realtimepublishers.com™

The Definitive Guide™ To

Security Inside the Perimeter

Apani

Rebecca Herold

Copyright Statement

Chapter 6: Tools in 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 basically 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

A common perception regarding network security tools is that such tools are different from others within your organization. If you ask seasoned information security practitioners to list network security tools, you will get a wide range of diverse answers. This variation is understandable because what are considered important information security tools depends upon the roles and responsibilities for each information security practitioner within each unique organization and its accompanying threats, risks, vulnerabilities, geographic locations, and applicable laws, regulations, and contractual requirements.

An informal survey of five highly seasoned information security practitioners—each with 15 to 30 years of security management experience—asked the professional to list what popped into their minds when thinking about network security tools. Their combined responses resulted in a list of 32 tools, which the following list highlights:

- 802.11X WLAN controls
- 802.1x authentication
- Access control lists (ACLs) between network zones
- Application system controls
- Awareness and training for network users
- Centralized security management
- Database system ACLs
- Deep packet inspection devices
- Digital certificates
- Firewall appliances
- Firewalls between network zones—stateful inspection, application firewalls, proxies
- Identity management
- Intrusion Detection System (IDS) monitoring tools

- Kerberos
- Network partitioning
- Network segmentation
- One-time passwords, such as those used with the RSA SecurID
- Operating system (OS) controls
- Physical access control cards
- Physical separation of high-risk computers from the network
- Physically protecting network devices (employing data center physical access controls, protecting cables from tampering, and so on)
- Policies and procedures
- Quarantining tools that check a host when it connects to the network for a baseline configuration (current antivirus, patch level, and so on) and, if the baseline is not met, does not allow the host access or allows only limited access
- RADIUS, TACACS+, TACACS, DIAMETER
- Role-based access controls
- Single-Sign On (SSO) tools
- Traditional passwords
- Two-factor authentication tools (smartcards, tokens, and so on)
- Screensavers and other endpoint security actions
- VLANs
- Software tools such as those from BindView and Arbor Networks
- Content monitoring and data leakage prevention tools, such as NetIQ WebMarshall and Vericept monitoring solutions

All their responses are valid for each of their own situations and business environments. There was some overlap, but there were clear differences between the lists based upon the primary concerns for each practitioner.

Each organization must determine the risks to their own unique organization, create the security zones as explained in Chapter 4, then identify the best tools to address the threats, risks, and vulnerabilities within each of the identified zones.

> ✎ There isn't one list of network tools that will provide the magic solution for securing network information resources.

The wide range of network security tools that will give organizations the most bang for their buck and help to provide the most effective security to their enterprise information resources can be generally discussed within four categories:

- Access controls
- Encryption
- Monitoring
- Awareness and training

> ☞ To be effective and meet the numerous legal and regulatory requirements that now apply to basically all organizations, these tools must be used in accordance with established, formally documented, and executive management supported policies and procedures.

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. As this guide has emphasized, it is no longer sufficient to simply apply security at the network perimeter. 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.

Changing access controls from perimeter-based to zone-based will require changing the security architecture, and it will require careful planning and resources. Use the people and skills within the organization to leverage the time, effort, and costs involved. Structure the network architecture to consolidate resources and leverage security zoning. Tighten internal access controls by restricting access appropriately to support and facilitate business processing within the identified security zones. Network security administration tools have come a long way in the past few years, and what used to seem like prohibitively expensive or impossible to implement centralized access control solutions are now quite achievable and affordable.

Types of Access Controls

Access controls block or facilitate a user or system to communication and interaction with network resources such as computers, databases, email, Web servers, routers, or any other systems or devices. Access controls protect systems from unauthorized access and determine what levels of authorization are appropriate for a user or system. Access controls can be technical or operational. The following list highlights examples of different types of access controls:

- Access control policies and procedures
- Proxy servers and firewalls
- Physical access control cards
- OS capabilities
- Application system capabilities
- Database system ACLs
- IDS monitoring tools
- Access control security auditing
- Identity access or SSO tools
- Two-factor authentication tools (smartcards, tokens, and so on)

Laws and Regulations Require Access Controls

Besides being a prudent business activity, implementing access controls within the network is required by multiple laws and regulations, and additional legal requirements are established each month along with new contractual obligations for effective access controls.

HIPAA

The following excerpt is from the United States HIPAA security rule (http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf), which includes the following directive for access controls:

> "§ 164.312 Technical safeguards.
>
> A covered entity must, in accordance with § 164.306:
>
> (a)(1) Standard: Access control.
>
> Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
>
> (2) Implementation specifications:
>
> (i) Unique user identification
>
> (Required). Assign a unique name and/or number for identifying and tracking user identity.
>
> (ii) Emergency access procedure
>
> (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
>
> (iii) Automatic logoff (Addressable).
>
> Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
>
> (iv) Encryption and Decryption
>
> (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information."

This excerpt demonstrates the clear need for policies and procedures to create a framework for an information management program, to serve as types of access controls for an organization, and to meet compliance with HIPAA. Access controls need to be appropriate within each identified security zone.

The Gramm-Leach-Bliley Act

The following excerpt is from the United States Gramm-Leach-Bliley Act (GLBA) safeguards rule (http://www.ftc.gov/os/2002/05/67fr36585.pdf), which includes the following directive for access controls:

> "§ 314.3 Standards for safeguarding customer information.
>
> (a) Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.
>
> (b) Objectives. The objectives of section 501(b) of the Act, and of this part, are to:
>
> (1) Insure the security and confidentiality of customer information;
>
> (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
>
> (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."

This excerpt demonstrates how access controls are often legislated through implication. Although not explicitly stated, access controls are needed to achieve actions 1, 2, and 3.

European Directive on Privacy and Electronic Communications

The following excerpt is from Article 5 Item 3 of the European Directive on Privacy and Electronic Communications (http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf), which includes the following implications for access controls:

> Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

This excerpt demonstrates the need for access controls worldwide. In fact, countries other than the United States have much broader data protection laws that require organizations to be much more diligent in establishing information security controls. Notice this particular law emphasizes the need to give access to only those necessary to perform business activities, described as an "information society service."

Canadian Personal Information Protection and Electronic Documents Act

Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) contains many requirements for access controls. The safeguards section includes the following directives, which include access control requirements:

> 4.7 Principale 7 — Safeguards 4.7 Septième principe — Mesures de sécurité
>
> Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
>
> 4.7.1
>
> The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.
>
> 4.7.2
>
> The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.
>
> 4.7.3
>
> The methods of protection should include
>
> (a) Physical measures, for example, locked filing cabinets and restricted access to offices;
>
> (b) Organizational measures, for example, security clearances and limiting access on a ‘‘need-to-know’’ basis; and
>
> (c) Technological measures, for example, the use of passwords and encryption.
>
> 4.7.4
>
> Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.
>
> 4.7.5
>
> Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

This excerpt demonstrates that laws requiring data protection do not focus solely on technology security requirements but also on organizational and physical security controls.

Japanese Personal Information Protection Law

The following excerpt from the unofficial English translation (Proskauer Rose LLP © 2005 unofficial English translation at http://www.proskauer.com/hc_images/JapanPersonalInformationProtectionAct.pdf) includes the following directive that has implication for access controls:

> Section 20 Security Control Measures
>
> A Business must take steps to prevent the unauthorized disclosure, loss or destruction of Personal Data and it must protect Personal Data security.

This excerpt demonstrates that some laws are written very broadly and result in wide interpretation by not only different organizations but also different positions within an organization, such as information security and legal. You must consider carefully what actions will be able to justifiably demonstrate your organization truly has tried to comply with the laws.

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 and there were only dumb-terminals sitting on the end users' desktops. Now the network environment in most, if not all, enterprise networks is a mix of systems owners scattered throughout the enterprise in various departments and locations, assortments of operating systems (OSs), and applications servers of every type imaginable. The complexity of networks is growing by leaps and bounds while the implementation and availability of security solutions correspondingly seems to grow by what sometimes seems to be creeps and crawls.

✎ According to the 2005 Network World 500 Research Study of 500 participating organizations (http://www.networkworld.com/pdf/nw500study05.pdf):

—Wireless LANs (WLANs) will be deployed within at least 73 percent of organizations by 2007

—82 percent will deploy IP VPNs in 2006

—64 percent provided business partner access to their networks

Today, enterprise networks are composed of numerous devices, differing technologies, and wide ranges of applications that always seem to be pushed to internetworking with Internet components, business partner systems, and even directly with customers.

The complexities of internetworking multiple systems and the accompanying information create great risk that organizations will not be able to address the security of new business demands and functionality.

The network perimeter is porous. In complex enterprise networks and in today's business processing environment, there is no longer a clear line between the good guys, the bad guys, and the incompetent guys. Access controls can no longer be plunked down on one system and successfully control access to all the enterprise information resources. Zones are a necessity in today's computing environment. The ever-increasing complexities of interconnected networks and the utilization of the Internet for business transactions has not only exposed organizations to the vast global array of threats from online ne'er-do-wells but also created an amalgamation of networks, people, applications, and systems that can each impact any other point on the network through one weakness. The concept of the weakest link in the chain has never been more compelling than in today's network environment. To successfully incorporate security throughout a complex network, there must be a common thread; centralized points of security management that can oversee, guide, and manage all the diverse environments.

Headless Servers

A server that lacks a monitor, keyboard, or mouse is typically called a *headless server*. A headless server can also lack a video card. Headless servers are being used more and more within organizations. They offer several advantages:

- Organizations save space by not having monitors, keyboards, and mice for the servers.
- Organizations do not need to purchase a monitor, keyboard, mouse, or cables and switches to support servers, saving what could be considerable amounts of money, especially in a multiple-server hosting situation.
- Organizations improve the physical security; with no keyboard, monitor, and mouse, an unauthorized person can do little with or to the system.

However, headless servers also present some new security challenges:

- Without a mouse, keyboard, or monitor, administration will need to be different than the traditional approach. Remote administration tools will need to be used.
- Because a headless server does not have an associated user, it must be authenticated at the device level rather than at the user level.
- When the headless server is unavailable, administrators must be able to perform remote-management and system recovery tasks through the network or other standard remote-administration tools and mechanisms.

> ✎ Just a few examples of remote administration tools include: terminal services, VNC, and Remote Administrator.

More organizations are using headless servers for the advantages listed earlier. These organizations need to ensure they have adequately addressed the identified challenges.

> Before launching a headless server, organizations must prepare the server to ensure it can be fully and remotely administered.

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 by leaps and bounds as organizations depend more upon Internet presence and online sales to boost revenues.

> ✎ According to the December 20, 2005 edition of the New York Sun, “For the first half of 2005, the Interactive Advertising Bureau estimates such [online] advertising was $5.8 billion. Online advertising appears to account for more than 5 percent of total advertising and to be growing much more rapidly.”

The increase in advertising and Internet sales demonstrates the growing dependence upon Web servers for Internet commerce. These Web servers are increasingly connected to enterprise networks in more locations and using more methods that increase the number of threats to the network information resources. Establishing consistent and centralized controls for all enterprise Web servers is essential for information security, regulatory compliance, and continued network availability.

> ✎ According to a November 2005 report from the United States Census Bureau:
>
> —Online sales accounted for $22 billion in retail activity in the third quarter of 2005
>
> —For 2005, online retail sales are projected to approach $90 billion (2.3% of total U.S. retail activity)
>
> —E-commerce is growing by about 25 percent annually

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 and requirements must be clearly documented and communicated to all systems and applications developers in terms applicable to the development processes. Such security requirements should be incorporated into the formal SDLC process in the same way that the business requirements and end-user requirements are defined.

The first phase in the SDLC is typically initiation. It is during this phase that an organization establishes the information security requirements. Such requirements must be based upon analysis of the application or system, and typically the requirements will be refined as the other SDLC requirements are refined. Normally the security requirements will be expressed at a high level, addressing the system or application objectives.

> ☞ An effective starting point for these high-level security requirements is the organization’s information security policies, procedures, and standards.

High-level requirements are the basis for creating more detailed functional requirements and specifications.

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.

Organizations are realizing that effective management is being accomplished best through identity management. Very generally, identity management establishes and controls identity changes and access rules to resources using a variety of centralized actions:

- User enrollment and provisioning
- Password management and personal information updates through self-care capabilities
- Privacy preferences management
- User profile management
- Credential management
- Identity policing management, such as access rights change processes, user ID creation, and password strength

There are notable benefits to using identity management systems to centrally control access across a variety of application types:

- Enables easier and more effective management of access control to applications, Web services, and middleware
- Provides a single point of access control decision for new and legacy applications
- Allows for more granular control of access to multiple system resources
- Creates the ability for end users to make access control decisions to private personal information
- Enables a single point of user activity monitoring and auditing
- Allows for single, or reduced, sign-on and entitlements

Typical Application Developers

Typical application developers are quite knowledgeable about their particular applications but unfortunately often do not truly have the security experience or knowledge for that application to make prudent security decisions. However, because of their knowledge of the applications, they often believe that they know all there is to know about security for the applications for which they are responsible. When there are no clearly defined policies or requirements for including information security within the development process, there is great risk that developers will create a new system without adequately building in information security—or will include security in such a way that creates weaknesses and exposes organizations to threats and legal noncompliance.

> ☞ Organizations must create and implement a clear and explicit set of information security requirements for application developers to use to ensure security is appropriately built-in to applications.

Organizations must not only provide clear direction to detail the security requirements for applications but also monitor compliance to ensure the security is actually being implemented. Organizations need to establish ways to monitor applications security development requirements.

> ☞ Organizations should periodically review user access authority to ensure it is limited to the minimum required access level based on job requirements. Such reviews will discover and appropriately limit the access of application development staff to sensitive system resources.

Because of the need to separate responsibilities between application development and production, organizations need to monitor access to production resources.

> 💣 Without monitoring and proper access controls, there is great risk that application developers with access to production programs and data could add, alter, or delete payroll and personnel information (for example) without being detected.

Encryption

No organization can completely defend against all threats; the number of potential risks and threats is generally infinite, and many (if not most) are unknown or unanticipated until after they have happened. Those unknowns are typically what wreak the most havoc on organizations.

Of course, organizations must implement appropriate safeguards to protect against threats and demonstrate due diligence. One of the best ways to protect information, particularly information such as personally identifiable information that is covered by multiple laws and regulations, from unknowns is to make it virtually incomprehensible and unusable to unauthorized individuals by encrypting it. Assume one of those infinitely unknown threats will visit an organization; having sensitive data encrypted will significantly lessen the business impact when it happens.

The Need for Encryption

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

> 💣 A large number of both commercial and freeware software tools allow information passing through a network to be intercepted and copied. These tools, commonly called sniffers, can be very beneficial for network administrators for troubleshooting. However, as you can imagine, in the hands of someone with malicious intent, any clear-text data—such as passwords and user IDs, credit card numbers, and other sensitive data—can be captured and, as an effect of these tools, no trail is created to indicate that the information was intercepted and copied. Imagine how many times user ID and password pairs may have been intercepted and then used to access databases with sensitive data without the knowledge of the legitimate account owner or the network administrator.

Contributing to these compelling technology factors is the exponentially growing numbers of regulatory requirements for organizations to implement safeguards to protect data more effectively than has been demonstrated in the past.

> The December 25, 2005 issue of Iowa's Des Moines Register reported 3000 Iowa State University (ISU) employees may have had their personal data viewed by hackers who gained access to two computers earlier in December. One computer held about 2500 encrypted credit card numbers of athletic department donors. The second computer contained clear text Social Security numbers for more than 3000 ISU employees. The intruder could not have read the credit card numbers because they were encrypted; however, the Social Security numbers are at risk of being inappropriately used. ISU officials said they would not contact police to try to find the identity of the intruder because it would be very difficult to track a hacker who could have come from almost anywhere in the world.

It is interesting to read about incidents and note that sometimes there are pockets of sensitive information that is encrypted while other times other equally sensitive information is not encrypted, all within the same organization. For example, in the December 2005 ISU incident, credit card numbers were encrypted but the Social Security numbers were not. This variance is likely the result of the strict and specific requirements from the credit card companies to encrypt credit card numbers while in storage, but the lack of similar explicit regulatory requirements to encrypt Social Security numbers while in storage.

Although encryption will not protect data from every type of incident—such as when authorized insiders abuse or misuse their privileges—it does provide protection by ensuring only authorized users with valid decryption credentials can see the data, and keeps inappropriate viewing and use from occurring when data is lost, stolen, or otherwise compromised. Just consider the June 2005 Citigroup incident in which a backup tape containing information about 3.9 million individuals was lost by UPS while in transit (see http://www.msnbc.msn.com/id/8119720). If the information had been encrypted, the incident would have had much less business impact to Citigroup, and would have presented significantly less risk to the individuals whose information was on the tape. Unfortunately, many organizations still consider current encryption solutions to be too complex to realistically implement enterprise-wide or to have too much of a negative impact on application and network response times. It will be interesting to see how encryption practices change throughout 2006.

> In August 2005, Forrester Research reported only 16 percent of North American companies implement data-at-rest encryption for their databases, and only 48 percent implement data-in-motion (network) encryption to support critical applications.

Legal Requirements for Encryption

In the ISU case, the fact that credit card numbers were encrypted on one system while the Social Security numbers were not encrypted on another system provides a classic example of implementing a narrow interpretation of doing only what is required by the "letter of the law" or the "letter of the contract" instead of implementing a wider interpretation of doing what is right according to the spirit of the law or performing due care activities to protect sensitive information.

Consider the PCI Data Security Standard (see a copy at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf), which requires cardholder data to be encrypted. If ISU wanted to process credit cards, they had to meet this standard. However, there are no laws that explicitly require Social Security numbers to be encrypted in storage. Even if this wasn't why ISU encrypted credit card numbers but did not encrypt Social Security numbers, it provides an example of a common practice—many organizations have only done, and make it a point to only do, the minimum required with regard to encryption (and any other security controls for that matter) as explicitly or specifically contractually or legally required.

Often in meetings with legal counsel and CISOs who are talking with their CEOs and CIOs, the legal counsel's strongest argument to not implement the security the CISO was requesting/recommending (even if it was a result of a risk analysis) was because it was not explicitly required by law or contract. Although this discussion isn't meant to be an argument against legal counsel, it demonstrates that their role within the organization is much different than an information security practitioner's role and often their bonus or pay is impacted by the amount of money they can save an organization by providing defendable opinions and reasonable interpretations that prevent excessive money from being spent.

☞ Identify the legal and contractual requirements for encryption to demonstrate the clear need for encryption solutions within the enterprise.

Need for Transparency

Currently, data is more commonly encrypted for remote access transmission instead of encrypted for storage. One common reason why is because 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.

✎ A virtual private network (VPN) is an example of a transparent encryption solution. Most VPNs are engineered in such a way so that authorized individuals do not have to do anything to encrypt data that is being transmitted using the VPN solution; encryption occurs automatically without any involvement from the end user.

As the perimeter becomes more porous, it becomes more important to encrypt data-in-motion, especially user IDs and passwords, within the perimeter as well as outside of it. Data-in-motion encryption will need to be completely transparent since a growing number of systems within the perimeter are headless, many applications are legacy, and modifying enterprise legacy systems is simply not an option in most cases.

The demand to encrypt data at rest (while in computer storage) has not been as great and, as a result, vendors have not provided easy-to-implement transparent solutions. DBMS vendors that offer encryption application interfaces (APIs) often require changes to the application, especially when joining multiple tables and scanning data using encrypted columns, besides requiring creation of stored procedures, triggers, and views. However, as more incidents occur with unencrypted data at rest and as more regulations require organizations to consider encryption as part of their compliance activities, organizations are asking vendors to make transparent data-at-rest encryption solutions available. Until transparent data-at-rest encryption solutions are available, though, most organizations are depending upon access controls to protect the databases and the applications that access them.

A data-in-motion encryption solution must be able to work with all OSs found throughout a heterogeneous network. A native IPSec solution has restrictions for the type and revision of OS that can be supported. Only the latest Linux OS uses native IPSec, potentially leaving a huge portion of the network vulnerable to attack. Encrypting the data communications requires providing end users with a transparent interface to access applications. If end users must use a different, separate authentication action each time a non-supported application is run, it is more likely the end user will decide to find a workaround or to find a way to bypass the additional security interfaces. In addition to this increased end user risk, additional training will be required for end users to ensure they know how to correctly and consistently use the encryption solution.

> ☞ Encryption solutions must be as transparent as possible to be as effective as possible.

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, as discussed in Chapter 2. Network intruders realize that they can gain access to internal corporate networks 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. However, as the number and severity of internal network attacks increases, organizations realize that using encryption is an essential tactic to prevent theft of intellectual property and personally identifiable information.

Encrypted data is hidden while it moves through the network from one point to another, such as a database to a client on an end-user computer or vice-versa. Encryption for data in motion should be done based upon risk to the information, for information transmission through the enterprise network, through the Internet, and through wireless networks.

> ✎ The most common data in motion standards include Secure Sockets Layer (SSL), Transport Layer Security (TLS), and IPSec. Most database vendors use the SSL standard. This standard allows data to be sent between client and database vendor through an SSL tunnel that encrypts the data using some combination of RSA, RC4, DES, or the Diffie-Hellman algorithm.

It is important to encrypt sensitive data in motion to prevent the data from being intercepted by someone also using the network as the data is going back and forth between the client and the database.

> ✎ Encryption helps to effectively prevent session hijacking, replay attacks, and access to user ID and password combinations.

To most quickly, easily, and cost efficiently meet the directives of enterprise leaders, systems administrators have typically chosen to use native IPSec, found in both Windows and the most recent version of Linux, to implement the enterprise encryption strategy. They do so because it is a proven standard, works transparently to users and applications at the network layer, and is well suited for enterprise use. Its weakness is in its deployment; it is difficult to administer and this difficulty increases exponentially as more servers are interconnected using it. Consequently, even though most organizations use it, it is used in small segments where the deployments can be managed manually.

> ✎ IPSec is effective for the inside of the network but is difficult to administer. SSL works well outside the enterprise, but presents difficulty within enterprise networks.

Organizations are increasingly using add-on solutions that are specifically engineered to encrypt data-in-motion within networks. There are many new data-in-motion add-on solutions that are quite good and some of these focus on making the deployment of IPSec simple and highly scaleable, providing the best of both worlds— a transparent infrastructure to encrypt data-in-motion without the pain of the deployment issues. Organizations should consider these when developing their enterprise encryption strategy. A few vendors that provide data-in-motion encryption solutions include:

- Apani Networks
- CipherOptics
- Ingrian Networks, Inc.
- OpenConnect Systems, Incorporated

Encrypting Data at Rest

One of the most important decisions when implementing a data-at-rest encryption solution is selecting which data to encrypt. 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. There are many possibilities for encrypting data at rest, including:

- Encrypt the actual database files at the OS level. Doing so provides protection from theft of the disk but can have a serious performance impact and does not provide for granular user access control.
- Encrypt on a column and row basis. This method is a more efficient and effective way to encrypt information in a database. This option requires tight integration with the database. However, if implemented properly, column- and row-level encryption solves problems that have stopped database administrators from implementing data-at-rest encryption solutions in the past.

Encrypt at the Network Layer

The ideal solution is to 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.

> ☞ Correctly implementing encryption within security zones can not only save time and costs but also mitigate the impact of a perimeter security breach.

Centrally Managing Solutions Is Crucial

Possibly the biggest challenge when implementing an encryption solution is solving key management challenges. Encryption implementations often hard-code the keys into procedures or scripts. This type of implementation will provide little security because reviewing the code will reveal the keys.

> 💣 It is critical for keys to be protected. Such protection must include encrypting the keys in storage and limiting access to only authorized owners.

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 any activity that can have negative impact on the business.

Personnel Monitoring

It is necessary to monitor business information processing to demonstrate due diligence, obtain evaluation information, and to comply with applicable laws and regulations. Doing so will often include some type of personnel monitoring. The types of employee information and methods for collecting it are quickly expanding. However, be aware that individuals are concerned with the monitoring that occurs—the growing number of court actions each year reflects this concern for workplace privacy.

Personnel Monitoring Examples

The following examples provide an idea of the breadth of concern and how court considerations are changing over time with regard to how monitoring activities within business are used to catch personnel doing bad things—supporting both the need for monitoring of some type in addition to addressing employee privacy protections:

United States v. Harrison, 1/13/04. A New York City Human Resources Administration (HRA) employee was arrested January 13 for an alleged multi-million-dollar tax and identity theft scheme. Veronica Harrison allegedly sold thousands of identities under the scheme, which involved filing thousands of false and fraudulent individual income tax returns in order to receive tax refunds from the Internal Revenue Service. Nineteen defendants were charged February 4, 2003, with engaging in this same scheme from 1997 through January 2003.

United States v. Fennessee, 1/8/04. A former employee of the Illinois Department of Human Services received a 2-year prison sentence for her role in an identity theft ring that stole personal information about state employees and used it to fraudulently obtain cash and personal property.

Haynes v. Kline, 12/23/03. A federal district court ruled that, even though a public employer's policy stated employees had no expectation of privacy in using their computers, it did not negate a staff attorney's expectation of privacy in electronic communications where he was informed during orientation that his computer contained private files inaccessible by others and there was no evidence that his employer had ever monitored or viewed other employees' private information.

Sieglock v. Burlington Northern Santa Fe Railway Company, 12/18/03. The court remanded the case, saying Burlington's faxing of 300 employees' confidential information might have subjected each to harm, and that Sieglock might be able to demonstrate relevant facts sufficient for a class action in Montana.

Privacy and monitoring at work is a complex subject. Organizations must determine the extent of monitoring controls and mechanisms needed for adequate security and demonstrated due diligence, and at the same time balance that with employee privacy needs. Technologies capable of invading privacy are being created every day and implemented by many organizations, typically not for the purpose of privacy invasion, but to improve the business efficiency, security, and controls in some way.

📖 Employee monitoring is not new. In 1913, the Ford Motor Company established a Sociological Department, which included monitoring activities to determine whether employees participated in activities for which Mr. Ford did not approve, such as gambling, smoking, drinking, or other unseemly and unapproved behavior; even during their personal time.

Over the years federal and state laws have emerged to address employee privacy rights. However, employee privacy issues are still gray with regard to many types of private information and personally identifiable information, such as, but not limited to, the following:

- Background checks
- Physical and work area searches
- Surveillance (closed circuit television—CCTV, videotaping, audio taping, hidden microphones, and so on)
- Location tracking (Smart ID cards, RFID tags, and so on)
- Drug and alcohol testing
- Biometrics
- Employee non-business information (memberships, activities, hobbies, and so on)
- Personnel files
- Telephone and cell phone monitoring
- Keystroke monitoring
- Electronic message monitoring
- Internet monitoring (Web sites, blog activity, and so on)
- Wireless monitoring
- Health information
- Physical mail
- Job applications
- Personality tests and psychometric or aptitude testing
- Packet-sniffing software
- Keystroke loggers

Laws, Regulations, and Guidelines

In 1996, the International Labour Organization (ILO), a United Nations agency promoting human rights, adopted a code of practice for protecting workers' personal information. The ILO code is the standard used by privacy advocates for protecting workers' privacy rights. The protections advise:

- Employees to be given notice of information collection processes
- Personal information to be collected and used lawfully and fairly
- Employers to collect the minimum necessary information required for employment
- Personal information should only be collected from the employee, absent consent
- Information to only be used for reasons directly relevant to employment, and only for the purposes for which the information was originally collected
- Information to be secured
- Employees should have access to their personal information
- Employee information should not be transferred to third parties without consent or to comply with a legal requirement
- Employees cannot waive their privacy rights
- Employee medical data should be treated as private and confidential
- Certain information, such as sex life and political and religious beliefs, should not be collected
- Certain collection techniques, such as polygraph testing, should be prohibited

Several United States laws provide for employee privacy rights in various ways. Just a few of these include:

- Americans with Disabilities Act (ADA) prohibits employers from asking certain questions about employees.
- Privacy Act protects against disclosures by government entities and applies to government employee information under certain situations.
- Electronic Communications Privacy Act (ECPA) prohibits intentional interception of electronic communications. However, it generally gives employers the right to access employer-provided voicemail and email systems. The constitutions and statutes of some states, such as the California Constitution, may restrict this right, though. Additionally, employers do not have the same right to access email that is outside the company's system, such as on another Internet mail server.
- National Labor Relations Act provides the framework for fair labor practices and labor organizing, which addresses some privacy issues.
- Employee Polygraph Protection Act protects private-sector workers from exposure to polygraph "lie detector" testing. Government employees and certain government contractors are still subject to examination.

- HIPAA has requirements for ensuring protected health information privacy and impacts health information monitoring for employers who are covered entities under this law, as well as employers who are plan sponsors to protect their employees' privacy.
- The Fair Credit Reporting Act (FCRA) regulates methods of obtaining credit information about an applicant or employee. See the Federal Trade Commission's fact sheet on what employers need to know about using consumer reports at http://www.ftc.gov/bcp/conline/pubs/buspubs/credempl.pdf.

Most states have laws that address employee privacy rights in one way or another. At least 31 states in the United States allow employees, and sometimes former employees, to review, and sometimes copy, their personnel files under specified conditions. For example, Alaska law gives employees and former employees the right to inspect and copy personnel files. All states have laws that cover and could impact employee surveillance, including telephone monitoring, CCTV, audio taping, videotaping and wiretapping. At least one state, Connecticut, requires employers to notify their employees of monitoring practices. Additionally employees may sue employers for privacy invasions under privacy torts. For example, such torts may include intrusion upon seclusion, public disclosure of private facts, and false light.

International Issues

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. There are several major issues you should consider for the privacy of your non-U.S. personnel. The following list provides a very brief discussion of some of the workplace privacy and monitoring laws; use this list as a springboard to launch your own research on applicable multi-national employee privacy requirements:

- In the United Kingdom, the Data Protection Act of 1998 regulates workplace monitoring. Detailed guidance for employers about how the legislation applies to monitoring at the workplace is set out in Part 3 of the Information Commissioner's Employment Practices Data Protection Code on Monitoring at Work.
- Although Germany does not have any specific legislation or codes of practice addressing workplace monitoring, employees (actually all individuals) have a right to privacy under the German constitution. The Federal Data Protection Act and Telecommunication Act also regulate workplace monitoring, and violations of monitoring prohibitions can lead to criminal prosecution.
- In Sweden, the Penal Code (Brottsbalken 1962:700) and the Data Protection Act (Personuppgiftslagen 1998:204) regulates monitoring and recording telephone calls and email. The Data Inspection Board published a report and guidelines relating to this area in 2003.
- In Italy, the main regulations for workplace monitoring include Sections 4, 8, and 15 of the Workers Charter and Sections 114 and 115 of the Personal Data Protection Code. Generally these, together with prevailing case law, protect employees from concealed workplace monitoring.

- In France, workplace monitoring is regulated by detailed legislation contained within the labour, civil, and criminal codes. The French Data Protection Authority has also published two reports containing guidelines on email and Internet usage.
- In Alberta, Canada, the Personal Information Protection Act, S.A. 2003, c. P-6.5 covers the information employers may and may not collect and disclose about workers.
- In Australia, Guidelines on Workplace E-mail, Web Browsing and Privacy, published March 30, 2000, is directed to organizations in both the public and private sectors.

Works Councils, Trade Unions, and Labor Unions

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.

Be aware that restricting employee communications may violate fair labor laws when there is interference with union activities. For example, in Pratt & Whitney, Feb. 23, 1998, the National Labor Relations Board (NLRB) reported in an advice memorandum that a company’s computer network was a “work area.” Accordingly, monitoring email on the company network for non-business use could be unlawful. Employee monitoring that can be considered as selectively punishing labor-organizing activities could violate the National Labor Relations Act (NLRA).

Know what personnel monitoring you can and cannot do. The following list highlights areas of consideration regarding personnel monitoring:

- Identify employee privacy laws and regulations applicable to the organization and worksites.
- Determine the employee monitoring activities and technologies needed to support business security and due diligence, and activities that could be considered as violating privacy rights.
- Know what personal information can be requested on job applications. For example, in the United States it is illegal to ask about arrests or charges but you are allowed to ask about convictions. Some states, such as California, have restrictions on using information about convictions. It is also illegal under the United States Americans with Disabilities Act, which applies to organizations with 15 or more employees, to ask job applicants if they have ever been treated by a psychiatrist. Some state laws also prohibit discrimination on the basis of disability for organizations that have fewer employees (for example, California applies to 5 or more employees).
- Be aware of the types of employee information that is gathered throughout the company, such as on sign-in sheets, forms of identification, records retrieval and use, photo images, and posting personally identifiable information on bulletin boards, in newsletters, in lobby areas, and so on. Determine the necessity for this information and revise processes where appropriate.
- Evaluate the risks for misuse when releasing employee personally identifiable information to third parties.

- Keep up with changing technologies and laws related to employee privacy and implement additional safeguards as necessary.
- If applicable, let your employees clearly know your company reserves the right to review and monitor all types of communications.
- Implement comprehensive employee privacy policies that include notice and consent language. Identify the activities or areas that are subject to monitoring and tracking. Be sure to address all types of information and monitoring, including monitoring of instant messaging, email, wireless communications, cell phones, work areas, phone conversations, Internet use, and other technologies and information storage media as appropriate.
- Establish procedures and safeguards for protecting employee private information and personally identifiable information in all forms.

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 and use to have an effective information security program. At a 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
- Monitoring the effectiveness of security controls
- Monitoring user access to mission-critical and sensitive information

Organizations must determine—based upon their industry, business services and goals, contractual requirements, network configuration, and applicable laws and regulations—what types of monitoring will provide the most benefit and are required.

Awareness and Training

For network security tools to be effective, the tools administrators and end users must be properly trained in how to use them. Awareness and training, in and of themselves, are also highly valuable, but sadly underused, network security tools.

Awareness and training are important activities and key components of an effective information security program. In fact, many regulations require awareness and training as part of compliance. Currently, the most commonly discussed regulations are HIPAA, the Sarbanes–Oxley Act, and GLBA. However, personnel education has been a requirement under other guidelines and regulations for several years. For instance, the Federal Sentencing Guidelines enacted in 1991, used to determine fines and restitution for convictions, have seven requirements, one of which is for executive management to educate and effectively communicate to their employees the proper business practices with which they must comply. Many issues that impact the severity of the judgments, along with accompanying sentences are information security activities.

Much has been written about the need for security and privacy education through effective awareness and training activities. A regulatory education program should address the organization’s interpretation of applicable security and privacy laws and regulations as well as support the activities the organization will take to mitigate risk and ensure security and privacy.

Executives must understand not only their own organization’s training and awareness requirements but also the related requirements and legal considerations of their business partners, subsidiaries, and parent company. Information security leaders must also consider the training and awareness requirements of applicable international laws and regulations. It is vital for organizations to evaluate, and to reevaluate, the effectiveness of these education programs. Too many organizations spend considerable time and money to launch awareness and training programs only to let those programs then wane, wither, and die on the vine because they did nothing beyond the big implementation; they failed to put forth the effort and activities necessary to evaluate, update, and modify their programs as necessary to be truly effective.

Organizations must spend time not only on creating awareness and training programs but also on evaluating the effectiveness of the information security education efforts. Organizations will find that as they make improvements based upon evaluations, training methods will be more effective.

Legal Considerations

Always include legal counsel in decisions regarding information security and privacy—especially the education program activities. It is important to have knowledge of 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 (HR) personnel. A plethora of international, federal, and state laws govern how personnel and individuals with access to personal and confidential information must be trained.

> Consequences of inadequate training span a wide spectrum, from regulatory penalties and fines all the way to lawsuits for failure to show due diligence by the training of employees and establishment of an environment that clearly has a standard of due care that is known to all personnel.

There are generally three ways in which an organization may legally establish the duty to train and make personnel aware:

- In certain industries, there may be a minimum standard of care that applies to organizational training and awareness programs. The standard of care is considered the level of activity and conduct expected of similarly trained professionals within similar organizations or industries; for example, in the healthcare and financial fields.
- A statute or a regulatory requirement may establish a standard of care that governs a specific type of information or specific type of industry. For example, the Children's Online Privacy Protection Act (COPPA) governs specifically how information must be handled and controlled, establishing a standard of care over that information. Such expected standards of care, often in combination with an organization's policies and published promises, can result in judicial decisions beyond applicable regulatory fines and penalties.
- An organization's own policies, procedures, and other practices can establish a standard of due care, especially when the organization clearly exceeds any applicable minimum regulatory or statutory requirements. Exceeding requirements can certainly help to draw more customers, establish a better public perception, and increase business competitiveness by showing the organization's concern about security and privacy, which is possibly greater than the competitors'. However, keep in mind that by doing so, the organization may establish a new, higher standard of due care with which the organization must comply. This higher standard could be considered within any potential and related legal action within which the organization is involved.

Summary

Many security practitioners are frustrated with trying to communicate the risks involved and threats to assets to decision makers, only to have the decision makers look at the bottom line cost and then decide it is worth a gamble that nothing will happen if it saves some money by not implementing controls. Some, perhaps many, business leaders are willing to gamble that the risks identified during risk assessments will not happen to their organization because the risk odds are unknown and cannot be communicated to them. However, good leaders do not want to be in noncompliance with laws or legal contracts and put the business at risk of significant negative business impact; or put themselves at risk of taking a potentially long vacation behind bars and/or selling their vacation homes to pay for fines and penalties.

Business leaders must be able to see the financial impact of a security incident or legal noncompliance upon the organization to understand the need for requested information security controls. One security breach can easily cost millions of dollars with impact lasting many years. When the cost of a security incident, and noncompliance with laws and contracts, is weighed against the cost of security solutions/tools, the security defense costs do not seem to be cost-prohibitive.

Exercises to project the cost of an incident and/or legal noncompliance as compared with the cost of controls can be a powerful motivator to executives. There are a number of impact calculators available. I created a comprehensive privacy breach impact calculator for my Privacy Management Toolkit; you can use a free scaled down version at http://www.informationshield.com/privacybreachcalc.html. Apani also provides a free, flexible security cost/benefit calculator at http://www.apani.com/tools/cost-benefit-calculator. Information security practitioners need to recommend what makes sense and is reasonable security-wise for their particular organization. Too many make the mistake of damaging their credibility with their business leaders by asking for large amounts of money to spend on security "solutions" just because it is a "best practice" or a "leading edge" security tool. Security must be implemented to the extent necessary to meet legal and contractual requirements, to demonstrate due diligence, and to mitigate risks to an acceptable level within the particular business environment.

All organizations must implement effective information security programs, which include the use of network security tools. Organizations need to realize that, even if they are not explicitly covered by laws and regulations and have made no data protection promises, they are still responsible for securing data and can be found liable if inappropriate access occurs for the information. Governments worldwide are becoming more proactive in addressing organizational information security problems, incidents, and practices.

✐ On December 1, 2005, DSW Inc. settled United States Federal Trade Commission charges that their data security failures constituted an unfair practice under federal law, ultimately allowing hackers to access the credit card, debit card, and checking account information of more than 1.4 million consumers that were in their systems. This is the seventh FTC case charging a business with failing to exercise due care to protect sensitive consumer information and having inadequate and faulty data security practices.

The proposed settlement would require DSW to establish and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards in addition to obtaining, every 2 years for the next 20 years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the order. The proposed settlement subjects DSW to standard recordkeeping and reporting provisions to allow the FTC to monitor compliance for 20 years.

The next chapter will discuss how to manage all these security tools, the security zones, the security layers, and compliance with data protection laws, regulations, and contractual requirements.