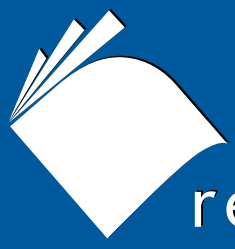

realtimepublishers.com™

The Definitive Guide™ To

Security Inside the Perimeter

Apani

Rebecca Herold

Copyright Statement

Chapter 5: Layered Security

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 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 (your critical information infrastructure) can be reached. Such layering establishes a more reliable security posture; if a failure or breach occurs in one layer, it will not compromise the other concentric layers.

Chapter 3 discussed the need for a multi-dimensional security program that includes the use of

- Protection strategies
- Risk analysis and assessment
- Security policies, procedures, and standards
- Education
- Audit and validation

Implementing security within these multi-dimensional layers appropriate to each of the zones discussed within Chapter 4 will provide a comprehensive enterprise information assurance framework within which organizations can then apply the appropriate tools and establish appropriate corresponding management activities. Taking the time to establish this framework may seem overwhelming at first, but doing so in a thoughtful way will truly result in simplifying the complexity of managing security and will distribute and incorporate security responsibilities throughout the enterprise.

Effectively layering security will incorporate security activities into all business layers throughout the enterprise.

The layers that comprise an effective information assurance program will consist of at least the following elements, in addition to any other elements an organization needs for its own unique and specific risks, threats, and vulnerabilities, as well as industry, regulatory, legal, and contractual requirements. These elements are essential because they cover logical security (networks, hosts, and programs), physical security (things that can be touched), personnel, and preventative and reactive measures:

- Security program management
- Application security
- Network security
- Node-level security
- Physical security
- Human resources security
- Monitoring and evaluation
- Disaster preparedness
- Incident response

When implementing these layers, organizations must carefully plan and implement to

- Make security as transparent and tolerable as possible
- Plan for effective enterprise-wide security integration
- Implement an effective information security education program
- Balance the activities for security with the business processes to achieve optimal security to address risks, but no more than is necessary

Always remember that information security should be implemented to most effectively support and protect the business, not to unnecessarily inhibit or disrupt the business.

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.

Security initiatives are only effective when a framework exists that controls and manages information security activities throughout the organization.

Information security program management layers, when implemented most effectively for each enterprise's specific needs, will be complementary. Each layer will help the other be more effective for information security assurance.

Effectively layering the security management program will generally involve two levels of information security management:

- Centralized enterprise information security management with ultimate accountability and oversight responsibilities.
- Distributed information security management with various information security accountabilities spread throughout the enterprise business units, operations areas, and geographies.

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. In addition, it will allow the organization to enforce security requirements centrally as well as to centralize monitoring, evaluations, and updates to the enterprise security program. Centralized security management should include the following components:

- **Clearly defined and documented accountable security program management responsibility**. The security program management function must be clearly defined and supported by enterprise management as being the area ultimately responsible and with the authority for instituting information security initiatives and enterprise requirements. This area must consist of stable resources and personnel who have the responsibilities and can perform the necessary tasks.
- **Enterprise information security charter**. An effective program must be based upon a documented enterprise security charter that clearly defines the function of the information security program and defines the responsibilities for not only the information security area but also the related enterprise programs and departments.
- **Enterprise information security policies, procedures, standards, and guidelines**. An effective program must include information security policies, in addition to standards, procedures, and guidelines as appropriate to address the information security needs of the enterprise and support the documented charter.
- **Information security strategies**. Effective information security management must have both short-term and long-term strategies to incorporate information security into the enterprise business functions as well as existing, new, and emerging technologies.
- **Compliance**. Effective information security management must address how non-compliance with the security requirements will be discovered and how the program requirements will be enforced.
- **Inter-departmental partnership**. Information security activities overlap with other operational areas such as physical security, quality assurance, internal audit, safety, and legal, just to name a typical few. Effective information security management will include established communications and partnerships with these areas to more successfully integrate information security into the management of the enterprise as a whole.
- **Liaisons with external entities**. Effective information security management must be knowledgeable and up to date on the latest trends and issues. This function should participate in outreach activities to obtain information from external sources to access more comprehensive information, ultimately resulting in more comprehensive knowledge and more resources to contact when situations arise that are new or particularly challenging to the organization.

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. Distributed information security management will incorporate security into their respective areas in the following ways:

- **Area-specific security procedures and guidelines.** Distributed information security management personnel will address the specific activities within the business area while at the same time support the enterprise information security program.
- **Manage incorporation of information security into the systems development life cycle**. Distributed information security management personnel will ensure appropriate and cost-effective security by ensuring security is built-in to their associated business processes from the very beginning, through systems launch, update, and retirement.
- **Manage integration of information security into the business unit operations.** Distributed information security management personnel will understand their areas, mission, technologies, and operating environments better than any corporate area. They will be able to most effectively integrate information security activities into the daily management of their departments and activities.

Application Security Layer

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

- Completeness
- Accuracy
- Validity
- Authorization
- Data encryption
- Segregation of duties

Although the design and implementation of application security controls is typically the task and responsibility of the IT and engineering areas, the chosen controls must be based upon business requirements. The centralized and distributed information security management areas must define the requirements clearly and effectively to allow the IT areas to deliver and support the appropriate applications security services in addition to including successful links to the corresponding security within the supporting databases and infrastructures.

The centralized and distributed information security management areas should understand the following types of application control objectives in order to work most successfully and efficiently with the IT areas while they are creating and updating applications:

- Data authorization and origination controls
    - Data preparation—Procedures that IT follows to ensure consistency and completeness in data preparation activities; for example, input forms can be provided to help minimize, or perhaps even eliminate, errors and omissions
    - Source document authorization—Procedures to appropriately prepare source documents and sources and to adequately segregate duties between origination and approval of source documents
    - Source document data collection—Procedures to ensure appropriately authorized source documents are complete, accurate, accounted for, and transmitted for timely entry
    - Error handling—Procedures to ensure the detection, reporting, and correction of source document errors, problems, and irregularities in data collection
    - Retention—Procedure to ensure the original source documents are retained to the required and appropriate amount of time to meet regulatory contractual and litigation requirements, in addition to allow for retrieval or reconstruction of the data within a reasonable time following transactions
- Data input controls
    - Authorization—Procedures to ensure that only authorized personnel perform data input
    - Accuracy, completeness, and authorization checks—Procedures to ensure that the data entered for business transaction processing (whether it is generated by people, systems, or through other interfaces) are checked for accuracy, completeness, and validity; the procedures should ensure that such checks are performed as close to the data origination point as possible and produce accuracy metrics for each source to identify problems.
    - Data input error handling—Procedures to correct and then resubmit erroneously input data
- Data processing controls
    - Data integrity—Procedures to ensure separation of duties is maintained during data processing, along with verification procedures to appropriately update the control totals, master file, and other application resources
    - Validation and editing—Procedures to ensure processing, authentication, and editing validation (manual checks should be performed whenever automated checks cannot); it is also a good practice to sometimes perform manual and automated checks (manually checking a sample of data will confirm that the automated checks are valid)
    - Error handling—Procedures to identify bad transactions before they are processed and without unnecessary interruption of other transaction activities

- Data output controls
    - Handling and retention—Procedures to handle and retain output from applications; such procedures must incorporate privacy and security requirements from applicable laws, regulations, and contractual requirements
    - Output distribution—Procedures governing how to distribute applications output; to be effective, these procedures need to be clearly documented, communicated, and enforced
    - Balancing and reconciliation—Procedures to balance output and relevant control totals; use audit logs to enable transactions processing to be traced, along with reconciling data disruptions
    - Review and error handling—Procedures to ensure that the area generating the output and appropriate persons using the report check the accuracy of the information; the procedures should include how to identify and handle the errors
    - Securing output—Procedures to ensure output reports are appropriately secured and maintained during the distribution period as well as after they have been delivered to the appropriate persons
- Boundary controls
    - Authenticity and integrity—Procedures to appropriately check the authenticity and integrity of all information that originates outside the enterprise such as that received by telephone, within papers documents, and via fax or email
    - Transmission (via electronic methods) and transport (via physical methods) protection—Procedures to ensure appropriate and sufficient security to ensure accidental or unauthorized access modification or misdirection of sensitive information does not occur during information and report transmission and transport (for example, blocking out sensitive data on hardcopy that will be sent to an auditor, when the auditor does not need that sensitive data, using encryption, and so on).

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. The current hot topic of identity management focuses on integrating these activities into the business environment.

Identity Management in a Nutshell

Identity management seeks to ensure that all types of network users, and their corresponding activities and capabilities on systems and applications, are uniquely identifiable. Identity management processes work to ensure user access rights to network resources and information are in line with each user's documented business responsibilities and needs. Identity management implementations usually involve a formal process implemented by information security personnel of assigning user access rights following requests by management and approval by systems owners. In addition, a central repository is maintained that defines user identities and access rights. Both technical and procedural methods are used to establish and keep user identification, authentication, and access rights up to date.

Identification and Authentication

Identification and authentication are important for preventing 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.

> It is not only a leading information security practice but also required by many laws and regulations to grant system users access to only those resources, information, and applications necessary to perform their job responsibilities. This setup is commonly referenced as access control based upon "least privilege."

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, which Chapter 6 will discuss in more detail. Certificates are also frequently used to provide identification for users and devices.

> To create accountability for activities, organizations should not allow user IDs to be shared.

Authentication

Authentication is used in conjunction with identification to validate the entity using the identifier as 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 their identity validated. Certificates are the primary method used to authenticate the identity of network devices.

> The method of authentication is strengthened when more than one authentication method is used.

Logical Access Control

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

> ☞ Establish logical access controls upon the principle of least privilege, granting access to only the information resources necessary to perform business activities.

Network Security Layer

Although the Transmission Control Protocol/Internet Protocol (TCP/IP) is an important part of the network security layer, it is also important for business leaders to understand that 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.

Security within the network layer must be incorporated into, and addressed, within many different components and using many different techniques. 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. There will be the need for additional security to be applied within the network to protect sensitive information that passes through public and business partner networks and zones that are not trusted.

Organizations must have layers of security that are implemented within the appropriate network zones to ensure appropriate and effective security techniques and related management procedures are used to authorize access and secure and control information flows from and to networks.

Examples of network security tools and techniques include:

- Firewalls
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Network segmentation
- Malicious code prevention
- Remote access controls
- Encryption

Network Security Controls

Networks must be sufficiently and effectively managed and controlled using the following tools and techniques to protect the network and associated components from a multitude of threats and to provide security for the systems and applications that depend upon the network for business processing. There are a wide range of security controls within the network layer that business leaders must carefully consider:

- **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. The initiation of a network change must be separated from the authorization of that change. When designing network controls, this collusion possibility 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. Encryption, discussed in Chapter 6, is one example of an effective tool to protect data transmissions. The endpoint systems and applications must be protected from the threats these open networks present.
- **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 important, not only for regulatory compliance but also to enable the correlation of multiple network activities throughout all security layers.
- **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. Network services can range from simple to complex and include such things as:

- Provisioning network connections
- Private network services
- Value added networks
- Managed network security solutions such as firewalls and IDSs

Well-documented security agreements and requirements make it very clear the expectations the organization has for network security activities. Consider defining the following network services and security requirements:

- Monitor the management of the network security services
- Periodically and regularly audit the management and success of the network security services
- Implement technology—such as authentication, encryption, and network connection controls—based upon risk
- Specify technical parameters for secured connections with identified networks services to support the security and network connection policies and requirements
- Enable procedures to restrict access as appropriate to specific network services and applications
- Implement node-level security where appropriate, including the use of identity authentication and logical access controls

Physical Security

The physical information security layer is a very important component of information security that is often overlooked by information security practitioners. This aspect of information security is commonly left solely to the facilities security personnel. However, it is important in preventing unauthorized physical access, damage, and interference to information assets and resources to consider the physical security risks, threats, and vulnerabilities. Then 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. These information processing facilities and systems should be located within secure areas and protected by defined security perimeters; in addition, 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.

The following physical security controls can serve as a checklist to help you 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

- Account for the risks of natural and man-made disasters
- Consider applicable laws and regulations, such as the United States Occupational Safety and Health Act (OSHA)
- Establish physical security perimeters (using things such as walls, card controlled entry gates, and manned reception desks), physical security zones (discussed in Chapter 4), location of critical equipment, and shipping and receiving areas to control physical access to information processing sites and buildings, restricting access to only authorized personnel.
- Establish responsibilities for monitoring and procedures for reporting and resolving physical security incidents.
- Ensure information processing building and site perimeters are physically sound.
- Put alarms and monitors on all fire doors on the security perimeter and test them regularly.
- Install physical intruder detection systems on all external doors and accessible windows, in addition to unmanned areas containing information processing resources.

Give special consideration to physical access security within buildings where multiple organizations are located.

Public Access, Delivery, and Loading Areas

Control the areas and access points where unauthorized persons could enter organization premises, such as in delivery and loading areas. If possible, isolate these areas from the information processing facilities to further avoid unauthorized access. Implement appropriate controls in the public access areas:

- Restrict access to a delivery and loading areas on the outside of facilities to properly identified and authorized persons.
- Design delivery and loadings areas so that supplies can be unloaded without obtaining access to any other parts of the building.
- Put alarms and surveillance cameras on external delivery and loading area doors. Keep the video according to applicable laws and contractual requirements, and store for analysis in case of an incident.
- Implement procedures to inspect incoming packages and materials for potential threats.
- Physically segregate incoming shipments from outgoing shipments.

Physical Entry and Access Controls

Access to organization premises, and often specific buildings and rooms, should be restricted to only those with a business need to enter:

- Justify, authorize, log, and monitor access to organization premises, buildings, and areas for all persons, including personnel, temporary staff, clients, vendors, visitors, and all other third parties.
- Record the date and time of visitor entry and departure. Supervise all visitors unless their access has been previously approved, and grant them access according to specific, authorized purposes.
- Ensure only authorized persons can access areas where sensitive information is processed or stored. Use authentication controls (such as access control cards with PINs) and keep an audit trail of all access.
- Require all personnel to wear some form of visible identification.
- Do not allow third-party support personnel access to secured areas or areas where sensitive information is located unless absolutely necessary for them to perform their job responsibilities, under which circumstances access should be authorized and monitored.
- Regularly review access rights to secured areas and update appropriately.
- Maintain a list of who has access control devices, such as keys and access control cards.
- Implement policies addressing how to protect the access control devices. For example, keys must not be kept in locks or hanging on the wall, and key cards must not be left unprotected on a desk.

Securing Offices, Rooms, and Facilities

Physical security for offices, rooms, and facilities should be designed and applied based upon the risk to the particular facilities and to the accompanying legal and contractual requirements. Consider applying the following controls:

- Implement applicable health and safety regulations and standards
- Site key rooms and facilities to avoid public access
- Do not make directories and internal telephone books identifying locations of sensitive information processing facilities accessible to the public
- Give only personnel with a need to know information about the existence of, or activities within, secured areas
- Avoid unsupervised working in secure areas not only to prevent opportunities for malicious activities but also for safety reasons
- Physically lock and regularly check unmanned secured areas
- Do not allow photographic, video, audio, or other recording equipment such as cameras in mobile devices into secured areas
- Document requirements and procedures for employees, contractors, and third parties to work within secured areas
- Use clean rooms when outsourcing processing of confidential and mission-critical information to third parties

When discussing protection of information processing that has been outsourced, a clean room typically means that all the computer machines and output devices—except for terminals—used by the third party are disabled. This does not allow for information to be copied, hard drives and handheld devices cannot be used to get information, and hard copies of information cannot be obtained. The servers are physically located in a completely different geographic area, so there is no way to get data from a clean room facility. In addition, personnel are physically searched when entering and leaving.

Environmental Security

Avoid as much damage as possible from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters. Information security activities must include the design and implementation of measures to protect facilities and processing equipment against these adverse environmental conditions:

- Install equipment to monitor and control the environment, including temperature, humidity, and power within processing areas.
- Design and apply physical protection to help protect against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters.
- Implement protections from security threats presented by neighboring premises, such as a fire in neighboring buildings, water leaking from the roof or in floors below ground level, or an explosion in the street.
- Store hazardous or combustible materials at a safe distance from secured areas.

- Do not store bulk supplies, such as stationery, paper clips, or other types of supplies that are commonly needed on a daily basis, within a secured area.
- Locate fallback equipment and back-up media at a safe distance from the facility, within a secured site, to avoid damage from a disaster affecting the main site.
- Install and appropriately place fire-fighting equipment. Periodically test or inspect the devices to ensure that they are functional.

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 to help prevent loss, damage, theft, or the compromise of assets and interruption to the organization's activities. The following controls should be considered:

- Protect all types of computing equipment from physical and environmental threats.
- Implement policies for computer equipment siting (placing in appropriate locations) and disposal.
- Implement special controls as necessary to protect against physical threats and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.
- Position information processing facilities that process sensitive data to reduce the risk of information being viewed by unauthorized persons during their use, and secure all types of storage facilities and areas to avoid unauthorized access.
- Isolate computing equipment that requires special protection to reduce the general level of protection necessary.
- Implement controls to minimize the risk of possible physical threats, such as theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism.
- Establish policies addressing eating, drinking, and smoking in proximity to information processing facilities and equipment.
- Monitor environmental conditions, such as temperature and humidity, for conditions that could adversely impact the operation of information processing facilities.
- Install lightning protection to all buildings and lightning protection filters to all incoming power and communications lines. Be sure to include remote processing areas, such as home workers.
- Consider using special protection methods, such as keyboard covers, for computing equipment in industrial environments.
- Protect equipment processing sensitive information to minimize the risk of information leakage due to emanation.

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:

- Regularly inspect support utilities and test, as appropriate, to ensure proper functioning and reduce risk from their malfunction or failure.
- Provide electrical supply that conforms to the equipment manufacturer's specifications.
- Use an uninterruptible power supply (UPS) to support orderly close down or allow for continuous running of equipment supporting critical business operations.
- Consider using a back-up generator if processing is required to continue in case of a prolonged power failure.
- Regularly check UPS equipment and generators to ensure adequate capacity and test in accordance with the manufacturer's recommendations.
- Consider using multiple power sources, particularly for large facilities.
- Locate emergency power off switches near emergency exits in equipment rooms.
- Provide emergency lighting in case of main power failure.
- Ensure stable and adequate water supply for air conditioning, humidification equipment, and fire suppression systems (where used).
- Install an alarm system to detect malfunctions in the supporting utilities.
- Connect telecommunications equipment to the utility provider by at least two diverse routes to prevent failure in one connection path.
- Ensure adequate voice services are available to meet local legal requirements for emergency communications.
- Protect power and telecommunications cabling carrying data or supporting information services from interception and damage.

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:

- Maintain equipment in accordance with the supplier's recommended service intervals and specifications.
- Allow only authorized maintenance personnel to make repairs and service equipment.
- Keep records of all suspected or actual faults and all preventive and corrective maintenance.
- Implement controls for situations in which equipment is scheduled for maintenance. Consider whether personnel onsite or external to the organization perform the maintenance. Remove sensitive information from the equipment before allowing outsiders to perform maintenance, or obtain sufficient clearance and appropriate confidentiality and non-disclosure agreements from them.
- Comply with all insurance policy requirements for the processing equipment.
- Implement appropriate security for offsite equipment taking into account the unique and existing risks of working outside the organization's facilities premises.
- Implement policies to prevent equipment and media being taken off the premises to be left unattended in public places.
- Require mobile computing devices to be carried as hand luggage and disguised when possible when traveling.
- Implement policies and procedures for personnel who work from home or other locations off the organization's premises. Determine appropriate controls through risk assessment and apply as appropriate.
- Obtain adequate insurance coverage to protect off-site computing equipment.
- Implement physical security controls for all kinds of mobile computing devices, such as personal computers, organizers, mobile phones, smart cards, paper, smart phones, PDAs, Blackberries, storage media, and all other types of mobile computing and storage devices.

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 to outside the organization:

- Either physically completely destroy the devices containing sensitive information or use procedures and tools to ensure the complete removal of information from the storage devices using techniques to make the original information non-retrievable. Such techniques should go beyond just using the standard delete or format function; they should include using software that will permanently wipe data and degaussing.
- Assess the risk of damaged devices containing sensitive data to determine whether the items should be physically destroyed rather than sent for repair or discarded.

Taking Computing Equipment Off Premises

- Do not allow equipment, information, or software 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.
- Establish and implement time limits for equipment removal and returns. Establish procedures for ensuring compliance.
- Where appropriate based upon risk, log computing equipment as it is taken off-site and when it is returned.
- Perform spot checks to detect unauthorized removal of property in addition to detecting unauthorized recording devices, weapons, and other equipment presenting a threat to the organization and premises. Be sure to perform such spot checks in accordance with applicable legislation, policies, contracts, and regulations.

Human Resources

The most vulnerable of the information security layers, as discussed in Chapters 1 and 2, truly are the human resources that organizations depend upon to follow information security policies and procedures. It is vital that individuals 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 with clear career paths and incorporating security into job responsibilities which are used for job 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

To help reduce the human risks involved with information security, organizations should consider the following controls within the human information security layer.

Recruitment, Competencies, and Retention

- Implement procedures for recruiting information security personnel, and other personnel with information security responsibilities, to ensure they are appropriately qualified with the skills and experience necessary to achieve information security goals.
- Motivate personnel by incorporating information security as part of the annual job appraisal process.
- Regularly verify personnel remain competent to fulfill their information security responsibilities and continue to receive the appropriate education, training, and/or experience to stay up-to-date with changing technologies and threats.
- Define core information security competency requirements and verify they are being maintained, using qualification and certification programs where appropriate.

Roles

- Define, monitor, and supervise information security roles, responsibilities, and compensation frameworks for personnel. Such responsibilities should include complying with policies and procedures, along with the code of ethics and professional practices.
- Include within the terms and conditions of employment personnel responsibility for information security, internal control, and regulatory compliance.
- The level of supervision over roles should be in line with the sensitivity of the position and corresponding information handled, along with the amount of responsibility assigned.

Training and Awareness

Provide personnel with information security orientation when hired and ongoing training and awareness messages to maintain their knowledge, skills, abilities, and internal controls and security awareness at the level required to achieve organizational goals:

- Provide appropriate ongoing awareness messages, targeted group training, and regular updates to policies and procedures, as relevant for roles and job functions.
- Provide ongoing training specialized to the groups that handle information or support information processing systems. Such training should include security requirements, legal responsibilities, and business controls as well as training in the correct use of information processing facilities, such as log-on procedure, use of software packages, and information on the disciplinary process.
- Make information security awareness, education, and training activities suitable and relevant to the different organization roles, responsibilities, and skills
- Include information within training and awareness on known threats, who to contact for further security advice, and the proper channels for reporting information security incidents.

Personnel Clearance Procedures

- Include background and criminal checks, according to applicable laws, regulations, and union agreements, during the personnel recruitment process.
- Periodically perform background and criminal checks for positions with the most impact to business with regard to information handling and network support.
- Perform background and criminal checks not only for employees but also for contractors, consultants, vendors, business partners, and anyone else who will have access to the organization's information and systems. Periodically re-check personnel backgrounds to discover any events that may have occurred since hire that would put the organization at risk.

Job Performance, Change, and Termination

- Regularly perform job performance evaluations that include consideration of information security requirements and procedures.
- Establish procedures to expediently remove systems and information access and retrieve all equipment and information as soon as personnel terminations occur.
- Ensure that when personnel terminations occur, knowledge transfer is arranged, responsibilities reassigned, and access rights removed to minimize risks and provide for continuity of the personnel functions.

Monitoring and Evaluation

The monitoring and evaluation layer of information security is one that, unfortunately, is often only marginally 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; and performing evaluation activities.

Audits

Both self-administered and independent third-party audits provide important information about the technical, operational, procedural, and regulatory compliance status of an organization's information assets. A variety of tools are used to perform audits:

- Automated tools—These can be used to identify a wide range of vulnerabilities, such as inappropriate or inadequate access controls and access control configurations, bad passwords, systems software weaknesses, and necessary patch updates.
- Performing an internal controls audit—An internal or external auditor can review the controls in place and evaluate their effectiveness. A comprehensive audit will address both automated and human-based procedural controls.
- Security checklists—Checklists can be used to compare leading standards, baselines, or the organization's own policies and procedures with the existing information security environment.

- Penetration tests—Penetration testing, when performed correctly and appropriately, will use multiple methods to attempt to access a system or network. Automated tools can be used within penetration tests to automate the attempts and make the test more efficient. Penetration tests should be performed after security controls are implemented, which will test the effectiveness of some of the controls. Many organizations make the mistake of engaging in a penetration test before they have improved their information security program. Penetration testing can cause adverse impact to business operations if not performed properly; these types of tests should only be conducted with the knowledge and cooperation of systems and network management.
- Social engineering tests—Social engineering tests, such as trying to get a password from the Help desk, is an effective drill for ensuring personnel follow policies and procedures, and can help to reveal where additional training and awareness is needed.

Monitoring

Like audits, there is a wide range of methods that can be used for monitoring.

However, be aware that some methods of monitoring could be illegal based upon applicable laws, regulations, and contractual obligations. Always check with legal counsel before implementing monitoring to ensure it is being done within all the legal boundaries.

- Review logs—Periodically review systems- and applications-generated logs to detect security problems, such as attempts to perform unauthorized activities. Ensure inappropriate information and information under legal restrictions, such as certain types of personal information, is only logged when necessary.
- Utilize automated tools—Virus scanners, checksums, IDSs, and integrity verification programs are just a few of the types of automated tools that can be used for monitoring.
- Configuration change management—Monitoring configuration changes helps to ensure that the correct version of a system or application is being used and that changes are reviewed prior to being placed into production to consider security implications.
- Mail lists/vendor announcements/industry membership groups/publications—Monitor sources outside the organization to keep as current as possible with new and emerging security concerns and issues.
- Accreditation—Formally examine the security of systems and applications periodically to discover whether security is still sufficient and identify necessary changes and other high-level information security management issues along with the implementation status.

Audit and monitoring data can be used as business performance indicators as the following examples highlight:

- Business contribution including, but not limited to, financials, marketing, and customer service
- Performance within strategic business unit, information security, and IT plans
- Compliance with applicable laws and regulations and the associated risks and deficiencies
- Internal systems user satisfaction
- External customer satisfaction
- Key IT processes, such as development, service delivery, and patch management
- Activities to reach long- and short-term goals, such as the use of emerging technology, reusable infrastructure, business and IT personnel skill sets

Disaster Preparedness

Historically, the most unglamorous of the information security layers is disaster preparedness. However, events of the past decade demonstrate the importance and criticality of the components, which include contingency plans, business continuity plans (BCP), and disaster recovery (DR) activities. It is vital for organizations to have such plans in place to support the business goals for continued operations as much as possible under the circumstances.

Hurricane Katrina, which hit the United States' Gulf Coast at the end of August 2005, is an example of a significant natural disaster that had been a possibility for many years, but yet the effects for which were drastically underestimated. The destruction in primarily New Orleans, but also within the Florida Panhandle, Alabama, Mississippi, and Louisiana resulted in federal disaster declarations over a 90,000 square mile area. The total damage estimates at the beginning of December 2005 exceeded $100 billion. This situation compellingly illustrates how crisis management and continuity planning are of increasing concern to public and private sector executive decision makers.

Contingency Plans

Contingency planning addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. Contingency plans integrate the results of business impact analysis. Effective contingency planning will result in a plan for each critical business process and infrastructure component. Contingency plans should describe the implementation resources, staff roles, procedures, and timetables. Contingency planning involves five key components:

- Assessment of the cost and benefits of identified alternatives and selection of the best contingency strategy for each identified business process
- Identification and documentation of the contingency plans and implementation methods
- Definition and documentation of the triggers for activating contingency plans
- Establishment of a business resumption team for each identified business process
- Development and documentation of "zero day" strategies and procedures

The term *zero day* used in the information security context refers to having a security vulnerability exploited on the same day that the vulnerability becomes generally known.

Business Continuity Plans

Organizations need to develop BCPs to minimize the interruptions to business activities in addition to protecting critical business processes from the effects of major failures of information systems or disasters. In addition, BCPs must ensure the continued functionality, or in worst cases, timely resumption of critical business processes.

Implement a BCP to minimize the impact on the organization and recover from loss of information assets to an acceptable level by using a combination of preventive and recovery controls. The time to recover a business process must be within an acceptable time interval.

An effective BCP will identify critical business processes and integrate the information security requirements of business continuity along with the other continuity requirements relating to such activities and areas as staffing, materials, transport, and facilities.

A critical element of creating an effective BCP is to perform a business impact analysis (BIA) to clearly document and consider the consequences of disasters, security failures, loss of service, and service availability as well as to identify the most critical business processes. Organizations that do not perform a BIA will find they are likely woefully unprepared to react in the most optimized manner when business disruption occurs.

BCPs should include not only controls to identify and reduce information security risks but also actions resulting from performing a general risk assessment to limit the consequences of damaging incidents. In addition, BCPs should ensure that information required for business processes is readily available.

Disaster Recovery Planning

Every organization can experience a serious incident that can prevent it from continuing normal operations. This can happen any day and at any time. The potential causes are infinite and widely varied. An organization that cannot recover business processes in an acceptable time can easily go out of business. Every organization is fundamentally responsible for maintaining a DR plan.

> Many regulations require covered organizations to develop and maintain some form of DR plans. Such regulations include HIPAA, GLBA, the United States PATRIOT Act, the European Union Data Protection Directive, Canada's Personal Information Protection and Electronic Documents Act, ad Japan's Personal Information Protection Law.

The concept of disaster recovery planning (DRP) is nothing new. Traditional DRP addressed the recovery planning needs of the organization's IT infrastructures, including centralized and decentralized IT capabilities as well as voice and data communications network support services. As DRP evolves, practitioners have found it apparent that more is necessary beyond just the recovery of IT. Timely recovery of the necessary IT components is useful only if the organization's business units are also able to continue functioning in some manner during the recovery process. The business must be prepared to communicate with customers, business partners, stakeholders, personnel, personnel family members, and others associated with the business. The entire organization must take into consideration in what ways they will be able to continue with basic business processes, such as receiving and entering orders, producing goods, providing services, collecting payments and revenue, and so on.

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 component 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.

An organization should address information security incidents by developing an incident handling team or functional area. The incident handling team should be used to quickly and effectively respond to defined incidents by performing activities such as containing and repairing damage from incidents and preventing or minimizing damage from future incidents. The basic components of an information security incident response function will include:

- Service desk function to receive, log, communicate, dispatch, and analyze incident calls, incidents, service requests, and information requests
- Monitoring and escalation procedures based upon the specific type of incident
- Procedures to log and track all incident calls, incidents, service requests, and information needs
- Escalation procedures to ensure incidents are escalated according to predefined limits and to allow for workarounds
- Procedures for monitoring customer, consumer, and personnel queries regarding the incident
- Trend analysis reports to allow response actions to be measured and to identify trends and recurring problems

All personnel, contractors, and other third-party users should be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of organizational assets. They should be required to report information security events and weaknesses as quickly as possible to the designated point of contact. The information security awareness and training program should include teaching personnel how to recognize and properly report incidents.

When follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence as required by the applicable jurisdictions. The rules for evidence generally cover:

- Admissibility of evidence—Whether or not the evidence can be used in court
- Weight of evidence—Quality and completeness of the evidence

Organizations must ensure information systems comply with any published standard or code of practice for the production of admissible evidence to ensure admissibility of the evidence in court actions.

It will often not be obvious when an information security incident is first detected whether the event will result in court action. This ambiguity creates the danger that necessary evidence is destroyed either intentionally during clean-up attempts or accidentally before the seriousness of the incident is realized. This situation illuminates the need for clearly documented and closely implemented incident response plans.

Information security evidence may go outside organizational and/or jurisdictional boundaries. Be sure to include legal counsel to advise how the organization can collect the required information as evidence. Consider the requirements of all the applicable jurisdictions to maximize chances of admission across the relevant jurisdictions.

Summary

All the layers of security defenses and controls discussed previously need to be applied throughout the enterprise. The specific controls within these layers will vary from zone to zone within which they are implemented, as described in Chapter 4. In effect, these security layers will exist in all the zones, as represented and applied, using the zoning diagram discussed in Chapter 4. However, because the chosen controls are based upon risk, they will not be identical throughout the enterprise.

The chosen and implemented controls need to be based upon risk, and each security zone will have different risks.

Within each security zone, apply only the amount of security needed to maximize the benefit of information security to the business. Do so by assessing the risks within each identified security zone. However, do not think that this means that "less is more" when it comes to information security! In fact, the most efficient information security activities will utilize a wide range of information security tools and procedures that will comprise a multi-layered blanket of information resources protection for the organization. Chapter 6 will delve into a discussion of these security tools.

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.