realtimepublishers.com™

The Definitive Guide™ To

Security Inside the Perimeter

Apani

Rebecca Herold

Copyright Statement

Chapter 7: Managing Internal Security

A comprehensive and effective information security program and supporting infrastructure is much more than just hardware and software components. Although most organizations wish there were such a thing, there is no magic information security silver bullet. Effective information security management requires the implementation and coordination of many components. Success requires vigilance by the information security group.

In addition to the motivations for individuals to compromise an enterprise information system discussed in Chapter 1, there are the mistakes and actions resulting from being uninformed that put an organization's information and network assets at risk. Managing enterprise-wide information security is a much larger and challenging task than just the subtask of managing the security of the network perimeter. Information security is a process, not a one-time achievement.

Management Devices and a Pure Perimeter Security Paradigm Is No Longer Effective

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

The growing number of reported incidents not only demonstrates the impact of multiple breach notification laws but also indicate that organizations may still be focusing on just securing the network perimeter and not sufficiently securing all information assets wherever they are located. The following list highlights a few such incidents that have occurred. As you read through the list, consider how they could been prevented if effective internal controls and security management devices had been in place:

- From Risks Digest, posted by Thom Kuhn, January 27, regarding the auto-complete email feature: "Awhile ago I was listening to a public affairs program on NPR. One of the speakers was representing a trade association, and his comments really got to me. I Googled him and sent him a somewhat venomous email. A few hours later, I got an even more venomous reply. End of story? Not quite. My email address was now in his shortcut list. A few weeks later, I was copied on what was clearly meant to be an internal and confidential email from this gentleman to his colleagues."

- Reported July 11, 2005 in eGov monitor: “Central government departments have reported to have suffered at least 150 cases of computer theft in the past 6 months, according to official figures. The Home Office alone recorded 95 incidents of computer items being stolen between January and June 2005—equivalent to a theft taking place in the department every other day. By comparison, the Ministry of Defense reported 23 computer thefts to date in 2005, down from a total of 153 in the previous year. Ministers made the disclosures in response to a series of parliamentary questions tabled by Liberal Democrat MP Paul Burstow. In a written answer, Doug Touhig, a junior minister at the MoD, said the Ministry had also experienced 30 attempted computer hacking incidents so far in 2005, having only reported 36 for the whole of 2004. However, the Minister gave an assurance that ‘none of the reported incidents of hacking had any operational impact’.”
- Reported May 17, 2005 in VNUNet: “Lax firewall security is leaving companies open to the installation of malicious software on their internal networks, a newly published Harris poll has warned. Fewer than half of companies block executable files from the Internet, and the same percentage fail to prevent such software coming in via instant messaging. Some 40 percent do not even block executables in email, the major cause of virus infections. The phishing threat was highlighted in the research as a major problem. More than 80 percent of those questioned indicated that their company had received phishing emails, and 45 percent said that employees had clicked through to the bogus Web sites. Lack of awareness is key to this problem, according to the poll. Two-thirds of employees claimed not to know what phishing is, and half of all companies admitted to having no Internet security training.”
- Reported December 15, 2005 in The Register: “One in five workers (21 percent) let family and friends use company laptops and PCs to access the Internet, dramatically increasing the chances of infection of the device and potentially the corporate network. This behavior also exposes work documents to prying eyes as well as increased malware infestation risks through use of a potentially unprotected home network connection. More than half (51 percent) connect their own devices or gadgets to their work PC and a quarter of these do so every day. Around 60 percent admit to storing personal content on their work PC. One in ten confessed to downloading content at work they shouldn’t. Spanish workers were the worst offenders at this with just under one in five (18 percent) admitting to downloading inappropriate content, behavior that leaves firms at heightened risk to both security attacks and legal sanctions. Two-thirds (62 percent) of those quizzed admitted they have a very limited knowledge of IT security. More than half (51 percent) of those polled had no idea how to update the antivirus protection on their company PC. Most errant workers put their firm at risk through either complacency or ignorance, but a small minority is believed to be actively seeking to damage the company from within. Five percent of those questioned say they have accessed areas of their IT system they shouldn’t have (including access to HR and accounting files), while a very small number admitted to stealing information from company servers.”

- Reported August 17, 2005 by Reuters: “A judge in New York has sentenced a former employee of America Online (AOL) to 15 months in prison for stealing 92 million screen names from AOL and selling them to a spammer. Jason Smathers, who pleaded guilty earlier this year and cooperated with prosecutors, expressed remorse for his actions and asked the judge for leniency. Indeed, the judge could have given Smathers 24 months in prison for his crimes, which included conspiracy and interstate trafficking of stolen property. AOL has said it suffered monetary losses of $300,000 as a result of Smathers’ actions. The judge in the case has given the company 10 days to prove those losses, after which he said he will impose a fine, hinting that he is leaning toward a fine of $84,000.”

All these incidents could have been at least mitigated, but most likely prevented, if more attention had been placed upon internal security safeguards and controls. The risky behaviors described could virtually be eliminated with an effective enterprise-wide information security management program.

Unfortunately, too many organizations still believe that the same security management devices used for perimeter security can also be used to manage internal security. Perhaps they can for some activities. However, these perimeter network devices have some serious weaknesses when it comes to securing internal network resources. As discussed in Chapter 4, the network needs to be segregated into security zones; Chapter 5 discussed the need to layer security. These security methods are effective, but the effective management of all of them in unison takes planning and foresight to enable the security to be the most efficient and simple as possible. This process involves more than just the comparatively simple plug-and-play management devices that were used in typical perimeter security implementations. To effectively manage internal security organizations must:

- Understand that managing internal network security is more complex than managing perimeter network security
- Consider the porous perimeter
- Establish enterprise-wide responsibilities
- Comply with contractual and regulatory requirements
- Determine the value of information
- Secure outsourced access to information assets
- Track security program progress and incidents

Managing Inside Is More Complex than Managing the Perimeter

Implementing and managing information security within the network perimeter is much more complex than just managing the security of the perimeter alone. This idea makes sense when you consider what is involved with managing perimeter security. Generally, perimeter security includes four basic components:

- Firewalls
- Proxy servers
- Intrusion detection, and increasingly intrusion prevention, systems
- Malicious code prevention

This comparatively limited number of components is easy for most security administrators to grasp. When adding internal information security management to the picture, most organizations will get a list of components that look something like the following:

- Firewalls not only on the perimeter but also deployed within identified security zones
- Proxy servers not only on the perimeter but also deployed within identified security zones
- Unified intrusion detection, and increasingly intrusion prevention, systems between security zones
- Malicious code prevention between security zones
- Consolidated management consoles
- Unified alerting and reporting
- Unified monitoring
- Encryption systems
- Access control devices and systems
- Audit capabilities
- Policies and procedures
- Application controls
- Network controls
- Systems controls
- And even more information security controls ad infinitum ad nausea

There truly are a limitless number of activities to address for internal security management. The delimited list of activities will be unique for each organization and will depend upon the unique threats, risks, locations, operating systems (OSs) and applications, regulatory and contractual requirements, and industry of each. Table 7.1 compares just a few of the general key security management issues and how they differ from perimeter-only security to enterprise-wide internal security.

Perimeter-Only Security Management	Enterprise-Wide Inside Security Management
Typically one small team is responsible for performing systems security administration for all perimeter security devices.	Multiple teams, typically a different one within each security zone, have their own specific systems security administration rights.
A single set of information security tools and systems are implemented.	The set of information security tools and systems deployed within each security zone may vary greatly based upon the security needs for each zone.
A limited number of audit trails are maintained for the perimeter devices.	A large number of audit trails are maintained throughout all the security zones, systems, and applications.
Overall goal is to protect access to corporate environment	Overall goal is to protect corporate and confidential data.
A limited number of applications and systems need to be secured.	A wide range and large number of heterogeneous systems and applications must be secured.
A small group of people with perimeter management responsibilities must understand and appropriately apply information security practices.	Everyone on the enterprise network must understand and appropriately apply information security practices.

Table 7.1: Perimeter-only vs. enterprise-wide security management.

Effective and efficient internal information security management requires:

- Defining security relationships between data, users, applications, and systems
- Segregating the network into security zones to facilitate effective management
- Enforcing the established security relationships within and across the security zones
- Regularly performing applications, network, and systems audits to ensure security relationships are enforced
- Updating security relationships as business needs, systems changes, and compliance requirements dictate
- Securing data in motion between and within segments and protecting confidential information as well as usernames and passwords
- Creating audit trails and reporting capabilities to demonstrate due diligence and regulatory compliance

Plan your information security infrastructure carefully. Remember, the more solutions you have, the more you need to manage. If you get too many different security tools and solutions, it is likely many will not communicate with each other and you will have a difficult time managing them all. Also, the greater the complexity and variety of management systems, the greater the likelihood of inadvertently leaving a security hole that could expose confidential information or systems. Without proper management, your information security efforts will be ineffective, and ultimately, you will damage your information security program by having it viewed as being too complex, too expensive, and ineffective to boot. Transparency is also important here, as the more intrusive security systems are on users, the greater likelihood of them being circumvented.

Before making an information security management decision and purchase, research the interoperability issues. Many of the current security products are designed to work on a standalone basis and do not work well with other security solutions. For example, some personal firewall programs intended to protect roaming users with VPN connections do not work well with VPN clients.

Although multiple products working together provide a strong security infrastructure, not all solutions work well together.

The Porous Perimeter Must Be Considered

The perimeter is porous. Wireless connections, mobile computing, Web-based applications, back-office connectivity, and connections to business partner and outsourced vendor networks have eliminated the once clearly defined network perimeter. With all these complex relationships, it is difficult to tell who should have access to network components and who needs to be blocked. There are so many ways in which networks can now be accessed that information security management has become more challenging than ever before.

The Information Security Leader's List of "Things That Keep Me Up At Night"

- Wireless networks
- Remote and mobile users
- E-commerce and Web services
- Email attachments and hidden spyware
- Corporate spies
- Disgruntled employees
- Bribed security administrators
- Social engineering and gullible personnel
- Attackers setting up rogue Wi-Fi access points near hotspots tricking users into logging onto their networks
- Newly found security vulnerabilities and how to best apply security patches
- Malicious code
- Outsourced vendors with access to enterprise systems and/or information
- Careless disposal of sensitive information
- Consultants and contract workers attaching their computers to the enterprise network
- Unencrypted data on multiple backup tapes and media

Firewalls, once considered the network security savior, are now mere islands of security in an ocean of threats; they will stop a small percentage of enterprise information pirates, but many more threats exist to the internal network than firewalls alone can stop. Various studies demonstrate how porous the perimeters of almost all enterprise networks have become:

- The CERT/Secret Service 2005 Insider Threat Study reported the predominant means of executing an insider attack was through remote access.
- A 2005 Nemertes Research study reported that 90 percent, on average, of employees work away from the business facilities. Another 2005 Nemertes Research study reports there has been an 800 percent increase in virtual (remote) employees based in different geographies from their managers and peers, from 2000 to 2005.

The fact that organizations today are predominately in part virtual, with IT, sales, support, and executives potentially scattered all around the world has blurred the network perimeter to such a degree that it truly is very difficult to determine where the “workplace” really is. Organizations must understand that in today’s world, it is not a question of “if” unauthorized individuals will penetrate their perimeter; it is a case of “when”. Inside the perimeter must be treated with the same level of security as has traditionally been provided to the “outside”—including access control and encryption.

Enterprise-Wide Information Security Responsibilities Must Exist

For many years, organizational leaders have regarded the IT unit as being the only area needed to manage and address all information security issues without any need for input or cooperation from other areas of the enterprise. Many business leaders mistakenly believed the only threats to data were electronic threats. As more accountability is created for business leaders to ensure information security, and as they then become more aware of the related issues, they are starting to understand that information security must be integrated throughout the entire enterprise. To be most effective in integrating information security responsibilities throughout the organization, two very important factors must exist:

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

Security Goes Beyond Technology Products

Simply implementing firewalls, VPNs, IDS servers, and auditing products will not create a secure environment. Unfortunately, many organizations believe this product implementation is all they need to do and, as a result, many have experienced some significant information security incidents. Technology tools certainly are part of the solution. However, risk assessment, information security strategy, operational procedures, security education, and appropriate personnel behaviors are also necessary components.

Education Is Imperative for Success

If you expect information security to be addressed enterprise-wide, you must implement an effective information security awareness and training program to educate all personnel about their responsibilities and policies and procedures. Awareness must be an ongoing activity. Training must be regularly provided and mandatory. Executive leaders must actively support these efforts.

The enterprise information systems and information assets are not secure until all personnel know and understand the importance of securing information and network resources as it relates to their job activities. People truly are the weakest link in enterprise information security programs.

✎ According to the Deloitte 2005 Global Security Survey:

Only 65 percent of organizations have trained their personnel how to identity and report suspicious information or network-related activity.

Only 6 percent of organizations provide information security education as part of the new hire orientation.

Even though 86 percent of organizations are concerned with employee misconduct involving information systems, the amount of funds allotted to the awareness and training budget was less in 2005 than it was in 2004.

You cannot expect your personnel to know how to do the right thing if you do not effectively teach them what the right thing is to do!

Centralization and Decentralization

As discussed in Chapter 5, a centralized security management area with ultimate enterprise-wide security oversight has distinct benefits to organizations, including increased security efficiency, economy of scale for security implementation, and the ability to enforce security requirements centrally through monitoring, evaluation, security activity, and program updates.

There are also appropriate activities that through divide-and-conquer methods can be made more efficient and effective. Decentralized security management will help to ensure appropriate and cost-effective security is addressed within each of the organizational business and operations areas. It can also be used to more effectively ensure appropriate authorization is given to personnel based upon their job functions and to more effectively incorporate security into all the business processes.

The key is to identify those activities that are best performed centrally and which are best performed within each of the business units. The right combination of the two will lead to cost reduction, better risk management, regulatory compliance, and more effective security operations.

Cost reduction through the right combination of centralization and decentralization can be achieved in such areas as:

- Password resets
- Demonstration of compliance with enterprise policy and security/privacy regulation
- Awareness and training
- Adequate service level provision
- Access administration
- Acquisition and maintenance of security solutions
- Account disablement for dismissals and job changes

The right combination of centralization and decentralization can also result in better risk management practices, helping enterprises better address the following questions:

- Who can access the enterprise's sensitive information databases and intellectual property?
- What is the enterprise's vulnerability to new or existing threats?
- What is the state of the enterprise's compliance with its own security policy, guidelines, and procedures, and how can compliance be enforced?
- How quickly can the enterprise react to new threats (assessment, solution design, solution testing, and solution/patch implementation)?
- How can the enterprise mitigate the security weaknesses inherent in users having to remember multiple user IDs and passwords?
- How can the enterprise be confident that its systems are configured securely, as the IT professionals doing so are not necessarily security professionals?
- Are user actions contributing to, or detracting from, security?

Contractual and Regulatory Requirements

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

Contractual Requirements

Unfortunately, many information security leaders have not been informed of, or have not thought about, the types of safeguards they must put in place to comply with existing third-party business partners. Visa provides a good example of the importance of contractual requirements for information security.

When Visa announced the Visa Cardholder Information Security Program (CISP) in April 2000, and mandated compliance by June 2001, the organizations that processed credit card purchases suddenly realized the importance of such contracts. Visa gave merchants and service providers until September 30, 2004 to submit their compliance documentation.

✎ The Visa CISP requires organizations to implement security to comply with 12 basic security requirements, including implementation of appropriate physical and logical controls and performance of regular audits. The program also requires organizations to immediately report security incidents as well as be able to investigate and take appropriate action to limit exposure of cardholder information. Organizations in compliance are automatically indemnified against any fines.

All entities that stored, processed, or transmitted Visa cardholder data were required to comply with CISP and were responsible for ensuring the compliance of their merchants or agents. If organizations did not comply, Visa contractually reserved the right to fine them up to $500,000 per incident. Very large organizations were scrambling to comply with the Visa requirements because they had been notified, after sending a perfunctory checklist to Visa to demonstrate their compliance, that they needed to provide solid documented evidence of their compliance or they would have their ability to process Visa card payments discontinued.

✎ On December 15, 2004, credit card associations created a set of industry security requirements referred to as Payment Card Industry (PCI) compliance. Generally, the agreement among the credit card industry was that, if a merchant is Visa CISP compliant, MasterCard, American Express, and Discover would honor the CISP compliance and consider the company PCI compliant.

In the past few years, I have performed many security reviews for organizations’ business partners, and almost all the contracts the organizations had with the third parties contained some very clear information security requirements within the Master Service Agreements (MSAs). However, upon speaking with the third-party representatives responsible for information security, I found that only a small handful were even aware that the MSA contained such information security requirements.

In today’s business environment, contracts with third parties should include requirements to protect information. A breach of contractual requirements could result in a costly court action.

✎ Organizations must include information security requirements within the contracts they have with their business partners and know their contractual information security obligations.

Regulatory Requirements

Governmental regulations cover almost all aspects of corporate operations, scrutinizing and controlling everything from how the physical security of computer labs are managed to how new employees are trained on security responsibilities. Security management is at the heart of almost all data protection regulations. Without a strong security infrastructure that protects systems, applications, data, and processes from unauthorized use or access, compliance with any regulation is very difficult. The requirement for strong security management cuts across all major regulations.

Staying on top of legal and regulatory compliance is a comparatively new, but hugely important, task for managing internal security. Table 7.2 provides a high-level overview of the information security requirements of prominent laws and regulations.

Regulation	**Example of Information Security Management Principles Covered**
Sarbanes-Oxley Act (SOX)	Continuity of secured network operations Data confidentiality Data retention Detailed auditing capability Enterprise and application-level policy enforcement Secured information access
Gramm-Leach-Bliley Act (GLBA)	Application-, systems-, network-, and data-level security Data confidentiality Data secured in transit Detailed auditing capability Security and integrity of stored data
Health Insurance Portability and Accountability Act (HIPAA)	Application-, systems-, network-, and data-level security Authentication and access controls Data confidentiality Data retention Data secured in transit Detailed auditing capability Security and integrity of stored data
California State Bill 1386 (CA SB 1386)	Alerting capability with reporting Confidentiality of personal data Detailed auditing capability Detailed policy controls Monitoring capability Notification procedures Personal data secured in transit Security of personal data in storage

Table 7.2: Overview of the information security requirements of prominent laws and regulations.

As you can see, there are some very apparent commonalities between these regulatory requirements. This chapter will discuss this idea in detail a little later.

And Many More Regulations Worldwide

The number of data protection regulations is increasing rapidly. It seems a week does not go by without reading about a new proposed bill or law. Just a few of the other existing laws and regulations impacting information security management, beyond those discussed earlier, include:

- Canada: Personal Information Protection and Electronic Data Act (PIPEDA) of 2000
- European Union Data Protection Directive of 1998
- Japan: Personal Information Protection Law of 2005
- Australia: Privacy Act of 1988
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) of 2001
- Children Internet Protection Act of 2001 (CIPA)
- Fair Credit Reporting Act of 1999 (FCRA)
- Children Online Privacy Protection Act of 1998 (COPPA)
- Privacy Act of 1974

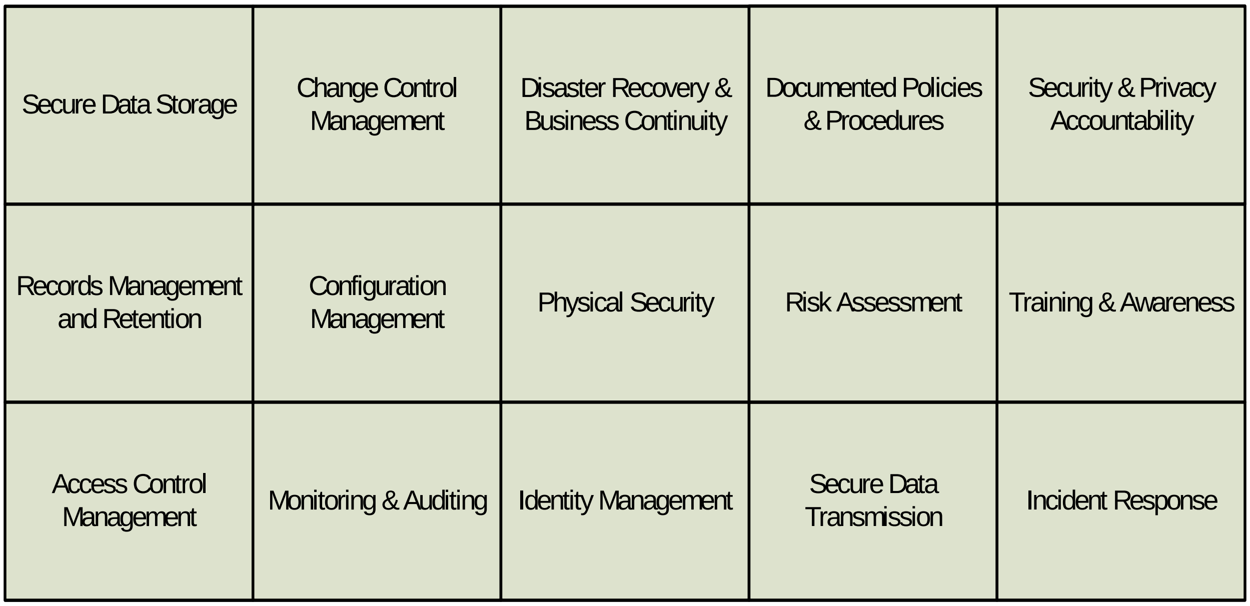
> ☞ Effective information security management practices must include a way to stay up to date with all the laws and regulations that apply to the enterprise.

Common Regulatory Data Protection Requirements

In a panic to answer corporate executives' questions regarding their accountability requirements for specific information protection practices, and meet the "letter of the law" for each individual regulation, many information security and privacy professionals have been trying to address regulatory requirements in a piecemeal fashion, looking at one law, and the corresponding minute applicable detailed requirements, at a time. This practice is not only stressful to those responsible for compliance but also generally inefficient.

As Table 7.2 demonstrates, when you examine the multitude of data protection laws and regulations, common themes of information security requirements reappear. By viewing these commonalities between the regulations and managing information security to them, then addressing any outstanding specific requirements within any one particular law, information security management will be much more effective.

Figure 7.1 illustrates common information security management areas covered by most of the major regulations. Although each regulation typically includes specific differences within these areas, a common requirement of all regulations is for organizations to have implemented a strong set of information security controls and practices to protect critical enterprise information assets. A strong information security management platform is necessary to achieve this requirement.



Secure Data Storage	Change Control Management	Disaster Recovery & Business Continuity	Documented Policies & Procedures	Security & Privacy Accountability
Records Management and Retention	Configuration Management	Physical Security	Risk Assessment	Training & Awareness
Access Control Management	Monitoring & Auditing	Identity Management	Secure Data Transmission	Incident Response

Figure 7.1: Common information security regulatory requirements.

Determining the Value of Information

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

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

Information Valuation

So what is the value of information? There are few, if any, organizations that do not place a high dependency upon information for their business success. This dependency alone has great value.

There are many types of enterprise information, including customer data, patient files, accounting records, Human Resource files, marketing plans, product designs, emails, and basically an infinite number of others.

The amount of information within an enterprise is growing exponentially. Consider email. According to IDC, a typical 1000-user organization generates more than 3 terabytes (TB) of email data annually. CIOs, CTOs, legal, IT departments, and enterprise managers in every industry must address the growing challenge of complying with multiple regulations that cover the types of information found within email messages.

> 📖 IDC reports the current (2006) number of daily emails worldwide is 35 billion.

The value of information is greatly impacted by the state, federal, and regulatory requirements governing the management and safeguarding of information. Noncompliance with those information-handling directives can, and has, cost organizations millions of dollars. The value of each kind of information changes as it goes through its life cycle. The usefulness of information typically lessens. However, the financial impact of a breach to sensitive information can be as damaging no matter where in the life cycle information is.

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

Considerations for Outsourced Access to Information Assets

Many organizations are outsourcing very specialized data processing and management activities in an effort to save money or because they just don’t have the resources, experience, or capabilities to do it themselves. Organizations also often outsource to get specific expertise that they may not possess and cannot afford to hire full time. Organizations that outsource application programming probably expect that the individuals doing this work will know about application security and will incorporate it into the product they create. These same organizations probably also expect the individual to know how to protect information in a shared customer environment; making sure that the code created for the organization is not accidentally sent to another customer, and so on.

When an organization entrusts third parties with the organization’s confidential data, they basically place all direct control of security measures for the data completely into the hands of someone else. That trust cannot be blind. Numerous recent security incidents have resulted from loose security practices within outsourced third-party organizations:

- Reported January 12 2006: UPS lost People’s Bank computer backup tapes containing clear-text information about approximately 90,000 customers.
- Reported December 16, 2005: DHL lost an ABN Amro computer backup tape containing clear-text information about approximately 2 million customers.
- Reported March 17, 2005: A computer at Boston College with access to an alumni database was infected with a virus that might have exposed personal information about more than 100,000 individuals. According to officials at the college, the computer was operated by a third-party IT service, which officials declined to name.
- Reported May 2, 2005: Iron Mountain Inc., lost Time Warner Inc.’s computer backup tapes with clear-text Social Security numbers and names of 600,000 current and former employees and dependents. This was the fourth time so far in 2005 that Iron Mountain lost tapes during delivery to a storage facility.
- Reported October 7, 2004: A Pakistani transcriptionist (a subcontractor) hired to transcribe records for the University of California San Francisco (UCSF) Medical Center, informed UCSF via email that she would post its patients’ private medical records on the Internet if she was not paid for the work she was hired to do by the company she was subcontracted by—Texas MT. Texas MT was subcontracted by a Florida subcontractor, Sonya Newburn, who was hired by a Sausalito, California company, Transcription Stat, which was contracted to provide transcription services to UCSF.

When organizations outsource critical data processing and management activities, they must implement measures to stay in charge of their own business data security and minimize business risks. Many organizations indicate the security issues related to outsourcing are a big concern. Alarmingly, it seems few organizations actually address this issue.

✎ In a May 15, 2005 CIO Magazine article titled “Don’t Maroon Security,” Atul Vashistha, CEO of NeoIT, an offshore outsourcing consultancy, said, "I'd say fewer than 20 percent of my clients audit the security of their providers. They just accept the suppliers' defined security plan and don't check to see if they are living up to it." Steven DeLaCastro, a consultant with offshore outsourcing company Tatum Partners, indicated he believes it is more like 10 percent. "Sarbanes-Oxley requires the right to audit outsourcers, yet companies aren't putting [audits] into the contract," he said.

How do you know the third party is complying with your regulatory responsibilities? How can you demonstrate to regulators that you are in compliance when someone else possesses your data? You need to hold third parties to strict security standards. In many instances, such standards will be more stringent than your own organization’s security requirements.

The measures you take to make sure your business partners are taking appropriate actions to protect the data with which you've entrusted them depends upon the situation and existing legal restrictions. The following list highlights general actions you should consider taking:

- Require a potential third party to provide a copy of a recent security audit of their operations that was performed by an independent reputable party. Even if the audit is broad, it will demonstrate they have gone through an audit by a reputable company.
- Require third parties to complete a security self-assessment questionnaire, provided by your company, about their information security and privacy program. When creating this questionnaire, it is an effective practice to structure the questionnaire around the ISO/IEC 17799 topics as they apply to third parties protecting another company's information.
- Include security and privacy requirements within the contracts you have with third parties. Include enough detail that you cover all issues but don't be so specific that you allow them a way to avoid doing a security activity just because you did not specifically state it within the contract. Include within the contracts citations of the specific laws for which your company must comply that the third party must also then comply with.
- Require third-party personnel to have training for appropriate security practices prior to handling or accessing your company's information. Don't limit the training to electronic data; if they handle storage media such as paper documents, make sure it is covered in the training. Require regularly scheduled training and awareness to occur following the initial training.
- Review the third party's information security policies. Ensure the policies cover all the topics related to the activities they are performing for your company. Ensure the wording is strong enough to actually impact the personnel activities. Look for executive endorsement of the policies and for clearly stated sanctions for policy infractions.
- Require an abbreviated form of the self-assessment form, a type of information security and privacy attestation, again provided by your company, that they must complete each month, have their executives sign, and submit to your company as a requirement of continuing to do business. The signatures and contract language will help to demonstrate due diligence on the part of your company and will also hold the third party to a legal standard of due care.
- For third parties handling particularly sensitive and/or regulated information, require a clean-room environment to keep information from walking out the outsourced company's door. In a clean-room environment, all the machines and output devices except for terminals are disabled. Copies of data cannot be made, hard drives cannot be used, PDAs cannot get information downloaded from any of the computers, and data is otherwise not available for downloading, printing, copying, or accessing beyond the contracted purposes. The servers reside in your country of residence. There is no way for the information to leave the outsourced company. Typically, in such arrangements, the outsourced company's employees are physically searched when entering and leaving. These are very strict precautions, so they will not work for every company, but they definitely should be used if your level of risk warrants such measures.

- Limit the amount and types of information the outsourced personnel can see based upon the business needs. For example, if the outsourced company verifies a customer is a good credit risk, don't send all parts of the application; just send the information required to approve the application.
- Require criminal and, where appropriate, financial checks to be performed on the third-party personnel prior to their hire. No matter how many safety precautions are taken, it's difficult to stop an opportunist who will steal data for money, revenge, or some other reason. Ensure that the people handling your data have not been convicted of criminal activity that would make them a high risk for handling your data. This may be tricky in some countries because records of criminal activity may not be centralized or such information may be labeled differently. As mentioned earlier, and worth emphasizing again, make sure the outsourcing workers are trained properly about procedures and legal consequences.
- Make sure none of your disgruntled ex-employees are now employees of the organization to which you are outsourcing your data handling. Such situations have led to devastating situations for companies.
- Send personnel from your company to visit the outsourcing sites regularly to view the facilities, meet employees, and monitor employee turnover and subcontracting activities.
- Find out how the third party screens and monitors employees. It is ideal to require that they perform criminal, credit, and reference checks as part of their background check process. However, this is not possible in some countries that do not have a centralized criminal database system. It is also not possible in some countries where doing such checks are against their privacy laws.
- Obtain documentation for how the third party will handle a system breach. Formal breach identification and notification procedures should exist.
- Determine where disputes will be resolved. Have you contractually required that any legal actions will be resolved in your jurisdiction? Make sure you discuss this carefully with your legal counsel.
- Ensure the third party has liability insurance and identify what the insurance covers. If there is a problem that occurs with your information while in the third party's control, liability could rest with your organization—and will likely rest with your organization if the third party is located outside your country.
- Identify the laws and regulations that apply if a system breach occurs at the third party.
- Determine whether your organization's liability insurance covers outsourcing activities.
- Contractually require the third party to obtain your organization's authorization before they subcontract any work that involves your organization's information or access to your systems.

Common Weaknesses

The following list notes recurring vulnerabilities for third parties; be sure to pay particular attention to these:

- The information provided within the vendor's security self-assessment responses often does not match the security requirements within the third party's security policies. For example, the respondent for the self-assessment may indicate the passwords used are a minimum of six characters, but the policy may indicate passwords must all be a minimum of eight alphanumeric characters. Such conflicting information should raise a red flag for you; it may indicate the third party does not enforce compliance or communicate the security policy requirements to its personnel.
- The third party may be subcontracting the processing of your data to yet another company that does not have good security practices and/or may be located in a different country from yours or the third party. Be sure to cover this within your contract with the outsourced company.
- The third party may not have any security policies or controls in place for mobile computing devices (laptops, PDAs, Blackberries, smart phones, and so on) or for their employees who work from home. However, they may have personnel who use these types of computers to process your data. Be sure appropriate security is in place for such situations.
- Business continuity and disaster recovery plans are often either missing or were written several years ago and never tested. Make sure the third party has up-to-date plans in place and tests them regularly.
- The third party may have been involved with a security or privacy breach. There are multiple services you can use to check on this in addition to dozens to hundreds of useful Web sites to search for news about the third-party company and any security breaches for which it was involved. If you find the vendor had a breach, be sure to ask the company about it and find out what actions they have taken to prevent such a breach from occurring again.

- A few of the sources to check whether an organization has been involved in a security or privacy breach include:
- http://www.google.com
- http://www.bna.com for the Privacy and Security Law Report
- http://www.ftc.gov
- News sites such as http://www.CNN.com
- http://www.supremecourtus.gov (Supreme Court Cases)
- http://www.virtualchase.com/resources/criminal_records.html (Criminal Records Check)

- Encryption is often not used to protect information in storage, in transit, or on mobile computing media and devices, such as laptops, PDAs, backup tapes, USB drives, and so on. Be sure encryption is used by the vendor to mitigate the risk involved in such situations and when the company is storing information from other companies in the same servers as they are saving yours.

Tracking Progress and Incidents

Unfortunately, information security leaders cannot track their success and progress with information protection initiatives. Not only is it wise and necessary to track information security progress and incidents in order to have an effective information security program, it is a requirement of many laws and regulations. The following regulation examples illustrate this requirement:

> The HIPAA Security Rule requires covered entities in § 164.308 Administrative Safeguards:
>
> *(a)(1)(ii)(D) Information system activity review*
>
> *(Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*
>
> The GLBA Safeguards Rule requires covered entities in § 314.4 Elements:
>
> *(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.*

Effective information security leaders will establish formal monitoring and program evaluation procedures and implement appropriate tools to help them keep up with the day-to-day status of their enterprise information security posture.

Items to Monitor and Log

There is a wide range of activities throughout your enterprise you will need to monitor, and multiple types of activities you will need to log. These will not all be electronic based. You should have identified many of them while establishing your security zones (discussed in Chapter 4) and implementing your layers of security (discussed in Chapter 5).

> Carefully consider the cost, resources, and liabilities associated with each considered logging and monitoring activity.

The following list highlights items most organizations will need to log to meet compliance with a wide range of regulatory requirements and keep up with an ever-changing network environment in which new threats are introduced every day:

- Email messages and activity
- Paper mail
- Work areas
- Log-in attempts
- Voice communications
- Access to personally identifiable information
- Software and system vulnerabilities and patch updates
- Malicious code (viruses, Trojans, spyware, worms, and so on)

- Personnel awareness and training activities
- Network and remote access points and connection activity
- Mobile device inventories
- Business partner contracts
- Enterprise-wide compliance with the organization’s policies
- Authorization capabilities
- User access capabilities
- Backup tapes and media
- Disaster recovery plans and sites
- Systems administrator activities
- Intrusion detection and intrusion prevention systems
- Data and media disposal records
- Regulatory compliance

As you can see, this list covers all the layers of security you need to have implemented throughout your organization.

> ✎ The logging and monitoring activities you implement within your organization need to be determined based upon an analysis of the risks to your enterprise’s unique network and systems environment.

Auditing and Tracking Mechanisms

Establish auditing and tracking mechanisms for personally identifiable information and other sensitive and mission-critical information. Doing so will likely require one or more of the following:

- Audit software and systems
- Database logs
- Servers dedicated to housing the audit and monitoring logs and information
- Secured physical locations to house the audit and tracking information
- Sign-in sheets
- Closed circuit television and other surveillance equipment

Summary

If all you do is protect the perimeter, you will lose the information security battle. Effective information security management requires security throughout the entire enterprise. To effectively manage internal security organizations must:

- Establish information security management with the understanding and expectation that it will be more complex than simply managing perimeter network security
- Realize the network perimeter is increasingly porous and address all the many ways in which threats can enter the insider of the perimeter as well as mitigate the risk within the perimeter when it is penetrated
- Establish a comprehensive enterprise-wide information security framework that includes not only centralized responsibilities but also decentralized information security functions
- Identify, understand, and take action to comply with contractual and regulatory data protection requirements
- Identify and inventory the information stored, handled, and processed by your organization, then establish appropriate security for the information based upon the determined value
- Take action to ensure the security of information assets that are handled, stored, or accessed by outsourced business partners
- Ensure that—as much as possible—your security elements are automatic and transparent to users.
- Track and monitor information security program progress, security incidents, and incident resolutions

The next, final, chapter will discuss how to put together the ideas and practices discussed so far into an effective enterprise-wide information security management plan.

Download Additional eBooks from Realtime Nexus!