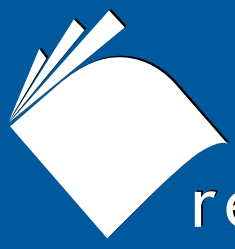

realtimepublishers.com™

The Definitive Guide™ To

Security Inside the Perimeter

Apani

Rebecca Herold

Copyright Statement

Chapter 8: The Recipe for Security Within the Perimeter

The past seven chapters have discussed the myriad reasons why organizations must address security within the perimeter as diligently, or even more so, than they approach security of the perimeter. This chapter will boil all this information and advice down into an information security recipe for effectively addressing security within the perimeter. With this in mind, this chapter reviews the key concepts within each chapter, then identifies the key actions organizations need to take—the information security recipe—to ensure the entire enterprise is secured within the perimeter.

New Threats Continue to Emerge for the Same Security Issues

Executives must be concerned about and address information security in today's business environment. Information security incidents not only cost companies significant time and money to resolve, they also significantly impact company brands, customer loyalty, and reputations and can have hard-hitting legal penalties, fines, and long-lasting judgments—with many consent orders requiring annual reviews and audits for 20 years.

The threats and challenges for today's business information processing environment are many:

- Network perimeters are now like sieves—The well-defined perimeter has disappeared. Mobile employees, wireless access, Web-based applications, remote workers, contractors, and business partners who have access to your network have put an end to the perimeter fortress. Attacks can come from anywhere at any time.
- Issues are nothing new, but the threats continue to grow—Businesses face numerous issues with regard to handling and protecting information. The number and type of threats created by computers and innovative technologies continues to grow.
- Urgency to address old problems with new solutions—Businesses must address the problems of technology evolving faster than the associated security solutions. Businesses must keep employees vigilant with their security practices for mobile computing devices. What used to work is no longer effective.
- Scalability—The internal network environment presents unique challenges compared with perimeter security. Internal security involves significantly greater scale of the environment, scope of the environment, numbers of users, speeds, and volume of traffic.
- Multi-national considerations—Businesses must comply with world-wide regulations to ensure the privacy of their customer information as well as the security of the intellectual property that resides on internal networks. These global requirements drive an increased need for internal security. There is also an increased awareness about malicious network attacks on internal networks that can be launched from anywhere in the world.
- Addressing compliance issues and requirements—Numerous laws and regulations mandate businesses maintain adequate information safeguards and controls to ensure that only authorized individuals are able to access personal information, and to ensure the continued availability and integrity of the information.

Gumball Security No Longer Works

The long-used gumball approach to securing networks by making the perimeter like a hard outer impenetrable shell and leaving the inside of the network soft with less vigorous security in place is no longer effective or acceptable.

Addressing Security Within the Perimeter

The overall value of data inside the perimeter has skyrocketed, which has lead to a new class of cyber criminals who are organized, well funded, and very focused on attacking organizational data. At the same time, the perimeter is becoming more porous, and attackers have new techniques for bypassing perimeter security barriers.

The attackers are not only coming from the outside—the increased value of data elements also represent a significant temptation for internal people, and these internal threats in many ways are more dangerous than external threats because the internal threats are difficult to detect and prevent.

Network perimeter security can be defeated in many ways—for example, by tricking inside users and systems to execute code containing worms, which then spread to other systems behind the firewall, and by tricking users who have JavaScript and ActiveX enabled in their Web browsers to execute malicious code hidden in external Web sites.

Identifying Internal Security Requirements

Businesses must identify security requirements in the context of how those requirements impact business with regard to existing risks, threats, vulnerabilities, and legal and contractual requirements. Alternative paths into organizations, along with application-layer attacks, are increasing the threats that highlight the need to complement perimeter security with a comprehensive and pervasive range of internal security activities and tools.

At a high level, there are three main ways to identify security requirements inside the perimeter:

- Assess risks to the organization, taking into account the organization's overall business strategy and objectives. A risk assessment will identify threats to assets and network components and evaluate the vulnerability and likelihood of occurrence.
- Identify legal, statutory, regulatory, and contractual requirements with which your organization, trading partners, contractors, and service providers must comply.
- Take into consideration the particular set of principles, objectives, and business requirements for information processing that your organization has developed, formally or otherwise, to support its operations.

A Wide Range of Factors Are Working Against Securing Just the Perimeter

Tribal thinking must change. Businesses cannot blindly trust that everyone with access to their internal network knows the right things to do or will not do bad things on purpose. The numbers of people with access to the typical business network goes well beyond employees. And employees are often motivated to take advantage of operational and systems weaknesses to inappropriately obtain information or wreak havoc on network and systems resources availability.

Trust Where Trust Makes Sense

Not only are security measures necessary to help protect against the malicious activities of those employees who cannot be trusted, such security measures are also necessary to help protect against well-meaning employees' mistakes and lack of knowledge that could lead to business-closing incidents.

Preventing Crime by Insiders Is Difficult

It is difficult for companies to guard against crimes in which internal staff is involved. This reality makes it even more important to implement internal security measures.

New Technologies Make Securing Networks Increasingly Difficult

New technologies make it very easy to link networks and information. Authorized network users who do not realize the threats they present use new technologies widely inside the network, often without the knowledge of management. Inexpensive technologies are easily accessed by large numbers of people, employees, and outsiders alike. More employees work away from the office and on their home computers. Putting security responsibilities and decisions into the hands, and control of, employees makes businesses more vulnerable to unauthorized network intrusion and abuse. Recent studies demonstrate the devastation insiders can have on network and information resources.

The Perimeter is Porous

Perimeter-based security fails because there is no longer a clearly defined perimeter. An explosion in outsourcing, mobile computing, wireless networking, business partner connections, and Web-based applications has created a spider web configuration of connections to virtually anyone, from anywhere, with any device. Significantly large numbers of individuals who are not employees have access to business networks and information. A "trusted" internal network environment is now likely connected directly to the Internet through a home or partner link or through an unapproved wireless connection.

Mobile and wireless computing increases threats to business because:

- Business use of these technologies is increasing. The top-tier executives are among those most likely to make extensive business use of mobile computing devices; they are also the personnel with the most critical and confidential business information.
- Mobile devices store increasingly large amounts of data. Handheld computing devices are now capable of storing gigabytes of information. If a mobile computing device or memory stick falls into the wrong hands, it is likely to expose huge amounts of business information, potentially including customer information, business email, corporate plans and strategies, and so on.

Legal and Regulatory Compliance

Regulations and laws governing the implementation of information security safeguards are becoming more common. Virtually all businesses are impacted by legislation with which they must comply. Penalties and fines for non-compliance with these requirements can have a huge impact upon an organization.

Inappropriate Technology for the Purposes Being Addressed

Organizations have often tried to use inappropriate technologies to address internal network security challenges, often spending inordinately too much time and money trying to create in-house solutions or succumbing to false promises of vendors selling them software and hardware that really doesn't address their business environment and needs. Security solutions must be appropriate to the risks, threats, and vulnerabilities being addressed to be effective.

Increasing Data Value Increases Threats

Data is extremely valuable to business. This value is another compelling reason to protect data in all places.

Organizations Must Implement Multi-Dimensional Enterprise-Wide Security

Multi-dimensional security protects information assets and associated resources within all areas of an enterprise and in compliance with all regulatory, policy, and contractual requirements. It places protection at not only the perimeter but also wherever information is stored, processed, or transmitted.

Multi-dimensional security involves more than just technology solutions; it also utilizes operational, administrative, and human forms of protection to help reduce the risks to information wherever information can be found.

Multiple Protection Strategies Are Needed

There is no such thing as a single solution that, in and of itself, will secure all enterprise information assets and systems in compliance with all contractual and legal requirements. Multiple protection strategies must be used to most effectively reduce and manage the risks that exist within today's highly decentralized and widely connected systems.

Risks Today Are Different Than Those of Yesterday

Businesses used to address risks within the insurance coverage portfolio for the organization. Information security risk was not something that business leaders considered when risk management was discussed. Smart business leaders now know information is a cornerstone of successful business, and needs to be effectively protected to reduce the risks to the confidentiality, integrity, and availability of the information.

Risk Assessment and Analysis Methodologies

There are a wide range of risk analysis and assessment methodologies and technologies. Organizations must choose what is best for them based upon their business environment and the goals for their assessment.

You Cannot Predict the Future… But You Must Still Identify Your Risks

Organizations cannot realistically calculate with any amount of accuracy the threats that will impact their organization or the dollars needed to invest in information security. However, performing risk assessment/analysis is still necessary for businesses to be able to understand information risks and to determine which controls and tools to use to prevent the risks. The most realistic way to do so is through the use of qualitative risk analysis based upon regulatory requirements and the potential impact from non-compliance fines and penalties. The assessment/analysis should then communicate what the financial impact experiences for each risk have been in other companies.

Risk Analysis and Assessment Must Be Part of a Multi-Dimensional Security Strategy

Business leaders must recognize two facts:

- Each information system and process has its own risk environment
- Each information system and process has its own unique inputs, outputs, level of activity, and associated costs

Because of these differences, each information system and process has unique security requirements that are determined by the associated risk environments.

Security Policies, Procedures, and Standards

Information security policies, procedures, and standards are all important and organizations must formally document and implement them to have an effective information security program as well as to comply with multiple data protection laws and regulations. Each type of document serves a different purpose.

What Does an Information Security Policy Do?

An information security policy establishes the framework within which the business rules and regulations for handling information and reducing risk are described. Effective policies are created to help bring the organization into compliance with applicable laws and regulations as well as to address how to secure the business information processing environments within the organization.

What Does an Information Security Procedure Do?

Information security procedures describe how to implement the policies. Procedures document the step-by-step detailed actions necessary to successfully complete a task that supports the policies. Procedures provide personnel with the information necessary to complete a task and provide assurance to management that the tasks are being completed in a consistent approved manner. Procedures improve efficiencies in employee workflow and assist in the prevention of misuse and fraud.

What Does an Information Security Standard Do?

An information security standard is a detailed specification for hardware, software, and human actions to support the information security policies. Standards can detail the requirements for a wide range of issues, from the software and hardware that must be used to the remote access protocols that must be implemented to describing who is responsible for making information security approvals. Standards provide a documented way of ensuring that programs and systems will work together. By establishing standards, the enterprise limits the possibility of rogue application, systems, platforms, hardware, or software; in addition, there is less time spent in supporting non-standard activities or products. In short, standards define cost-savings processes that support the efficient running of the enterprise.

Regulatory Requirements for Information Security Documents

Many laws and regulations require organizations to formally document data protection requirements in policies and procedures. Additionally, these documents demonstrate that a standard of due care has been established within the enterprise.

Education

Organizations must supply personnel with the information they need to appropriately safeguard data while performing their job responsibilities. If personnel do not know or understand how to maintain the confidentiality of information, or how to secure it appropriately, organizations risk having information mishandled, inappropriately used, and obtained by unauthorized persons, as well as being in noncompliance of a growing number of laws and regulations that require certain types of information security and privacy awareness and training activities. Issues under the United States Federal Sentencing Guidelines that impact the severity of the judgments include consideration of the types of training and awareness organizations provide to their personnel.

Audit and Validation

Security audits and compliance validation reviews provide an in-depth examination of an organization's security infrastructure, policies, people, and procedures. When performed effectively and successfully, they will identify areas of weakness within the infrastructure. The auditor or reviewer can then provide recommendations for appropriate actions to address the weaknesses and reduce the accompanying risks.

Simplifying Complexity

The enterprise information security strategy must simplify the complexity resulting from highly diverse, dispersed, and multi-dimensional environments. Organizations must simplify the complexity of information security management by taking the large number of technology, human, and compliance issues and making them understandable to the business, while at the same time implementing solutions to integrate them throughout all business processes so that information security is built into all products and services from the beginning of a business idea right through until the resulting service or product is no longer offered.

Information security complexities can be simplified using a common framework of information security disciplines and by obtaining the support and cooperation of leaders throughout the organization rather than focusing on each individual issue one at a time. The first step in simplifying information security is by appointing an enterprise-wide information security position to oversee and coordinate information security activities and decisions for the entire enterprise. This position will not only be the first step in simplifying complexity but also lead to consistency in addressing information security issues throughout the enterprise.

Use Security Zones

Business leaders must not only be aware of, but also strive to be in compliance with, the multitude of regulations that are applicable to their companies. This complexity can be made more manageable and more clearly provide demonstration of due diligence by tackling the requirements in zoned chunks across the enterprise.

Establish Network Security Zones

The network should provide a solid first layer of defense against outside attacks, complementing operating system (OS)- and application-level security. Separating the network into security zones allows security managers to consolidate resources in a cost-effective manner and control user access to each application and related information. The network then creates a secure environment not only at the perimeter but also in security zones throughout the enterprise.

Enterprise Security Zone Management

Dependence on the network, along with functional enhancements to the business systems, increases the importance of security and dependable accessibility to information. Implementing network security zones helps organizations achieve their goals of scalability, availability, security, manageability, performance, supportability, and geographic distribution, while realizing savings at many levels throughout the enterprise. Enterprise security zones must be centrally managed to be most effective and prevent gaps. Enterprise network security zoning provides many benefits to the enterprise:

- Streamlines business processes
- Mitigates risk within the network perimeter
- Saves organizations time, money, and human resources
- Reduces operational risk

By implementing security zones, an organization will shift reliance from perimeter security to an asset-centric business-supported model that protects the right assets from the right threats with the right measures. Security zones will allow assets of greater organizational criticality and value to be held to higher security standards and protected by additional layers of defense. If possible, they should be compartmentalized, or zoned, into their own networks and segments. By doing so, the perimeter will be considered an asset like everything else.

Use Physical Security Zones Along With Network Zones

Physical and environmental controls are also an important component to protecting enterprise information and systems. Effective physical and environmental controls are necessary to prevent a complete network failure. Consider the following steps when planning security zones.

Identify Critical Enterprise Information and Network Assets

Create a list of critical enterprise information and network assets, then document the ones essential to the reliable and necessary operation of the enterprise. Follow a documented, risk-based process for your identification methodology. Establish risk-based criteria that correspond with the unique environment, requirements, services, and products of an organization.

Create an Asset Inventory

Create an inventory and corresponding classification of critical enterprise information and network assets if this has not already been done to facilitate business continuity processes and comply with numerous regulatory requirements for identifying and protecting certain types of information.

Identify Security Zones by Grouping Assets

Segment the enterprise data processing centers into areas that are logically separated from one another based upon their associated critical assets and revenue areas to contain an attack and keep the impact as minimal as possible to the overall business. Zones can support individual applications or application tiers, groups of servers, database servers, Web servers, e-commerce areas, and storage resources.

Create a Road Map to Implement Security Zones

After identifying the security zones, create a plan, or road map, to ensure the efficient and effective implementation of the security zones into the enterprise, based upon criticality, over a reasonable period of time. Integrate the security zones into the existing enterprise network. Define the access and security requirements for every service so that the network can be divided into security zones with clearly identified security and access levels.

Work with each security zone separately. It is likely each zone will have a different security model necessary to address the identified risks. Security controls should be implemented so that security breaches and incidents can be confined to a particular zone or part of the network as much as possible.

Implement Zone-Specific Protections

Each identified security zone needs to have controls and protections implemented based upon the risks specific to that zone. It is likely all zones will have some similar protections, such as virus control systems. However, each zone will likely need unique controls that no other zones may have, such as a zone with a remote access server (RAS), or a zone that houses a credit card processing system. There will probably be zones that need to have internal firewalls to protect them, and other zones that will not need such firewalls.

Integrate Security Zones Within a Layered Security Strategy

Do not stop at zoning alone, though. Zoning is just one of the key components of an organizational security strategy. To successfully defend against the multiple and varied types of threats and address the numerous and diverse vulnerabilities, organizations need to create and implement a layered security strategy.

Perimeters, infrastructure devices, OSs, applications, and data must be assessed and appropriately fortified to mitigate the risks that threaten your organization. Use multiple complementary approaches for security enforcement and defense at various points in the network, which will remove single points of security failure.

Implement Layered Security Throughout the Enterprise

Using just one tool or performing just one activity will not accomplish an effective information security program. An effective information security program consists of many layers.

Using many different layers of many different types of security, based upon business goals, services, and risk evaluation, will most effectively protect the enterprise from the attacks and threats that exist from all directions and in all ways, both malicious and accidental, to information resources. This layered defense is often compared to the layers of an onion, creating many different types of security layers that must be penetrated before the target at the core of the onion (the critical information infrastructure) can be reached.

Security layering establishes a more reliable security posture; if a failure or breach occurs in one layer, it will not compromise the other concentric layers.

Security Program Management Layer

The information security program is an information security layer that permeates multiple levels of the enterprise and benefits the organization in many ways. Every level enhances the entire information security program by making use of various types of expertise, authority, and resources. Generally, as a result of this layered security program management:

- Executives will better understand the organization as a whole and have better knowledge to most appropriately and effectively use their authority to protect the enterprise information assets.
- Managers within each of the business and operational units will be more familiar and cognizant of the specific security requirements, including technical and procedural requirements, and the associated challenges of the systems and information users.

Centralized Security Management

Establishing a centralized security management area with ultimate enterprise-wide security oversight will result in distinct benefits to organizations.

- It will increase the efficiency of security throughout the organization, allowing security to be implemented with an economy of scale that is more resource efficient than having security assigned independently to different groups.
- It will allow the organization to enforce security requirements centrally as well as to centralize monitoring, evaluations, and updates to the enterprise security program.

Distributed Information Security Management

The enterprise information security management program will address the entire range of information security issues for the enterprise. Distributed information security management programs will help to ensure appropriate and cost-effective security is addressed within each of the organizational business and operations areas.

Application Security Layer

Information security controls built-in to business process applications are an important enterprise information security layer. Examples of how to build information security into applications include programming checks and controls for segregation of duties and for data:

- Completeness
- Accuracy
- Validity
- Authorization
- Encryption

Node-Level Security

Another important information security layer is node-level security. Leading practices to accomplish node-level security implementation use a combination of identification, authentication, and logical access controls. Identity management focuses on integrating these activities into the business environment.

Identification and Authentication

Identification and authentication are necessary to help prevent unauthorized user and process nodes from being able to access networks, systems, applications, and information. Access control mechanisms are used to differentiate between these users and processes to allow only those authorized to perform the activity they are requesting.

Identification

Identification is the information the end-node user or process provides to uniquely distinguish their activities and capabilities. The most common form of identification is the user ID. However, there is also a need to identify devices, especially inside the perimeter where there can be a large number of headless servers. Certificates are also frequently used to provide identification for users and devices.

Authentication

Authentication is used in conjunction with identification to validate the entity using the identifier is truly the associated user or process it claims to be. There are three ways in which identification can be authenticated:

- Using something the user knows, such as a password or PIN
- Using something the user possesses, such as a token or smart card
- Using something with biometric characteristics, such as voice patterns or fingerprints

Network devices also need to have identity validated. Certificates are the primary method used to authenticate the identity of network devices.

Logical Access Control

Logical access controls are system-controlled ways for a node (such as an end user or process) to be explicitly enabled or restricted to do something with a computer resource, such as view, update, or delete data.

Logical access controls not only allow the user or process to have access to a specific network or system resource but also provide the specific type of access to the resource.

Organizations should implement logical access controls based upon the information security policies that cover the corresponding systems, networks, and applications. Logical access controls should be based upon business processes and goals, with information security, operational requirements, and ease of use incorporated into the control decisions.

Network Security Layer

Security within the network layer must be incorporated into, and addressed, within many different components and using many different techniques.

Transmission Control Protocol/Internet Protocol (TCP/IP) is an important part of the network security layer, but security within the network information security layer goes beyond TCP/IP. The open nature of TCP/IP complicates security implementation and makes it more challenging.

Networks can span many organizational and business partner boundaries. Organizations must understand and take into account the risks associated within the data flow as well as ensure that legal and contractual issues exist in harmony with the business services and practices. Additional security must be applied within the network to protect sensitive information that passes through public and business partner networks and zones that are not trusted.

Network Security Controls

Networks must be effectively managed and controlled using multiple tools and techniques to protect the network and associated components from a multitude of threats as well as to provide security for the systems and applications that depend upon the network for business processing. There is a wide range of security controls within the network layer that business leaders must consider and appropriately utilize, such as:

- Separation of duties—Separate operational network responsibilities from the other computer authorization responsibilities. No single person should be able to access, modify, or use network assets without the separate authorization or detection from another distinct position or area. Network change actions must be separated from the authorization of the actions. When designing network controls, this separation of duties must be considered.
- Remote network access—Clearly document and communicate the responsibilities and procedures for managing remote systems and how they connect to the network.
- Data transmission protection—Establish controls to protect and safeguard the confidentiality, availability, and integrity of data that is sent over public, shared, and wireless systems. The endpoint systems and applications must be protected from the threats these open networks present.

Encryption is one example of an effective tool that can be use to protect data transmissions.

- Logging and monitoring—Determine the appropriate logging and monitoring necessary to record relevant security and network activities to enable successful security incident investigations in addition to providing other necessary evidence for business processing. Logging and monitoring is also mandated and restricted by laws, regulations, and contractual requirements and aids troubleshooting. Audit trails created from logging and monitoring are becoming more and more important, not only for regulatory compliance but also for being able to correlate multiple network activities throughout all security layers, and for computer forensics activities following network security incidents.
- Management coordination—Network security activities must be carefully coordinated with network operational management activities to ensure security is applied consistently throughout the network and information-processing infrastructure. Without effective communication and coordination, there could easily be conflicting activities taking place or the failure to accomplish necessary tasks because one area thinks another area is performing specific security activities. For example, without coordination, a system may never get backed up because two groups assume that the other is performing the backup.

Securing Network Services

Identify, and include within networks services agreements as appropriate, network security features, service levels, and management requirements for all network services. This task should be done with not only outsourced services but also the services provided in-house.

Physical Security

The physical information security layer is a very important component of information security, though it is often overlooked by information security practitioners. This aspect of information security is commonly left solely to the facilities security personnel.

> Physical security controls are necessary for preventing unauthorized physical access, damage, and interference to information assets and resources.

Organizations must consider the physical security risks, threats, and vulnerabilities and address them within the information security program. The information security area must work in partnership with physical security departments, end users, business partners, and other identified areas to ensure adequate physical security is implemented to protect mission-critical and sensitive information processing facilities.

Information processing facilities and systems should be located within secure areas and protected by defined security perimeters:

- Appropriate security barriers and entry controls should be applied.
- Data and processing centers need to be physically protected from unauthorized access, damage, and interference.
- Mobile information systems must be appropriately physically secured using a variety of methods.

> All information security physical protection methods need to correspond with the identified risks, threats, and vulnerabilities as well as the corresponding potential business impact.

Use the following physical security controls checklist to help determine the types of controls to be considered and implemented as appropriate to the organization's industry, size, geographic locations, and regulatory and contractual requirements:

- Site selection and physical security
- Public access, delivery, and loading areas
- Physical entry and access controls
- Security for offices, rooms, and facilities
- Environmental security
- Computer processing equipment security

> Organizations cannot depend upon facilities security alone to adequately protect computer-processing equipment; too many vital computer devices are mobile. Appropriate controls must be implemented for mobile computing devices and storage media to help prevent loss, damage, theft, or the compromise of assets and interruption to the organization's activities.

Supporting Utilities

Organizations depend upon power to keep information processing and computing facilities going. Protect processing equipment from power failures and other disruptions caused by failures of supporting utilities

Equipment Maintenance

Information processing equipment must be properly maintained to ensure the continued confidentiality, availability, and integrity of the information and systems processed on it.

Securely Decommission Equipment

Check all types of processing equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal, re-use, sale, or donation outside the organization.

Taking Computing Equipment Off the Premises

Do not allow equipment, information, or software to be taken off-site without prior authorization. Maintain documentation of the employees, contractors, and third-party users with authority to permit off-site removal of assets.

Human Resources

The most vulnerable of the information security layers are the human resources that organizations depend upon to follow information security policies and procedures. Individuals must know and understand how to appropriately handle and safeguard the information and associated computing resources that they use while performing their job responsibilities.

Organizations must invest time and resources to help ensure personnel do the right things by:

- Hiring qualified and appropriate individuals
- Providing effective training and awareness
- Motivating individuals through clear career paths and making security part of job responsibilities that are used for performance appraisals
- Establishing a defined compliance review process
- Mitigating risk of overdependence on key resources by using more than one person for a role in addition to cross training and ensuring proper separation of duties

Monitoring and Evaluation

The monitoring and evaluation layer of information security is one that is often not adequately addressed. Organizations must establish methods for monitoring and evaluation to maintain operational assurance and information security.

There are various methods for monitoring and evaluation, including:

- Performing scheduled audits
- Implementing ongoing monitoring of key applications, systems, and network components
- Performing evaluation activities

Disaster Preparedness

Events of the past decade demonstrate the importance and criticality of security components such as business continuity plans and disaster recovery activities. Organizations must have business continuity and disaster recovery plans in place not only to support the business goals for continued operations as much as possible under adverse circumstances but also to meet regulatory requirements.

Incident Response

An information security incident can result from a number of events that can range from a computer virus, other malicious code, a system intruder, and denial of network services to a lost laptop computer or lost backup tapes.

The definition of an information security incident is what an organization determines it means to its own particular environment.

Incident response is sometimes included as a part of contingency planning because of the need to quickly and efficiently respond to business disruptions and get back to normal processing as soon as possible. However, there are specialized activities within incident response that are compelling reasons to make this a separate information security layer within organizations.

Implement Business Appropriate Tools Within the Zones

Organizations must manage information security in multiple ways throughout the enterprise and as appropriate within each of the identified security zones. Network security management must effectively manage access to information assets and establish rules that network users must follow, limit access to network information resources to only those that have a business need for the access, and create notifications whenever incidents and inappropriate actions occur.

Powerful security safeguard tools must be implemented within established security zones to make the zones effective. When determining the security tools to implement, keep in mind that most reported information security incidents stem from three business weaknesses:

- Poorly implemented security measures revolving around improper access controls
- Lack of encryption
- Trusted insiders purposefully or accidentally accessing, using, or damaging information resources

Access Control

Problems will quickly emerge if proper access controls are not implemented throughout the enterprise and appropriate to each of the zones within which the controls are applied.

Authorized users within the zones will download and install mobile code from the Internet onto the organization's computers, carry in problems on their mobile computing devices, or introduce problems from their remote locations.

Workstations and endpoints within the network perimeter must now be viewed as hostile territory and potential threats. Desktop access controls must be managed centrally, including such controls as desktop firewalls, malicious software prevention tools, security policies for the zones within which they reside, and user authentication and authorization. Information and network asset protection success relies on the measures implemented close to the IT resource, within multi-tiered applications, and on active security management.

There Are No Longer Homogenous Environments

Implementing effective access controls is no longer the comparatively easy task it used to be when all information resided on one mainframe with only dumb-terminals sitting on the end users' desktops. The network environment in most, if not all, enterprise networks is now a mix of systems owners scattered throughout the enterprise in various departments and locations, assortments of OSs, and applications servers of every type imaginable. The complexity of networks is growing exponentially while the implementation and availability of security solutions seems to grow fractionally.

The types of resources to manage and secure now are many. A couple of challenging ones include:

- Headless servers—Implementing headless servers throughout the enterprise should be done consistently, following documented procedures and guidelines. Centralized oversight and administration of the servers will ensure the servers within each of the security zones are protecting sensitive data consistently from one zone to the next.
- Web-based servers—The number of Web-based servers organizations deploy also continues to grow exponentially as organizations depend more upon Internet presence and online sales to boost revenues.

Incorporating Access Controls into the Development Life Cycle

To successfully incorporate access controls into the systems development life cycle (SDLC), the organization's required security parameters must be clearly documented and communicated to all systems and applications developers in terms applicable to the development processes. Security requirements should be incorporated into the formal SDLC process in the same way that the business requirements and end-user requirements are defined.

Variety of Application Types

Today's enterprises have many more types of applications to manage than ever before, and usually the applications are completely different from one business unit to another. Managing access controls consistently throughout the enterprise in this type of situation is quite challenging and is often the impetus to many stressful workdays for the typical information security leader.

The Need for Encryption

The increasingly porous network perimeter combined with the growing number of ways in which data can be shared with all locations throughout the world has generated a growing need to protect information by using encryption. This protection should include encrypting not only the actual data but also, and perhaps more important, the authentication credentials (user IDs and passwords) for the applications that access the data.

Legal Requirements for Encryption

The use of encryption is often listed as an option organizations must consider within the wide number of data protection laws and regulations throughout the world. Encryption is a consideration within the many United States state-level breach notification laws. For example, notification activities do not need to occur if the data breached was encrypted.

Need for Encryption Transparency

Data is currently more commonly encrypted for remote access transmission than for storage. One common reason is that data-in-motion encryption is usually seamless to the application and requires minimal effort to deploy and little action from the end user. Another reason is that companies have historically been more concerned about hackers getting the information as it passes through the Internet than with someone getting to the data in storage. However, as many recent data breaches demonstrate, protecting data at rest is just as, if not more, important.

Encryption must be as transparent to the end user as possible in order for it to be successfully, consistently, and effectively used throughout the enterprise.

Encrypting Data in Motion

Securing data that goes outside the network perimeter presents challenges. VPNs have been the most common way of protecting information that must pass through a public network (such as the Internet) through the use of multiple security controls including encryption.

Insider attacks are increasing at alarming rates. Network intruders realize that they can gain access to internal corporate information resources because internal networks are more vulnerable and typically do not use encryption to protect data in transit that does not go outside of the network. As the number and severity of internal network attacks increases, organizations must recognize that using encryption for data in motion within the network is an essential and practical tactic to prevent theft of intellectual property and personally identifiable information.

Encrypting Data at Rest

Encrypting data at rest is another essential and practical tactic for protecting information within the network perimeter. A successful information security strategy will identify not only the types of encryption methods to use for data at rest but also the types of data that need to be encrypted.

> ☞ When encrypting databases, remember database lookups are designed to be very efficient. Unlike typical file systems, databases are expected to look through millions of rows, searching for specific items in seconds. These speed features present challenges for encrypting databases. It is not feasible for a database to decrypt each data element it must search. It is critical to consider how applications will use the database while planning to deploy encryption.

Encrypt at the Network Layer

Implement encryption at the network layer so that it is transparent to both users and applications and requires no modification to existing software applications, such as CRM, ERP, and inventory tracking systems.

> ✎ The success of VPNs to encrypt data in motion for remote access demonstrates that implementing encryption within the network layer allows for phased deployments within targeted security zones to add immediate benefit to enterprises.

Implementing network-layer encryption solutions within identified security zones with careful planning and the right tools can even eliminate the challenging deployment and management of VLANs.

Centrally Managing Encryption Solutions Is Crucial

A well-designed encryption system will operate separately; generating, storing, and protecting keys with very little user intervention. Mistakes or weakness in key management can quickly lead to system compromise. Key management is a critical area to focus upon when purchasing or building an encryption solution because mistakes and weaknesses within a key management system can quickly allow for system compromise.

Monitoring

An important tool for network security management is monitoring:

- Monitoring compliance
- Monitoring access attempts
- Monitoring for malicious code
- Monitoring for security incidents and breaches
- Monitoring for any activity that can have negative impact on the business

Personnel Monitoring

Most states in the United States have laws that address employee privacy rights in one way or another. In many European jurisdictions, the employee's right to privacy is protected in the constitution, limiting the employer's ability to monitor in the workplace. Additionally, employers must often show regard for the rights of employees' representatives to be consulted regarding the implementation of any monitoring.

If an organization has work councils or trade or labor unions, those councils and unions need to be included in discussions regarding employee privacy and planned policies, procedures, and actions. Whether the employer is required to seek the agreement of employee representatives or just needs to consult with them will depend upon the local requirements of each jurisdiction and the terms of the applicable agreements.

Other Types of Monitoring

Monitoring goes beyond just checking one or two types of network activities by using some sort of automated method. There is a very wide range of monitoring activities that organizations need to consider for an effective information security program. At minimum, types of monitoring to implement should include:

- Intrusion detection to identify when inappropriate access is occurring
- Intrusion prevention to keep unauthorized individuals from getting to information resources
- Systems and applications monitoring to ensure conformity with information security policies and standards
- Systems monitoring to detect unauthorized activities
- Systems monitoring to determine the effectiveness of security measures adopted
- Event logging
- Clock synchronization
- Log file entries standards
- Internet usage
- Business partner connections and related network activities
- The effectiveness of security controls
- User access to mission-critical and sensitive information

Awareness and Training

For network security tools to be effective, administrators and end users must be properly trained in how to use them. Awareness and training are important activities and key components of an effective information security program. Many regulations require awareness and training as part of compliance.

Legal Considerations

Always include legal counsel in decisions regarding information security and privacy, especially education program activities. It is important to know the legal ramifications and requirements for training and awareness activities.

The legalities of information security and privacy risks and managing legal compliance with applicable laws and regulations are a growing concern for managers, lawyers, and Human Resources personnel. An overabundance of international, federal, and state laws govern how personnel and individuals with access to personal and confidential information must be trained.

Managing Information Security Throughout the Enterprise

It is no longer sufficient or prudent to depend upon securing only the perimeter of the enterprise network with security management devices in order to protect all the enterprise information assets. The number of new entry points through most enterprise network perimeters can increase on a weekly, or even daily, basis.

The growing number of reported incidents not only demonstrates the impact of multiple breach-notification laws but indicates that organizations may still be focusing on just securing the network perimeter and not sufficiently securing all information assets wherever they are located.

Managing Inside Is More Complex Than Managing the Perimeter

Implementing and managing information security within the network perimeter is much more complex than just managing the security of the perimeter alone. When adding internal information security management to the picture, most organizations will get a list of components that look something like the following:

- Firewalls—Not only on the perimeter but also deployed within identified security zones
- Proxy servers—Not only on the perimeter but also deployed within identified security zones
- Unified intrusion detection, and increasingly intrusion prevention, systems between security zones
- Malicious code prevention between security zones
- Consolidated management consoles
- Unified alerting and reporting
- Unified monitoring
- Encryption systems

- Access control devices and systems
- Audit capabilities
- Policies and procedures
- Application controls
- Network controls
- Systems controls

The Porous Perimeter Must Be Considered

As more accountability is created for business leaders to ensure information security, and as they then become more aware of the related issues, they should understand that information security must be integrated throughout the entire enterprise. To be most effective in integrating information security responsibilities throughout the organization, two very important things must exist:

- Information security must be clearly supported and promoted by the highest executive leaders within the company.
- The information security function needs to be as high in the corporate structure as possible in order to set and enforce information security directives and policies. As history has proven, unless the information security department is powerful enough to establish and enforce information security administrative, operational, and technological initiatives, the rest of the organization will not follow information security requirements, but instead choose the ease of use and functionality they see information security as inhibiting.

Address Contractual and Regulatory Requirements

It is vital to ensure that information assurance activities support, and information security leaders understand, the existing regulatory and legal requirements for safeguarding information throughout the enterprise. The penalties, fines, and jail time for noncompliance can have devastating impact on not only the business but also to the business leaders personally.

Determine the Value of Information

Something lacking in most organizations is an inventory of information assets that have been classified according to their sensitivity and criticality. With today's regulatory requirements to notify individuals of security breaches, it is a necessity to know the information you have, and where it is located, if you expect to know when the information has been compromised.

After the information inventory is compiled, you can ensure appropriate security is applied based upon the value of the information. It is not feasible, or prudent, to try to secure all information at the same level. By knowing the value of the information, you can then more successfully manage the security within your security zones and layers by applying the most robust security within the zones where your high-value information assets are located, and using appropriate mechanisms within the security layers, and not investing as many resources in those zones that have information assets with lesser values.

Information Valuation

Organizations need to determine the types of information that could have the most financial impact and build security around those high-value items appropriately. What will make this challenging are the many unstructured forms in which sensitive information may be saved, such as in email, Word, Excel, PowerPoint, and other end-user controlled formats. This emphasizes the need to implement a clear, strongly supported set of information security policies that contain a very good information classification policy.

Considerations for Outsourced Access to Information Assets

When an organization entrusts third parties with its confidential data, the organization basically place all direct control of security measures for the data completely into the hands of someone else. That trust cannot be blind. When organizations outsource critical data processing and management activities, they must implement measures to stay in charge of their own business data security and minimize business risks.

Tracking Progress and Incidents

Not only is it wise and necessary to track information security progress and incidents in order to have an effective information security program, it is also a requirement of many laws and regulations.

📖 Chapter 7 discussed these requirements in detail.

Items to Monitor and Log

There is a wide range of activities throughout the enterprise that must be monitored and there are multiple types of activities that need to be logged. These are not all electronic based. You should have identified many of them while establishing your security zones and implementing your layers of security.

Auditing and Tracking Mechanisms

Establish auditing and tracking mechanisms for systems activities, key security-related events, personally identifiable information, and other sensitive and mission-critical information.

The Recipe for Achieving Information Security Inside the Perimeter

Business leaders must consider all the issues involved with managing an enterprise-wide information security program as discussed throughout this guide, and create a type of information security recipe to successfully create a secure enterprise-wide information processing environment. Each organization's recipe for success will be unique to their business goals and environment, but the following generic recipe, based upon proven security concepts, can be used as a foundation.

Ingredients

- A top-level executive leader, such as the CEO, with strong, obvious support for information security efforts
- A position or team with formally documented and well-communicated overall enterprise information security responsibility
- Business unit leaders from all areas throughout the organization to cooperate and work with the information security position to successfully integrate effective security throughout the enterprise
- Knowledge of the business environment, goals, products, services, and legal and contractual requirements
- Well-written information security policies and procedures
- Technology tools to support and enhance the information security strategy goals
- Evaluation techniques to ensure appropriate changes are made to ensure the most successful information security strategy

Instructions

- Simplify information security complexity.
    - Appoint a position to be responsible for enterprise-wide network security
    - Support the position from the highest leadership positions
- Identify legal and regulatory requirements for data protection and safeguards.
- Identify risks—using the appropriate risk analysis processes for your environment—to the organization and information systems and assets throughout the entire enterprise.
- Develop a multi-dimensional security plan to protect information assets and associated resources within all areas of an enterprise and in compliance with all regulatory, policy, and contractual requirements.
- Establish enterprise network security zones.
    - Thoughtfully plan the zones with input from the business areas and by considering risks
    - Complement effectiveness with physical zones
    - Centrally manage security zone activities through the help of decentralized responsibilities

- Implement security layers.
    - Security program management
    - Application-layer security
    - Node-level security
    - Network-level security
    - Identification and authentication
    - Network services
    - Physical security
    - Human Resources
    - Monitoring and evaluation
    - Disaster preparedness
    - Incident response
- Implement security tools.
    - Access controls
    - Encryption
    - Monitoring
    - Education
- Create organization-appropriate and well-written policies, procedures, and standards.
- Educate all individuals using the enterprise information assets and resources about the policies, procedures, and other information necessary to successfully safeguard information.
- Establish audit and monitoring functions to constantly stay aware of the information security environment.

Implementer Tips

- The porous perimeter, new and emerging technologies, and legal and regulatory requirements necessitate that security be addressed and risks be identified throughout the entire network, not just at the perimeter.
- Many information security threats and risks exist in today's business environment, both outside and inside the organization.
- Laws, regulations, and customers demand information to be adequately safeguarded no matter where it resides.
- Information security safeguards are necessary to protect against not only malicious intent by insiders but also against mistakes.

- Trusted insiders with authorized access to sensitive information will sometimes still choose to take part in malicious activities. Controls need to be in place to help prevent or catch such activities.
- New and emerging diverse technologies create threats to the enterprise network. Information security leaders must keep up to date with them.
- Using inappropriate technologies and tools for security will leave data vulnerable.
- As data increases in value, the number of threats to the data also increases.
- Incorporate access controls into the development life cycle.
- Use encryption to effectively protect data at rest and data in motion.
- Create and maintain an information inventory.
- Evaluate the information security program regularly and report to business leaders.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.