Security Program Management

By: Harris Kern’s Enterprise Computing Institute

Introduction

As information technology continues to grow in scope and importance, the value of managing the security of mission-critical computer systems running an organization's most sensitive processes and functions cannot be overstated. With security being one of their highest priorities, executives are searching for effective techniques to deliver maximum security while simplifying security management. In this regard, it is essential to develop forward-looking strategies to build and manage effective security programs that address both technical and management issues, since you cannot achieve long-term security without dealing with both.

Strategic Assets

Your organization depends on information technology to access critical information and promote communications and coordination among groups inside and outside the organization. In other words, information technology is a strategic asset vital to your organization's viability. It's essential to build a secure information technology infrastructure and manage it with well-deployed processes and tools.

Effective Security Programs

A secure information technology infrastructure depends on an effective security programs that must be integrated, dynamic, and support high service levels. This means users have reliable and timely access to data and applications without having to deal with and understand obscure underlying security technologies and procedures.

For your organization to adapt and survive in a fast-paced international and competitive environment, it depends on a security program that is also adaptable. An effective security program is dynamic, flexible, and extensible, so it changes as your organization and its environment change. The security program can support current requirements as well as future enhancements. It can change as user requirements and technology change.

Since information technology is a strategic asset, it must be secure. A secure information technology infrastructure has the levels of availability, confidentiality and integrity that your organization requires to achieve its strategic objectives. This simply means that it is manageable and supports your mission-critical applications and other production systems.

Real Cost of Security

Security is more than a collection of security technologies - it's about managing business, technology and security-related decisions. Because this can be a complex and costly undertaking, you must design a security program with the processes and tools to manage the program.

Although your security architecture has many components – firewalls, scanners, intrusion detection systems, hardened operating systems, access control systems, and so on - the capital costs for the security hardware and software components are only a small portion of the total cost of ownership. More than 80% of the costs are related directly to the costs for security operations and management. Installing security hardware and software, configuring firewalls, detecting and responding to security incidents, analyzing new technologies, managing systems changes, performing backups, adding and modifying user profiles - all are time-consuming and costly activities.

Other high-priced items revolve around issues related to the availability, integrity and confidentiality of critical data. Depending on the nature of your business, low levels of data availability and integrity caused by downtime, unauthorized access, security administrator errors or disaster can cost your organization thousands to millions of dollars per hour in lost business activity.

So an underlying objective for planning, designing, implementing, and managing your security program is to minimize the cost of downtime. The only way to do this is to ensure that your security program supports high levels of availability and security, so every authorized user has uninterrupted and protected access to critical information and effective communications.

State of Security

The general state of information security in many organizations is dismal. Recent reports and events clearly demonstrate that security efforts are not keeping pace with growing threats. Critical operations and assets are highly vulnerable to attacks that have the potential to cause great damage. With the potential for harmful and disastrous effects increasing, security is a serious matter. As a result security is a leading concern among executives.

Surveys indicate that many organizations do not have formal risk management processes and security policies - the foundation for any effective security program. Also security awareness among staff is low and many organizations still lack security-related expertise.

While many organizations implement common security technologies, it is not clear they provide the protection these organizations are expecting, or really need. It is impossible for any organization to completely eliminate all security risks – that is, an organization can never be completely secure.

All security technologies have weaknesses and limitations. While many organizations may acknowledge this, they often fail to manage the corresponding risks. For example well-know penetration systems fail to explore many security technology issues, and completely disregard policies, processes and facilities, among others. Virus protection programs are always out-of-date. Firewalls are directed at outsiders, but do nothing to protect against malicious inside attacks. Most companies still rely on simple userid and password controls that are ineffective for sensitive systems. And, all security technologies are subject to human errors, failures and disasters.

Security can be costly. In addition to the cost of hardware, software and staff, security often disrupts normal operations. For many users, access to information and communications is blocked or delayed. Also many security technologies interfere with normal communications and transactions between organizations and their customers, suppliers and partners.

.

Without a clear understanding of security threats and their impact on the organization, the recognition of security technology limitations and weaknesses, and an awareness of the relationships between security and business operations, organizations cannot implement and manage cost-effective security programs.

Before an organization can begin to improve its state of security, it needs to consider a key security management issue - why is security in this dismal state and what are the limitations to moving forward. The answer is simple – complexity.

Complexity

Complexity is the greatest obstacle to security. Today more than ever, security professionals are forced to operate in a complex environment in which success is no longer determined by a single factor, such as getting the best firewall or having the right technical skills. Now, complexity is the norm with every aspect of the environment becoming more complex.

Why should we be concerned with complexity? There are many reasons, but the overriding one has to do with the cost of ownership. If we can't control dependencies, we can't set realistic levels of security, manage risks, allocate resources, and ultimately control costs. We can't ensure that the security program is aligned with the business objectives *and* control the total cost of ownership.

- *Dependencies and control* - Today, even small IT environments have many interrelated components. *Complexity* arises from the interdependencies among these components, which increase exponentially as you add hardware and software to your IT architectures (servers, networks, storage systems, and management systems); upgrade facilities; and expand the scope of security policies, processes and organizational structures.

  Management and control become critical issues as the IT environment becomes more complex. With millions of interdependencies, many are difficult to identify, some are difficult to understand, and others are outside our domain of control. Security management is a formidable undertaking if we can't understand and control the interdependencies.

- *Multiple technologies* - Security professionals are living in a world where they must deal with many different products from many different sources, deploying and managing them efficiently.

  Your options for implementing security technologies can be overwhelming: scanners, intrusion detection systems, firewalls, access controls, virus protection, VPNs, PKI systems, DBMS access mechanisms and others.

  Secure computing systems can run on a variety of platforms including UNIX, Linux, OS/400, Mac OS, Windows, OS/390, NetWare, Palm, Java-based devices and many other alternative platforms. These may be connected through Ethernet, Fast Ethernet, Gigabit Ethernet, ATM, ISDN, frame relay, xDSL and many others.

  Each set of security technologies presents unique deployment, management, and availability challenges.

- *Multiple locations* - With the growth of networks comes the challenge of securing computing resources that are physically distant from each other – many outside your domain of control

- *Rapid change* - Anybody who follows the information technology industry can attest to the fact that the rate of new product developments is growing exponentially.

We must address the second key security management issue - how do we overcome the complexity of managing security. The answer is a comprehensive structured approach.

Guidelines for Success

Security programs comprise intricate and complicated webs of technologies, processes, facilities, and people. It only makes sense that you should plan carefully and put the kinds of controls in place that will ensure its success from the outset. There are four main areas that need equal attention when implementing and managing security programs: unless you deal with complexity and change properly, invest in personnel, maintain a broad scope, and plan to manage security carefully, all will surely transform into an affliction that affects the health of your organization:

- *Manage complexity and change* - You can't avoid the problems and constraints that complexity and change bring. You can, however, facilitate and manage them through a structured, standardized security program.

- *Invest in personnel* - You need well-trained staff capable of implementing and managing your security program. Plan for adequate personnel training from the very beginning.

- *Maintain a broad scope* - Make sure that the plan and design of your security program has a broad scope. Don't limit the scope, or it will surely become an impediment to change, or worse, it can be costly to implement and integrate key elements of the security program after the fact.

- *Focus on the processes* - In addition to security technologies, put in place the processes and tools to manage your security program.

Multi-Dimensional Approach

Because the security program must be well planned from the start, we use a formal approach that brings discipline and structure to your security program. Our approach to assessing, building and managing security programs ensures that business processes, technologies, policies, security processes, access controls, tools and people are properly aligned. Every world-class security program arises from a comprehensive approach combining all of these.

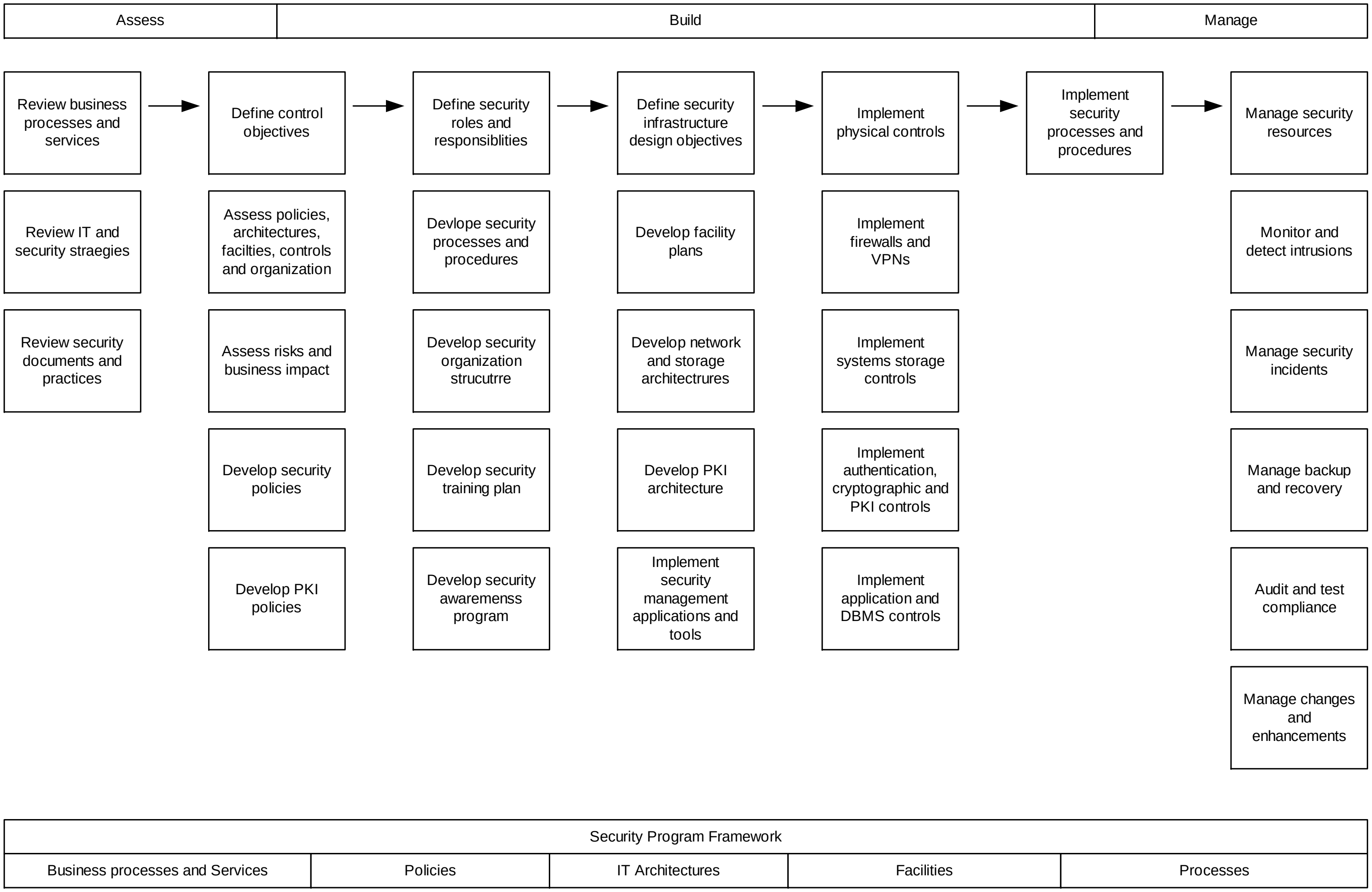
Assess, Build, Manage Model

Our model to assess, build and manage security programs is an ongoing cycle. We assess and define acceptable levels of risks for key processes and information, develop and implement security architectures, technologies and processes that are designed to mitigate those risks to acceptable levels, and manage the security technologies and processes with tools making ongoing adjustments, enhancement and improvements.

The model leverages and integrates three important elements:

- *Security standards* – To ensure security programs are based in best practices, the model leverages prominent industry security standards. Being flexible the model can

Security Assess, Build, Manage Model



Assess	Build	Manage

Review business processes and services	Define control objectives	Define security roles and responsiblities	Define security infrastructure design objectives	Implement physical controls	Implement security processes and procedures	Manage security resources
Review IT and security straegies	Assess policies, architectures, facilties, controls and organization	Devlope security processes and procedures	Develop facility plans	Implement firewalls and VPNs		Monitor and detect intrusions
Review security documents and practices	Assess risks and business impact	Develop security organization strucutrre	Develop network and storage architectrures	Implement systems storage controls		Manage security incidents
	Develop security policies	Develop security training plan	Develop PKI architecture	Implement authentication, cryptographic and PKI controls		Manage backup and recovery
	Develop PKI policies	Develop security awaremenss program	Implement security management applications and tools	Implement application and DBMS controls		Audit and test compliance
						Manage changes and enhancements

Security Program Framework				
Business processes and Services	Policies	IT Architectures	Facilities	Processes

accommodate different standards depending organizations' objectives and industry. These include, among others, CoBIT Controls, SysTrust Principles and Criteria, WebTrust Principles and Criteria, ISO 15504 Common Criteria, British Standards 7799/ ISO 17799, X.800 (formerly ISO 7498-2), and HIPAA.

- *Security framework* – The model is based on a security framework that ensures all aspects of the security program are assessed, built and managed in a comprehensive and logical manner. Comprising more than 50 operational areas, the framework ensures that all elements of security technologies, policies, processes, access controls, organizational structures and people are well planned, well deployed, integrated and systematically evaluated for improvement.

Security Program Framework

Our framework to assess, build and manage information security programs comprises more that 50 operational areas:

Business and Services
Business process definitions
Service definitions
Service levels
Growth projections
Critical assets
Threats and vulnerabilities
Control and design objectives

Policy Environment
Regulations
Management polices
Security policies

Technology Architectures
Service architecture
Logical architecture
Application architecture
Database architecture
Network architecture
Storage architecture
Continuous and resilient service strategies
Security architecture
Management systems architecture
Standards

Facilities
Facility infrastructure

Access Controls
Physical access controls
Application controls
DB controls
System software controls

Network controls
Firewall controls
PKI and cryptographic controls
Intrusion detection controls
VPN controls
Wireless controls
Authentication and authorization controls
Other controls

Processes
Service management
Production acceptance management
Change management
Capacity planning management
Performance management
Problem management
Security management[1]
User access management
Backup and recovery management
Disaster recovery management
Release/configuration management
Production operations management
Assessments and auditing[2]

[1] Includes intrusion detection and response

Organization and Staffing

- Organization structure
- Functional descriptions
- Key interfaces
- Job descriptions
- Awareness programs
- Training programs

[2] Includes risk assessments and frameworks for ongoing auditing and evaluations for improvement

- *Subject matter experts* - We engage and coordinate subject matter experts to address specific technical aspects of security.

Assessing Security Programs

We have conducted assessments for different types of organizations in both the private and public sectors. Taking a comprehensive view, we recognize that people, process and technology play prominent roles in all security programs. In this regard we assess and define acceptable levels of risk covering policies, technology architectures, facilities, access controls, processes, organization and personnel.

Our main methods typically involve reviewing security documents, conducting interviews, observing processes and running penetration tests. Key deliverables may include:

- Critical asset profiles covering business processes, information and others;
- Security policy assessments;
- Risk analysis with identifiable threats and vulnerabilities;
- Business impact analysis;
- Disaster recovery assessments;
- Descriptions of the exiting security program;
- Descriptions of enhancement and alternatives with cost/benefit analysis; and
- High-level work breakdown structures to implement enhancements.

Building Security Programs

In building security programs we develop strategies and detailed plans covering security policies, technologies, facilities, processes, access controls and organization. We also provide project management expertise to ensure the security program is implemented cost-effectively and in a timely manner.

Typical deliverables may include:

- Security polices;
- Security architectures covering applications architectures, database architectures, network architectures, server configurations, storage architectures, management systems architectures;
- Facility plans covering N+X designs;
- Access control architectures covering physical access controls, access control systems, firewall configurations, virtual private network configurations, access control lists, intrusion detection systems and PKI configurations;

- Security processes covering change management, production acceptance, intrusion detection, intrusion response, user access management, backup and recovery, and disaster recovery; and

- Organization structures, functional descriptions and training plans.

Managing Security Programs

We have been implementing and managing key elements of security programs for large organizations including international financial institutions and others. For example, we provide 24 by 7 monitoring, incident detection, incident response. We also establish and manage incident response teams. This involves developing detailed security polices and procedures for intrusion detection and response. We also develop standards and procedures to managed the intrusion detection systems and firewall configurations. Other responsibilities include the deployment and configuration of firewalls, intrusion detection systems and virtual private networks.

In managing security programs, key deliverables may include, among others:

- Configuration management;

- Intrusion detection;

- Intrusion response;

- Ongoing security assessments and audits;

- Security awareness education; and

- Disaster recovery testing.