

Protecting Critical Information Assets: Countermeasure Systems for Information Security

Stan Stahl, Ph.D.
President & Chief Security Officer
Citadel Information Group, Inc.

© Copyright 2002. Citadel Information Group, Inc. All Rights Reserved.

Abstract

This paper identifies the need to view information security countermeasures from a holistic systems point-of-view. The paper articulates a method for developing a layered strategy for implementing a system of information security countermeasures. The paper integrates several performance tools and methods, including an “information security management maturity model” to provide guidance to organizations desiring to effectively evolve their countermeasure system.

Introduction

As business and commerce becomes increasingly information-based, the need to protect information assets has grown accordingly.

Critical information assets requiring protection include *critical* and *sensitive information* — financial information, customer lists, price lists, customer orders, manufacturing schedules, inventory levels, product specifications, trade secrets, proprietary information, intellectual property, and other confidential information — as well as the computer-communications systems in which they reside.

Traditionally, protecting a critical information asset has meant ¹

- Keeping it confidential, providing access only to those having a legitimate need for it
- Maintaining its integrity, assuring that all changes are authorized and intended
- Ensuring its availability

Critical information assets must be protected against attacks from ordinary hackers, industrial spies, disgruntled employees, and cyber-terrorists. It must also be protected from accidents or natural disasters that might disclose, damage, or destroy critical information assets, or make them otherwise unavailable.

In the last 10 years, as organizations have become connected through the Internet, there is emerging a direct communication path between any two computers anywhere in the world. This communication path exists regardless of the extent to which the organization makes use of it.

While this connectivity has dramatically increased business efficiency, it has also dramatically changed the nature of business risk. It’s always been easy for the ‘bad guys’ to break into information systems, provided they had physical access to the computers. Now these cyber-outlaws can break in from anywhere in the world—Alabama, Australia, or even Afghanistan. All that’s needed is an Internet connection. Unless an organization takes proper security precautions, cyber-crime - financial fraud, theft of proprietary information, destruction of information, etc. - can occur anytime from anywhere.

¹ *Information Technology — Code of practice for information security management*, ISO 17799, 2000.

According to the *2001 Computer Crime and Security Survey*², a survey of large and small companies done by the *FBI* and the *Computer Security Institute*, the problem is extremely serious. 40% of surveyed companies reported their systems had been penetrated from the outside, 40% suffered denial of service attacks, 78% reported employee abuse problems, and 85% reported computer virus infections. Those companies able to quantify losses report the average internet crime results in a loss of \$750,000. Internal theft averages a whopping \$2,500,000. The greatest loss categories are theft of proprietary information and financial fraud.

Every business is at risk. The risk is greatest among middle market companies. Cyber-criminals love middle market companies with lots of information assets and not a lot of security. Lacking the security resources of larger companies, they are easy to break into and detection is unlikely. *The FBI estimates that 50% of these companies will be penetrated by 2003.*

The problem is getting worse, not better. New system vulnerabilities are continually being discovered and disseminated throughout the cyber-outlaw community. Automated penetration tools are making it even easier for cyber-outlaws to do their work. Technology providers directly contribute to the problem, both by sloppy software development procedures and by their general lack of adequate concern for security issues. Unprotected wireless networks only exacerbate the problem.

The Need for a Systems Perspective

A major challenge organizations face in protecting their information assets is illustrated by the aphorism: *A chain is only as strong as its weakest link*

As examples, consider the following:

- A company invests in firewalls to block outside intruders but fails to assign responsibility to an employee to maintain firewall effectiveness. Some time later, the cyber-outlaw community identifies a security vulnerability which is exploited.
- A company invests in firewalls to block outside intruders. A salesperson installs a wireless network behind the firewall so that he can synchronize his laptop computer with his desktop. Cyber-outlaws bypass the firewall to gain access to the corporate network through the insecure wireless network.
- A company uses strong passwords to limit access to system resources but fails to train employees on password protection. The receptionist receives a phone call from someone claiming to be from IT who is working from home and needs the receptionist's password to make some minor system changes. The receptionist complies and now a cyber-outlaw has her password.
- A company installs an expensive intrusion detection system to identify attempted system break-ins but fails to assign anyone the responsibility to review audit logs. Weeks go by

² *Computer Security Issues & Trends*, Computer Security Institute, Spring 2001.

without an audit log review during which time cyber-outlaws have undetected access to the system.

- A company terminates an employee. The IT Department, notified of the termination by the employee's department manager, delays removing the employee's access to the system because its policies require notification from Human Resources. Human Resources fails to notify IT, believing the department notification is adequate. In the meantime the discharged employee has access to the system.
- The operations department of a company establishes a communication link with a key supplier. No one thinks to ask the supplier how secure its computer systems are. As a result, cyber-outlaws are able to exploit vulnerabilities in the supplier's systems to gain illegitimate access to the company's systems.

All of these examples illustrate the need to take a holistic systems perspective in security management.

Amplifying the above are the words of Patrice Rapalus, Director of the *Computer Security Institute*, writing in the 2001 *FBI / Computer Security Institute Computer Crime and Security Survey*:

*The survey results over the years offer compelling evidence that neither technologies nor policies alone really offer an effective defense for your organization. Intrusions take place despite the presence of firewalls. Theft of trade secrets takes place despite the presence of encryption. Net abuse flourishes despite corporate edicts against it. Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions. They also need to properly fund, train, staff and empower those tasked with enterprise-wide information security.*³

Elements of the Information Security System

There are five major elements to the information security system:

1. Information assets needing protection
2. Organizational objectives requiring the access and sharing of critical information assets
3. Threat agents (internal and external) seeking to illegitimately disclose, modify or make these assets unavailable
4. Vulnerabilities (technical and management) which threat agents seek to exploit to accomplish their nefarious ends
5. Countermeasures (technical and management) which the organization implements to protect critical information assets

³ *Computer Security Issues & Trends*, Computer Security Institute, Spring 2001.

As with most dynamic systems, the elements of the information security system evolve over time. Assets requiring protection change; organizational objectives change; threat agents change; discovered vulnerabilities change; and countermeasures must change in response.

It is management's responsibility to manage the system of countermeasures so as to maintain appropriate protection in the face of dynamic changes to other system elements.

Countermeasure System Objectives and Constraints

An organization's system of countermeasures has four objectives:

- *Prevent* critical information assets from successful attack
- *Detect* critical illicit attacks on critical information assets
- *Recover* from attacks, accidents or natural disasters and, in the case of attack, apprehend, prosecute/punish, and recover damages from the culprits
- *Comply* with applicable security and privacy laws, regulations, and policies.

There are four primary constraints on the system of countermeasures:

1. Cost, measured in dollars, time, and resources
2. Impact on business mission
3. Availability of trained, knowledgeable, motivated people to design, implement, monitor and evolve the system of countermeasures
4. Extent of senior-level leadership and management capabilities

Developing Strategy for Implementing Security Countermeasures

Given that security resources are finite, and that security countermeasures must be implemented in the context of other organizational constraints, one can't "buy" security merely by implementing all available countermeasures. Trade-offs must be made and, consequently, the organization needs a strategy to determine which security countermeasures it is to implement and what "strength" these countermeasures are to possess.

Illustrative strategic "trade-off" questions include:

- How much money should be invested in firewalls (given that every such dollar is now unavailable for other purposes)?
- How frequently are security patches to be installed (given that it takes the time of security personnel to install the patches and patching may require bringing down system services)?

- How many hours per month of security training and education are employees to receive (given that every hour of training and education is an hour taken away from meeting the organization's mission)?
- How much access are suppliers to have to information (given that as suppliers have more access, the more management can drive costs and time out of the supply chain, yet the less secure the organization's information will be)?
- What is the "right" mixture of technology countermeasures, management countermeasures, legal structures, and cyber-insurance to most cost-effectively mitigate information risk?

Landscape Setting^{SM 4} is a structured methodology for identifying and strategically resolving these types of trade-offs. In *Landscape Setting* key organizational stakeholders are brought together to jointly analyze the relationship between the evolving performance needs of the organization and its information security needs. The outcome of a successful *Landscape Setting Workshop* is a clear strategic consensus among stakeholders that provides direction to the organization in implementing security countermeasures.

Security Countermeasure Controls

The emerging international standard, ISO 17799, identifies the following classes of information security controls⁵.

⁴ *Landscape Setting* is a proprietary methodology of Citadel Information Group, Inc.

⁵ *Information Technology — Code of practice for information security management*, ISO 17799, 2000.

Information Security Controls	
<p>Information Security Policy</p> <ul style="list-style-type: none"> • Information Security Policy Document • Review and Evaluation <p>Organizational Security</p> <ul style="list-style-type: none"> • Information Security Infrastructure • Security of Third Party Access • Outsourcing <p>Asset Classification and Control</p> <ul style="list-style-type: none"> • Accountability for Assets • Information Classification <p>Personnel Security</p> <ul style="list-style-type: none"> • Security in Job Definition and Resourcing • User Training • Responding to Security Incidents and Malfunctions • Disciplinary Process <p>Physical and Environmental Security</p> <ul style="list-style-type: none"> • Secure Areas • Equipment Security • General Controls <p>Communications and Operations Management</p> <ul style="list-style-type: none"> • Operational Procedures and Responsibilities • System Planning and Acceptance • Protection Against Malicious Software • Housekeeping • Network Management • Media Handling and Security • Exchanges of Information and Software 	<p>Access Control</p> <ul style="list-style-type: none"> • Business Requirement for Access Control • User Access Management • User Responsibilities • Network Access Control • Operating System Access Control • Application Access Control • Monitoring System Access and Use • Mobile Computing and Teleworking <p>Systems Development and Maintenance</p> <ul style="list-style-type: none"> • Security Requirements of Systems • Security in Application Systems • Cryptographic Controls • Security of System Files • Security on Development and Support Processes <p>Business Continuity Management</p> <ul style="list-style-type: none"> • Business Continuity Management Process • Business Continuity and Impact Analysis • Writing and Implementing Continuity Plans • Business Continuity Planning Framework • Testing, Maintaining and Re-Assessing Business Continuity Plans <p>Compliance</p> <ul style="list-style-type: none"> • Compliance with Legal Requirements • Reviews of Security Policy and Technical Compliance • System Audit Considerations

The management challenge is to integrate these controls together, evolving them over time, so as to provide the “appropriate” extent of security to information object. It is to this “orderly” implementation that we now turn.



The Orderly Implementation of Security Countermeasures

Implementing a system of countermeasures must, of necessity, be done in an evolutionary fashion. An organization cannot expect to shut the doors on Thursday evening and return to the office Friday morning with a full-suite of countermeasures. And, even if it could, some cyber-outlaw might discover a new vulnerability Friday afternoon.

While the specific sequence for implementing security countermeasures is a function of the organization's existing security countermeasures, its security needs, its available resources and its business realities, there is a general structure for the orderly implementation of countermeasures. This structure is illustrated in the following figure.

The following tables illustrate typical countermeasures associated with each level. It is important not to take too seriously the association of specific countermeasures to levels as each organization will want to structure the implementation of security countermeasures in accordance with its specific circumstances, as identified during *Landscape Setting*.

Level 1A: Infrastructure Protection
Physical Security
Technology Security Management
Anti-Virus Software
Firewall Implementation
Back-Up & Recovery Systems
Configuration Maintenance
Vulnerability Maintenance

Level 1B: Mandatory Access Control
Technical Policies and Procedures
Access Controls
Password Management
Security Architecture

Level 2: Detection & Response
Intrusion Detection
Incidence Response
Communications Security
Cooperation with Police and Law Enforcement

Level 3: Organizational Security
Executive Security Management
Information Security Response Team
Employee Policies & Procedures
Forensics Management
Cyber-Surveillance
Employee Risk Management
Employee Training and Education

Level 4: Information Continuity
Information Labeling
Information Continuity & Contingency Planning
Supply-Chain Security Management

Level 5: Integrated Risk Management
Integrated Risk Management

An Information Security Management Maturity Model

Drawing upon work of the *Software Engineering Institute*⁶, the *IT Governance Institute of the Information Systems, Audit and Control Foundation* has developed a six-level hierarchy for use in assessing the “maturity” of an organization’s management of its information security system⁷.

Level 5: Optimized	Information security best practices are followed
Level 4: Managed	Security management is monitored and measured; regular feedback is used to assess and improve management effectiveness
Level 3: Defined	Security management flows from organizational strategy and from an organization-wide risk management policy; employees receive regular training and education
Level 2: Repeatable	Basic security countermeasures and processes are implemented; management responsibility, authority and accountability are assigned
Level 1: Initial	Security management is <i>ad hoc</i> and not organized; management responsibility is fragmented or non-existent
Level 0: Non-Existent	The organization does not manage the security of information assets

It is neither necessary nor appropriate for all organizations to seek to achieve Level 5. As citizens, we have a right to expect our critical military and critical infrastructure systems (water, power, etc.) to follow best practices. Banks and financial institutions should also manage the security of their financial systems at Level 4 or Level 5. But achieving these levels of information security is overkill for most organizations and would not be a cost-effective way of managing information risk.

On the other hand, no organization should be content at Level 0 or Level 1. In accordance with the aphorism *An ounce of prevention is worth a pound of cure*, organizations at these two lower levels are wasting money (and other organizational resources) by being completely reactive to security incidents. They also put themselves at risk in three important ways.

First, by paying inadequate attention to protecting critical information assets, they put these important organizational assets at undue risk. Second, because of lax management they put themselves at risk of being sued by others who might be negatively impacted by their poor management. This includes customers, suppliers, and stockholders. Finally, security incidents resulting from lax security management can result in adverse public relations.

For these reasons, every organization should strive, at a minimum, to reach and sustain Level 2 or Level 3 management of their information security system.

⁶ The *Software Engineering Institute* is a federally-chartered R&D center, based at Carnegie Mellon University, whose mission is to further the practice of software engineering.

⁷ *Information Security Governance: Guidance for Boards of Directors and Executive Management*, IT Governance Institute, Information Systems, Audit and Control Foundation (ISACF), 2001.

Putting it all Together: Effectively Evolving of the Countermeasure System

An organization needs a “performance improvement methodology” if it is to effectively implement and evolve its system of countermeasures. The methodology must take into account the evolving nature of threats, vulnerabilities, and business realities. The methodology must support strategically-focused top-down approaches to countermeasure system implementation while also being flexible enough to handle tactical necessities. The methodology has to be powerful enough to support and extend the creativity of the organization. And the methodology has to be easy enough to implement that people will actually use it.

The *Spiral Model*^{SM 8} is a powerful easy-to-use methodology for evolving performance systems, including systems of countermeasures. It supports continual learning and the application of that learning to the information security needs of the organization. And it does so in real-time, at the moment of need, supporting what Fritz Dressler has called “evolution on the fly.”

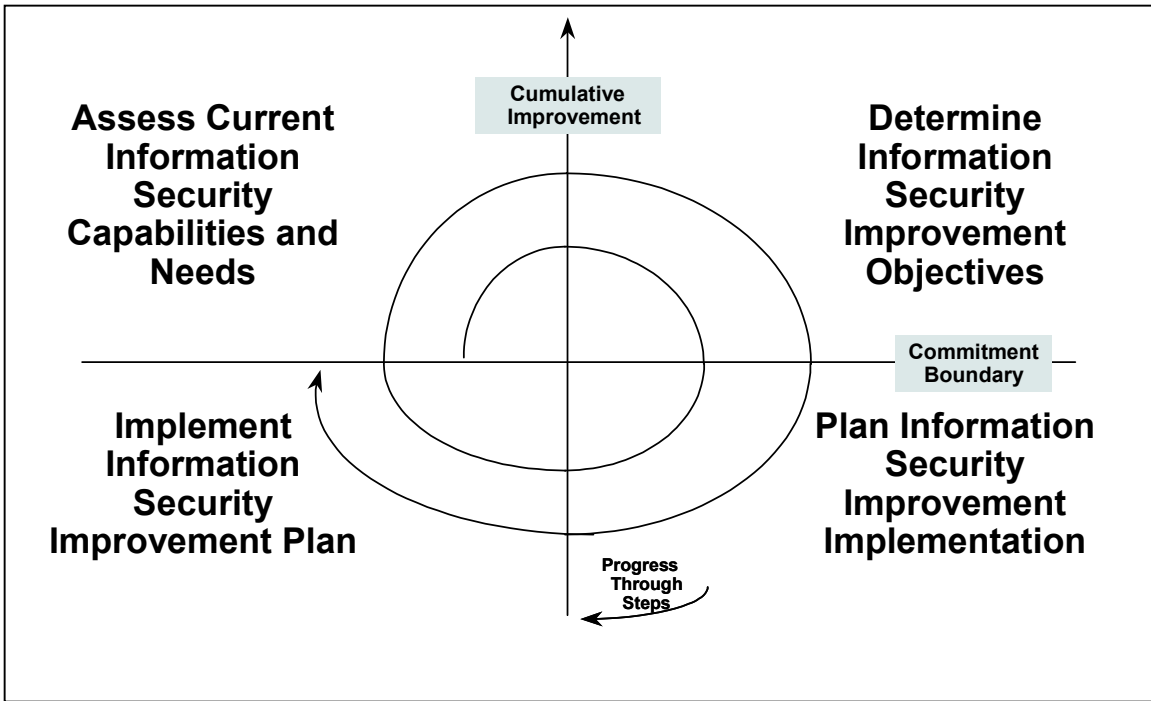
The *Spiral Model* has its origins in three earlier performance methodologies. One is the famous *Plan-Do-Check-Act* method taught by Deming. A second is the *OODA cycle*—*observe, orient, do, act*—that emerged in fighter pilot studies in the 1950s. The third is a systems development methodology I learned while a research scientist at TRW. Like the *Spiral Model*, all embrace the fundamental arrow of purposeful evolution: *Action, Feedback, and Synthesis*.

There are four basic steps to the *Spiral Model*:

- Assess the situation
- Decide what to do to improve the situation
- Plan the improvement project
- Implement the improvement plan

The first assessment can be undertaken in coordination with *Landscape Setting*. Subsequent assessments should assess both the organization’s countermeasure system and its effectiveness in using the *Spiral Model*. Of particular interest are (i) its effectiveness in planning information security improvements and (ii) gaps between planned and actual improvement.

⁸ *Spiral Model* is a proprietary methodology of Citadel Information Group, Inc.



Concluding Remarks

Effectively implementing information security countermeasures requires taking an evolutionary systems approach. The system of countermeasures must flow from organizational strategy, reflecting trade-offs between organizational performance needs and the need to protect critical information assets. Countermeasures need to be implemented in a methodical way designed to support an appropriate level of “information security management maturity.” Improving the overall quality of the system of countermeasures is enhanced by frequent feedback, both on the effectiveness of countermeasures and on the organization’s effectiveness in managing the evolution of its countermeasure system.



Citadel Information Group ... Securing the Critical Information Assets of Middle Market Businesses, Mid-Sized Government Agencies, and the Non-Profit Community

To schedule a free no-obligation *Information Security Executive Briefing* or for additional information, please contact:

Stan Stahl, Ph.D.
Kimberly Pease

323.876.1441
323.397.5752

sstahl@citadel-information.com
kpease@citadel-information.com