

Why a security policy?

Skill Level: Introductory

[Sean-Philip Oriyano](mailto:sean-philip.oriyano@oriyano.com) (sean-philip.oriyano@oriyano.com)
IT instructor

22 Apr 2008

If you were to assemble a "top ten" list of issues affecting the IT industry in the past decade, security would have a prominent place on the list. Organizations can throw money at technologies to upgrade security, but any successful solution requires proper planning, starting with a security policy.

A *security policy*, in its purest sense, is a document or set of documents that defines how an organization intends to protect its assets. By definition, a security policy provides high-level guidance for the organization but does not specifically cover technologies or techniques. This article shows how to create a security policy and discusses some of the tools you can use to develop the policy and enforce it later.

Getting started

Before you can start developing your security policy, it's important to cover a few points that will ensure the success of the project:

- **Executive support.** For a security plan to succeed, it is absolutely essential to have support from above—in other words, an executive sponsor. The executive sponsor for this project can assist in obtaining resources such as money, personnel, and other items that will undoubtedly be needed. Without "support from above," a security planner will have difficulties assessing all parts of the enterprise for risk. In addition, executive staff members in most countries are the ones ultimately responsible, in a legal sense, for data in the organization.
- **Threat identification and risk management.** Part of the process of developing a security policy is identification of threats and risks. *Threats* are issues such as an attacker targeting the infrastructure or its personnel

(although this article leaves personnel to others to discuss). *Risks* deal with the probability that a given event will take place (for example, a Web server being hacked or a password being cracked).

- **Legal and regulatory issues.** All organizations have some sort of legal requirements that they must adhere to (for example, management of customer and financial records). Requirements in this area affect technical decisions such as encryption strengths, data storage, and availability requirements.
- **Responsibility for data.** For a plan to be fully effective, an organization must accept responsibility for the data it possesses. An organization must accept that it has certain responsibilities when handling data and be cognizant of all the implications that come with it, such as how to keep data from being stolen or accessed improperly. Always remember when addressing security that IT only maintains and secures the data. The organization's executives are the ones who ultimately have their proverbial "necks" on the line.
- **Getting the right resources.** An executive sponsor will assist in getting personnel, budgets, and other resources. The security planner generally identifies the specific resources that are needed. On the technical side of the resource equation come the software and hardware tools that make the security planning, assessment, and implementation work.

Create the policy

The process of creating the security policy is broken into steps that outline how a policy evolves from start to finish.

Step 1: Data classification

Before you can create the policy, you must classify data to determine how it will be protected. During this step, you evaluate data against a series of criteria that should ideally include:

- **Value to the organization.** Will business operations be affected? How much would it cost to replace and redevelop the data?
- **Sensitivity of data.** If the data were lost, stolen, or accessed in an unauthorized manner, what would the consequences be (risk of lawsuits, loss of public trust, or the disclosure of other items such as how security measures work)?
- **Risk of loss.** How likely is the data to be attacked or stolen?
- **Retention requirements.** How long should the data be stored before it

can be discarded?

For each source identified in the organization, record answers to the previous questions. You'll use the information collected here later to determine everything from administrative policy to the technical controls that will be put in place (access control lists [ACLs], encryption, and so on).

After data is identified and sorted by sensitivity, you next must classify it. The classification level assigned to data directly affects how it will be protected and the amount and strength of countermeasures (technical and other controls) put in place to protect it.

For each data recorded, determine:

- The definitions for each classification.
- The security criteria for each classification for both data and software.
- The roles and responsibilities of each group of individuals charged with implementing the policy or using the data.

You'll use this information in step 3 to determine specific classification levels for the data.

Note: This classification represents the bare minimum needed for a data classification program. For financial, health, federal, military, or other organizations that have increased security requirements, you may have to consider additional factors that are outside the scope of this article. In addition, some of the data classification-related information may be contained in a separate policy, such as an information management policy.

Step 2: Business impact analysis

The next step in this process is to conduct a high-level business impact analysis on the major business functions within the company. Eventually, this process should be carried out on all business functions, but initially, it must be done on the business functions deemed most important to the organization.

A study team comprising individuals from information security, information systems (application development and support), and business continuity planning, as well as business unit representatives, should be formed to conduct the initial impact analysis. Others who may want to participate include internal audit and legal representatives.

The team uses the business impact analysis process to:

- Identify those entities within the organization that have critical data to be

protected.

- Analyze the threats posed to business assets.
- Determine the risk associated with each threat.
- Evaluate the impact of loss of information to the organization.
- Record the information detailing the impact of a breach or loss of data.
- List the applications that support business operations.

The information recorded during this step will be used to determine common threats to all parts of the organization. Furthermore, this information assists in the placement of controls such as firewalls, intrusion detection systems (IDSs), router ACLs, and many other potential measures.

Step 3: Classification levels

In step 1, you recorded the data within the organization that needed to be classified. This process categorized the data and recorded the special characteristics of each. In this step, you use the collected information to create and assign classification levels.

When building classification levels, consider the following points for simplifying the process:

- **Numerous classification levels.** Some organizations may be tempted to create a large number of different classification levels for data that later proves to be problematic. Ideally, use a small and manageable number of classification levels to make assignment and tracking easier.
- **Special classifications.** Classification types should be universal across the organization. Special or unique types can cause confusion as well as unnecessary complication.
- **Insufficient number of classification levels.** Having too few classification types can cause data to be placed in a category it might not fit into, resulting in the application of inappropriate security.
- **Characterization.** Each classification level should have clear definitions of what information should be placed in it. Also, each classification level must include guidance on how data should be maintained. Finally, make sure that each classification level has clear boundaries and doesn't infringe on another security classification that could cause later confusion.

As mentioned in step 1, different organizations will have different classification levels. However, here's one of the more common schemes used in commercial organizations:

- **Public.** Information that can be publicly disseminated without concern for harm to the organization
- **Internal use only.** Information that is to be used within the organization but could cause harm if released publicly
- **Company confidential.** Restricted-access information inside the organization—specifically, information that carries a "need-to-know" requirement

Up to this point, the discussion has mostly focused on data and software, but hardware is also a part of security. Hardware, software, and the data that each manages must also have appropriate controls to ensure that the system (hardware, software, and data) is secure. Below are some of the controls that you can use to control hardware and software. (Keep in mind that the controls here are only a starting point for protection. Numerous other controls exist that can increase and enhance security.)

- **Encryption.** Sensitive data can be encrypted to protect it from unauthorized disclosure. With encryption, only those who possess the correct key will be able to open the data, thereby restricting access. Encryption can protect, for example, portable hard disks or flash drives as well as increasingly common mobile devices such as cell phones if they are lost or misplaced.
- **Change control.** In this type of process, changes are not made without the appropriate review and approval first.
- **Backup and recovery.** All hardware and software fail; having a backup can ensure that there is a copy of data, even when a catastrophic failure occurs.
- **Separation of duties.** Sensitive job functions are distributed among multiple individuals, meaning that no one person can perform sensitive job functions alone.
- **Access control.** These controls provide restricting factors such as who can access data, when, and even from where, if needed.
- **Antivirus protection.** No network, computer, mobile device, or other system attached to a network—or even as a stand-alone—should be without virus protection. Viruses can destroy as well as potentially disclose data.

Step 4: Roles and responsibilities

Because a security plan is carried out by people and enforced by technology, different roles and responsibilities must be created. In this step, you create roles

based on business needs, and define responsibilities for each role.

The focus during this step is on determining which job roles are necessary for the organization as well as which responsibilities each role should have. Each organization is obviously different; as such, the roles and responsibilities will be different, too.

The following list shows some of the more common roles that are used. However, not all organizations will define each role the same way, so this list is provided as guidance only:

- **Information owner.** The executive (or equivalent) who is responsible for a company business information asset
- **Information custodian.** An individual or group of individuals responsible for maintaining data
- **Application owner.** The individual who is responsible for the proper functioning of the application
- **User manager.** The immediate manager or supervisor of an employee who has ultimate responsibility for all IDs and information assets owned by company employees
- **Security administrator.** An individual who owns a user ID that has been assigned attributes or privileges associated with ACLs
- **Security analyst.** The person responsible for determining the data security directions to ensure that information is controlled and secured based on its value, risk of loss or compromise, and ease of recoverability
- **Change-control analyst.** The person responsible for analyzing requested changes to the IT infrastructure and determining the impact on applications
- **Data analyst.** The person who analyzes the business requirements to design the data structures and recommend data definition standards and physical platforms; also responsible for applying certain data-management standards
- **User.** Any employee, contractor, or vendor of the company who uses information systems resources as part of his or her job

As stated earlier, you should evaluate the way the organization performs normal business operations and determine the roles and responsibilities assigned to each.

Step 5: Determining data owners

The next step in creating a security policy is to assign responsibility for the various

data sources—the individuals who will be responsible for overseeing the management and security of the data as well as making sure maintenance is taken care of. When assigning data owners, consider the following points as part of the process:

- Ideally, data ownership should not be given to IT but should be assigned to someone outside IT.
- Individuals responsible for managing any given data source require the ability to fully take care of a given piece of data.

Typically, data owners will not be assigned all at once. The most important data sources (as identified above) will have their owners chosen first, and the least important will be chosen last. Also consider during the identification and assignment step that those assigned the data ownership role must be aware of what their responsibilities are, and you should provide training for those tasks that they have been assigned.

Step 6: Information and data classification

After data owners have been assigned, instructed, and given control of their respective data sources, the next step is to gather information. During this step, owners examine their own data sources and the job functions around them to determine any special requirements or needs.

After the information has been collected, data owners should compare the earlier data classification criteria and classify their data in accordance with it. Owners should consider the following when examining their assigned data and the controls that will be put in place:

- Is auditing of data required?
- Is separation of duties needed?
- What are the encryption requirements and strength?
- What access controls are needed?
- What are the change-control procedures?
- How will data integrity be ensured?
- What are the data retention guidelines?

Step 7: Monitoring

After a plan has been designed and implemented, the final step is monitoring the effectiveness of the policy. Monitoring, sometimes known as auditing, is the process of checking how well a system is working. In the case of a security policy, auditing

determines whether the process is being followed and finds trouble spots in the plan (if they exist). Monitoring can be undertaken by many different entities, including internal organizations, external contracts, or (in some cases) the government or regulatory agency.

Monitoring should be done on an ongoing basis not only to catch problems but to aid in the remediation process. Audits may pick up issues, and it will be the job of the security administrator and other parties to apply the results toward a resolution quickly and effectively.

Conclusion

This article outlined the development of a security policy. By following the steps presented here, you can get a great start on developing your organization's policies. Just remember that each organization should evaluate its own unique needs to determine any special cases or issues that may affect it.

Resources

Learn

- Learn more about security-related issues at [Security Focus](#).
- [SANS Institute](#) is a trusted source for information security training, certification, and research. Check out its training programs and resources.
- [Global Information Assurance Certification \(GIAC\)](#): The primary goal of the GIAC program is to validate the skills of security professionals and developers. By having GIAC certification, you prove that you meet a minimum level of ability and possesses the skills necessary to do the job.
- In the [developerWorks Architecture zone](#), get the resources you need to advance your skills in the architecture arena.
- Browse the [technology bookstore](#) for books on these and other technical topics.

Get products and technologies

- Download [IBM product evaluation versions](#) and get your hands on application development tools and middleware products from DB2®, Lotus®, Rational®, Tivoli®, and WebSphere®.

Discuss

- Check out [developerWorks blogs](#) and get involved in the [developerWorks community](#).

About the author

Sean-Philip Oriyano

Sean-Philip Oriyano has been actively working in the IT field since 1990. Throughout his career, he has held positions such as support specialist to consultants and senior instructor. Currently, he is an IT instructor who specializes in infrastructure and security topics for various public and private entities. Sean has instructed for the US Air Force, US Navy, and US Army at locations both in North America and internationally. Sean is certified as a CISSP, CHFI, CEH, CEI, CNDA, SCNP, SCPI, MCT, MCSE, and MCITP, and he is a member of EC-Council, ISSA, Elearning Guild, and Infragard.

Trademarks

IBM, the IBM logo, DB2, Lotus, Rational, Tivoli, and WebSphere are registered trademarks of International Business Machines Corporation in the United States, other countries, or both. United States, other countries, or both.