Global Information Assurance Certification Paper

Jennifer Hogan
Version 1.2f

BUILDING ENTERPRISE-WIDE INFORMATION TECHNOLOGY SECURITY POLICES

BUILDING ENTERPRISE-WIDE INFORMATION TECHNOLOGY SECURITY POLICES

Introduction

Developing Enterprise-wide Security Policies, Standards, and Procedures can have its' challenges and may be one of the most difficult tasks an organization can face. Imagine, having the responsibility of championing the development of security polices and standards for an entire local government. Government's generally consist of many independent businesses operating quite autonomously from one another enabling them to conduct whatever level of Information Technology (IT) planning they feel is appropriate. The lack of consistent, Enterprise-wide planning may affect the overall security of the entire organization. IT security needs an integrated planned approach and cannot be performed in isolation.

Network connections, both internal to other Business Units and external to branch offices and third parties, create more opportunity for security breaches than ever before. Enterprises must have consistent security goals and must ensure that information system resources are utilized in an appropriate and responsible manner. Security must be a component of an Enterprise's overall business plan.

Enterprises require security policies to meet legal and regulatory requirements and to:

- Prevent financial loss and loss of confidentiality;
- Prevent misuse of service and systems or information; and,
- Protect the Enterprise from embarrassment and harm to it's reputation.

The passing of Bill C-6 "The Protection of Personal Information and Electronic Document's Act" outlines requirements for the collection, use and disclosure of personal information. As of January 1, 2001, this act applies to all organizations under federal jurisdiction and international and inter-provincial trade involving personal information. On January 1, 2002, the act applies to any organization dealing with personal health information and on January 1, 2004, the act applies to all organizations that collect, use and disclosure of personal information in the course of commercial activities.

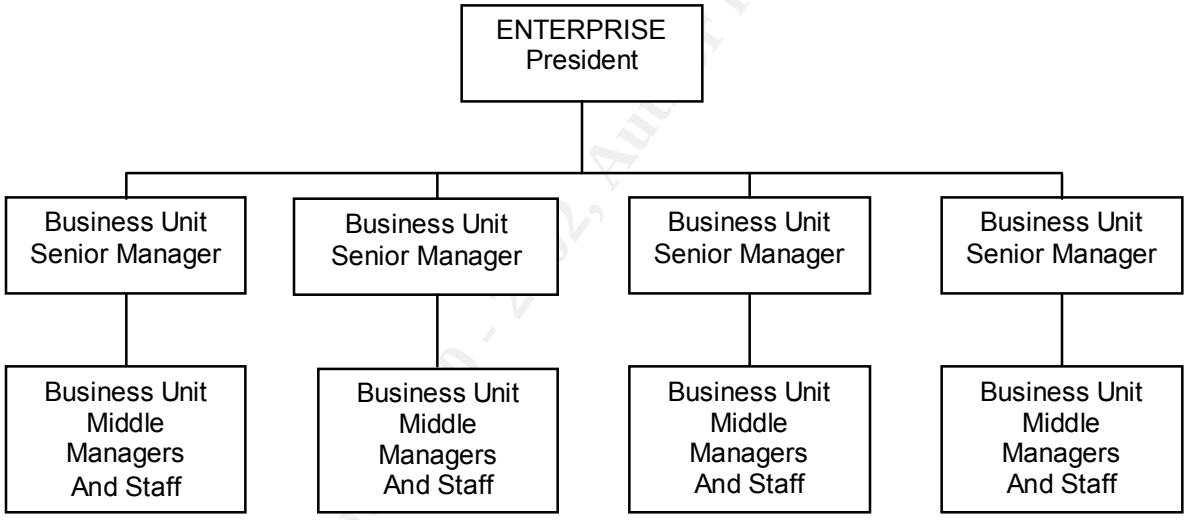
Senior Management should become familiar with Bill C-6 to determine the impact it has on the delivery of internal and external services. For more information on Bill C-6 and Canadian Privacy Laws, refer to the following Web Site: http://www.media-awareness.ca/eng/issues/priv/laws/lawcdn.htm[1].

This paper outlines a strategy for addressing security issues when faced with the many challenges and barriers inherent in large, organizations with many autonomous Business Units that characteristically establish their own goals and objectives and are responsible for their own IT staff, budget dollars, procurement and IT requirements. The basis of this strategy draws upon experiences and lessons learned while developing Security Policies,

Standards and Procedures for a large organization made up of many diverse Business Units.

This document outlines a method for developing Enterprise-Wide Security Policies, Standards and Procedures for a large organization, i.e. (>10,000 employees), with very diverse autonomous Business Units in variety of sizes (100-2,000 employees each).

In this example, Business Units are highly autonomous in nature. Business Units are responsible for their own IT budgets, staff, planning, procurement and IT requirements. Some Business Units have established security policies, while others are just beginning. While all Business Units require security policies they will vary in scope and complexity due to individual business needs. Business Unit staff referred to in this document report to middle management, who in turn, report to a Senior Level Business Manager. Business Unit Senior Managers report to the President of the Enterprise.



Security Policy Development

Steps for security policy development are shown in logical order of progression.

1. Obtain Senior Level Direction and Commitment

Senior Management sponsorship in all Business Units is essential to the success of security policy development. All Senior Managers need to be cognizant of potential security risks and threats to internal assets and need to have a clear understanding of the consequences of poor security. To demonstrate the need for security polices, a high-level security awareness presentation should be given to Senior Management. Presentation topics should include:

- An overview of the security components: confidentiality, availability and integrity of information and assets;
- Examples of threats to internal assets as shown in **Appendix A** of this document;

- How threats can be used to comprise confidentiality, availability and integrity of assets;
- Examples, demonstrating the growth of security incidents. Refer to the CERT/CC Statistics 1988-2001[2] in **Appendix A** of this document;
- Security statistics such as Likely Sources of Attack (by percent), or, Types of Attack or Misuse Detected in the Last 12 Months (by percent). Refer to CSI (Compute Security Institute) Computer Security Issues & Trends for surveys that may be included: http://www.gocsi.com/pdfs/fbi/FBIsurvey.pdf[3]; and,
- Impact of security incidents to the Enterprise based on loss of revenue, loss of service and embarrassment to the Enterprise's reputation.


All Business Units within the Enterprise must recognize that security is important and requires attention. Senior Mangers within the Enterprise must commit to the development of comprehensive security policies and accompanying documentation and be willing to refine security on an on-going basis.

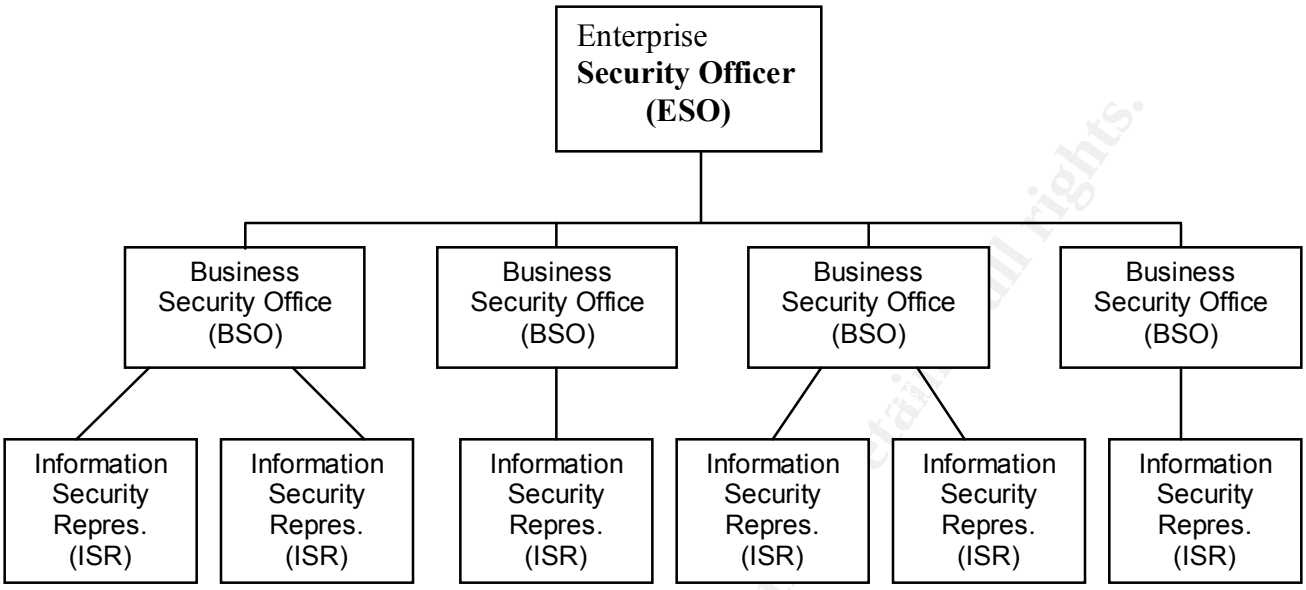
To ensure that Senior Management is committed to security, it may be judicious to have them sign a Security Action Document that commits them to:

- Recognizing that security is important;
- Obtaining a commitment for the completion a Security Threat and Risk Assessment and development of Security Policies, Standards and Procedures;
- Allocating the required budget dollars and resources to the project and assigning representations from respective Business Units to participate on an Enterprise Security Committee; and,
- Working towards having the Business Unit's Policies, Standards and Procedures completed by an agreed upon target date.

2. Establish a Security Infrastructure and Assign Security Personnel

By signing the Security Action Document, Business Units commit to allocating resources to the security project. Resources should include management, IT administrators, program managers, auditors, and in some cases, end users of technology. Shown below is an example of a recommended Security Infrastructure.

SECURITY INFRASTRUCTURE



Enterprise Security Officer

The (President) head of the Enterprise must assign the responsibility for IT Security to a Senior Manager. The Senior Manager will have the responsibility of championing the development of Enterprise-wide Security Polices, Standards and Procedures and will be referred to as the Enterprise Security Officer (ESO). The ESO will work with the President to establish a Corporate Security Policy for the Enterprise, which will reflect the broader Enterprise policies, including legal requirements, security objectives for the Enterprise, expectations and time frames. The ESO and President together will communicate the strategy to respective Business Unit Security Officers.

Business Unit Security Officers

Each Business Unit requires a Business Security Officer (BSO). Typically the BSO will be a Senior Manager within the Business Unit who is responsible for leading their Business Unit through the development, implementation, and on-going maintenance of IT security. The BSO is also responsible for ensuring that funding, resources and tools are allocated to the security project. The BSO will ensure that the security policies are consistent with business plans.

Information Security Representatives

BSO's will have to appoint Information Security Representatives (ISR's) within their Business Unit. ISR's should be a combination of business and IT staff. The ISR's are assigned the job of coordinating and completing the security tasks throughout their Business Unit. These tasks include, but are not limited to the following:

- Representing the Business Unit on an Enterprise-wide Security Committee;
- Completing a Threat and Risk Assessment, including the collection of internal Acts and Regulations;
- Working with internal staff to develop Security Policies, Standards and Procedures unique to their Business Unit;
- Creating and implementing an Employee Security Awareness Program; and,
- Monitoring the effectiveness of the Security Policies.

Enterprise Security Committee

The BSO's and ISR's are required to represent their respective Business Units on a Security Committee chaired by the ESO. The representative(s), in combination, will require knowledge of:

- Security issues within their respective Business Units;
- Internal business processes;
- Systems and networks; and,
- Business Unit's goals and objectives.

The Security Committee will be responsible for:

- Developing a Security Template Document to be used by the Business Units when developing their respective security polices and accompanying documentation. The template will ensure that there is consistency within the Enterprise and ensure that appropriate policies are developed. Refer to **Appendix B** of this document, for an example of a Security Framework Document;
- Leading the Business Unit through the development of it's Security Policies, Standards and Procedures; and,
- Working with Security representatives from other Business Units to improve the security in the overall Enterprise.

3. Provide Security Personnel with Security Training

Security Representatives require detailed information on their project responsibilities and instruction on information technology security. Security training sessions would be an excellent mechanism for communicating security details to the security personnel. Because of the magnitude of information that needs to be communicated, more than one training session will be required. Shown in **Appendix C** of this document are topics that may be covered in each security training session. After completing each training session, the security representatives may be assigned tasks (homework) to be completed by the next training session and is shown in **Appendix C** of this document. To ensure that Business Units are progressing as required, BSO's should keep themselves informed on internal Business Unit security progress.

Tip To facilitate the security training and educate the security personnel on IT security, the Enterprise should contract services with a security firm (supplier) that has extensive knowledge and experience in the security field. The supplier may lead the Business Units through a security policy educational process and provide assistance to security personnel throughout the duration of the project. The BSO's and ISR's will then have an understanding of what constitutes security policies and will have a Security Policy tailored to their organizational requirements. Shown below are addresses of companies that will provide security awareness training. Also shown are addresses of good security sites that provide extensive security information that may be helpful in the development security sessions and may be of assistance in leading the Enterprise through a security educational process..

- Information Technology Security Branch of the RCMP http://www.rcmp-grc.gc.ca/tsb/train/its01-02.pdf[4]
- EWA Canada http://www.ewa-canada.com[5]
- Computer Security Resource Center http://csrc.nist.gov/publications/nistbul/itl98-03.txt[6]
- SANS Online Institute Resources–System Administration, Networking & Security Institute http://www.sans.org/newlook/resources/index.htm[7]

4. Perform a Threat and Risk Assessment

Asset Identification

To determine security requirements for the Enterprise, the security organization needs to have a clear understanding of what assets require protection and what threats could potentially harm the system.

Assets may be divided into two categories, *tangible and intangible.* For a list of assets, refer to **Appendix D** of this document.

When completing the Threat and Risk Assessment, assets need to be identified and assigned values: either: low, medium or high. Assets of low value may not be subject to great safeguard expenditures, whereas, high valued assets may require significant future expenditures for safeguarding the asset.

Asset identification and corresponding value assignments are difficult to complete when working in a large environment. The BSO's and ISR's may not be familiar with internal programs and may have to survey their respective Business Units to identify the assets and assign values to them. Shown in **Appendix D** of this document is an *Asset Identification Form* that may be used when surveying the Business Unit program staff. A formal interview may also be required to obtain a clear understanding of the asset and its sensitivity.

Threats

Threats to internal assets can help an organization define what it's trying to protect. It is important to understand what type of threats can cause great impact to the Enterprise. According to the RCMP *Threat and Risk Assessment for Information Technology Threats*[8], threats to assets may be classified in the following ways: "disclosure; interruption; modification; removal, and destruction". Threats can also be viewed as deliberate, accidental and environmental events and can originate from either outside or inside the internal information technology environment. The Enterprise needs to be cognizant of the fact that it cannot be protected from all threats but should concentrate on those with greatest consequence of impact.

Once the asset and the threats have been identified, the *Likelihood* of the threat happening and the *consequences* of the threat occurrence should be reviewed. Again, low, medium, high, may be used as values to identify the *likelihood*. The consequence of the threat may be based on the potential impact of the threat. Examples of the consequence may include:

- Loss of the asset itself;
- Embarrassment to the Enterprise;
- Unavailability of services;
- Loss of reputation and trust;
- Violation of regulations and law; and,
- Financial loss.

Based on the threat assessment, the impact of the threat should be measured in how serious the impact is to the Enterprise. If the measurement is serious, then serious attention needs to be given to safeguarding the asset. Shown in **Appendix D** of this document is an example of a threat assessment.

Risks

Risks are generally measured in terms of the potential loss that occurs due to exploitation of a known vulnerability by threats to a system.

The process of identifying, analyzing and assessing, mitigating, or transferring risk is generally termed "Risk Management" and provides answers to the following questions:

- What could happen to the asset (threat)?
- What is currently protecting the asset (safeguard)?
- What are the current vulnerabilities?
- What is the level of risk?

Vulnerabilities are condition(s) or weaknesses that may allow a threat to cause harm. Not all vulnerabilities will be susceptible to a threat. Vulnerabilities should be monitored,

especially over time as they become exposed to new threats. Vulnerabilities can be reduced or even prevented as long as you recognize them.

Vulnerabilities may be found by reviewing Enterprise documentation, interviews with staff, automated tools, etc. Many tools are widely available on the Internet to help identify Enterprise vulnerabilities. These tools include system, network and telephone vulnerability scanning tools. Vulnerability Scanners search for security holes or ways of penetrating systems. Described below are utilities that may be used to find security vulnerabilities within the Enterprise. Before running these tools in a production environment, be sure to test them first in a lab environment.

- SARA (Security Auditor's Research Assistant)
  Used for Analyzing Unix Networks
  URL:http://www-arc.com/sara/index.shtml[9]
- Nmap is used for gathering information about the network
  Unix URL:http://www.insecure.org/[10]
  Windows NT URL:http://www.eeye.com/[11]
- Modemscan
  Windows utility that scans a range of phone numbers for modems in auto-answer mode
  URL:http://www.verttex.com/index.htm[12]
- Somar Dump
  Windows utility used for reporting file permissions, audit settings, printer and user/group shares
  URL:http://www.somar.com/[13]
- Chronicle
  Utility that checks for existence of hot fixes in software
  URL:http://www.technotronic.com/rhino9/software/chronicle.htm[14]


Many vulnerabilities lay hidden, undiscovered until it's too late!

Existing safeguards currently protecting assets will need to be reviewed. Over time, an asset's threat impact may change, either requiring strengthening or allowing weakening of safeguards. The vulnerabilities need to be documented and the risk assessed. The risk may be assessed using the low, medium and high values. Low may be defined as *an asset that requires some attention for safeguard implementation with minimal expenditures*; Medium may be defined as *an asset that requires attention and safeguarding in the near future;* and, High may be defined as *the asset requires immediate attention and safeguard implementation and may require significant expenditures.* If the risk is assessed as high, it may require the implementation of new safeguards. Once the asset has a proposed safeguard and project risk, an assessment of safeguards is required to review their adequacy.

Senior Management within each Business Unit must determine what their willing to do with the risk:

- Accept the risk;
- Eliminate the risk by removing the asset;
- Mitigate the risk and implement safeguards; and,
- Transfer the risk by adding insurance to the Asset.

Shown in **Appendix D** of this document is an example of how the Risks to an asset may be documented.

Risk Assessment Methodologies

Generally, there are there types of assessments: Quantitative, Qualitative and Best Practices.

Quantitative assessments use complex calculations and require an automated tool. The Qualitative assessment is much easier to complete, therefore, making it easier on internal staff to complete an accurate assessment of risks. For a detailed description of the pro's and con's of qualitative and quantitative methods of risk assessment, refer to Risk Assessment in the University Setting, by Kent Knudsen at the following address: http://www.sans.org/infosecFAQ/audit/risk_univ.htm[15] - (adapted from the "Information Security Management Handbook")[16].

The Best Practices assessment is very straightforward. As reported in the SANS Security Essentials Course, the following tasks are required for a Best Practice assessment:

- "Identify the problem domain;
- Identify the primary threats;
- Identify potential countermeasures;
- Select and test countermeasures; and.
- Develop step by step instructions for implementing and auditing countermeasures."[17]

Reducing risks can be very costly and needs to be balanced against the benefits. One of the challenges organizations face is determining cost effective fixes for common attacks. The Enterprise should implement safeguards for vulnerabilities identified on the SANS/FBI Top Twenty Most Critical Internet Security Vulnerabilities, where applicable. The list may be found at the following address: http://www.sans.org/top20.htm[18].

Shown below is a list of sites and links to additional information on risk assessment methodologies:

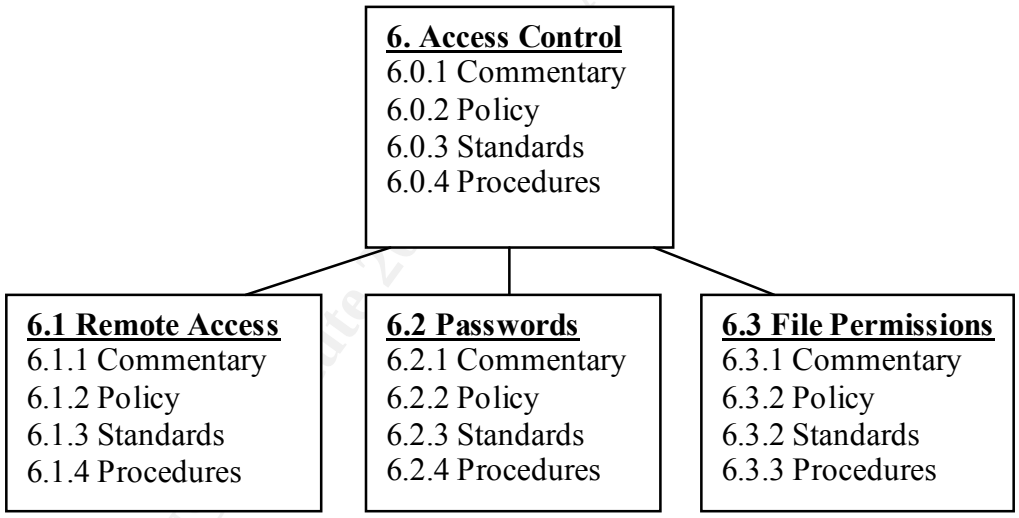
- Computer Security Resource Center
http://csrc.nist.gov/publications/nistbul/itl98-03.txt[19]

- SANS Online Institute Resources
http://www.sans.org/newlook/resources/index.htm[20]
- Communications Security Establishment – A Guide for Security Risk Management for IT Systems
http://www.cse-cst.gc.ca/cse/english/manu2.html[21]

5. Develop Security Policies, Standards and Procedures

Business Unit security policies must be based on the Corporate Security Policy developed by the President and ESO and must be consistent with the Enterprise goals and objectives.

Security Policies are comprised of security principles and directives for the Enterprise and should include commentaries describing the purpose and application of the policies; policies to address the risks reviewed during the risk assessment; standards to depict technical requirements and roles and procedures to provide how the policy and supporting standards will be implemented and who is responsible. The chart below demonstrates how each component of security may be formatted.



Policies need to be clear, concise and unambiguous, and should answer the questions: *who, what,* and *why.* Procedures address *how, where* and *when.*

Many good documents describe appropriate content for Security Policies. Shown below are recommended documents on Security:

Information Technology – Guidelines for the management of IT security (Reference Number ISO/IEC TR 13335) [22]

BS 7799 – The Code of Practice for Information Security Management.
http://www.bsi-global.com/index.html[23]

Information Security Policies Made Easy – Charles Cresson Wood, CISA, CISSP. http://www.baselinesoft.com[24]

SANS Online Institute Resources–System Administration, Networking & Security Institute – www.sans.org[25]

NIST Special Publication 800-12- National Institute of Standards and Technology. "An Introduction to Computer Security NIST Handbook - Publication 800-12". http://csrc.nist.gov/publications/nistpubs/800-12/[26]

6. Security Awareness

Security Awareness is the key to effective security. After policies are written they must be communicated to staff. Security training develops a positive attitude towards security. Training helps users understand the benefits of security measures. Users who understand the need for security may not circumvent the security measures. An appropriate level of security awareness must exist within the Enterprise. Security Awareness needs to be implemented at all levels of the Enterprise, including, employees, management, system design and developers, ISR's, contractors; IT staff, and, employees with security administration requirements.

Industry best practices recommend having staff sign in writing, that they have read, understood, and will abide by the policies.

Tip When developing the awareness session for information technology staff, include a description of the SANS/FBI Top Twenty Most Critical Internet Security Vulnerabilities and how to eliminate them (this was referred to early in the document).

Security awareness needs to be communicated to employees on a continuous basis. Posters may be posted throughout the organization to remind employees of their security responsibilities. The picture shown above may be found at the following address: http://www.infosec.spectria.co m/materials/index.html[27]. A picture is worth a thousand words!

Security awareness training should be fun and exiting for the employees. Spend time developing an awareness session that is interactive and informative!

Tip To reduce the amount of Security documents that an employee is required to read, develop an easy to read, Employee Security Brochure that outlines the Enterprise's security expectations and the employee's security responsibilities. Hand out the brochure at the Security Awareness Presentation and during new employee orientation sessions.

7. Monitor Security Effectiveness and Policy Compliance

Security monitoring is required to ensure that existing safeguards protect the assets as needed. Over time, as computer systems are modified, software upgrades occur and new technologies are deployed, the vulnerabilities and threats to the assets change.

Security Policies, Standards and Procedures require monitoring to:

- Detect any changes that may affect risks;
- Ensure that high valued assets are still appropriately classified;
- Ensure that the safeguards comply with policies and standards;
- Ensure that the safeguards protect the asset; and,
- Ensure that employees are adhering to the policies.

Security Policies are useless unless compliance is enforced. It is important that a review of Security Policy compliance occurs. Corrective actions must be considered when an employee or contractor deviates from the Policies. A non-compliance policy should be communicated to staff.

Conclusion

There is no silver bullet when it comes to protecting the Enterprise. A multi-layered defense system must be deployed. There is no single tool that will solve all security problems.

Security is dynamic. Policies, Standards and Procedures must be reviewed on a continuous basis. Employees are the Enterprise's first line of defense. Employees need to understand the current and latest security issues and they must know their responsibilities.

Security is dynamic. Security requires continuous attention. The Enterprise will need to consider its strategy for reviewing and updating its security policies.

The Enterprise will never be 100% safe from prying eyes, but it can have a relatively secured perimeter that makes it difficult to penetrate.

APPENDIX A – SENIOR MANAGEMENT SECURITY PRESENTATION

1. Threats

The following table provides examples of threats. A threat can be classified as deliberate, accidental and/or environmental in nature.

Deliberate	Accidental	Environmental
Theft	Software Failure	Power Fluctuation
Impersonation	Inadvertently bypass security	Smoke
Virus Attack	File Modification	Fire
Denial of service	Denial of service	Flood
Social Engineering	Illegal Use of Software	Dust
Network Access by Unauthorized Persons	Air Conditioning Failure	Heat
Eavesdropping	Staff Error	Ice Storm

2. Incident Statistics

Rapid growth of Security Incidents

The following tables demonstrate the rapid growth in IT security incidents over the last decade and may be instrumental in describing the importance of the Security. The tables may be found at the following site: http://www.cert.org/stats/#incidents

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999*
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2001

Year	2000	Q1,Q2, 2001
Incidents	21,756	15,476

Total incidents reported (1988-Q2, 2001): 63,187

APPENDIX B – SECURITY FRAMEWORK DOCUMENT

1. Security Framework Document

The Security Framework Document should identify specific sections that the policy should cover.

	Security Policy Framework
1.	Vision (Security strategy, security infrastructure, roles/procedures, acceptable use, disciplinary action, policy management)
2.	Risk Management Methodology
3.	Data Management and Classification (sensitivity levels, custodian)
4.	Hardware (Infrastructure components, computers, servers, mobile devices, disposal)
5.	Software Policies (Licensing, malicious software, asset management, operating systems)
6.	Access Control (Network access, remote access and passwords, file permissions)
7.	Communications (Internet, E-mail, Online Credit Card Transactions)
8.	Physical Security (Locks, Alarms, perimeter, sensitivity areas – electrical and wiring rooms)
9.	Personnel (Security Awareness, security responsibilities, maintenance agreements, contracts)
10.	Business Continuity (Data backup, off site storage, hot site, test strategy)
11.	Change Control (Authorizations, procedures)
12.	Appendices (Glossary, Acts, Regulations, Laws)

APPENDIX C – SECURITY TRAINING SESSIONS

1. First Training Session (Introduction to Security and the Security Project)

The first training session should be at least one day in length and may cover the following items:

- Senior Manager's security expectations including project scope and timeframes;
- Clear definitions of security policies, procedures and standards;
- An overview of the security principles: confidentiality, availability and integrity of information and assets;
- Examples of threats to internal assets;
- How threats can be used to compromise confidentiality, availability and integrity of assets;
- Examples, demonstrating the growth of security incidents as described in **Appendix A** of this document;
- Example of a major recent security incident(s), such as the Code Red Worm as described in section 1.1.1 below;
- Examples of Security Polices, Standards and Procedures;
- Clear picture of security steps that are required throughout development of the Security Policies and supporting documentation; and,
- Work Assignment 1, as described below.

1.1 Work Assignment 1 – Collect Acts and Regulations & Review Legal Requirements

The first assignment needs to be completed by the next training session. The Security Committee will need to identify any Acts and Regulations and become familiar with any legal requirements that must be met by the program areas within the Business Unit.

1.1.1 Code-Red Worm Security Incident

A computer worm is a program that is designed to replicate itself. On July 19, 2001 more than 359,000 computers were infected within a 24-hour period with the Code Red Worm. The worm spread itself by searching random Internet addresses and infecting all web servers running the Microsoft Internet Information Server (IIS) and looking for vulnerabilities. After infecting the IIS Server, the worm launched a denial of service attack (an attack that renders a system un-operational) against the Whitehouse at www1.whitehouse.gov. The IIS vulnerability was discovered on June 18, 2001. The following animation depicts the geographic expansion of the worm through a 14-hour period:

http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml#animations

The animation was created by Jeff Brown (UCSD CSE department), based on analysis by David Moore (CAIDA at SDSC)[28].

2. Second Training Session (Threat & Risk Assessment)

The second training session should be at least two days in length and should include detailed information on how to create a threat and risk assessment. Security representatives will need to learn the following:

- How to identify assets and assign sensitivity values using the Asset Identification Form shown in **Appendix D** of this document;
- What type of pertinent security documents need to be gathered throughout out the Business Unit;
- What type of threats can impact identified assets;
- Understand how to assess the class of threats, likelihood, consequence and impact of the treat;
- How to complete a Threat and Risk Assessment; and,
- Work Assignment 2, as described below.

2.1. Work Assignment 2 – Asset Identification and Valuation

The Security Committee will be required to:

- Complete an asset identification and valuation before the next training session. Security Representatives may be required to interview specific program areas to ensure that they have a full understanding of the assets and their security characteristics;
- Collect existing network infrastructure schematic's, including internal and external connections;
- Gather any existing Security Policies, Standards, Procedures; and,
- Identify a Risk Methodology; and,
- Complete the threat and risk assessment for assets that are assigned a value and require safeguarding.

3. Third Training Session (Security Policy Development and Awareness Training)

The third training session should be a least two days in length and should include the following:

- Security Policy Writing;
- Policy attributes: clear, unambiguous, etc.
- Overview of the Enterprise Security Framework Document;
- Practice session at writing Security Policies, Standards and Procedures;

- Security Awareness importance and recommended ways of communicating security policies to the staff should be covered; and,
- Work Assignment 3, as described below.

Sample security polices and reference material should be provided at this session.

3.1 Work Assignment 3 – Security Policy Development and Awareness Strategy

The Security Committee will be required to:

- Complete Security Policy development for sections outlined in the Security Framework document; and,
- Development a Security Awareness Strategy.

APPENDIX D – ASSETS

1. Asset Categories

Tangible Assets

- Hardware: workstations, servers, printers, routers, local area networking Components;
- Software, source code, utilities, operating systems;
- People: users, administrators;
- Data: stored online, backups, audit logs, databases, briefing material;
- Documentation: procedures; manuals;
- Environmental equipment; and,
- Buildings.

Intangible Assets

- Intellectual property;
- Knowledge;
- Image/reputation of the Enterprise; and,
- Trust.

2. Asset Identification Form

Contact Name: _____ **Date:** _____
Business Unit: _____
Address: _____
Phone: _____

Software/Hardware Asset
Custodian: _____
Name of Asset: _____ Confidential Rating: Yes or No: ___
If applicable physical location or location on Network: _____

Specify consequence if disclosed to unauthorized personnel:

	Yes	No
Embarrassment to Enterprise		
Legal Implications		
Loss of Service		
Loss of Trust		
Financial Impact		
Loss of Life		
Other		
Other		

How long (in days) can this asset (software/hardware) be unavailable? _____

Are there contingencies made for recovery of this asset? _____ If yes, explain:

If the asset was unavailable what is the consequence?

	Yes	No
Embarrassment to Enterprise		
Legal Implications		
Loss of Service		
Loss of Trust		
Financial Impact		
Loss of Life		
Other		
Other		

If a software asset, how critical is the Accuracy of the information?
Very Critical_____ Slightly Critical _____

If Accuracy is comprised what is the consequence?

	Yes	No
Embarrassment to Enterprise		

Legal Implications
Loss of Service
Loss of Trust
Financial Impact
Loss of Life
Other
Other
Rate the Value of the Asset to program delivery: Low Medium High

---

3. Risk Assessment

Asset	Threat	Existing Safeguards	Vulnerability	Risk
Data on Server	Malicious Worm	Antivirus Software on data Server, all Workstations and E-mail Server Firewall denies all .exe, .com and .bat attachments	Virus Lists and Software not kept up to date	High
Notebook	Theft	Cables to lock notebook to desk when unattended	Notebook lock not used	High
E-Mail Server	Server destroyed by disgruntled employee	Server stored in locked, secured room	Locks fail	Low

4. Threat Assessment

Asset	Threat	Class of Threat	Likelihood	Consequence	Impact
Data on Server	Malicious Worm	Disclosure Interruption Modification Destruction	High	Loss of Privacy Loss of Service Time/Cost rebuilding Loss of Trust	Serious
Notebook	Theft	Disclosure Interruption Removal	High	Loss of Privacy Loss of Service	Less Serious
E-Mail Server	Server destroyed by disgruntled employee	Interruption Destruction	Low	Loss of Asset Loss of Trust	Serious

References

1. Canadian Privacy Laws. Feb. 2000. URL: http://www.media-awareness.ca/eng/issues/priv/laws/lawcdn.htm (3 Oct. 2000).
2. Carnegie Mellon. "CERT/CC Statistics 1988-2001". (18 Jul. 2001)URL: http://www.cert.org/stats/ - incidents. (3 Sept. 2001).
3. Power, Richard. "Computer Security Issues & Trends". 2001. URL: http://www.gocsi.com/pdfs/fbi/FBIsurvey.pdf (3 Oct. 2001).
4. Information Technology Security Branch. "Information Technology Security Workshops 2001-2002. URL: http://www.rcmp-grc.gc.ca/tsb/train/its01-02.pdf.
5. EWA Canada. URL: http://www.ewa-canada.com/. (25 Sept. 2001).
6. Computer Security Resource Center. "Management of Risks in Information Systems: Practices of Successful Organizations". URL: http://csrc.nist.gov/publications/nistbul/itl98-03.txt. (30 Sept. 2001).
7. Sans Online Institute Resources-System Administration, Networking & Security Institute. URL: http://www.sans.org/newlook/resources/index.htm.
8. Information Technology Security Branch. "Guide to Threat and Risk Assessment for Information Technology. (Nov. 1994). URL: http://www.rcmp-grc.gc.ca/tsb/pubs/reports/tra_guide.pdf. (10 Sept. 2001).
9. Advanced Research Corporation. "SARA (Security Auditor's Research Assistant)". (18 Sept. 2001). URL: http://www-arc.com/sara/index.shtml
10. NMAP. Unix Utility. (26 Jul. 2001). URL: http://www.insecure.org/. (5 Sept. 2001).
11. NMAP. Windows Utility. URL: http://www.eeye.com/. (5 Sept. 2001).
12. VerTTex Software, LLC. "Modemscan Windows Utility". URL: http://www.verttex.com/index.htm. (29 Sept. 2001).
13. Somarsoft. "Somar Dump Utilities". URL: www.somar.com. (28 Sept. 2001).
14. Rihino9. "Chronicle". Version 1.0 Beta. URL: http://www.technotronic.com/rhino9/software/chronicle.htm (27 Sept. 2001).
15. Knudsen, Kent. "Risk Assessment in the University Setting". URL: http://www.sans.org/infosecFAQ/audit/risk_univ.htm (25 Sept. 2001).
16. Tipton, Harold F. and Krause, Micki. "Information Security Management Handbook". Dec. 1999. URL: http://secinf.net/info/misc/handbook/242-244.html (24 Sept. 2001).
17. Sans Institute. Security Essentials. Internet Threat Brief. Risk Assessment and Auditing. Pg. 6-15.
18. Sans Online Institute Resources-System Administration, Networking & Security Institute. "The Twenty Most Critical Internet Security Vulnerabilities". (Version 2.100). (Oct. 2, 2001). (Oct. 9, 2001). URL: http://www.sans.org/top20.htm.
19. National Institute of Standards and Technology. "Management of Risks in Information Systems". URL: http://csrc.nist.gov/publications/nistpubs/800-12/. (24 Sept. 2001).
20. Sans Online Institute Resources-System Administration, Networking & Security Institute. "Information Security Reading Room". URL: http://www.sans.org/newlook/resources/index.htm. (2 Sept. 2001).

21. Communications Security Establishment. “Guide for Security Risk Management for IT Systems”. (1996). URL: http://www.cse-cst.gc.ca/cse/english/manu2.html. (14 Sept. 2001).
22. “Guidelines for the management of IT security”. Reference Number ISO/IEC TR 13335.
23. British Standards Institute. “BS 7799-The Code of Practice for Information Security Management”. URL: http://www.bsi-global.com/index.html. (2 Sept. 2001).
24. Cresson Wood, Charles. “Information Security Policies Made Easy”. Version 7. (Oct. 1999). URL: http://www.baselinesoft.com/.
25. Sans Online Institute Resources-System Administration, Networking & Security Institute. URL: http://www.sans.org
26. National Institute of Standards and Technology. “An Introduction to Computer
27. Security NIST Handbook - Publication 800-12”. (07 Feb. 1996). URL: http://csrc.nist.gov/publications/nistpubs/800-12/. (24 Sept. 2001).
27. Spectria Infosec. URL: http://www.infosec.spectria.com/. (3 Oct. 2001).
28. Brown, Jeff. Moore, David. “Code Red Worm – CAIDA (Cooperative Association for Internet Data Analysis)”. 2001
URL: http://www.caida.org
(09 Sept 01).