time and effort.
- Current systems are still too complex.
- Allowed or forbidden behaviors are in the majority of cases hard to define because workflows vary in terms of behavior.
- Even though IPS and behavior monitoring mechanisms are not practical for every workstation, they have potential to be a good mechanism to identify malicious activities performed by insiders.

Countermeasures

Network Security (2)

- One interviewee mentioned that the patching level of network hardware is in many cases up-to-date, but in some cases outdated.
- Critical systems without sufficient network security measures in place are generally more vulnerable to misuse and confidential data ship-off.
- Some very large FSS organizations experiment with honeypots as an instrument for identifying compromised hosts within the corporate network.
- One interviewee mentioned that those honeypots might rather be a part of honeynets which are already installed in diverse organizations across different industries for the general purpose of learning and analyzing attacker's activities.
- Another interviewee said that there are too many other problems which have to be solved before it makes sense to implement such measures.
- However, honeypots obtain little attention even though they could be a good extension to IPS and a good mechanism to disguise the real network topology.

Countermeasures

Risk Management and Personnel Security

- Risk assessment is seen as the initial step for security.
- There is a general trend to institutionalization, formalization, and standardization of risk management methods.
- The main focus in Europe lies on Basel II and Solvency II. Further measures like the BSI IT-Baseline Protection Manual are widely accepted.
- Security policies need to be developed based on the risks identified and enforced utilizing compliance management mechanisms. It is hard to say if security policies are always sufficiently implemented.
- To counter threats arising from insiders, personnel security is very important.
- Common methods are next to technical measures:
 - Employee screening including criminal records and reference checking
 - Awareness seminars
 - Methods to improve employee satisfaction.
- In very sensitive areas people often need to perform a vetting or even lie detector tests.
- Moreover, the “need to know principle” is applied in sensitive areas.

Countermeasures

Operating System and Application Security

- Antivirus as well as OS hardening and patching are essential countermeasures especially in terms of mobile computing. The question is:
 - with which tutorials system hardening is performed and
 - if certified software and hardware is used at least for critical systems.
- Vulnerability scans need to be performed regularly at least against network infrastructure and critical systems.
- Patching mechanisms for software and hardware have significant optimization potential.
- Systems often remain unpatched for hours or accidentally even for days, especially in organizations that utilize many proprietary products.
- In addition, patching often has side effects on diverse applications.
- This makes it necessary to perform copious tests before finally implementing patches on productive systems.
- The application landscape in banks seems to be generally more standardized than in insurance companies.
- It can be assumed that malicious software has a higher vulnerability probability in insurance companies than in banks.

Countermeasures

Cryptography and Authentication

- There are still unencrypted protocols in place, sometimes even for system administration.
- In some cases cryptographic measures are incorrectly used or implemented which makes them potentially vulnerable to, for example, man-in-the-middle attacks.
- In terms of mobile computing there is a backlog demand in encryption mechanisms of data stored in mobile devices and additional mediums.
- Moreover, computational constraints of mobile devices often force manufacturers to the implementation of insufficient cryptographic measures.
- Authentication mechanisms are one of the main measures to counter unauthorized access and need to be addressed from several perspectives, including:
 - Particular physical environments
 - Critical systems
 - Particular remote services
 - Mobile devices
- A backlog demand of secure and resource-friendly authentication mechanisms especially in mobile computing exists.

Countermeasures

Physical Security

- Physical security is mostly 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.
- At present, physical security plays a big role especially in mobile computing.
- In sensitive areas “sally ports” with strong physical security, such as “no lone go zones” which ensure that one person cannot be in that area unattended, as well as strong authentication mechanisms are in place, mostly as a mix of
 - what you know (PIN, password, pass phrase),
 - what you are (verified utilizing, for example, cameras, hand recognition, and weighing machine), and
 - what you have (smart cards).
- But there are still areas remaining which could be protected much better.
- One interviewee mentioned that FSS infrastructure is likely to be vulnerable to attacks due to weak physical security in some areas.
- Insiders who know about those less secured areas could give away this knowledge or start targeted attacks.

Countermeasures

IA and CIP

- Sufficient backup mechanisms are mostly in place, including redundancy across different locations.
- There is a trend to storage area networks, mostly offered by outsourcing providers.
- Further methods protecting availability of data and resources include
 - business continuity planning (BCP) and
 - disaster recovery (DR).
- BCP and DR combined are also known as incident management which is similar to security risk analysis and can be performed as part of such.
- Critical infrastructure protection can generally be seen as a good measure if sufficient encouragements or resources are provided.
- This seems to be the case at least in most large FSS organizations.

Countermeasures

Essence

- Risk assessment
- Security policy
- Awareness seminars
- Compliance management
- Behavior monitoring (critical systems)
- Access control (password, smart card, biometry)
- Physical security (infrastructure, devices)
- OS security (hardening, patching, antivirus)
- Network security (IDS / IPS, honeypots)
- Cryptology, mainly cryptography
- Information assurance
- Employee satisfaction
- BCP / Incident management
- Insurance policies

- Major countermeasures can be identified as risk assessment, access control, physical security, OS security, network security, and cryptography.
- But obviously all other countermeasures need to be addressed as well.

Agenda

Introduction

Background

- Critical Infrastructures

- Current Trends

- Threats

- Countermeasures

Methodology

Research Results

- Expert Interviews

 - Threat Sources

 - Current Trends

 - Weaponry

 - Countermeasures

- Case Study**

Conclusions



Case Study

Main Concerns

- The participant (CIO in a small NZ FSS organization) regarded IO as a possible threat to his organization.
- Main concerns were that sensitive data files or figures could be accessed, deleted, or damaged especially by competitors within the industry.
- Whilst not directly IO related, the main issues were privacy aspects.
- An informal risk analysis has been performed.
- Main threats related to IO were identified as lack of user awareness (also applying to the managing director level) especially in the following areas:
 - Unauthorized access to data and therefore arising privacy matters.
 - Security settings (e.g. firewalls) and why they should not be downgraded to a lower level than is necessary for the business to operate.
 - Various threats arising from malicious software.

Case Study

Countermeasures

- Current countermeasures in place are:
 - Ongoing operating system hardening
 - Regular updates of virus and spyware signatures
 - HIDS and behavior monitoring on critical systems
 - Firewalls in terms of network security
 - Basic compliance management mechanisms to enforce the security policy
- Access control is based on individual user log in with passwords.

Case Study

Countermeasures (2)

- Future countermeasures will especially address:
 - Network security, in particular the establishment of NIPS capabilities.
 - Continuously monitoring of user actions to identify and rectify risk practices.
 - Simple matters like rotating staff through specific areas and not having one person doing the work to minimize fraud and misappropriation.
- Regular updates of key programs with service packs as soon as they become available to reduce the risk of system compromise are necessary.
- If utilizing local software, an independent audit has to be commissioned to check in detail all financial formulae to make sure nothing is being skimmed off by truncating and the like.

Case Study

IO Awareness

- Insufficient encouragement or resources were provided from Critical Infrastructure Protection initiatives.
- In fact, the participant was not aware it existed.
- The participant feels that the FSS as a whole is not sufficiently aware of IO and the threats it poses.
- Moreover, he believes that the FSS is not adequately prepared to withstand a significant IO attack.
- Especially at small business levels, management and staff are generally not aware of real threats and how to minimize or prevent the likelihood of their occurrence.
- In his opinion, the FSS has to be addressed at all levels with at least an overview, with more specific detailed tuition being promulgated to manager units and personnel.
- Information should be updated on a regular basis, especially when new threats are identified or solutions to existing possible threats are found.

Agenda

Introduction

Background

- Critical Infrastructures

- Current Trends

- Threats

- Countermeasures

Methodology

Research Results

- Expert Interviews

 - Threat Sources

 - Current Trends

 - Weaponry

 - Countermeasures

- Case Study

Conclusions



Conclusions

Threats

- 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.

Conclusions

Countermeasures

- 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.

Conclusions

Weaknesses and Improvements

- 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.
- 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 measures must 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.

Conclusions

Finally...

- In general, information concerning specific organizational security issues in this area is hard to obtain.
- However, 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.

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.

Thank you ...
Any questions?



References

- Alberts, D. S. (1996). *Defensive information warfare*: CCRP publication series.
- Alfonsi, E. (2005). Alliance addresses VoIP security. *IEEE Security & Privacy*, 3(4), 8.
- Anderson, R. J. (2001). *Security engineering: a guide to building dependable distributed systems*. New York: Wiley Computer Publishing.
- 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.
- Bosworth, S., & Kabay, M. E. (2002). *Computer security handbook* (4th ed.). New York: Wiley Computer Publishing 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.
- Elbirt, A. J. (2003). Information warfare: are you at risk? *Technology and Society Magazine, IEEE*, 22(4), 13-19.
- Federal Office for Information Security (BSI) Germany. (2004a). *Critical infrastructure protection (CIP) - a sector-oriented introduction*. Paper presented at the Critical Infrastructure Protection and Civil Emergency Planning Conference, Zurich, Switzerland.
- Federal Office for Information Security (BSI) Germany. (2004b). *IT baseline protection manual*. Retrieved July 28, 2005, from <http://www.bsi.de/english/gshb/manual>
- Ghosh, A. K., & Swaminatha, T. M. (2001). Software security and privacy risks in mobile e-commerce. *Communications of the Acm*, 44(2), 51-57.
- Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3), 81-85.
- Haeni, R. E. (1997). *Information warfare - an Introduction*. Washington D.C.: George Washington University.
- Ierace, N., Urrutia, C., & Bassett, R. (2005). Intrusion prevention systems. *Ubiquity*, 6(19), 2-2.
- Jajodia, S., Ammann, P., & McCollum, C. D. (1999). Surviving information warfare attacks. *Computer*, 32(4), 57-63.
- Jeun-Yet, L. (2002). *Information technology - the dark side (working paper)*. Auckland, N.Z.: University of Auckland.

References (2)

- Kemmerer, R. A., & Vigna, G. (2005). Hi-DRA: Intrusion detection for Internet security. *Proceedings of the IEEE*, 93(10), 1848-1857.
- Lam, K. Y., Chung, S. L., Gu, M., & Sun, J. G. (2003). Lightweight security for mobile commerce transactions. *Computer Communications*, 26(18), 2052-2060.
- 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>
- Ning, P., & Xu, D. (2003). Learning attack strategies from intrusion alerts. In *Proceedings of the 10th ACM conference on Computer and communications security* (pp. 200-209). Washington D.C., USA: ACM Press.
- Overill, R. E. (2001). Information warfare: battles in cyberspace. *Computing & Control Engineering Journal*, 12(3), 125-128.
- 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.
- Schwartz, W. (1996). *Chaos on electronic superhighways: information warfare* (2nd ed.). New York: Thunder's Mouth Press.
- Sequeira, D. (2002). *Intrusion prevention systems - security's silver bullet?* Retrieved September 28, 2005, from <http://www.sans.org/rr/whitepapers/detection/366.php>
- 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>
- U.S. Government Accountability Office. (2005). *Critical infrastructure protection: Department of Homeland Security faces challenges in fulfilling cybersecurity responsibilities*. Retrieved July 28, 2005, from <http://www.gao.gov>
- Wilton, D. R. (2005). *Information systems security (PG seminar)*: Auckland, N.Z.: Massey University.