CHAPTER 1

Resource Inventory

Forty-three percent of companies surveyed don't take the basic step of classifying their data into security categories.[2]

A resource is something that has value to the organization, which if lost or damaged, would cause a loss to the organization as a whole. Resources are more than just assets; they include employees, infrastructure, relationships with customers or partners, and corporate reputation.

All of these resources have security requirements that vary depending upon the importance of the particular resource. However, before proper security measures can be applied, the company's resources must be identified and their value and cost to the company should they be disclosed or destroyed, must be assigned. A complete inventory of company resources is required to know what the company needs to protect. All major information resources must be accounted for and have a designated owner and security classification.

A comprehensive documentation of resources is required to appropriately evaluate the level of security necessary to protect the organization.

Identifying Resources

The first step is to identify the organization's information resources. This will determine the scope of the security evaluation. In theory, all of the organization's information resources would be considered. However, constraints of time, money, and area of responsibility often limit the evaluation.

The various assets and security processes associated with each individual system should be identified and clearly defined. The responsible individual for each information asset and for each specific security process should be agreed upon and the responsibility documented; authorization or approval levels for any changes should also be defined and documented.

[2] PricewaterhouseCooper, " Global Security Survey," *Information Week*, 1998.

Every asset should be clearly defined. These include information and processes as well as physical assets. Often these assets can be put into logical groupings of closely associated information and processes. These asset groups can then be managed as a single asset.

Information

Defining information resources at the appropriate level is a task that requires experience with the information. Data items that are always used together as a unit of information can be considered a single information resource. It is safest to evaluate the information at the data element level. After the information is evaluated, it can be aggregated together to simplify administration. These aggregates must be clearly defined and equivalent to the sum of their parts.

Algorithms

Many organizations have proprietary processes and information contained in the algorithms and software which they have created that need to be adequately protected. In many of the process industries, it is the process more than the data that is unique and has value to the company. They first need to be identified and inventoried.

Software

Purchased software is a significant investment for most organizations. It needs to be accounted for so that if it is stolen an appropriate value can be determined. Adequate software inventories are also necessary to demonstrate that the organization is following its contractual requirements as described in the license agreement for each software package.

Equipment

Physical assets are usually already inventoried and the value and owner for them defined. Be sure to utilize this existing information when it is available. However, information system equipment needs to be evaluated for costs associated with unavailability to be able to create appropriate risk reduction plans.

Assigning Ownership

Ownership assigns accountability. Accountability helps ensure that adequate security protection is maintained. Owners of major assets should be identified and assigned responsibility for maintenance of appropriate security measures. The implementation of the security measures may be delegated, but the owner of an asset will remain ultimately accountable for its protection.

The information owner should be the individual or position in the organization who has fiduciary responsibility for the information. This person should understand the responsibility of maintaining the security of the information. This individual should be able to help define the

value of the information. The owner of a resource will need to evaluate it to be assured that the resource receives the appropriate level of security.

The asset owner is responsible for determining the value of the information asset as well as assigning a security classification to the information. The owner will be expected to have significant input to the handling procedures for the information.

Creator

The creator of the information usually has a good understanding of the value of the information and often controls the utilization of the information. He often feels a personal ownership of the information.

Maintainer

The person who is responsible for maintaining the information, controlling its use, and ensuring its integrity is often selected to be its owner, since the maintainer has the greatest control over the information. Assigning fiduciary responsibility can help ensure proper management.

User

The manager of the user community for the information has a vested interest in the information, since it is his people who rely on it for their work. This person would be the first choice to be the information owner. However, the user community does not always have a single manager who is responsible for their work.

Determining who should be the owner of an information item can be as easy as evaluating who would have the greatest impact on its business function if it suffers a loss.

Determining Value

Determining the value of information assets is pivotal to determining the appropriate level of security. Assets may have an obvious tangible value, such as their purchase price, or an intangible value assigned to them by their owner or creator. The asset owner defines how the value of the asset is to be determined. Identifying the value of an asset is required to understand the possible loss and the appropriate level of security required.

This value is composed of the cost of creating or acquiring the information and the business impact if the information is lost or compromised. The business impact is an estimate of the degree of harm from both short-term and long-term consequences. Long-term consequences are usually more financially significant than short-term. They can include loss of business, violations of privacy, injury, and death.

It is important to evaluate the cost of creating the information, the cost of re-creating the information, and the loss to the company if the information is disclosed to determine the value of the information.

Cost of Re-creation

What was the cost in time – man and machine hours – to collect, enter, and correlate the information? This is often the cost basis for information that is collected from real-time data collection systems. The data collected from nuclear tests or space probes is extremely expensive to create and may be impossible to re-create.

Information with a high cost of re-creation needs adequate protection to avoid the destruction of the information, usually by using redundant storage of information. The cost of recovering the information may be reduced though appropriate backup and recovery procedures. However, the value of the information does not change because of good backup and recovery practices. If it took millions of dollars to create the information archive, the information is not worth less because the cost of recovering the information from backups is less. This is different from the physical world, where the value of an asset is often based on the cost to repair or restore the asset and not necessarily the cost to re-create the item.

Cost of Unavailability

Many businesses, such as financial trading organizations, depend on rapid access to their information resources. The inability to access information to make decisions rapidly can have enormous financial effects on the organization. It can even be life threatening to individuals, as in the case of medical monitoring systems.

Unavailability is a slippery subject, since the cost of the information being unavailable is very dependent on timing, duration, and situation. For example, the information needed to shut down a nuclear power plant and avoid a nuclear meltdown may not be needed for years. However, if it is unavailable at the moment that the reactor needs to be shut down, the cost of unavailability is enormous.

Security often focuses on worst case scenarios. Typical scenarios must also be considered. The frequency, and the duration of critical needs, must be evaluated for business decisions. The "one in a million" scenario must be considered; however, the financial picture may require implementation for only the typical scenario.

Systems for which availability is of prime importance require a high level of redundancy to eliminate points of failure — not to protect the information, but rather to protect the access to the information.

Cost of Disclosure

The level of information detail will affect the cost of disclosure. The more detailed the information, the more costly a disclosure will be.

Information whose public disclosure would have drastic consequences will have a high security classification, which will in itself help define what precautions are necessary. However, there are two issues with the cost of disclosure. The first is with proprietary information, where the disclosure of this information will cause the business to lose sales, market position, or some

advantage. Disclosure of proprietary information has a direct effect on the business' ability to continue to conduct business in a profitable manner. It goes straight to the bottom line of the organization. The second issue is private information about individuals with which the company is entrusted. These individuals may be employees, customers, patients or partners. Disclosure of private information has an impact on both the individual, who the information is about, and the company, who is its caretaker. The organization can suffer indirect damages through a loss of confidence and through legal actions taken by those individuals who suffered because of the disclosure.

When it comes to the level of secrecy or cost of disclosure, most information often has a life cycle. In the area of planning, whether it is marketing plans or military plans, the longer in the future the information relates to, the higher the cost of disclosure. Plans that will become public tomorrow may not cause the same level of damage as plans that cover the next three to five years. The security classification of information needs to be periodically reviewed and reevaluated. Information security reclassification is a regular part of maintaining appropriate information security.

Security Classification

All resources do not have the same potential to cause an organization monetary loss and therefore all resources do not require the same expenditure for their protection. Resource owners must consistently convey the relative importance of loss through modification, destruction, disclosure, or unauthorized use of their resources to the company. Classifications are organized around the attributes of confidentiality, integrity, and availability as they relate to the organization's resources.

Assigning classification is only the first step into a classified environment. It is the continual, day-to-day use of the security classifications that is difficult. The information's classification determines how it is handled, transmitted and stored, who has access, and where the information is allowed to go. Classified information must be labeled appropriately, and this label must follow the information wherever it goes, in whatever form it takes, including printed information and screen displays.

Security classifications allow for a logical grouping of resources to assign general security levels so that information of a given classification always receives a defined minimum level of security. Most companies do this to some degree — papers are marked "Not for Publication" or "Company Confidential." In general, however, this security is only loosely used and minimally enforced.

Classification is conceptually very easy. Determine the value and risks and assign an appropriate classification. However, information has varying degrees of importance and sensitivity, and a classification system must be used to ensure that the information receives an appropriate level of protection. Classifications may be used to indicate the need and priorities for security protection.

The following factors should be considered when assigning a resource's security classifications:

- **Sensitivity of the information** is the leading factor when setting the level of security classification for the information.
- **Consequences of disclosure** define the financial impact of a loss to the information. This helps set the value of the information and thereby sets the appropriate costs of the safeguards to protect it.
- **Legal and contractual obligations and penalties** will define the minimum level of security required for the information to which the law or contract applies. Besides specific laws that place security requirements on information, such as the Privacy Act of 1974, there are laws, court cases, legal opinions, and other similar legal materials that may affect the security classification directly or indirectly.
- **Standards and guidelines** that are defined by government, industry, locality, or the organization itself will help determine the security classification for the information. They will likely define features, assurances, and operational practices for specific types of information. Many organizations specify baseline requirements for systems that have specific functions.
- **Information lifecycle** affects the security classification of the information, since the importance of the information changes over time. Generally, the closer the information is to being officially made public, the lower its security classification will be.

An information resource's overall security classification is the combination of a resource's individual availability, integrity, and confidentiality classifications.

Confidentiality

The confidentiality classification describes the impact from disclosure. It could be in the form of business losses from disclosed proprietary information or the personal damage caused by disclosed private information. Confidentiality classifications are what is generally thought of when the term "security classification" is used.

Availability

The availability classification indicates the urgency of the information and the systems that utilize it. The measure for availability is often based on the lost revenue or productivity that would result from an outage.

Integrity

The integrity classification reflects the severity of the damage that would be caused if the information was altered and then utilized. The damages derive from inappropriate decisions or behaviors based on faulty information. Compromised integrity can be responsible for everything from financial damage to loss of life.

Classification, and the periodic review of classifications in conjunction with risk assessment, will lead to appropriate expenditure in its protection, rather than unnecessary expense. Information classification requirements change over time so it is necessary to review these needs and reclassify information that has had a change in its requirements.

It is best to avoid using military classifications; they have very rigid definitions that may not fit a nonmilitary environment. Their use will create preconceived expectations of the information or its handling.

Checklist

— Make formal inventory of all your information assets.

— Identify all information resources (information, systems, networks, programs, etc.).

— Assign ownership based on business relationships (fiduciary responsibility).

— Determine the value of the resource to the organization.

— Create security classifications for availability, integrity, confidentiality.

This example spreadsheet illustrates the type of information required for the inventory.

			Value		Security Classification		
Identifier	Description	Owner	Dollars	Determination	Availability	Integrity	Confidentiality

Description of fields:

Identifier – the unique identifier of the information resource
Description – describes the information resource
Owner – the assigned owner of the information resource
Value
Dollars – the monetary value of the information resource
Determination – describes the process that was used to determine the value of the information resource. It should indicate if the value was based on the cost of creation, re-creation, unavailability, or disclosure
Security Classification
Availability – the classification based on the availability requirements of the information resource (*Chapter 12*)
Integrity – the classification for the integrity requirements of the information resource (*Chapter 13*)
Confidentiality – the classification based on the confidentiality requirements of the information resource (*Chapter 14*)