

**INFORMATION SECURITY
MANAGEMENT**

NOT A TECHNOLOGY PROBLEM

White Paper

September 2001

Onsett International Corporation

BUILDING COMPREHENSIVE INFORMATION SECURITY PROGRAMS

Introduction

The importance of information security and privacy programs is growing. The news is filled with stories of hackers penetrating companies' computers, denial of service attacks shutting down servers, and viruses wreaking havoc with corporate infrastructure systems. The roots of these problems are not new but they are broader and more public than in the past.

Mainframe data centers have been in operation for 40 years. For much of that time, management addressed security in direct and obvious ways: limited physical access, controlled environments, limited connectivity. As distributed systems and then the Internet expanded the reach of Information Technology they also expanded the sources of problems. Today, millions of computers are interconnected; the paths among them are too numerous to count, and anonymous users can reach around the world to exploit vulnerabilities.

For companies with substantial infrastructures the risks are many and varied. Establishing a perimeter of protection is necessary but not sufficient. External hackers continue to find and exploit vulnerabilities. Internal threats are substantial as well¹. The demand for vigilance increases with the complexity of the environment but deciding how to direct security and privacy efforts remains confusing. The dilemma is the need to create new connections to conduct business while maintaining sufficient security to protect information assets. A Comprehensive Information Security Program will improve the enterprise security posture if the information security organization engages all parts of the enterprise to manage business risk. This effort will be successful by leveraging a program framework that holistically analyzes each security element (operations, architecture, and governance).

What do we mean when we discuss Information Security?

Information security is the protection of information commensurate with its value and its associated risk of loss, unauthorized disclosure, or unauthorized use. This means making investments to prevent unauthorized activities and reduce risk. Typically the stated goal of an information security program is the reduction of technical risk of:

- Unauthorized disclosure
- Tampering
- Fraud
- Systems and IT infrastructure damage (viruses, worms)

In the past few years compelling business reasons have emerged for a comprehensive information security program. These include cost controls, regulatory requirements, and competitive position:

- Cost Efficiency
 - Economies of scale
 - Reusable security infrastructure components
 - Repeatable processes
 - Consistent architectures with which to integrate new services
- Regulatory compliance
 - GLBA, HIPAA, etc.
- Competitive advantage
 - Maintaining trusted relationships with customers and business partners
 - Confident and rapid integration of new channels, products and services, and technology

¹ FBI/CSI 2001 Computer Security Survey

At their core, information security programs are a mechanism for managing *business risk*—not just technical risk—in ways that enable the business to function and thrive. Alignment with business requirements is a key to implementing a program that makes sense.

Regulatory review is compelling but the need for security programs goes beyond industries where regulations require compliance. Every company needs to make sober choices to protect proprietary information in ways commensurate with its value. As illustrated Figure 1, information security must be viewed as a continuous method for mitigating risk. The goal is to reduce the risks to tolerable levels and make informed business decisions to accept the residual.

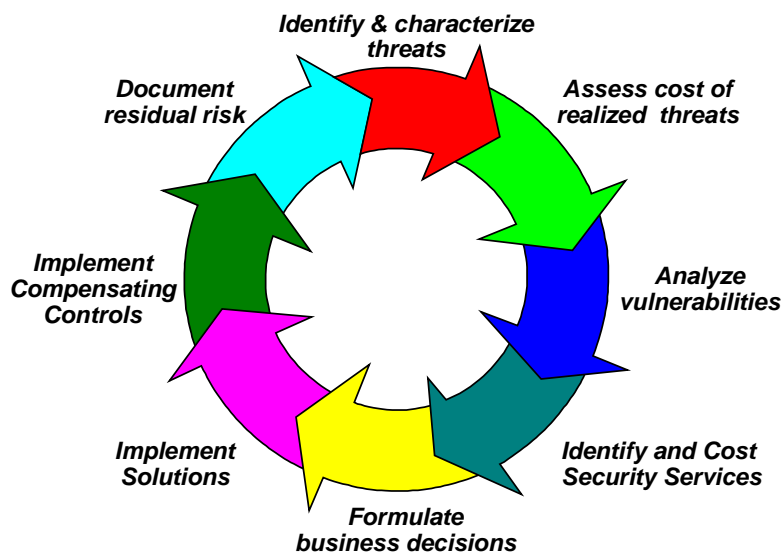


Figure 1. Information Security is the management of Business Risk

Why Information Security is not just technology?

Too often the first reflex is to wonder, “What tools should I buy?” But the trends running through security surveys and recent incidents clearly demonstrate that buying more security technology will not solve the problem. Prevention technology lags behind vulnerabilities. Simple, known vulnerabilities—as simple as unprotected modems—can be exploited in costly ways. Patches that protect systems against viruses and worms work only if they are applied in time. Organizations are confused over who does what.

The solution is to take an integrated approach to selecting and deploying tools, operational processes, and organizational roles.

Who should care about security?

Traditionally, and unfortunately, information security and privacy has been an after thought. Users value functionality over security. Business management does not want to miss a revenue growth opportunity because of technologist’s caution or a bureaucratic obstacle. The information security organization, if it existed, was left to influence improvements with limited support from the rest of the company.

The landscape changed during the 1990s. The value of the IT infrastructure as an important part of the revenue generating capability of the company became clear. At the same time, best practices emerged

wherein the role of the Chief Information Security Officer was established with reporting responsibilities high in the corporate hierarchy.

Regulations have recently placed the final accountability for securing corporate and customer information on the shoulders of the Board of Directors. The Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) require privacy and security programs in specific industries. Companies have distributed their Privacy Statements and are ensuring their corporate statements are backed with appropriate protection measures. Regulations (e.g. GLBA) and Standards (e.g. BS7799) contain lists of topics that should be addressed in a “Comprehensive Information Security Program.”

Everyone in the company needs to have a basic understanding of information security requirements. Specific responsibilities across the organization need to be clear. The information security organization has the implicit responsibility to raise and maintain the awareness of and establishing the responsibilities for:

- Executives
- IT professionals (Operations and Development)
- Information Security Professionals
- Employees
- Suppliers
- Partners.

The role of the information security organization varies from company to company. No model is perfect. No single model fits all companies. But all successful models demand that the organizations strike an informed balance between risk and business need. This in turn requires that the security organization, business users, and IT organizations have a direct mechanism to understand the risks that they face and the approaches to mitigate the risk.

What components define a comprehensive program?

Most information security problems arise from failure in processes or gaps in responsibilities. While the lengths and breadths of the challenges can be daunting, we have found that the following organizing framework can simplify the management of security across the enterprise.

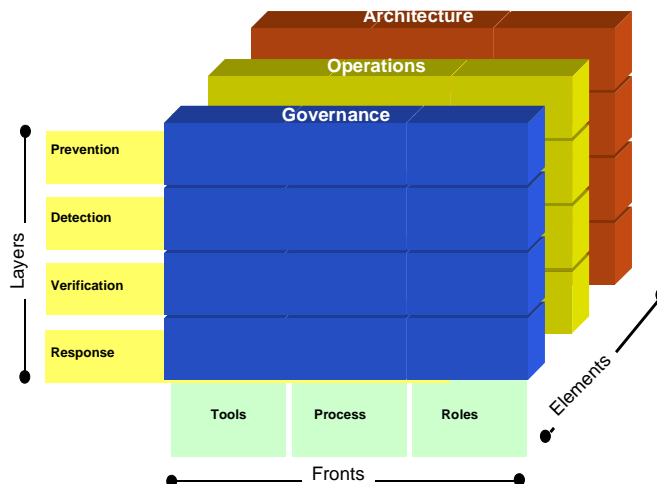


Figure 2. Dimensions of a Comprehensive Information Security and Privacy Program

As shown in Figure 2, a Comprehensive Information Security Program addresses requirements in three dimensions—Program Elements, Security Layers, and Operational Fronts. This organizing framework allows a company to determine the levels and priorities of the investments it needs to make.

Information Security Program Elements

Good information security programs need to include the following program elements. This does not mean that they need to address each element equally. The investment timing and priority depends on the needs and current state of the business.

Governance: Defining and overseeing the program:

- Security Policy, Standards and Guidelines
- Organizational roles and responsibilities
- Assessment of and security plans to control risk
- Metrics and processes to determine how well the company are adhering to information security policies, processes, procedures, and guidelines
- Personnel controls for who has access to sensitive systems and data
- Programs to increase the awareness of critical Information Security issues and responsibilities

Operations: Administering and enforcing:

- Information Security processes and access controls
- Controls for physical access to information systems and information assets
- Processes and procedures to minimize the likelihood of disruptions, recover from disasters, and respond to security incidents

Architecture: Designing and implementing:

- Development methodology for secure information systems
- Systems and controls that limit the risk of unauthorized access to business assets

Information Security Layers

Across the enterprise there should be layers of protection to ensure that the risks are managed effectively. Each security layer supports the next to minimize the probability of security problems and minimize the exposure the company faces when incidents do occur.

Prevention: Protecting information through effective use of technology, processes, and organizational responsibilities to limit the potential of a threat being realized.

Detection: Manual and automated mechanisms to identify and isolate security problems. This includes active and passive monitors and analytical procedures.

Verification: Manual and automated mechanisms to ensure that required security measures are in place. This can take forms including audit functions and monitoring tools.

Response: When prevention measures fail, companies need a rapid, pragmatic response capability. This requires planning for containment, triage, and direct response. Pre-planning for a set of probable incidents, and regular testing is key to rapid and effective response.

Information Security Fronts

Unfortunately, information security is not just a technology problem. There is no “silver bullet” to make a dramatic improvement in the security posture of a company. The posture depends on developing,

enforcing, and maintaining safe computing practices on the coordinated fronts of Tools, Processes, and Roles:

Tools: Protecting information through effective use of technology (e.g. firewalls and authentication tokens) that result in reusable solutions to business problems.

Processes: Establishing repeatable solutions or compensating controls for business risks, ensuring that they are measured regularly, and periodically aligning business and Information Security goals.

Roles: Creating the roles that ensure clear responsibilities and accountability in business units, Information Security Organization, outsource supplier and business partners. Eliminating gaps and reducing overlaps to ensure that requirements are met.

Where to invest?

The first steps are to determine the capabilities of the organization and determine the requirements of the business. Many companies waste money on ineffective information security measures. The funds invested must be kept in the perspective of the value to the organization.

Assessing the current posture requires taking a sharp look at current capabilities. This means asking:

- Am I doing the things I am supposed to do?
- How well am I doing them?
- Do we have the capabilities to do them well enough?
- How do I improve?

The result could be alarming or it could be reassuring. Figure 3 represents a current security posture for an organization. It is important to note that not every block needs to be complete. It depends on the requirements of the business.

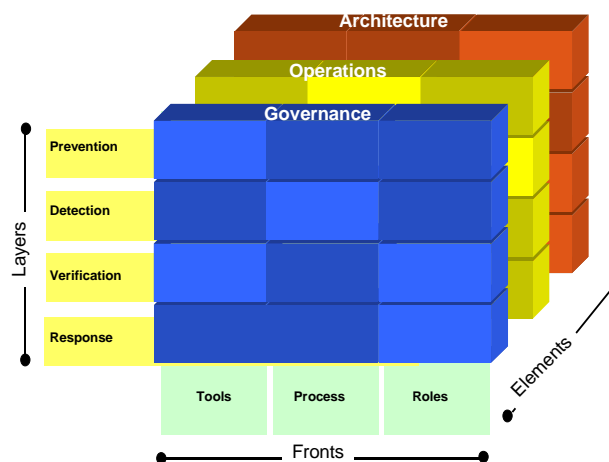


Figure 3. Determining what CISP Areas Need Improvement

Determining the importance of the components is critical. The approach to each type of threat needs to be aligned with the risks and the potential costs of it being realized. Addressing this requires building a

roadmap that makes sense in the context of your business. It also means avoiding the trap of searching for a perfect solution—especially on the tools front. As we said before, threats to the organization come in many forms; so the investment profile needs to be aligned in a way that shores up the blocks that meet your business objectives.

Establishing a roadmap is a determination of where and when to invest effort and money. The investment profile needs to account for the magnitude of a deficiency compared to the required posture, funding available in each projected period, and the ability of the organization to operationalize the results. The key is to make progress on what is important, rather than all areas at once.

How do we know we are getting better?

It is a maxim that information security is a journey not a destination. New technologies, new business requirements, and new threats keep changing the landscape. This demands that you close existing gaps quickly or you will fall further behind.

Progress requires establishing plans to address problem elements and executing the plans on schedule and on budget. It also requires regularly (or continuously) assessing the objective metrics of security posture. Stories of ten-year-old passwords are not exaggerations. Reductions in stale credentials, weak passwords, obsolete rule bases, and out-of-date signature files, are all measurable results of improvements.

As the program takes shape, use of a scorecard to measure continuous improvement will help the organization make and defend such statements as:

- We are reducing the vulnerabilities.
- Awareness is rising.
- We are keeping up with patches as they emerge.

The metrics selected for measurement cannot be just security technology-oriented; they must be aligned with business objectives. This alignment ensures that improvements in the security posture are linked to improvements in cost efficiency, regulatory compliance, and competitive position.

Conclusions

A Comprehensive Information Security Program is inherently complicated. An organizing framework that accounts for the posture of CISP Program Elements, Security Layers, and Operational Fronts simplifies the effort to improve the enterprise security posture.

To be effective, the information security organization must engage many other parts of the enterprise in managing business risk. It must ensure that the capabilities of the organization are appropriate for the business needs. Tools alone are insufficient to meet these needs. This means ensuring that the processes and roles within the companies, partners, and suppliers are sufficiently mature to meet requirements.

Infinite money does not buy infinite security. Making targeted strategic and tactical investments and tracking progress across the enterprise is critical. Regular assessment and measurement of progress against plans and improvements in security metrics is the only way to ensure that you are getting your money's worth. Instituting a periodic scorecard and continuous improvement processes ensures that you keep up.

Onsett International is an Information Technology Management consulting company based in Cambridge, Massachusetts. Onsett provides pragmatic solutions to enhance business performance through improved utilization of Information Technology (IT). Onsett focuses on the transformation of IT services in the areas of Service Management and Information Security for companies who continue to search for ways to improve the return on their IT investments. We work with our clients to define and align their IT service delivery organization to provide superior business value.

© 2001 Onsett International Corporation. All rights reserved.