TNC ENGINEERING

WHITE PAPER DEVELOPING A CORPORATE SECURITY POLICY

Abstract

This paper addresses the methods and methodologies required to develop a corporate security policy that will effectively protect a company's assets.

Date: January 1, 2000

Authors:
J.D. Smith, P.Eng.
Kevin Murray

Background

Data has no value until it is transformed by the application of intellectual processes into information. Because information is a company's most valuable asset, it must be the primary focus of corporate security.

The protection of information requires the corporation to identify information assets, classify them, define access, establish ownership, determine vulnerabilities and the consequences of compromise. These requirements are managed through the development of corporate security policies.

Information assets are both tangible (marketing plans, customer lists, strategic plans, servers, network components) and intangible (company reputation, goodwill, databases). For each of these business assets - both tangible and intangible -- a threat and risk assessment determines vulnerabilities, and develops strategies for safeguarding and protection.

Corporate security is a continuous, on-going process involving business threat and risk analysis, review of technical vulnerabilities and security policy refinement.

Purpose

The purpose of this paper is to outline the steps required for developing and maintaining a corporate security policy.

Discussion and Assumptions

The traditional building blocks of commerce - capital, labour, land and raw materials have been supplemented by a new, somewhat intangible element - information. Information contains the intellectual capital of a company and as such is probably the company's most important asset.

Information is versatile in its uses, malleable and easy to store. It is also intangible, unstable, corruptible and easily compromised, which leads to the paradox:

"The more uses made of information, the more accessible it must be, thereby increasing the risk that it's confidentiality or integrity will be compromised"

In this paper, we assume that the company has analyzed their business processes in sufficient detail to identify their information assets and is able to track information flow. We also assume that the company has developed or accepted a set of security standards.

Developing a Security Policy

Is There a Need?

Why do I need a policy for security? Isn't my statement that "security is everybody's responsibility!" sufficient?

A recent survey of 1,600 senior information officers by PricewaterhouseCoopers and Information Week finds, that of the companies surveyed, 73% experienced a security breach in the previous 12 months. Authorized employees accounted for 58% of these breaches.

Source of Security Threat	*** see note**
Authorized employees	58%
Unauthorized employees	24%
Former employees	13%
Outside agents (hackers, etc.)	13%
Competitors	3%

* Multiple responses were included

From this survey, 56% of the respondents stated that security was a high priority for their business. However only 19% said that they had a complete descriptive policy to monitor security practices and solutions.

Where Do I Start?

There are four steps in developing a security policy:

1. Identify information assets and who owns them

2. Assess the threat, likelihood of compromise and consequences of exposure for these assets

3. Define or develop protection strategies for each class of asset

4. Write policies that implement these strategies

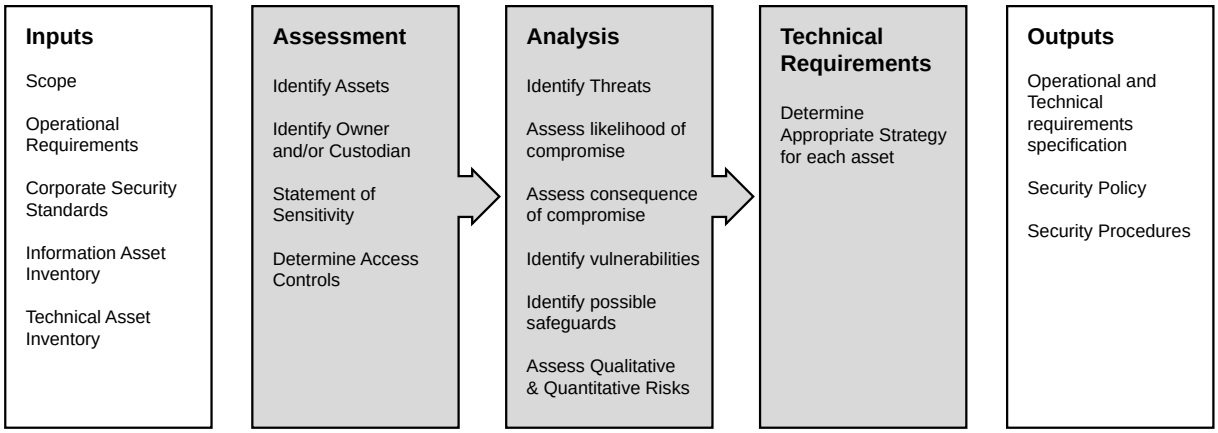
Assets can be both tangible and intangible, depending upon the point of view as shown below:

	Technical	Business
Tangible	Hardware Desktops Servers Physical Network	Financial Plans Marketing Forecasts Employee Information Customer Lists
Intangible	Databases Application Software Operating Systems	Customer Satisfaction Supplier Relations Company Reputation

A threat and risk assessment must be completed for each class of asset above. Once complete, there are three general protection strategies that can be applied for each asset: ignore the risks, severely restrict access to the information, or implement risk management procedures. These are all perfectly legitimate choices that will depend upon the level of risk associated with each business asset.

Threat and Risk Assessment

The process for determining threats and risks to business assets is shown in the diagram:



The technical requirements together with the operational requirements dictate which strategies should be employed for each asset and how it should be implemented.

What Should A Security Policy Contain

Once the information is gathered and identified, the company must put some administrative structure around IT in the form of a security policy. The following is the outline of TNC's generic security policies that serve as a foundation for a company's security policy.

Section 1: Corporate Security Guidelines

1.1 Information Security Policy
1.1.1 Information security policy

1.2 Information Security Management
1.2.1 Management information security committee
1.2.2 Information security coordinator
1.2.3 Responsibility for information security
1.2.4 Specialist information security advice
1.2.5 Security assessment for network services

1.3 Information Management and Classification
1.3.1 Inventory of assets
1.3.2 Classification guidelines
1.3.3 Classification labeling

1.4 User Passwords, Identification and Authentication
1.4.1 User identifiers
1.4.2 User-ID and password required for computer-connected network access
1.4.3 Periodic review and reauthorization of user access privileges
1.4.4 Use of duress passwords
1.4.5 Unattended user equipment

1.5 Physical Security
1.5.1 Physical security perimeter
1.5.2 Physical entry controls
1.5.3 Security of data centres and computer rooms
1.5.4 Clear desk policy
1.5.5 Removal of property
1.5.6 Secure disposal of equipment

1.6 Contingency Planning
1.6.1 Business continuity planning process
1.6.2 Testing business continuity plans
1.6.3 Updating business continuity plans

1.7 General Compliance Issues
1.7.1 Control of proprietary software copying
1.7.2 Safeguarding of organizational records
1.7.3 Protection of personal information
1.7.4 Prevention of misuse of IT facilities
1.7.5 Cooperation with other security organizations
1.7.6 Independent review of information security
1.7.7 Security audits
1.7.8 System audit controls
1.7.9 Protection of system audit tools

Section 2: IT System Use Guidelines

2.1 Human Resources

2.1.1 Security in job descriptions
2.1.2 Recruitment screening
2.1.3 Confidentiality agreement
2.1.4 Return of company property at time of termination
2.1.5 Employee termination through disciplinary process
2.1.6 Progressive disciplinary measures for information security violations
2.1.7 Information security education and training
2.1.8 Disclaimer of responsibility for damage to data and programs

2.2 Use of Email

2.2.1 Electronic mail messages are company records
2.2.2 Personal use of electronic mail systems
2.2.3 Forwarding electronic mail to an external network address
2.2.4 Recording and retention of electronic mail
2.2.5 Encryption of certain e-mail messages
2.2.6 Sending security and payments information over the Internet

2.3 Use of Internet

2.3.1 Internet privileges reserved for those with a business need
2.3.2 Internet representations about A company's products & services
2.3.3 Respecting intellectual property rights
2.3.4 Internet discussion group participation
2.3.5 Unofficial web pages permitted only by contract
2.3.6 Internet web page management committee
2.3.7 Internet web page design requirements
2.3.8 Management approval for Internet hot-links
2.3.9 A company blocks certain non-business Internet web sites
2.3.10 Handling software and files down-loaded from Internet
2.3.11 Posting company material on the Internet

Section 3: IT Planning and Operating Guidelines

3.1 IT Management and Planning

3.1.1 Change control procedure
3.1.2 Security requirements analysis and specification
3.1.3 Annual inventory of information management systems
3.1.4 Cross training for staff in critical technical jobs
3.1.5 Segregation of duties

3.2 Network Monitoring and Maintenance

3.2.1 Preventive maintenance on computer and communications systems
3.2.2 Technical conformity checking
3.2.3 Documented operating procedures
3.2.4 Event logging
3.2.5 Monitoring system use
3.2.6 Virus controls

3.3 Network Security Controls
3.3.1 Network security control devices
3.3.2 Separation of development and operational facilities
3.3.3 Sensitive system isolation
3.3.4 Remote diagnostic port protection
3.3.5 Segregation in networks
3.3.6 Control of production software
3.3.7 Restrictions on changes to software packages
3.3.8 Protection of system test data
3.3.9 Segmenting Information Resources by Recovery Priority

3.4 Network Access Control
3.4.1 Computer system access controls
3.4.2 Terminal timeout / Automatic Log-Off Process
3.4.3 Limitation of connection time
3.4.4 Information access restriction
3.4.5 Restricted and Monitored Use of Systems Software Utilities

3.5 User Authentication and Identification
3.5.1 Documented access control policy
3.5.2 Limited services
3.5.3 User authentication
3.5.4 Positive identification required for system usage
3.5.5 User password management
3.5.6 User ID's must identify a unique user
3.5.7 Password use

3.6 Handling of Information Media
3.6.1 Data back-up
3.6.2 Management of removable computer media
3.6.3 Data handling procedures
3.6.4 Encrypting Back-up Media Stored Off-Site
3.6.5 Disposal of Sensitive Information

3.7 IT Environmental and Facility Security
3.7.1 Equipment siting and protection
3.7.2 Power supplies
3.7.3 Cabling security
3.7.4 Security of equipment off premises
3.7.5 Environmental monitoring
3.7.6 Clock synchronization

3.8 Third Parties
3.8.1 Identification of risks from third party connections
3.8.2 Security conditions in third party contracts
3.8.3 EDI/e-commerce security

Section 4: Security Incident Response

4.1 Security Incident Management
4.1.1 Incident management procedures
4.1.2 Information security alert system
4.1.3 Organization and maintenance of computer emergency response team

Conclusion

A security policy is easier to develop and implement when all the stakeholders have a thorough understanding of what it is they are protecting.

The consequences of compromise must be quantified, so that everyone understands the importance of adhering to the policies.

Policy management is an on-going affair. Asset characteristics and importance change as well as their inter-relationship. If one part of a policy is not enforced because it lacks relevance, then that casts doubt on the relevance of the other parts of the policy.