2

The Security Review Process

"I was caught breaking into a DMZ with a loaded URL—What are you in for?"

2.1 Introduction

It is 1860, and you are the bank manager. Your number-one goal is to keep the money safe. What steps will you take to keep the money from the men in the black hats? Some of these steps may be to understand how the bank will be robbed:

- Will the robbers enter by the front door?
- Will they enter by the back door?
- Will they try to use explosives on the safe?
- Will they use "social engineering" to get the money? "Joe sent me down to get his money. Give it to me and I will give it to him in the bar."
- Will they try to use someone on the inside to help get the money?

Next, the manager will determine what steps are needed to keep the bad guys out:

- Use a safe with a combination lock.
- Put bars on the door.
- Get a security guard—Hire a gun slinger.
- Keep a gun and use it if needed.
- Train employees how to keep the money safe.
- And, most important, make sure that the bank manager knows the sheriff.

You will need to take similar action as the owner and/or manager of your network infrastructure. Using the following five steps will get you started with your security review:

1. Start by reviewing the current state of the business.
2. Analyze the technology currently being used.
3. Start a risk analysis process.
4. Create the plans.
5. Begin your security implementation process.

Each step will link into a succeeding step. This approach should be used for each process or department within the business, as well as for the holistic enterprise.

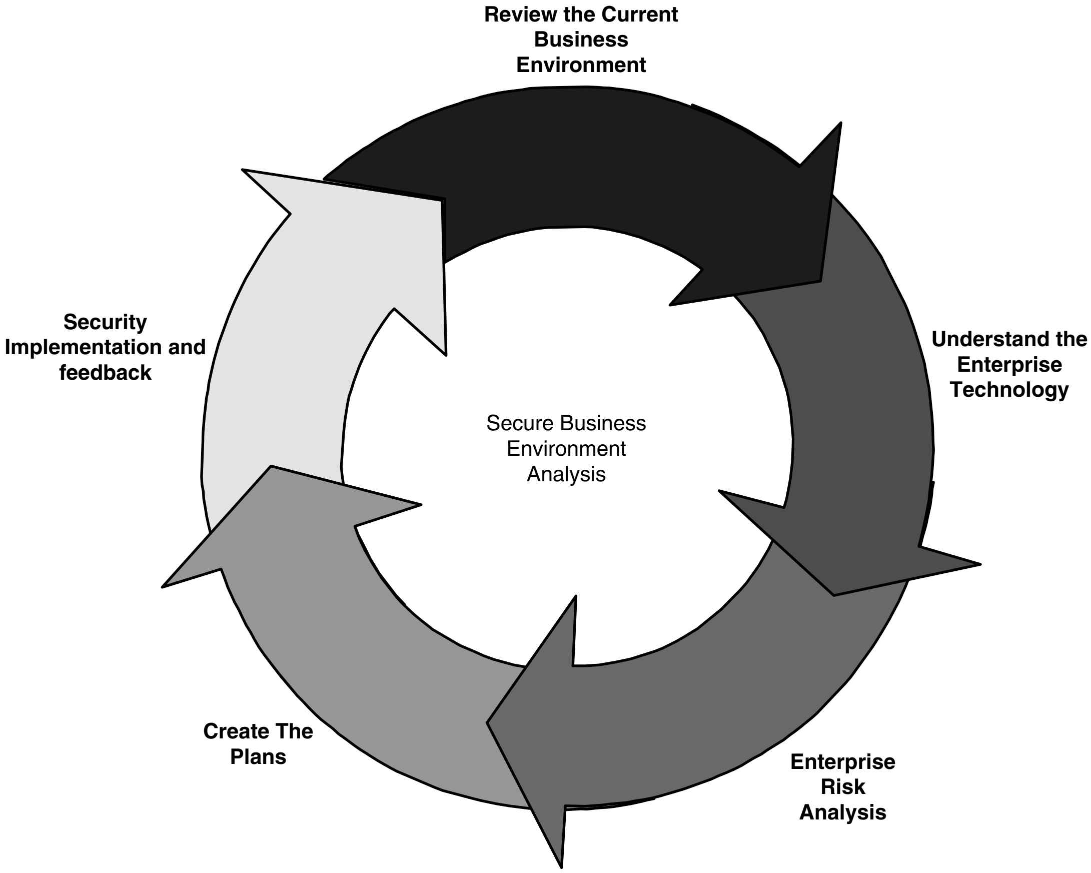

Review the Current Business Environment
Understand the Enterprise Technology
Enterprise Risk Analysis
Create The Plans
Security Implementation and feedback
Secure Business Environment Analysis

Figure 2.1

2.2 Review the state of the business

In most companies some type of systemic security is already in place; it is unlikely that you will need to start your security analysis from scratch. An evaluation must be performed to allow you to review the security already in place relevant to current security requirements.

The following steps will help you identify the security requirements for your Internet interfacing enterprise:

1. Identify the core business.
2. Identify the stakeholders.

3. Compile customer demographics.
4. Identify the vendors and business partners.
5. Identify the competition.
6. Identify industry trends and standards.

2.2.1 Identify the core business

Unless you are a business consulting company and/or a security software vendor, security is likely not a core competency of your business. One of the biggest mistakes companies make is that they start with security first and look at the business after the fact. When asked, "Why did you install a firewall?" the answer is commonly, "Well, because we needed one!" The next question, "What policies did you use to determine that you needed a firewall and what procedures did you use to effectuate that decision?" may elicit the response, "Well, because we thought we needed a firewall." Following are the questions a business should start with:

1. "What are we protecting against?"
2. "What segments of the business do we need to protect?"
3. "How can we conduct business securely[1] and safely?"
4. "How can we use a secure infrastructure as a competitive advantage?"

To answer these questions we need to understand what the core business is and why it needs an interface to the Internet or any network. As part of any analysis, you will need to document your findings. In each step, write a short summary of the results of your analysis.

Example: The Company is a publicly traded enterprise that provides the automotive industry with Widgets. The core business is to manufacture Widgets and market and sell the Widgets to automotive parts distributors and to individual customers. The Company currently sells most of its products via a dedicated sales force, mail order catalogs, and an 800 number advertised in trade publications. The Company wants to expand its Internet presence quickly and, at the same time, securely.

This example provides a quick start on what your business needs are and where you will need to start putting your time and resources.

[1] Business continuity and disaster recovery plans should be included with this analysis.

2.2.2 Identify the stakeholders

The stakeholders can be the company owners and stockholders. The CxOs are the owners of the applications. In many enterprise companies, there will be several applications or processes that will need to be secured. Each application and/or process will have an owner who makes the decisions about the application or process and is responsible in the event that the application or process does not function. The stakeholder can also be anyone who has any type of ownership in security.

2.2.3 Compile customer demographics

Understand the company from both an internal and external perspective. Identify the number of employees, the customer base, and the volume of sales.

Example: The Company has been in business for 15 years and has 800 employees. The Company has 500 parts distributors to which it sells Widgets. The Company has 15 vendors that supply raw materials. The Company has few direct sales customers. Selling directly to the parts distributors generates the most sales for the Company. Once you have this data, you can begin compiling the types of access rights each group has and will need.

2.2.4 Identify the vendors and business partners

It is important to understand the vendors with which you do business. In many cases, you may have the vendors connected directly to your data processing systems. This is a great advantage but it can also be a point of entry for unauthorized access.

Example: All but three of the Company's vendors connect directly into the data process systems. This allows for the vendors to automatically process orders for the JIT (Just in Time) Widget manufacturing process.

The business partners are not necessarily the same as a vendor. In many cases, the business partners will work with the business to extend products or services rendered.

Example: The Company has five business partners that take raw Widgets and create "extended Widgets." The business partners need to share encrypted e-mail and will need to access secure web pages for product updates.

Be sure to map out in detail the business partners' access levels, account names, and what trusted networks they have access to.

2.2.5 Identify the competition

Yes, the competition will keep track of what you are doing. In fact, they may even be using these steps to create a profile on what your business is doing. So you are well advised to complete the profile before they do. (Beware if you see one of your competitors with a copy of this book!) Begin by compiling a list of your competitors and what information or resources they would be interested in obtaining. For example, you may have a secret formula or some specialized personnel that you would not want to lose. In today's changing economy, it is hard to keep first-rate personnel. Your competition also faces this problem, and they may find that your company web site is a great place to acquire potential candidates' names.

Example: The Company's main competitor is Bubba Inc. Bubba Inc. creates Sprockets, which can be used in place of Widgets. Bubba Inc. has a strong web presence and has many of the same customers, business partners, and vendors as the Company. Bubba Inc. could hurt the Company if it could access the Company's internal price list and sales commission rates. Also, the Company could lose valuable people to Bubba Inc. if Bubba Inc. could access the Company's corporate personnel directory. In the September 2, 2002 issue of *Business Week*[2] an article on page 78 reviews a case in which a series of passwords may have been stolen and used by a competitor. According to the article, industrial espionage was used via web sites to download data about a set of new products. The advice here is to know your competition and also try to monitor if any previous employees have moved to a competitor company.

[2] A McGraw-Hill Company magazine.

2.2.6 Identify industry trends and standards

This step can identify a common trend that businesses in all sectors are currently undergoing. Your business may be moving data via the Internet. Supply chain integration may use virtual private networks (VPN) to communicate with the vendors, including on-line ordering and JIT (Just in Time) raw material order and delivery management.

Example: Both companies that create Widgets and Sprockets share the same parts distributors (customers), vendors, and business partners. All the major players in this market communicate with their suppliers via a VPN over the Internet. Also, the parts houses are requesting the ability to generate JIT orders and on-the-fly orders via the Internet.

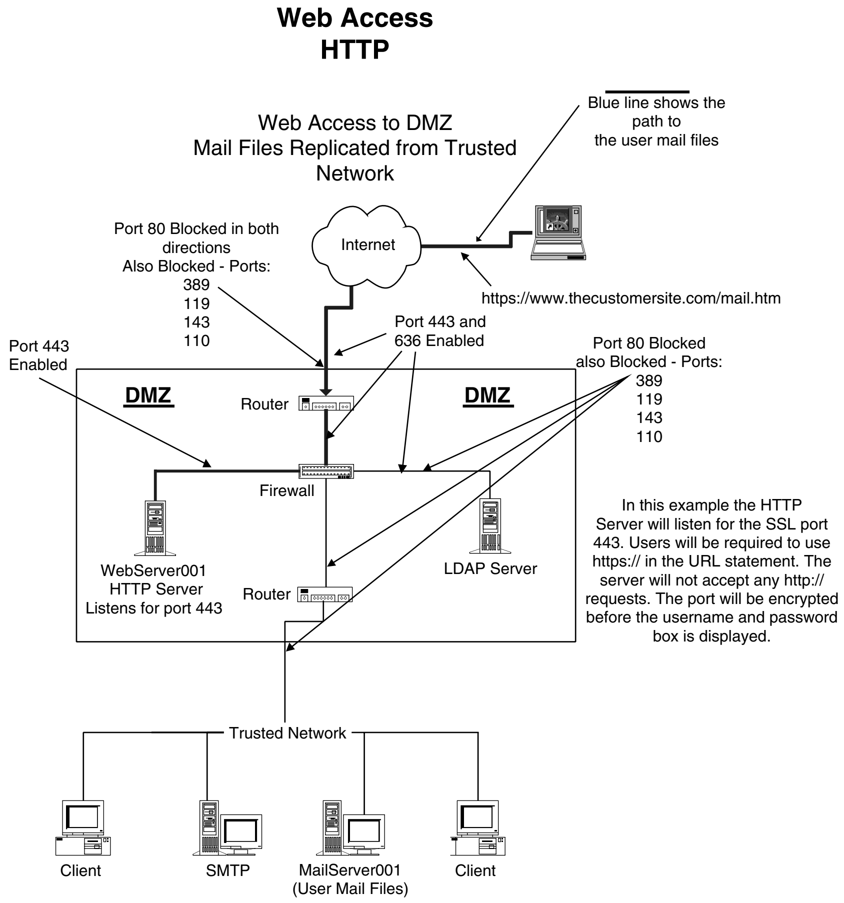
2.3 Analyze the technology being used

Next, you need to review your current use of technology. This review will include your "trusted network." A trusted network is the network that a company uses to conduct internal business. In many cases, the trusted network is by default defined in the organization as "secure." The trusted network typically supports the backend systems, internal-only-based web pages, data processing, messaging, and, in some cases, internal instant messaging. In many companies, the trusted network allows direct interaction between systems without encryption. Also, various protocols will exist within the trusted network without any type of filtering or even virus scanning.

The problem with this definition is that many assumptions are being made at these companies. A trusted network is not always a secure network. In fact, in many cases the trusted network cannot be trusted, because an internal network is composed of many different networks. These include new acquisitions, old acquisitions, international access points, and even several access point to the outside world.

A common practice is to define the trusted network as the network that internal employees use when at the office or via a secure, controlled dial-in mechanism. A single access point is established to the outside world via a mechanism called the DMZ (demilitarized zone). A DMZ is an isolated network placed as a buffer area between a company's trusted network and the nontrusted network. The DMZ prevents outside users from gaining

Figure 2.2



In this example the HTTP Server will listen for the SSL port 443. Users will be required to use https:// in the URL statement. The server will not accept any http:// requests. The port will be encrypted before the username and password box is displayed.

direct access to the Trusted Network. There are several methods to set up/configure a DMZ.[3]

For most of our discussion in this book, we will use the following example.

Example: Our DMZ will have flanking routers on either side of a firewall to shield us from unwanted traffic. The firewall's job is to work within the DMZ to filter all network packets to determine whether to forward them to another server or to a computer workstation.

Firewalls will be covered in detail in a later chapter. Let's focus on the DMZ for now, as seen in Figure 2.2.

[3] Access this URL at Cisco for several examples. http:/www.cisco.com/warp/public/cc/cisco/mkt/security/iosfw/tech/firew_wp.htm

A DMZ is similar to a set of steel bars set up between the bank tellers and the bank customers. That way a person cannot just reach in, grab some money, and run off. The "bad dudes" will need to jump over the steel bars to get to the money. In the same way, DMZs are configured to keep someone from directly accessing the trusted network. Sets of DMZ rules are enabled in the DMZ. These rules are controlled by the policies and implemented via the procedures for your organization. One of the most common rules is that a single protocol cannot transverse the DMZ. So if you are entering into the DMZ via http on port 80, you cannot continue into the trusted network on the same port and protocol. This is what the DMZ does: It keeps "untrusted" traffic from entering the trusted network. It is the job of the DMZ to filter the traffic and limit access to the trusted network via filtering and authentication and even to completely block traffic as needed.

What can a DMZ do for inbound traffic?

- Filter and manage Denial-of-Service attacks
- Scan e-mail messages for virus, content, and size
- Provide passive eavesdropping/packet sniffing
- Prevent application-layer attack
- Provide port scans
- Limit access to the trusted network via a single protocol
- Provide IP address spoofing

The following example is used for discussion only. We cannot make a recommendation on DMZ configurations for all cases.

Example: Some companies will make a partial copy of the data that is in the trusted network and then place it (or replicate it) onto servers in the DMZ. This is a good idea, unless the company has stated, "No business data is to be placed into the DMZ." Okay, now what do we do? A complex application needs to be created to intercept requests, possibly authenticate the users, and then forward the requests into servers in the trusted network. As you can see, one size does *not* fit all.

So far, we have discussed using the DMZ to control inbound traffic, but the DMZ is also used to control outbound traffic. It is also used to hide (mask) the design and configuration of the trusted network. The DMZ can be designed to limit access to the Internet via proxy servers and filter servers. These servers, as regulated by the limits set in the policy documents, can do the following.

- Control e-mail messages based on destination
- Control e-mail messages based on size and even content
- Scan for viruses going out of the DMZ
- Limit access to unauthorized access sites
- Monitor access to unauthorized web sites

Why should we care about messages that might have a virus going out of the company? This will be covered in detail in a later chapter, but for now, imagine these headlines: "Dimwitted User at the Company Sends Out Virus to Their Competitor Via a Résumé!" We are all responsible for controlling viruses. You can do your part by checking for viruses before you send out a message.

Make a list of your network configuration. Identify the access points to the Internet. Determine if you are using a trusted network. In the process, you will determine if you have any unauthorized access points.

Example: Someone uses a PC connection product to check his or her work e-mail by dialing into his or her computer from home. This is a common technique and may be authorized by your company. But without proper controls and procedures, this can be an access point for a hacker to access your trusted network.

Mergers and acquisitions are the norm of the business world, but with each merger there is some of type of change to a network. Many businesses will merge the trusted networks between the companies. This may seem like good business, but it may not be good security sense. If you have a "new" network that has been created by combining previous networks, review the following.

1. Access points to the Internet
2. The number of DMZs each company involved has in the merger. Why?
3. The protocols being used on each network
4. Directories being used to authenticate users

5. Is there an authoritative directory?
6. The type of remote access available to the new combined network

Now for the opposite scenario. Your corporation has just sold a company or division. Review the same points in reverse. You may need to completely isolate the networks.

1. What access points to the Internet are/were in common?
2. How many DMZs does each company created from the split have?
3. What protocols are being used on each network?
4. What directories are being used to authenticate users?
5. Was there an authoritative directory?
6. What type of remote access is available to the new network?

So far in the discussion we have talked about a trusted network as a single entity in a company. This is not always true. In a large enterprise or multinational company, there can be many trusted networks, and each network does not necessarily trust each other. Due to individual country laws and requirements you may need to isolate your trusted network, and you may even separate your networks via mini-DMZs. The common term for this is "zones and perimeters." Security zones define the areas that need to be protected. Each zone may have different security requirements. The zones may be within a perimeter area that protects all zones or specific zones.

Now you may be saying, "I don't have a DMZ or a trusted network." No problem—all that means is that we have a lot of work ahead of us. So let's move on to the next phase: initial risk analysis and the determination of whether you need a DMZ or a trusted network.

2.4 Risk analysis

We have reviewed the business and the network. At this stage in the process we will combine the information we have collected, which will give us a high-level snapshot of our organization and our network.

Look at each business statement that you created from the "Identify the Core Business" section. Identify each point where security could be an issue or a concern.

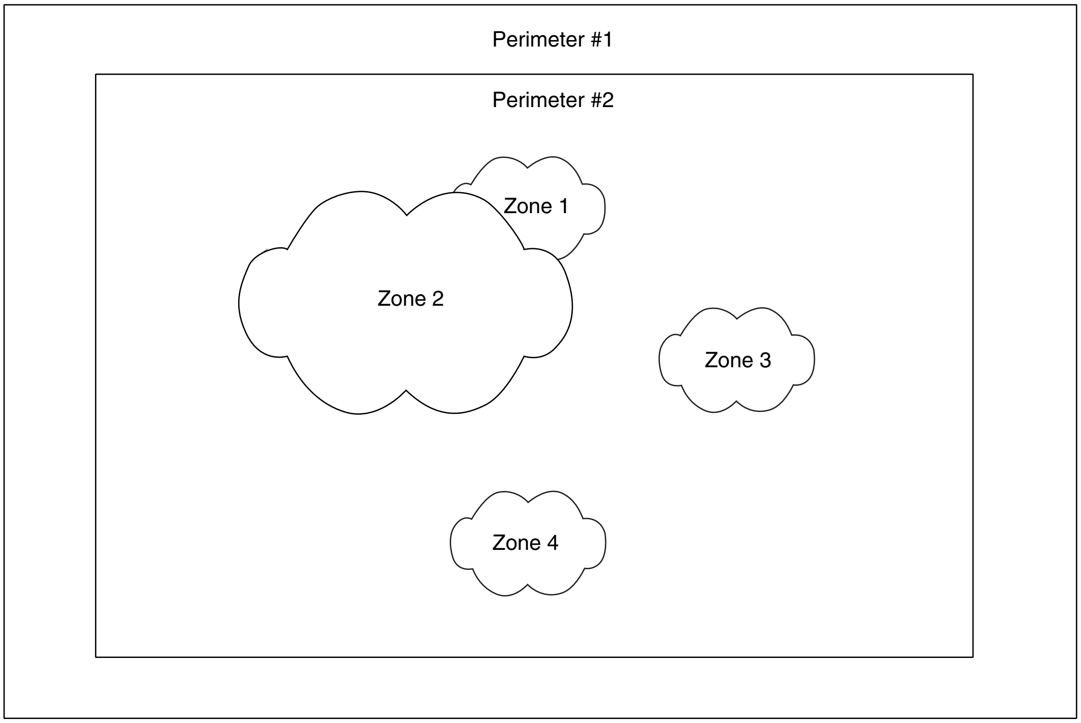


Figure 2.3

Example: The Company has been in business for 12 years and has 7000 employees. It has 600 parts distributors to which it sells Widgets. The Company also has 22 vendors that supply raw materials. The Company has few direct sales customers. Selling directly to the part distributors generates the most sales for the Company.

In this example we have several areas of concern.

- 7000 employees—security training awareness. What are the definitions of trust with each group of employees?
- 22 vendors—what is the trust level of these vendors? Do the vendors need to have direct access to the systems on the trusted network?
- Parts distributors—how does the company communicate with the parts distributors? Is encrypted mail used? Are secure web pages established?

Remember at all times what your goals are. Ask yourself, "Does this business need a web presence?" The answers can drive you to the solutions that you need. Security is not set up simply for the exercise of setting up security. It is set up to give you a competitive asset in driving your business. With that said, look at the security requirements from a business delivery model.

1. How can the business security enable the employees to drive the business in a cost-effective method?
2. How can the business save money by giving the vendors limited access to business data?
3. How can the business improve service by assisting the parts distributors with order and billing systems?

Next, combine your network analysis with your business needs. Your network may not have the necessary features that you would like it to have. No problem—list what features are needed to support your requirements.

1. The network will have a DMZ that will isolate traffic between the trusted network and the Nontrusted Network.
2. The network will provide support to the employees by giving them access to all authorized business systems.
3. The network will allow limited access to extension of systems in the DMZ for the parts distributors.
4. The network will allow for encrypted messages to be exchanged between employees and the parts distributors.

A detailed risk analysis will be covered in later chapters. This step is "priming the pump." You need to understand what your business requirements are before building the security. Some sites have such strong security requirements in place that the business just bypasses the security. For example, in one company, the security departments set up a file that prevented files greater than two megabytes from being sent. One department could not send its drafting files (four to six megabytes each), so they set up their own access point to the Internet via dialing into a private ISP (Internet Service Provider) and then sending the files. This creative solution caused several problems.

- The files sent were not encrypted and thus could not be controlled or monitored for viruses, inbound or outbound.
- An access point was made to the trusted network that was not controlled or monitored by a central security point.

The next step is to compile a list of high-level threats to the organization. Here are a few examples.

- Management does not encourage or support security measures. (Management must be involved in security from day one.)
- There are no security policies or procedures, or the policies and procedures have not been updated for months or years.
- There are no formal user training procedures.
- The trusted network is not defined.
- There is no DMZ (although not required in all cases).
- There is a direct connection to the Internet and no filters or firewalls.
- There are no monitoring systems in place. (This can be deadly for public utility companies.)
- No physical security is in place for the server room; anyone can just walk in.

2.5 Plans and policies

This is an area where many companies fall short of the mark. Check your environment to see if you have any existing security plans, policies, and/or procedures. These can include physical security, LAN security, Internet access, and even disaster recovery. At this point, you have decided which threats pose an unacceptable risk to your computing environment and what level of action you are willing to take to defend against them. Studying the security plans that your company has and their implementation may help you decide which security measures are most important for your environment. One of the most important parts of this review is the identification of policy compliance. Policies are only good if they are implemented; a thorough implementation plan is required. Part of your security implementation plan should be a review of any existing policies that concern security.

- Policy goals and objectives
- Scope
- Responsibilities
- Physical security
- Network security

- Data classification (data categorization)
- Access control
- Password change and enforcement policies and procedures
- Incident handling procedures
- Acceptable use policies
- Change control
- Training
- Compliance

2.5.1 Policy goals and objectives

Define what you are trying to accomplish with your policies. The objective defines your approach to Internet security. These approaches could include the use of tools, systems, and employee/user training.

2.5.2 Scope

The scope specifies the assets that will be protected by security policy. The scope could define a specific policy or a body of policies. The scope should include who is impacted by the policy: end-users, employees, customers, vendors, and so on.

2.5.3 Responsibilities

The responsibilities section of the policy document describes how the individuals defined in the scope section will be responsible for the security of your environment. Detail the security responsibilities as needed by region, department, or groups. Depending on the company size, responsibility may be assigned to the following personnel.

Executives

The top directors—the CxOs—are responsible for high-level security strategy and must make the necessary resources available to combat security threats to the business.

Security manager

The security manager is responsible for the entire enterprise security. The security manager defines the enterprise security policies and procedures and works with the business managers to implement the initial risk analyses as well as the individual process risk analysis. The security manager implements each facet of security, such as:

- Secure network
- Security applications
- Auditing
- Incident handling
- Facilitation of legal reviews of the various security issues

Process owner

The process owner is directly responsible for a particular business process and can be a department manager, a lead engineer, a specification custodian, or any employee tasked with accountability for a business system. The process owner will work with the security manager to analyze risks and recommend the countermeasures for each process. The process owner may not have extensive experience with security, so the recommendation may be at a business level only. For example, the process owner will say, "We need to limit access to this application to a single group." The security manager hears, "Access control will need to be set up and implemented for applicable personnel in the process group via the corporate policies and procedures."

Legal

The legal department needs to be involved with the design of the security policies and procedures from day one. Make sure the following issues/items are covered within each policy.

- Guidelines for acceptable use
- Ethics, for users and administrators
- Access by customers, including liability and damages, performance, and compliance
- Risk and exposures in the event that business data is compromised
- Analysis of communications sent to customers in the event of a security event (e.g., hackers, data compromised)
- Auditing and use of logs for evidence
- Copyright issues

- Use of electronic signatures and encryption
- Management of unauthorized access
- Review of any agreements with Extranet vendors, customers, and ISPs
- Interpretation of the Uniform Commercial code in relation to business use of the Web for your particular business (http://gopher.law.cornell.edu).

Developers

The developers define the responsibilities of the application developers. Security needs to be built into the application from day one of the development cycle.

Users

The users are responsible for security in the enterprise as much as the CxOs. Every user needs to be trained on the company security policy, data categorization, and system procedures as well as understand what the consequences of their actions are and how to act accordingly.

Auditors

The auditors should be familiar with but independent of the activities performed by the organization or group being audited. They will perform audits specific to requirements in the security policies and procedures.

2.5.4 Physical security

Physical security measures must provide for the protection and access to the physical assets of the business (e.g., servers and applications). The physical security document should describe how the various assets are to be protected (such as locked server rooms, card readers with limited access, or logging systems to track who has access to each type of server).

2.5.5 Network security

The network security document describes how you will protect assets stored on the network. This document could include security steps on the following.

- Network access
- Use of sniffers
- Access to Internet services
- Methods of DOS attacks

2.5.6 Data classification (data categorization)

Every business possesses data that is owned by someone. The value of this data can vary from one application to another, from one business to another, and even from one competitor to another. Business data should be classified based on the security requirements of that data. A data classification policy document should describe the requirements to classify the data. Do not confuse the classification of data and the service level of that data. You can have data that is open to the public, but if the public cannot read the data due to a DoS attack, then that data is useless no matter what your classification is.

Following are examples of data classifications.

Public

This data/information is available to the public. Access to this data by competitors is acceptable and does not represent a threat to the business.

Vendor restricted

This data is available only to approved vendors and/or business partners. Access to this data by competitors can pose a risk to the business. Access to this data must be logged and restricted.

Internal information (proprietary)

External access to this data is restricted. Access to this data by competitors or the general public could put the business at risk or cause embarrassment. Access to data is restricted to internal employees only and access will be logged.

Confidential information (limited)

This data is confidential within the company and protected from external access. Access to this data can give competitors an advantage in the marketplace. Access will be limited to select employees and groups. All access will be logged. Backup tapes will be controlled.

Secret information

This data will not be placed onto any networked systems. Access will be limited to very select individuals and all access will be logged and monitored. If this data is compromised, the business can be at risk.

2.5.7 Access control

Depending on the application and the data, users may need to be authorized. Define your requirements in this section of the document. Define the access to the authoritative directory for this authentication, and include the following access control features as needed.

- Users should be prevented from deleting other users' files in shared directories.
- Users should be able to manage the privileges of data elements that they own.
- Access control should be linked into data classifications.

Note: Not all authentications will necessarily be from an authoritative directory.

2.5.8 Password change and enforcement policies and procedures

Be careful with this section of the document. Not all applications or operating systems have the same password management systems or rules. You may need several documents to cover each type of password management. Also, consider using a single sign-on system, which can help manage passwords and the password rules. Consider the following examples when setting up your policy document.

Set up password rules to prevent "crackable" passwords

- Require a combination of numbers, upper- and lowercase letters, and punctuation.
- Use a password that you can remember without having to write it down.
- Use short passwords.

Create some guidelines for users on how to manage their passwords

- Do not share or give your passwords to others. Do not allow others to tailgate into applications using your password.
- Do not write down the password or send it to someone via e-mail.

- Do not create a single administration user name and password that will be shared between several administrators (this compromises the ability to audit).
- If possible, set up an administration account and password separate from the administrator's personal account. For example, your messaging administrator, Joe Smith, will be assigned two accounts: Joe Smith and Joe SmithAdmin, each with its own password. Additionally, the privileges will not be the same. The Joe Smith account will have the standard user access privileges that a typical user will have. The administrator will send all e-mail via this account, and will access any applications from this account. If the administrator needs to make any changes to the environment, he would then use the Joe SmithAdmin account. This account will provide the needed level of access to administer the environment. Joe will not use the Joe SmithAdmin account to send e-mail or to use any applications.
- Educate users about the dangers of password hacking/cracking.
- Encrypt passwords within the directory.
- Define the age expiration limit of the passwords and management and tracking of password history.
- Define the encryption strength.
- Define the mechanism and systems to track and stop directory attacks.
- Define the use of smart cards, tokens, and biometrics.

2.5.9 Incident handling procedures

An incident is an unplanned, unexpected event that requires immediate action to prevent a loss of business, assets, or public confidence. All policies must have an incident handling component plus a feedback component. The feedback loop is the mechanism that will keep the policies current and updated. An incident handling process is critical to permit continuity of important business processes in the event of an incident and allow the business to function. Service levels will be needed to determine what level of handling is needed based on each incident type. An incident where the web site is down and the business cannot conduct electronic transactions will generate a different response than a situation where a user may have lost an e-mail message.

The response team should include representation from these individuals.

- Management
- Technical personnel
- Legal counsel
- Team coordinators
- Communication specialists

Be sure to define the basic procedures for handling an incident. In case of an incident, each of the following points should be implemented.

1. Preparation. The team should have a charter.
2. Incident detection. The processes and tools to detect an incident should be in place.
3. Immediate action. This needs to be prioritized based on a scale of importance (more in Chapter 11).
4. Communications. This is critical to handling an incident.
5. Detailed situation analysis. Observe and report what happened.
6. Recovery. Get the business running again.
7. Feedback. How can we keep this from happening again?

Following are some general guidelines to help you set up and manage your incident response team.

- Take a look at http://www.cert.org/nav/recovering.htm.
- Create a hard-copy list of contact names, telephone numbers, and e-mail addresses.
- Test the processing on a regular basis.
- Test your backups.
- Test your communication process.

2.5.10 Acceptable use policies

The acceptable use policy section states how users will be allowed to use network resources. There should be several policies created.

- Acceptable use for e-mail
- Acceptable use for network access
- Acceptable use for data disclosures

2.5.11 Change control

Some people may argue that change control is not a security concern, but without adequate change control, a site can crash without warning. Hence, our future discussions will address change control as a security concern. Just a simple change can impact the infrastructure and/or application. A concrete check for this is, "Does the site have a change control system and/or policy in place?"

2.5.12 Training

End-user training if very important. A successful security program will include various training methods. These can include:

- Classroom training
- Frequently Asked Questions (FAQs) documentation
- An Internal Web page (Intranet) shows
  - Current Bugs
  - Virus information
  - Corporate Security policies
  - FAQs

An educated user is an important weapon in keeping your environment secure.

2.5.13 Compliance

The Compliance section of your security policy will show how you maintain your security. Compliance can include:

- Audit procedures
- User training schedules
- Vendor use, via audits, of corporate resources.

Most companies also include an employee compliance application. This application is used to track when employee read and agree to the corporate security policies. Most companies required employees 'certify' themselves every year.

2.6 Implementation

We started by reviewing the business, looking for the methods to securely conduct business both internally and externally. From this analysis we determined the core business requirements and identified the stakeholders, customer requirements, and our business partners. We also identified our competition as well as industry trends and standards. As a result, we know what we are trying to protect and from whom to protect it. We also saw that security can be a competitive asset.

Our next step was to review our network and determine what was needed to set up a secure network. We then examined the risks involved and saw how to expand business influence by mitigating the various identified risks.

The policies were defined to protect and educate the various parts of the business. Now we are ready to create our first plan. This first cut will drive us throughout the rest of the security implementation process. Create a plan (the "security project") that will detail the steps required to secure your business environment.

Your project should address the design, structure, and configuration of an evolving secure business infrastructure. The technical infrastructure will ensure that a business security environment is in place to support the user community and keep the business running.

The security project should include the following:

1. Definitions of the goals and objectives of what is needed based on the analysis obtained so far. This will include designing, building, and configuring the technical infrastructure environment.
2. Definitions of the scope of what is needed to secure your environment. This will include implementing performance and tripwire monitoring of the new security environment.
3. The plans for roll-out of the new infrastructure that you designed. Be sure to include a pilot run(s) to test your assumptions about what you have designed.
4. Finally, the roll-out of the new infrastructure. Indicate the communications systems needed to support the implementation, including training requirements and end-user support.

2.6.1 Goals and objectives

Following are the overall goals of the security project.

1. Deliver a steady-state platform to support the business's security "vision." This includes design, implementation of a comprehensive common security infrastructure, effective support organization, and technology management processes needed to support the use of security by all business professional and support staff.
2. Define and facilitate enterprise strategies for secure network evolution and remote connectivity.

2.6.2 The scope

The scope should describe key elements of the project, including the following.

- Designing, building, and configuring secure business networks.
- Creating the budget to implement the security. Each process in the organization should drive the budget. Every process has a security component.
- Procuring the equipment and/or tools, including secure facilities, equipment, and tools.
- Configuring and testing the secure environment, including equipment and internal and external connectivity.
- Reviewing any recommendations for short-term and long-term modifications to the network environment as necessary.
- Establishing an interim strategy until any identified network traffic issues can be resolved. Understand the network traffic volume and network SLAs (Service Level Agreements).
- Designing the security for servers and workstations (e.g., physical and logical topology, replication schedules, remote access, external connectivity, etc.).
- Defining the migration strategy for existing security plans, procedures, tools, systems.
- Establishing a security infrastructure implementation plan.

2.6.3 Infrastructure

The network(s) will need to be set up and configured. One mechanism to help determine the appropriate level of security is to monitor the existing networks before and after the security changes. The performance monitoring of the traffic on the various networks (trusted and nontrusted) will drive a better understanding of the actual usage of security within the business. Performance indicators should be defined in the following areas.

1. End-user applications—from both the end-user workstation and the server
2. Server-to-server traffic
3. Overall network traffic utilization
4. Remote communications

The performance indicators should be derived from the business requirements. These service levels will need to be tied in to the security requirements. The performance indicators will show both the SLA performance and the security performance. If the security implemented is impacting the business service, then that particular security tool/service will need to be reevaluated. The performance monitors will generate information that, when analyzed, will show the historical system performance trends. It is expected that the type of user and the applications used will affect the performance of the network. The roll-out plan will need to include all the various aspects of the security project. Be sure to include the following items:

1. End-user training
2. OS security
3. DMZ design
4. Incident handling procedures
5. Disaster recovery
6. Pilot (test the systems before going on-line)
7. Change control systems
8. Schedule for: pilot, training, network changes, and OS changes

Once the implementation recommendations have been generated, they need to be piloted or tested before the deployment begins for the following reasons:

1. Prove the processes
2. Check assumptions
3. Determine potential failure points before production
4. Assess individual systems and risks

A pilot will identify critical path issues, risks, and potential roadblocks. It is most interesting that the biggest detractor of a new technology solution will magically appear during a pilot. You will get all types of responses such as, "Why did you choose that tool?" and, "I know a better one." Yet this is an opportunity to refine your implementation plan and revise your tool or system selections. Just make sure you are selecting the process or tools based on security and business requirements and not the ad hoc political environment. Thus, the message here is to pilot your assumptions before going into production.

2.6.4 Pilots

Create a pilot plan. This should include the goals of the pilot, the scope, the user groups to be included, specific applications, and the evaluation criteria. The following items should be included in your pilot:

1. Definitions of pilot goals
2. Pilot scope
3. Pilot evaluation criteria—what will make the pilot a success?
4. Pilot participants—select a known group of users.
5. Definitions of the pilot application and systems
6. Training schedule—yes, you need to pilot the training!
7. Pilot schedule—Who, when, and where

2.6.5 Training and execution

This is it. It's time to implement what you have been building: the client/server hardware and software to the end-user community. This includes network connectivity, operating systems, user accounts, and definition of security access levels. This should also cover the administration and support requirements, server network configurations, and maintenance procedures. This step must involve pushing the technology to the end-user community and should focus on end-user acceptance as well as evaluation of the administrative impact of end users. The following items should be considered in the final roll-out:

1. Training—“train the trainer” and user training
2. Installation and/or upgrading of hardware
3. Setting up and configuring servers and network
4. Assigning security/privileges
5. Installing client and server software
6. Setting up user/server accounts
7. Evaluating and refining system and maintenance procedures
8. A published schedule
9. Use of ethical hackers to “confirm” the security of the environment
10. Communications documents and memos