Global Information Assurance Certification Paper

Implementing Information Classification within the Enterprise

GIAC Security Essentials Certification (GSEC)
Assignment v1.4c, Option 1

Terry Furness
25 Nov 2004

Abstract

"Knowledge is power"
Sir Francis Bacon

Information is the lifeblood of the organization and, as such, must be protected appropriately. Failure to adequately safeguard sensitive data can adversely influence the fortunes of the enterprise. The challenge for organizations lies in identifying which information needs to be protected, how it should be protected and how to achieve that protection with a reasonable amount of surety.

An information classification system is a product that management can employ to ensure that information within the organization is adequately protected. This paper highlights the importance of effective data classification and provides guidance to management on the process required to create, implement and maintain an effective information classification system within their organization. It defines key products that comprise the system, detailing the purpose and major components of each.

Classification: How important is it?

It is a truism that a requirement to protect information exists within all organizations. There are myriad reasons for protecting information. Examples include[1]:

- **Intellectual Property.** The compromise of this type of information could result in the loss of a competitive advantage and market share. In a recent example, InstallShield accused a rival software manufacturer of using proprietary information to design software to help customers migrate to their competing product[2].

- **Privacy.** Privacy is becoming a significant issue for all companies and increasing legislation in the area requires companies to be aware of their responsibilities for protecting this type of data.

- **Legal issues.** Non-disclosure contracts, archive acts and requirements of taxation law are all examples of external influences on your data classification requirements. It is important that you are aware of all relevant requirements in this area prior to formulating a classification scheme.

[1] Chapple et al.
[2] Semilof

- **Sensitivity.** While the release of some information may not damage the company or breach privacy legislation, it may still be desirable to protect sensitive data such as the companies payroll details.

The purpose of classification is to ensure that personnel are aware of the sensitivity and handling requirements of a particular piece of information. Armed with this knowledge, an individual is less likely to act in a manner that could allow unauthorized access to the information.

While most companies are aware that different data requires different levels of protection, ad hoc implementations of data classification are more susceptible to failure. A formal approach to information classification allows a consistent standard to be implemented across the enterprise, removing doubt and reducing the risk of confidential information being released to inappropriate sources.

Information Classification System

The purpose of an information classification system is to limit access to the information through procedural and technical methods[3].

There are five (5) predominant steps involved in the process of creating and maintaining an information classification system, as depicted in Figure 1.

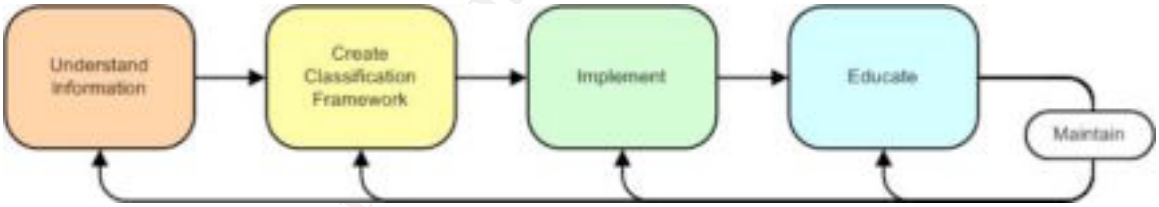

Figure 1: Information Classification System Management

Gather Information

Understanding the requirements of your organization and the environment that it operates within is required before you can develop an effective information classification system. Specifically:

- **Information Types.** Understand the types of information that may require protection within your organization.

- **Identify Risks to Information.** Understand the importance to the organization of each type of data, why you need to protect it, where the

[3] Department of Prime Minister and Cabinet (NZ)

information is used / stored and methods an attacker could use to access the information. Recognize the impact of the information becoming available to unauthorized personnel.

- **Applicable Legislation.** Determine the requirements of any legislation that effects information stored by the organization. Multi-national firms should ensure that they understand the requirements of all countries in which they operate if they intend to have a single corporate policy.

Key personnel within the company (department heads, security staff, legal counsel) should be involved in this part of the process as either contributors or reviewers to ensure that a comprehensive data set is developed. Omissions / inaccurate information during this stage may result in flaws throughout the classification system.

Create Classification Framework

A classification framework consists of a classification scheme and a set of standards and procedures that detail subjects such as how classification occurs and how to manage data of each classification level. You may find that many of the areas highlighted for consideration in this section are already addressed at some level within your existing security policies and procedures.

Classification Scheme

Analyzing the information gathered during the initial phase will allow you to determine the different general levels of protection required for classes of data held within your organization. From this you can determine the number of levels of data classification that are appropriate for your company. Try to use as few classification levels as possible to meet the needs of the organization. As you increase the number of categories you increase the likelihood of confusion and incorrect assignment[4]

In larger organizations, multiple classification schemes may be appropriate. For instance, the Australian Government has a two tiered approach. The first defines classification levels for the protection of information that has the potential to cause damage to national security. The second scheme provides protective markings for non-national security information.

The classification scheme should detail each of your classification levels, a description of the type of data that it is intended to protect and examples of the impact to the company should the information be compromised. This information should be of a general level so that classification scheme provides an easy

[4] Peltier

reference and does not become a formidable document that personnel are reticent to access and have trouble understanding.

Standards and Procedures

Once you have created a classification scheme you need to define how it will operate within your organization. A set of standards and procedures that cover the following areas should be created based on the requirements of the organization and information gathered during phase one.

- **Access to data.** The implementation of an information classification system does not remove the need for providing access on a need to know basis. For instance, the fact that a employee is cleared to view the highest level of classified data within the organization does not provide a satisfactory justification for providing them access to payroll data if it is not part of their job.

  Consider who should have access to classified data and the methods that you will use to control this. The implementation of a system of personal clearances will add significant overhead for your organization so ensure that the benefits justify the cost before taking this approach. Rather, a more general approach, such as restricting access to certain levels of data to company employees only may be appropriate.

- **Classifying information.** It needs to be clearly established who is responsible for classifying information, changing the classification of information and in some cases, determining the duration of the classification. It is recommended that the person creating the document is responsible for assigning the classification, based on the classification scheme. There are a number of advantages to taking this approach. Primarily, it forces all employees to be aware of, and involved in, the process of protecting information. In addition, it ensures that sensitive data is treated appropriately from the moment it is created, removing any periods of vulnerability between creation and when it is provided to a designated person for classification. Finally, you are more likely to get an accurate classification from a person who is familiar with the information and it's context than from a person who must rely solely on the guidance provided within the classification scheme.

  Similarly, changing the classification of a document may best be left to the original author. However, consideration should be given to how to manage the classification of documents if the author leaves the company.

  As the controls placed on classified data generally make the information less accessible and more expensive to maintain, you may consider providing guidance on the longevity of certain classifications. For instance, while a

marketing plan for a new product may be classified leading up to the product release, there may be no reason to protect it after this date.

- **Creating and handling classified information.** Covers a wide range of issues such as what markings are required on classified documents, what requirements must be met to permit access, do you use a distinctive color for markings that represent each classification to easily identify information of this type, are there any restrictions on the number of copies or the control of copies and how do you dispose of the information. This topic needs to be addressed on a per classification basis.

- **Storing classified information.** What controls need to be instigated to protect classified information when it is being stored in a hard copy format (eg: classes of safes) and in a electronic format. Technical requirements that define the minimum security measures that need to be built into a network that contains data of each classification level should also be covered. This topic needs to be addressed on a per classification basis.

- **Transmitting classified information.** Consider the controls that are necessary when transmitting information of each classification level. Transmission methods that should be covered include manual transmission (physical delivery, approved couriers), fax, e-mail and data transmission to both internal and external networks.

- **Receiving classified information from external parties.** If your company is subject to non-disclosure agreements or receive classified data from external sources then you may need to consider how the requirements of these agreements map to your classification scheme.

Implement

A number of products need to be developed to support the implementation of the classification framework developed in the previous section. These include:

- Classification Policy, and
- Security grading documents

In addition, for those organizations that are implementing information classification for the first time, existing data needs to be classified.

Classification Policy

Policy is the vehicle for authorizing the classification system and should be issued by senior management. Key points that the classification policy should contain include:

- Overview of the requirement for information classification within the organization.
- Mandate the use of the classification system within the organization.
- Highlight the department responsible for maintaining the classification system

As policy documents are authorized by senior management, generally require significant input from legal staff and can take some time to develop and have authorized, they tend to be less flexible than standards and procedures. Accordingly, policy documents should not include specific details on the classification system. Rather, they should authorize the detail provided in the standards and procedures and highlight those responsible for maintaining them. This allows the information classification system to be responsive to changing requirements.

Security Grading Documents

In organizations that devolve the responsibility of classification to a documents author, security grading documents can assist in ensuring that appropriate classifications are assigned. This is particularly the case for information where the appropriate classification is not immediately obvious. For example, while a classification framework will make it quite clear the level of protection that is required for a new product design, the appropriate classification for a document that details the security lockdowns of the network that stores that information is less obvious. This is due to the fact that the release of security lockdown information will not directly cause the loss of data, breach of privacy legislation or other impacts mitigated by implementing a classification system. Rather, in this case, this information increases the risk that technical controls put in place to protect the data are circumvented, which could then cause an incident.

As a classification scheme does not provide guidance on the correct classification of all possible types of documents, security grading documents can be a valuable tool by providing a more detailed level of guidance for a specific area.

Classification of existing data.

The classification of existing data can present a number of challenges for those tasked with implementing an information classification scheme. The amount of information requiring classification and lack of access to original authors can make the task more difficult. One approach is to create a team of personnel familiar with the classification system that are responsible for coordinating the task. This team can provide specialist assistance to individual departments who can then be made responsible for classifying their own data.

Educate

The greatest technical solutions can be rendered ineffective by personnel who are unaware of the requirements of an information classification system or who are ignorant of the need to protect sensitive information. A recent example where a senior Victorian police official utilized sensitive information in an inappropriate fashion shows the importance of balancing technical controls with appropriate training and processes[5].

Hence, to be effective, continuing education must be a component of the information classification system. If staff understand the need to classify data and the basis for certain classifications then they are more likely to comply with the relevant company policy. Approaches that should be considered when planning an education strategy include:

- **Formal training**. This is most appropriate for organizations that are implementing a data classification system into an environment that has not required classification previously.

- **Awareness campaigns**. It is important to make security a part of the culture of the organization as this increases the likelihood of compliance[6]. Increasing awareness can be achieved through various methods including posters and informal training.

- **Staff Induction**. The data classification system and relevant security grading documents should be part of the induction for all new staff. This is particularly pertinent for staff moving within the organization who may be moving to a department that has a security grading document that provides specific direction for handling particular classes of information.

A primary goal of the education process is to provide staff with a strong understanding of the classification system so that they can classify information appropriately. When discussing when to classify documents, Chapple et al contend that

> When tempted to assume that a document or resource has no value and therefore needs no access controls, ask, "What's the worst that could happen if our competitors got this?" or "How could this information be used to subvert or bypass security measures?"

This approach needs to be tempered with an understanding of the risk of the information being compromised, the cost to protect the information at a higher level and, in some cases, the additional activity required to access sensitive information. For example, consider a document that details the security policies

[5] The Age
[6] Van der walt

for a network. This information can provide an attacker with information that could be used to launch an attack aimed at compromising information stored on the network. Considered in isolation, using the approach highlighted in the previous quote, most employees would believe it necessary to classify this information. However, if the network in question was a small internal network, contained within a single building that had high level physical access protection, the risk of an attacker getting access to the network to launch an attack is significantly less than if the document referred to a large corporate network that traverses public networks.

In the Handbook of Risk Peter Bernstein notes that the level of perceived risk associated with a particular situation can depend on how the facts are presented[7]. An approach where classification is afforded dependent entirely on what is the worst that can happen can produce a culture where there is a tendency to over-classify information. While it is possible to assert that it is better to over-classify than to have an incident, over-classification can have the following detrimental effects:

- Increased cost to maintain data. Higher classifications require higher levels of control that can produce a higher administrative overhead to maintain.

- Information is not as accessible. As access to classified information is restricted, an incorrect classification may make valuable data inaccessible to relevant staff or external parties.

- Effectiveness of classification scheme diminished. If personnel believe classifications are undeserved the classification scheme can lose credibility, which may result in personnel treating the system less seriously or ignoring it completely.

Maintain

Implementing an information classification system is not a discrete project that is performed once and then considered complete. To be truly effective, a cycle of continuous improvement is required to ensure that the security classification system continues to support the business requirements for which it was originally designed.

As was suggested in figure 1, maintenance may include one or all phases of the classification system. For instance, as was discussed in the previous section, it is important that education is ongoing and adapts to the requirements of the organization. These changes may not impact the classification scheme or require changes in standards and procedures.

[7] Bernstein

Reviews of all documentation that comprise the classification system should occur at intervals no greater than twelve (12) months, with the review date appended to the document.[8]

Conclusion

The protection of information is vital for companies operating in the current environment where attacks are becoming more prevalent and legislative requirements are dictating specific levels of protection. A data classification system can assist an organization to protect information at an appropriate level. This document has highlighted both the importance of protecting a companies information, described the tasks required when creating a classification system and illustrated a process that management can utilize when designing and implementing their own information classification system to maximize the chances of success.

This paper has tried to highlight that the successful protection of data is as dependent on a companies culture, standards and procedures, approach to education and commitment to a process of continual improvement as it is about the implementation of the latest security technology.

[8] Defence Signals Directorate.

References

Chapple, Mike. Shinder, Debra. Tittel, Ed. "TICSA Certification: Information Security Basics" 22 Nov 2002. URL: http://www.informit.com/articles/article.asp?p=30077&seqNum=9 (18 Nov 2004)

Defence Signals Directorate. "Australian Government Information Technology Security Manual", 17 Sep 2004. URL: http://www.dsd.gov.au/_lib/pdf_doc/acsi33/acsi33_u.pdf (18 Nov 2004)

Peltier, Thomas R. "Best practices for writing an information classification policy". 03 Aug 2004. URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci995256,00.html (18 Nov 2004)

The Age "Police official 'abused database'" 25 Nov 2004. URL: http://www.theage.com.au/news/National/Police-official-abused-database/2004/11/25/1101219659935.html (25 Nov 2004)

Department of Prime Minister and Cabinet (NZ). "Security in the Government Sector" 2002 URL: http://www.security.govt.nz/sigs/chapter-3-information-classification.doc (18 Nov 2004)

Semilof, Margie. "InstallShield accuses Wise of corporate espionage". 16 Jul 2003. URL: http://searchwin2000.techtarget.com/originalContent/0,289142,sid1_gci914901,00.html?Exclusive=True (21 Nov 2004)

Van der Walt, Charl "Introduction to Security Policies, Part Two: Creating a Supportive Environment", 24 Sep 2001 URL: http://www.securityfocus.com/infocus/1473 (25 Nov 2004)

Warwick, Ben (Editor) "The Handbook of Risk" Dec 2002 http://media.wiley.com/product_data/excerpt/22/04710641/0471064122.pdf (18 Nov 2004)