GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

SANS Security Essentials
GSEC Practical Assignment
Version 1.2b

Margaret Flierman
April 2001

Data Classification

"The inherent limitations of paper-based systems provide a certain level of privacy protection. The migration of records of personal information to IT systems has made possible a far greater range of uses of personal information and has made it easy to transfer information…. "
Information technology and the internet, Australian Privacy Commissioner, 2001

Introduction

Data classification and allocation of responsibilities for its ownership are important to ensure that the value of information is properly recognised. It is the first step towards ensuring that the most valuable information assets have the highest level of protection.

Information varies in its degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. The information classification scheme should be used to define an appropriate set of protection levels, and communicate the need for specialising handling measures.

What is data (or information)?

The terms 'information' and 'data' are used interchangeably throughout this document.

Information can be defined as … any communication or information such as facts, data, or opinion, whether true or not, whether recorded in a material form or not, whether numerical, graphic or narrative, and whether maintained in any medium, including computerised databases, paper, microform, optical disk or magnetic tape.

Examples…
Customer information – payment history, personal history, pricing information for particular customers

Financial Information – performance history, projections, strong and weak points

Other Confidential Business Information – business allies, specific projects, employee-related problems, management-problems, marketing information, expansion, contraction, target markets, hiring, takeover targets, new products/services, inventions and discoveries.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Why do we (or must we) care?
We have a duty to protect the security of, access to, correction of, use of, and disclosure of data – often because it is a matter of law. A growing number of legislative mandates are appearing in the area of information security. Although these cover a variety of issues (computer misuse, etc) the area attracting most attention is that of Data Protection.

We are by law required to protect our customer data. It must be …
- Processed fairly and lawfully
- Obtained and used only for specified and lawful purposes
- Adequate, relevant and not excessive
- Accurate, and where necessary, kept up to date
- Kept for no longer than necessary
- Processed in accordance with the individuals rights (as defined)
- Kept secure
- Transferred only to countries that offer adequate data protection

Classification Levels
By classifying information, the correct level of protection will be defined and implemented. Information identification should be done at a high level and identify broad categories of information.

Here are four classification levels that identify the level of protection that should be given:

- Public (Class 1) - Non-sensitive information available for external release
- Internal (Class 2) - information that is generally available to employees and approved non-employees
- Confidential (Class 3) - information that is sensitive within the company and is intended for use only by specified groups of employees
- Restricted (Class 4) - information that is extremely sensitive and is intended for use only by named individuals within the company

Responsibilities
The security administrator does not 'own' company data. This should be the responsibility of the head of functional areas, eg Finance, HR, Systems.

The information owner is responsible for classification based on the value and sensitivity of the information, for approving access, and communicating additional risk-based requirements. The security administrator is responsible for ensuring the policy is controlled and complied with. All staff (and this is taken to include anybody with access to data, including contractors, consultants etc) are responsible for ensuring they comply, by marking and treating all computer media and printed information with the appropriate classification and following established processes. Each and every one of us has a responsibility for escalating any issues or breaches.

The information owner must identify and classify the information he/she is responsible for, and the classification must be based on the business requirements for:

© SANS Institute 2000 - 2002, Author retains full rights.

- *Confidentiality* of the information (it must be protected from unauthorised disclosure)
- *Integrity* of the information (it must be protected from unauthorised alteration or destruction, whether accidental or deliberate)
- *Availability* of the information (it must be available when required by the users)

Separate procedures and standards must be established to protect client and customer data, including clear responsibilities and liabilities. You must also determine legislative requirements for information when it is transferred to another country.

Building the Standard
The standard must clearly identify required actions relating to …

- The protection and disclosure of information
  - What are your company's protection requirements?
  - Do your client/third parties have special protection requirements?
  - What is the required authorisation procedure for disclosure of information belonging to internal or external parties?
  - Are there legislative requirements to consider when disclosing information?

- The handling of information
  - What are the physical storage requirements?
  - Must information be retained for specific periods of time?
  - How should information be disposed of?

- The distribution (removal and exchange) of information
  - What is the authorisation process?
  - How should information be dispatched (electronic and postal)?
  - Should the information be returned?

- Sign-off by all parties

The Tables below provide more detailed information.

Summary
Whatever form the information takes, it should always be appropriately protected to preserve Confidentiality, Integrity and Availability of your company's key asset.

Will implementation of a data classification standard ensure users dispose of sensitive items correctly? Will it stop users from sending attachments unprotected across the internet? Not immediately and you may need to implement further controls, but now you have a clear guideline which you can incorporate into your user awareness campaign.

References:

1. GE GCF Data Classification Standards, 2000

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. British Standards Institute. Information Security Management. Part 1: Code of practice for information security management, February 1998

3. KPMG. Information Security Survey 1998

4. Glenn S. Bacal. "What are Trade Secrets?"
http://www.azlink.com/lawyers/charts/whatare.htm

5. The Australian Privacy Commissioner's Website. "Privacy and the Public Sector" and "National Principles for the Fair Handling of Personal Information"
URL: http://www.privacy.gov.au/

6. SANS Institute: Consensus Information Security Awareness Draft Papers
URL: http://www.sans.org/newlook/projects/cap_draft.htm

7. Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definition of Terms"
URL: http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

8. Computer Crime and Intellectual Property Section (CCIPS). "Computer Intrusion Cases"
http://www.usdoj.gov/criminal/cybercrime/cccases.html for a list of cases relating to Confidentiality, Integrity and Availability

9. Computer Crime and Intellectual Property Section (CCIPS). "Privacy Issues in the High-Tech Concept"
URL: http://www.usdoj.gov/criminal/cybercrime/privacy.html

10. Baltimore Technologies. "Content Security Issues".
URL: http://www.mimesweeper.com/products/cs/datatheft.asp

© SANS Institute 2000 - 2002, Author retains full rights.

TABLE A: INFORMATION CLASSIFICATION RULES

Confidentiality Classifications

	PUBLIC (CLASS 1)	INTERNAL (CLASS 2)	CONFIDENTIAL (CLASS 3)	RESTRICTED (CLASS 4)
Description	Non-sensitive information available for external release.	Information that is only sensitive outside the company. Generally available to employees and approved non-employees.	Information that is sensitive within the company, and is intended for business use only by specific groups of employees.	Information that is extremely sensitive, of highest value to the company and intended for use by named individual(s) only.
Examples	Company advertising literature once issued.	▪ Company Telephone Directory ▪ Company Organisation charts	▪ Customer and Client information ▪ Personnel information	▪ Strategic plans ▪ Financial results prior to release
Impact of Unauthorised Disclosure	No adverse impact	Limited adverse impact	Significant adverse impact: ▪ May incur financial or legal liabilities ▪ May adversely affect the company, its employees, its clients or customers ▪ May assist a competitor ▪ May undermine confidence in the company	Severe adverse impact: ▪ May cause severe financial or legal damage to the company ▪ May prejudice the actual financial existence of the company, its employees, its clients and its customers ▪ May destroy confidence in the company ▪ May damage the company's reputation
Access Restrictions	Accessible to all employees	Access normally restricted to employees and approved non-employees for business purposes only	▪ Access must only be granted on a business need to know ▪ Access by external parties must be subject to a non-disclosure agreement as well as a business need to know	▪ Access must be limited to named authorised individuals ▪ Access lists must be maintained ▪ Information must not be shown to or discussed with anyone not authorised ▪ Access by external parties must be subject to a non-disclosure agreement as well as a business need to know

Integrity Classifications

INTEGRITY	DEFINITION	EXAMPLES/IMPACT OF UNAUTHORISED MODIFICATION
High	100% error free	Same as Confidentiality classification for Restricted information
Medium	96-99% error free	Same as Confidentiality classification for Confidential information
Low	90-95% error free	Same as Confidentiality classification for Internal information

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Availability Classifications

AVAILABILITY	DEFINITION	IMPACT
High	No interruption of access beyond 0.5 day	Severe adverse impact
Medium	No interruption of access beyond 1 day	Significant adverse impact
Low	No interruption of access beyond 7 days	Limited adverse impact

TABLE B: INFORMATION PROTECTION RULES

	PUBLIC (CLASS 1)	INTERNAL (CLASS 2)	CONFIDENTIAL (CLASS 3)	RESTRICTED (CLASS 4)
Storage of Information (electronic)	No security control requirements	Site/Department storage should be adequate to prevent casual disclosure	Information may require encryption, where it does approved methods must be used.	Information must be encrypted using company-approved methods
Storage of Information Medium	No security control requirements	Site/Department storage should be adequate to prevent casual disclosure	Medium must be kept in locked storage or a secure environment (Notes 1 and 2)	▪ Medium must be kept in a locked drawer or equivalent, to which the addressee has sole access ▪ Medium must be locked away when not physically in the presence of the originator or addressee (Note 3)
Labelling of Information (documents only)	Labelling not required	Must be labelled with the classification	Each page must be marked 'CONFIDENTIAL'	▪ Each page must be marked 'RESTRICTED' ▪ Individual copies of the document must contain a unique identifier
Labelling of Information Medium (e.g. diskettes)	Labelling not required	Must be labelled with the classification	Where information medium is not permanently held in locked storage or a secure environment, it must be labelled 'CONFIDENTIAL' (Note 4)	▪ The information medium must be marked 'RESTRICTED' ▪ Individual copies must contain a unique identifier
Disposal of Information (electronic)	Removal of Directory entry for file	Removal of Directory entry for file	In addition to removing the directory entry for the file, the space used by the file must be over-written using approved means.	In addition to removing the directory entry for the file, the space used by the file must be over-written using approved means.
Disposal of Physical Medium (e.g. paper/magnetic media)	ALL media must be regarded as CONFIDENTIAL information and be disposed of securely using methods approved by the Security Officer (e.g. shredding)	ALL media must be regarded as CONFIDENTIAL information and be disposed of securely using approved methods (e.g. shredding) and based on retention strategies.	ALL media must be regarded as CONFIDENTIAL information and be disposed of securely using approved (e.g. shredding) and based on retention strategies.	▪ Information must be disposed of securely using approved methods and based on retention strategies ▪ A record must be kept of how, when and by whom the information was destroyed (To provide an audit trail)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

N.B. Medium means any physical item that contains information e.g. tape, diskette, paper document, CD

Notes:
1. A secure environment is a physically secure area e.g. computer room, where written authorisation is required in order to remove any information storage medium (e.g. tape).
2. If any member of staff finds a confidential item and it is not properly secured, it is their responsibility to secure it in accordance with the classification label attached to it.
3. If any member of staff finds such an item that is not being actively used and is not stored securely, it is their responsibility to secure it in accordance with the classification label attached to it.
4. Examples when labelling would be required are; a printed report containing Confidential information being circulated around a department or a PC diskette containing Confidential information that is used during the day and locked in a drawer outside working hours.

TABLE C: INFORMATION DISTRIBUTION

	CONFIDENTIAL (CLASS 3)	RESTRICTED (CLASS 4)
Distribution	▪ Distribution lists of those groups authorised to receive information must be checked regularly to ensure currency ▪ Distribution must be kept to a minimium ▪ The item may only be copied or distributed by the originator of this item or the addressee ▪ Items must be labelled with the classification before any copies may be made	▪ Distribution is to named individual(s) only ▪ The originator of the information item must keep a record of the unique identifier associated with the copy, and the named individual designated to receive that copy ▪ The item may only be copied or distributed by the originator of the item ▪ Items must be labelled with the classification before any copies are made
Addressing	▪ The storage medium must have two envelopes/layers of packaging ▪ The outer envelope/layer must show the recipients name and address, be marked 'TO BE OPENED BY ADDRESSEE ONLY', and show the name and phone number of the sender of the information	▪ The storage of medium must have two envelopes/layers of packaging ▪ The outer envelope/layer must show the recipients name and address, be marked 'TO BE OPENED BY ADDRESSEE ONLY', and show the name and phone number of the Sender of the information
Dispatch of Information (except EDI)	▪ Packaging should ensure physical protection of the item. ▪ Normal mail service	▪ By hand or approved courier ▪ Packaging must ensure physical protection of the item ▪ Printed information sent through internal mail, external mail, or by courier must be sent by trusted courier or registered mail. The method of mailing must provide tracking.
Dispatch of Information (EDI)	Information may require encryption (if so approved methods must be used) if transferred via public networks (internet)	▪ Must be encrypted when transferred via public or private networks. (Note 1) ▪ Electronic mail should use digital signatures for

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

		sending non-public information. ▪ Information must not be faxed unless controls are taken to ensure proper control at the receiving end (password protected mailboxes, or person standing by to receive)
Voice	▪ Voice mail messages should be deleted as soon as possible (a written document from the sender is preferable). ▪ Messages must not be forwarded (in case of misdialling or unauthorised access to other mailboxes).	▪ Information must not be discussed on speaker-phones or during teleconferences unless all participating parties first acknowledge that no unauthorised persons are in close proximity, such that they might overhear the conversation. ▪ Information must never be discussed on cordless or cellular telephones

Note 1: Country specific legal and regulatory requirements should be reviewed concerning the use of encryption technology.

© SANS Institute 2000 - 2002 Author retains full rights.