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

Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b

Making use of Data Classification in the Corporate Environment

Bob Boyer, FLMI/M, CISSP
April, 2003

Abstract:

Privacy laws are now in place in Canada and in many other countries which require corporations to protect the privacy of both customer and employee information.

"Organizations shall implement policies and practices to give effect to the principles, including
(a) implementing procedures to protect personal information;
(b) establishing procedures to receive and respond to complaints and inquiries;
(c) training staff and communicating to staff information about the organization's policies and practices; and
(d) developing information to explain the organization's policies and procedures."[1]

The privacy laws also require that companies need to know what and where personal information about an individual is stored, so that it can be provided to the individual on request, and so that it can be deleted when no longer required.

"Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate."[2]

In large corporations, keeping track and protecting personal information can become an enormous task given the multitude of environments where the data can be copied, stored, or transmitted. Another complicating factor is the large number of individuals within an organization that have valid access to the information in their day to day work. Data classification has been in use for some time within the military to protect sensitive information. Corporations have been reluctant to adopt this methodology as it was seen as very expensive and overly restrictive.[3] This paper will explore whether data classification concepts, methodologies, and technologies can be adapted for use in the business environment. The paper will consist of the following sections:

1. Basic data classification schemes and methodologies
2. Provide an overall assessment of the state of data classification and its applicability to the corporate environment
3. Identify critical success factors and potential pitfalls
4. Provide conclusions and recommendations

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The conclusion will indicate that corporations will implement data classification and mandatory access controls, as these will be required to adequately protect information in the future. The time to start is now.

Introduction

The use of data classification schemes to secure confidential and private information (hereafter referred to as confidential information) has been in use for nearly as long as information has been recorded onto physical medium. Before the advent of technology that allowed for the instantaneous copying of the physical medium, securing confidential information consisted of marking the physical medium (normally paper) as confidential or secret, and then physically securing access to only those individuals who were allowed to view this information. This provided instant and permanent data classification, which was physically attached to the recording medium. Access to the recording medium could easily be controlled, as personal contact was required to access the information, and identification of the individual was easily done. As copying the information would be difficult and lengthy, it was also easy to ensure that no copies of the information were being made that could be circulated in an uncontrolled fashion. This control of confidential information has become exponentially more difficult over the last 50 years with the advent of technology that at first allowed for fast copying of documents ("in 1968, Xerox introduced its first office copier"[4]) followed by the introduction of the personal computer (1976) and the spread of the Internet. These new technologies made it simpler to copy and disseminate information that was now increasingly being stored in electronic format. This led to the issuance in 1983, and then revised in 1985, by the Department of Defense (DoD) in the United States a document entitled "Trusted Computer System Evaluation Criteria"[5] (TCSEC) commonly referred to as the Orange Book (part of the Rainbow series). This document defines in great detail the classification and security criteria required to protect sensitive and confidential government information. With the advent of Office Automation (OA) tools, the DoD issued a "National Telecommunications and Information Security Advisory Memorandum (NTISSAM)"[6] dealing with the increased risk and security challenges posed by OA systems and the emerging computer networks they are attached to.

"2.0 THE OFFICE AUTOMATION SECURITY PROBLEM
There are three major points to remember about Office Automation Systems when considering security of these systems throughout their life cycle. These points are:
(1) Most current Office Automation Systems do not provide the hardware/software control necessary to protect information from anyone who gains physical access to the system. Therefore, the most effective security measures to be used with these systems are appropriate physical, personnel, and procedural controls.
(2) All information stored on a volume of magnetic media (e.g., floppy disk, cassette tape, fixed disk) should be considered to have the same sensitivity level. This level should be at least as restrictive as the highest sensitivity level of any information contained on the volume of media.
3) There are different security considerations for OA Systems with fixed media versus those with removable-media-only."[7]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The challenge to protect confidential information has continued to escalate as the technology that interconnects our computing facilities becomes more sophisticated. The introduction of wireless networks, Personal Digital Assistants (PDA's), cell phones, and seemingly unlimited entry points to the Internet all pose significant additional risk in the protection of confidential information.

As identified in the abstract, corporations now have the requirement to protect their confidential information in a similar fashion as governments have in the past. There are many examples where large amounts of confidential information have not been adequately protected:

"The California State University's controversial $662 million computer system contains a security flaw that gives users access to student and employee Social Security numbers and other confidential data." [8]

"Up to 750,000 customer files may have been on the missing drive, the *Globe and Mail* reported Monday."[9]

Although the criteria identified by the DoD in the Orange Book referred to above provide a solid framework to protect confidential information, its implementation has always been seen as too costly and restrictive to be implemented in a corporate environment, therefore a lighter and more manageable criteria, along with security tools which can be cost effectively implemented in the corporate environment are required. The rest of this paper will explore the concept of data classification in the corporate environment.

Basic data classification schemes and methodologies

There are a number of essential elements that comprise a data classification scheme and methodology. These elements include:

- A corporate policy on information and data protection
- An inventory of all data and information in the corporation
- Assigning ownership of the data and information
- Choosing an appropriate classification scheme
- Classifying the data and information

We can now look into each of these elements in more detail.

Corporate Policy

There is a need to define a corporate policy on the protection of data and information that is held within the corporation. It is extremely important that this policy be a corporate policy, and not an Information Technology policy, or a Computer Security policy. The protection of data and information within an organization goes far beyond securing data that resides on computer media. It is as much of a people issue as that of a technical issue. Everyone within the organization must be aware of the need to protect data and information held in trust by the organization in all its forms. Everyone must feel responsible for protecting the data and information that they have access to, including ensuring everyone they may pass the information onto is also aware and responsible for

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

its safeguarding. A very simple sample Information Protection Policy could go as follows:

INTRODUCTION

The information and data stored within the organization are company assets of great value and steps must be taken to protect them from unauthorized use, modification, destruction, or disclosure whether accidental or intentional.
This policy defines guidelines for the protection of information and data stored and maintained within the organization including the need for disaster recovery and contingency planning, and sets forth the responsibility of management and staff in this regard.
Awareness about the need for information protection, and the knowledge that information protection is for the benefit and protection of the company and all its employees is of key importance to a successful information protection policy.
The Information Protection Policy also ensures compliance with the legal aspects of computerized data and to allow the company legal recourse in the event of a serious security violation, whether internal or external.
It must be realized that there is no single measure that on it's own will be able to eliminate all risks. The most effective approach must be comprised of several interdependent measures such as computer security, physical security, employee awareness, and personnel security, which will each be addressed by separate policies.

GENERAL PRINCIPLES

This Policy sets forth guidelines and responsibilities to protect all corporate computer information and data, software, and hardware of the Canadian Operations of XXX Company and its subsidiaries. It will address the following areas:

- Compliance with Corporate Information Protection Policy
- Protection against the loss or misuse of corporate information and/or data;
- Define employee responsibilities and accountability to maintain protection of corporate information and/or data;
- Define implementation of corporate information policy

COMPLIANCE WITH THE CORPORATE INFORMATION PROTECTION POLICY

The Policy's requirements are mandatory for all employees including temporary staff and consultants. It is also expected that they will observe not only the letter but also the spirit of the Policy. Any employee misconduct with respect to the Policy is subject to disciplinary action being taken, including termination of employment. Action may also be taken against consultants.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

PROTECTION OF CORPORATE INFORMATION AND /OR DATA

It is the Policy to permit authorized users only that level of access to corporate information and/or data that is required to perform their duties and functions. The information and/or data provided by clients, employees, brokers, agents, investment partners and any other business associates of XXX to the company must be held in trust and protected commensurate with the nature of the data. It is to be used internally, consistent with other internal policies and procedures, unless required by law, and is not to be released to external entities without the provider's consent. Senior management must authorize any exceptions or deviations.
The information or data owner will be responsible for classifying information or data groups that are highly confidential or that require a high degree of integrity or availability. Special security requirements needed to protect, verify, or backup this information will be defined by the owner. The associated measures will be developed and implemented by the appropriate area within the company.

EMPLOYEE RESPONSIBILITIES AND ACCOUNTABILITY
Because information is so important and so pervasive throughout Company XXX's business, all employees have an important role to play as well as a responsibility to protect the information entrusted to their care. All employee's who may come into contact with confidential information and/or data are expected to familiarize themselves with all information and/or data protection procedures, including the data classification system policy and to consistently use it in their business activities.
All employees having access to confidential information and/or data are responsible to ensure that it is not disclosed to unauthorized persons and that it is properly disposed of when no longer needed.

IMPLEMENTATION OF CORPORATE INFORMATION POLICY

The top level of management within the company should approve the policy, and the policy should have the full endorsement of the computer security, legal, audit, and human resource departments. This is essential to the success of the policy as it will ultimately be these departments charged with monitoring and enforcement of the policy.

Create an inventory of all data and information in the corporation

This will prove to be one of the most difficult tasks in implementing data classification within an organization. Within even a small to mid-sized organization, data and information reside on multiple platforms in multiple formats. Data and information will not only reside in the corporate databases, but will reside in spreadsheets, word processing documents, and personal data stores. One must also remember data or information that may not reside in electronic format, but is stored in filing cabinets and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

archives. This data and information must also be identified so it can be assigned an owner and assigned a proper classification.

Assigning ownership to the data and information

Once the data and information has been identified, ownership must be assigned. The person within the organization who will be assigned ownership will have the following responsibilities:

- Identify data of a highly confidential nature or data requiring a high degree of integrity or availability
- Define any special security requirements needed to protect, verify or backup those data identified as having special needs, commensurate with the value of the data
- Ensure the integrity and timeliness of the data, commensurate with its value and use
- Authorize access and use of the data
- Define security and audit requirements
- Ensure that the security features are developed to meet these requirements and that they function properly
- Ensure that all changes made to the software are approved and properly tested
- Administer application based security that does not require special technical knowledge
- Ensure the security, maintenance and backup of the user documentation.

To fulfill these duties the person chosen must have sufficient knowledge of the data and applications to make sound decisions on its protection. They must also have an adequate level of authority to enforce and backup decisions regarding the protection of the data under their responsibility.

Choosing an appropriate classification scheme

There are many classification schemes available from the very detailed ones described in the DoD Orange Book, to ones that simply divide the data into confidential and non-confidential. I believe a scheme somewhere in between would be most suitable for the corporate environment. For example:
HIGHLY CONFIDENTIAL: This classification applies to the most sensitive business, employee, and customer information. Its unauthorized disclosure could seriously and adversely impact the company. Examples include customer or employee health information, corporate level strategic plans, litigation strategy memos, reports on new product research, and trade secrets such as certain computer programs.
CONFIDENTIAL: This classification applies to less sensitive business information that is intended for use within the company. Its unauthorized disclosure could adversely impact the company, its business partners, its employees, and/or its customers. Information that is considered to be private is included in this classification. Examples include employee personal information, customer personal information, passwords, PINs, and internal audit reports.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

FOR INTERNAL USE ONLY: This classification applies to all other information that does not clearly fit into the above two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the company, its employees, its business partners, and/or its customers. Examples include the internal telephone directory, global financial results published to employees, and internal policy manuals.
PUBLIC: This classification applies to information that has been explicitly approved by the company for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

Once the classification scheme has been determined, the data must be assigned to one of the levels of classification. Once this is done this will determine the levels of confidentiality, integrity, and availability of the data. Good examples of this can be found at:

http://www.sans.org/rr/securitybasics/class.php[10]
http://www.hhic.org/hipaa/pdf/datamatrix.pdf.[11]
Article by warren Schmitt on Information Categorization and Protection[12]

Classifying the data and information

Once the data inventory is completed (or as complete as reasonably possible) the task of classifying the data begins. The following elements should be taken into consideration when classifying data into the various confidentiality categories:

1. The data should be categorized into major categories such as customer data, employee data, information about the company, and general information. The major categories should normally not number more than ten or twelve. Any more that this and you are probably identifying sub-category areas.
2. These categories could then be sub-categorized into areas such as financial information, personal information, health information, public information, strategic information and so on. These categories should be relevant to your company and business. All legal, human resource, and audit requirements, along with all applicable legislation should be taken into account when defining the sub-categories so the resulting categorization will provide the proper levels of protection as required by these elements.
3. Each of the sub categories should then be assigned a confidentiality level. Some of the levels will be assigned based on requirements laid out in legislation, internal policies, and sound business practices. Others will have to be established working with the business experts within the organization.
4. The threats associated with each sub-category should be identified. Threats would include such items as loss of confidentiality (data is copied or stolen), loss of data (data is deleted), loss of data integrity (data is modified or is incorrect), and loss of access (denial of service attack).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5. Each of the threats should be evaluated for the risk associated with the threat. Depending on the controls in place to prevent a given threat, the level of risk may be reduced.
6. The impact on the organization should a particular threat become reality should also be identified. For example, what impact would it have on the organization if customer financial information were compromised? Impacts could be financial, loss of reputation, legal proceedings, loss of license to operate etc.
7. A grid or table outlining all the information should be created, and each of the sub-categories should then be assigned a confidentiality level based on the levels of threat, risk, and potential impact.

Once this process is complete, the result will be information identifying what level of protection is required for all the data in the organization.

Other elements that could be addressed when classifying the data are data integrity, and availability, as much of the information required to do this categorization has been gathered. If these elements are important to your organization, it is a good opportunity to classify the data in these categories at the same time. Using the same grid as the one used to assign the confidentiality levels, the sub-categories can be identified as to their data availability needs and data integrity needs. The following scheme could be used:

INFORMATION AND DATA INTEGRITY CLASSIFICATIONS:
Essential: Information and Data in this category must always be accurate and up-to date. No errors in this data can be tolerated. Some examples include medical information, information required to make critical decisions, which could involve life-threatening situations, employee salary information.
Important: Information and data should be substantially accurate and up-to-date. Inaccurate information would be undesirable, but would not have dire consequences on the ongoing operations of the company, and would not be life threatening. A small number of inaccuracies on a periodic basis would be accepted. Examples would include customer phone numbers or addresses occasionally being out-of-date, employee family information on the HR system.
Normal: Information and data do not require a high degree of accuracy and timeliness. A certain amount of errors can be accepted. Examples would include the company cafeteria menu, the company's softball team schedule.

INFORMATION AND DATA AVAILABILITY REQUIEMENTS
Essential: Information and data must be available 24 hours a day, 365 days a year, with no interruption of service, and no acceptable data loss. Less than 1 hour of unavailability can be tolerated in a crisis situation. This type of information calls for redundancy and immediate fail over. Examples would include critical medical information in a hospital, criminal information required by law enforcement officers in the field, automated banking information and transactions,
Important: Information and data must be available the majority of the time, but some interruption in non-business hours is acceptable. Up to 24 hours of unavailability can be

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

tolerated in a crisis situation. Some data loss is acceptable as it can be reconstructed from source information. Examples include most regular business transaction, especially non-financial transactions.
NORMAL: Information and data can be unavailable outside of normal business hours. In a crisis the information or data can be unavailable for over 24 hours (sometimes for several days) before operations are severely impacted. A few days of data loss is acceptable because the data is easily reconstructed form other sources. Examples include accounting records, taxation data, and departmental data (time sheets, vacation records).

Overall assessment of the state of data classification

My research has not been able to find any mention of successful implementations of data classification outside the implementations done by Government agencies such as the DoD and NSA. The following article in Information Week indicates that data classification is low on the list of corporate priorities.

"Rollout Is Sluggish
Data classification promises many rewards, including avoiding possible mismanagement of customer and employee data through better understanding. Yet businesses remain reluctant to commit their IT departments to this endeavor. Of the 2,092 U.S. security professionals surveyed by *InformationWeek* Research, only one in five say data ownership and classification standards are a company priority. This number isn't expected to soar any time soon: Just one in four expect both initiatives will be company objectives in the next 12 months. That's surprisingly small, considering the public-relations disaster companies may endure if they're tarred publicly as abusers of customer data."[13]

© SANS Institute 2003, Author retains full rights.

It is my opinion that with the increased amount of legislation now being passed as law requiring corporations to adequately protect personal information, along with growing consumer demand to have their information properly protected due to the increase in

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

cyber crime and identity theft [14] [15] will cause corporations to reevaluate the need for data classification. The use of data classification will enable corporations to clearly identify and understand the data they hold within the organization, and will allow funds to be directed to implement proper security infrastructure to protect the most sensitive and valuable information. This will be taking computer security to the next level of information protection. Information that is the most sensitive and at risk will be protected beyond simple firewalls and access controls, with encryption schemes that allow only authorized individuals to unlock the data, and will prevent the transfer of confidential information to environments which are not secure. In order to do this sensitive data will be not only encrypted, but will also be permanently tagged and labeled so its movement can be detected. This will allow for monitoring to ensure confidential information is not moved to unsecured environments or individuals. The technique used to do this is known as Mandatory Access Controls.

"Mandatory Access Controls restrict access by means of special attributes that are set by the security administrator and enforced by the security software and or the operating system. These controls cannot be changed or bypassed at the discretion of any non-privileged users. Mandatory Access Controls are typically based on information *labeling*, where the administrator labels each item of information with a classification name such as Public, Internal, Confidential, and Restricted. Each user is assigned a clearance level from the same set of classifications. The security software and/or operating system then controls access to the information based upon these classifications"[16].

Implementing this type of security scheme will greatly improve the security of the data under its control, but it is a daunting task for corporations with huge amounts of data. This task will become more manageable as software solutions both at the operating system level and thru independent vendors become more available, affordable, and usable.[17] [18] [19]

In all likelihood this movement towards data classification will take place over the next 2 to 3 years, with many corporations implementing full data classification within five years, with the corresponding mandatory access controls in place to protect the data.

Identify critical success factors and potential pitfalls

There are a number of key success factors that will allow any data classification effort to succeed. Some of the key factors are as follows:

1. One that is always on the success factors list is making sure you have the buyin and support of upper management. This is easy to say, harder to do. There are a number of elements that can be used to get upper management on your side. Primary among these is to demonstrate this as a business project, not a technical project. The goal is to protect the company's data and information, not to implement the latest security gadget. Secondly, tie this project directly into corporate strategies. Show how data classification can improve customer service, improve the company's profile, and foster customer loyalty. Thirdly, show how this project can help the bottom line. Determine where money can be saved, and cost avoided by implementing data classification and improving the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

protection of one of the companies' most valuable assets, its data and information.

2. Make sure that this project is staffed by your best and you're brightest. This project requires people who understand the business, who understand the business processes, who understand computer security issues, and who understand the technologies that are available to protect the data once it is classified. It also needs strong project management to get all these factions to work together.
3. Make sure that internal audit and legal resources are members of your project team. Use their expertise and knowledge to guide your classification. They are the ones who should be the most knowledgeable of existing legislation, policies, and best practices. They can guide the project to ensure data is classified not only by its business importance, but also so that the corporation can comply with all existing legislation and industry regulations.
4. Implement in manageable pieces. The benefit of this is the corporation can begin to benefit earlier from improved knowledge of their data and information. It also shows that progress is being made and avoids pitfall number 2.

Some potential pitfalls include:

1. Don't underestimate the size of this undertaking. The initial project to classify the data would vary by size of the organization, but should take 1-2 years. But full implementation and maturity could take 4-5 years. Remember, this is a long journey to bring your company's data protection to another level.
2. Communication is essential throughout the project, especially to upper management so they can see that progress is being made. The last thing you want to happen is to have upper management pull the plug from impatience due to lack of information.
3. Don't wait until everything is done or everything is perfect to produce results. This will probably never happen, and in any case pitfall 2 will kick in and you won't finish the project.

Conclusions and Recommendations

I believe that this paper demonstrates that data classification can be applied in the corporate environment, and is an essential tool to improve the corporation's information protection profile. It is the basis for developing a computer security infrastructure that will be targeted to protect the corporation's most sensitive information in a manner that is most appropriate for that information using mandatory access control techniques. It is no doubt that implementing data classification is a major undertaking, so the best recommendation I can make is to start as soon as possible, for it is clear that protecting the information within the corporation will be one of the top priorities over the next few years.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

[1] [Bill C6] Government of Canada. 2nd Session, 36th Parliament, 48 Elizabeth II, 1999 The House of Commons of Canada
An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act
http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_3/C-6TOCE.html

[2] [Bill C6] Government of Canada. 2nd Session, 36th Parliament, 48 Elizabeth II, 1999 The House of Commons of Canada
An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act
http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_3/C-6TOCE.html

[3] [Info Week] Helen D'Antoni. Companies Struggle With Data Classification. InformationWeek. Aug 20, 2001 (12:00 AM)
http://www.informationweek.com/story/IWK20010817S0007

[4] [Hall of Fame] National Inventors Hall of Fame. 2000-2002
http://www.invent.org/hall_of_fame/27.html

[5] [TCSEC] Department Of Defense Trusted Computer System Evaluation Criteria. Rainbow Series Library. Last updated Wed Jun 28 13:44:26 2000.
http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

[6] [Advisory] Advisory Memorandum on Office Automation Security Guidelines. Rainbow Series Library. Last updated Wed Jun 28 13:44:26 2000.
http://www.radium.ncsc.mil/tpep/library/rainbow/N-C-1-87.txt

[7] [Advisory] Advisory Memorandum on Office Automation Security Guidelines. Rainbow Series Library. Last updated Wed Jun 28 13:44:26 2000.
http://www.radium.ncsc.mil/tpep/library/rainbow/N-C-1-87.txt

[8] [Sacbee] Hardi, Terry. CSU computer glitch reveals personal data. The Sacramento Bee. March 21, 2003
http://www.sacbee.com/content/news/story/6314106p-7267555c.html

[9] [CBC News] Written by CBC News Online staff. Investors Group says customer information on missing hard drive. February 3, 2003.
http://www.cbc.ca/stories/2003/02/03/ism_030203

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[10] [SANS] Flierman, Margaret. Data Classification, SANS. April 30, 2001. http://www.sans.org/rr/securitybasics/class.php

[11] [HHIC] Data Classification Matrix. Hawaii Health Information Corporation http://www.hhic.org/hipaa/pdf/datamatrix.pdf

[12] Schmitt, Warren. Information Categorization and Protection. Handbook of Information Management / Zella G. Ruthberg, Harold F. Tipton, editors. Auerbach Publications, 1993 (PP 467-479)

[13] [Info Week] Helen D'Antoni. Companies Struggle With Data Classification. InformationWeek. Aug 20, 2001 (12:00 AM) http://www.informationweek.com/story/IWK20010817S0007

[14] Verton, Dan. Internet fraud expanding, security experts warn. Computerworld. February 14, 2003 http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,78551,00.html

[15] Rosencrance, Linda. FBI: Internet fraud complaints up in 2002. Computerworld. April 10, 2003 http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,80200,00.html

[16] What Is Network Security? http://developer.novell.com/research/appnotes/1997/november/01/02.htm

[17] Dragonfly Guard Model G.12, Software Release 3.0 http://niap.nist.gov/cc-scheme/TTAP-CC-0001.html

[18] Trusted Solaris 7 Operating Environment. Mandatory and Discretionary Access Control http://wwws.sun.com/software/solaris/trustedsolaris/7/ts_feature_macdac.html

[19] Gateway Guardian. http://www.netmaster.com/products/ggos-tech-overview.pdf

Bibliography

Appleyard, Jim. Information Classification: A Corporate Implementation Guide. Handbook of Information Management / Micki Krause, Harold F. Tipton, editors. Crc Press LLC, 1998

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Smith, Martin R. Commonsense Computer Security: Your Practical Guide to Preventing Accidental and Deliberate Data Loss. Maidenhead, Berkshire, England. McGraw-Hill Book Company (UK) Limited. 1989.

Gahtan, Alan M., Martin P.J. Kratz, J. Fraser Mann. Internet Law A Practical Guide for Legal and Business Professionals. Scarborough, Ontario. Carswell Thomson Professional Publishing. 1998

POA Publishing, LLC. Asset Protection and Security Management Handbook. Boca Raton, Florida. Auerbach Publications, a CRC Press Company. 2003

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.