SANS | GIAC CERTIFICATIONS

WHITE PAPER

Protection of Information Assets

Odd Nilsen

Copyright SANS Institute 2021. Author Retains Full Rights.
This paper was published by SANS Institute. Reposting is not permitted without express written permission.

GSEC Practical Assignment version 1.3

PROTECTION OF INFORMATION ASSETS

Odd Nilsen

March 17 2002

Part 1 Summary

This paper is focusing on protection of information assets, or more specifically the security challenge we are facing in the process of protecting the businesses information assets. So were should we begin addressing this security challenge? This paper is focusing on physical security, but will also go thru the aspect of logical controls to put security in a broader perspective. Part 2 will give a short introduction to the topic, part 3 will focus on physical access exposures and controls, and part 4 will give an introduction to logical access exposures and controls.

Maintaining a good physical security is at least as important as logical security, but basically one is not good without the other. There are a number of ways to maintain both of them, and some of them have been mentioned in this paper. There are a number of ways to control-, authorize- and monitor access to a facility or computer system, both physically and logically. The real challenge is to find the right level of security that exactly fits your organization. This paper is going to address the issues that will affect most businesses concerning physical and logical security.

Part 2 Introduction to the topic

Continuity of operations and correct functioning of information systems are essential to all businesses. Threats to computerized information and processes are threats to business quality and effectiveness. The objective of IT-security is to put measures in place, which eliminate or reduce significant threats to an acceptable level.

The company should have a process for protecting data files, application programs, and hardware through a combination of physical and logical security controls. Physical security involves restricting physical access to computer- and information resources, usually by limiting access to the buildings, areas and rooms where they are housed. However, physical controls cannot alone ensure that computer- and information resources are sufficient protected. For this reason, it is important to establish logical security controls that protect the integrity and confidentiality of sensitive information. The security function in the company should be responsible for implementing and maintaining both physical and logical controls based upon authorizations provided by the owners of the resources.

Where do we start to improve the physical- and logical security? First the business needs to know what computer- and information resources that need to be protected, by

© SANS Institute 2002, As part of GIAC practical repository.

recognizing the threats and judging possible impacts. Then they have to calculate the risks and decide what risks are acceptable. Basically there are some important points concerning security to keep in mind[1]:

- *Keep it simple.* If security is very complicated, it is unlikely to be effective and likely to be expensive.
- *Keep it coherent*. It is better to have a minimum, coherent level of security than some system highly protected and other dependant systems wide open.
- *Keep to some known and well-tried standard if possible.* It will make evaluation easier.

Part 3 Physical Access Exposures and Controls

A business that is dependent on computer resources cannot be carefully enough with the computer security. But this includes more than enforcing strong passwords and using antivirus software. If the system itself is not *physically* secure, nothing else about the system can be considered secure. With physical access to a machine, an intruder can halt the machine, bring it back up in privileged mode, replace or alter the machine, plant Trojan horse programs, or take any number of other undesirable actions. Concern should also be given critical communication links like switches or routers. Overall a good physical security program is an organization's first line of defense. Physical security considerations in brief are an overall assessment of the security needs with regard to facility location, layout and construction of facility, access control to facility, monitoring access etc.

3.1. Physical Access Exposures

An almost unlimited number of threats can theoretically be of concern to an organizations well being. The main focus of physical security has often been on human-made disasters, such as an attack over the network from a outside hacker or plain human error from own employees. Even if these in fact are the most common threats, it is crucial not to forget that the same kind of threats also can occur from natural disasters such as fire, water leakage, electricity disturbance or other environmental failures.

The human factor

It is assumed among many computer security officials that a majority of theft, fraud, sabotage and accidents are caused by a company's own employees. The most probable causes are accidental human error or tampering from unauthorized users. This is supported by a survey reported on the SearchSecurity.com[2] in April 2001. This survey indicates that the respondents sees human error as one of the major security

[1] Boran. IT Security Cookbook, chapter 2
[2] SearchSecurity.com. Survey: Corporate security policies

© SANS Institute 2002, Author retains full rights.

challenges and the hardest part of the security policy to enforce. Who is the perpetrator? Some sees the typical computer criminal a non-technical authorized user of the system who has been around long enough to locate the control deficiencies and use them to cut corners, or it may be plain accidental errors.[3] But it also may be people not affiliated with the company or intruders from the outside trying to exploit deficiencies in the facility security to commit harm against the business. The challenge is to keep both of these groups outside restricted areas by enforcing proper physical access controls. This is the first step or first defense against intruders: keep intruders or unauthorized personnel out of the building, restricted areas and computer rooms. How could this be done? Everyone who should gain access to a business environment should have to pass an authentication and/or authorization test. This could be something the user knows (a password), that the user has (a badge, key, card etc) or of their physiognomy (fingerprint, voice etc).

Natural disasters

As mentioned earlier the main focus for physical access exposures is often given to the human factor. But it is very important to *consider* all potential threats, even unlikely ones. Natural disaster can actually have a major affect if they occur. Some of the natural disasters that can occur are discussed in the IT Baseline Protections Manual[4] and CISA Review Technical Information Manual[5] e.g. fire, electrical interruption, lightning, water, earthquake and other environmental disasters.

- *Fire*
  Basically a fire can be minor, major or catastrophic to the business. A fire may cause various damage to the building, but there also may be other consequences. Water, smoke or gases may influence sensitive IT-systems in a harmful way.

- *Electrical interruption*
  Power failures, even very short ones, can disrupt computer operations. It is not just computer operations that will suffer from electrical disturbance. In today's business environment there is a lot of necessary equipment that is dependent on electric power, e.g. alarm systems, air conditioning and telephones.

- *Lightning*
  The occurrence of lightning during a thunderstorm can cause an electrical surge to electrical power transmission lines, and thus destroy sensitive electronic equipment attached to transmission lines. A lightning can also cause damage by fire or structural damage to buildings.

[3] Tipton, Krause. Handbook of Information Security Management, chapter 4
[4] Bundesamt für Sicherheit in der Informationstechnik. IT Baseline Protections Manual, chapter 4
[5] ISACA. CISA Review Technical Information Manual 2001, chapter 4

© SANS Institute 2002, Author Retains full rights.

- *Water*
  The uncontrolled flow of water into buildings or rooms may come as a result from the burst or leaking of water pipes, accidental discharge of sprinklers, rain or water used to fight fire. Uncontrolled leakage of water can cause considerable damage to buildings and IT-equipment.

- *Environmental disasters*
  Any interruption in the supply of controlled environmental support provided to the operation center, e.g. humidity and temperature.

- *Earthquake*
  This may not be a big risk, unless your facility is cited in a earthquake exposes area. However, if they occur, earthquakes can be really disastrous to the business.

3.2 Physical Access Controls

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Computer resources to be protected include primary computer facilities, cooling system facilities, terminals that are used to access a computer, microcomputers, computer file storage areas and telecommunication equipment and lines, including wiring closets.

Before any controls can be implemented into the workplace, it is necessary to assess the current level of security in the facility. This can be accomplished in a number of ways. The easiest is a walkthrough in the facility and perimeters after hours and check some key controls e.g.:

1. Building, office doors, desks and cabinets are locked
2. Computer rooms and telecommunication rooms are secured
3. Ways of controlling access to company information
4. Ways of monitoring access to company information
5. In general check how company information is secured

This will give a basic understanding of the level of control already in place and a benchmark for measuring improvements once a security control system is implemented. It is important to evaluate the possible risks and likely impact against cost. Basically you have to find the right level of security to *your* business.

Types of physical access controls

Physical access controls can be classified as preventive or detective controls. Preventive controls attempt to avoid the occurrence of unwanted events, detective

© SANS Institute 2003, Author retains full rights.

controls attempt to identify unwanted events after they have occurred. Preventive physical security controls vary, but may include[6]:

- Manual door or cipher key locks.
- Magnetic door locks that require the use of electronic keycards
- Biometric authentication
- Security guards
- Photo ID's
- Entry logs
- Logs and authorization for removal and return of tapes and other storage media to the library
- Perimeter fences around sensitive buildings
- Computer terminal locks

Detective security controls e.g. are[7]:

- Motion detectors
- Smoke and fire detectors
- Electronic and visual surveillance systems
- Perimeter intrusions alarms

Which physical access control is to prefer, the preventive- or the detective access control? Detective controls do not influence the everyday work of the employees, they are in a sense "invisible" until someone have violated a restriction and we need to identify what's happened (e.g. alarms, surveillance systems). Preventive controls tends to limit the employees use of information systems and which area the employees can move around in (e.g. security guard, door locks). To secure necessary co-operation it is imperative that the employees understand why preventive controls are implemented. Preventive controls in general are a better way to enforce security, because its there to *avoid* unwanted events from happening in the first place. But if an unwanted event should occur, it is better to know about it using detective controls. If you e.g. have an intruder passing by a security guard unseen, it is better to detect this on a visual surveillance system or alarm system than have the intruder walking around in your "backyard". A preventive control is basically better off in co-operation with a detective control, in the sense that they tend to complement each other.

Restricted Zones

In a facility there are different kinds of areas, some areas are more sensitive than other and must be protected as much as possible. A way to do this is to establish restricted zones for areas where sensitive computer systems, assets, information and support utilities are located. These areas typically include computer rooms, LAN-server

[6] GAO. Federal Information System Control Audit Manual, chapter 4
[7] GAO. Federal Information System Control Audit Manual, chapter 4

© SANS Institute 2002, Author retains full rights.

rooms, telecommunication centers, media libraries, UPS room, and offices and their related computer equipment (PC's, printers, fax machines)

Zones could be defined as indicated in the IT Security Cookbook[8]:

- Zone 1: areas open to the public, e.g. reception area
- Zone 2: areas not open to the public, open to company staff
- Zone 3: Protected areas. Only accessible with identification, access strictly controlled.

Access to restricted zones should be controlled, authorized and monitored closely to avoid unauthorized access.

Controlling access

When proper zones are defined it is time to think of how to control access to the restricted zones. Access to restricted zones can be controlled by using appropriate methods such as proposed in the Technical Security Standard for Information Technology (TSSIT)[9]:

- Installing electronic access controls, mechanical combination locksets, or deadbolts;
- Limiting the number of entry points to the minimum required by the fire regulations; and
- Situating personnel (receptionists, office employees, guards) at entry points.

Buildings should in general always be locked, except for access via a reception area during office hours. Building must be monitored 24 hrs a day by security personnel. Especially concern should be given the computer room and other areas important to the system (e.g. telecommunication room). Computer rooms must be locked, if possible with electronic card access. Only a very limited number of people should have access to this area. Access should be recorded on video.

Authorizing access

It is important to maintain a list of persons authorized to access rooms especially designed for sensitive IT-assets and operation, such as computer rooms, server rooms and telecommunication rooms. Make sure that the access records for restricted zones as a minimum include details as name of the person entering, date and time of entry and departure, and restricted zone entered. Make sure that security personnel review access control records for restricted zones regularly.

[8] Boran. IT Security Cookbook, chapter 8
[9] Royal Canadian Mounted Police. Technical Security Standard for Information Technology, chapter 4

© SANS Institute 2002, Author retains full rights.

Monitoring access

Access to security zones should be monitored continuously. Monitoring methods could include security guards, electronic intrusion detection systems or electronic access control systems with recording capability. All persons authorized to enter restricted zones should be issued, and required to wear an approved access badge. The access badge should meet some minimum requirements such as badge control serial number, be sealed in a tamper proof enclosure, bear a facial-view color photo and uniquely associate restricted zone.

When implementing an identification card or access badge system it is important to establish procedures for issuing and retrieving cards and badges. Also maintain records documenting the issue and retrieval of security-related items such as keys and cards for card-access systems. The Technical Security Standard for Information Technology from the Canadian Mounted Police gives examples of issues to consider when establishing procedures for issuing and retrieving cards and badges[10].

Backup media

The most effective solution to prevent loosing business information due to human error or natural disasters is to create backups. Many types of backups are possible: daily, weekly and monthly. Backup media should be stored in locked safes or locked rooms. The backup media should be stored far enough away from the origin to avoid the same kind of incident that destroyed the original. Regular backups (at least one per month) should be stored off site. In general backups of sensitive information should have the same level of protection as the active files of this information. The IT Baseline Protection Manual from Bundesamt für Sicherheit in der Informationstechnik gives examples of how to establish procedures for backup[11].

Workplace

Desks should be kept "clean" every evening when the employee leaves his place of work. This ensures that sensitive or confidential information is not made available for unauthorized personnel. It is also important to position IT-equipment handling sensitive information in a manner that prevents unauthorized overview or access. This can be achieved by e.g. facing monitor screens away from windows or adjacent areas and place printers fax machines and other peripheral equipment appropriate. Especially printers used for printing confidential information should be placed in restricted rooms.

[10] Royal Canadian Mounted Police. Technical Security Standard for Information Technology, chapter 4
[11] Bundesamt für Sicherheit in der Informationstechnik. IT Baseline Protection Manual, chapter 3

© SANS Institute 2001, Author retains full rights.

Contingency plan

The business should have a contingency plan in case of extraordinary events. The contingency plan should cover events such as power cuts, theft, fire, flooding, explosions etc. This document should be a plan to ensure that an essential level of service would be provided following a loss of processing capability or destruction of the facility. The contingency plan should cover on-site and off-site recovery, and e.g. consider recovery from any failure to the system and information resources, forced evacuation of the facility, loss of critical support system and identification of key personnel. The GAO Federal Information Systems Control Audit Manual and the Bundesamt für Sicherheit in der Informationstechnik's IT Protection Manual gives suggestions concerning the aspects of a contingency plan[12].

3.3 Personnel physical access control

In the last pages it has been given attention to strictly *physical* access controls. In the past few years another aspect of access control has become more important than before; the personnel physical access control. The company and the employee have specific legal and ethical responsibilities to each other. This goes for both during and after the period of employment. Hiring and termination criteria, trade secrets and noncompetition clauses are all issues that can cause serious legal problems for a corporation and it employees.

The Handbook of Information Security Management suggests some precautionary measures that the company could take to safeguard their information assets[13]:

- Choose employees carefully
- Create an good work atmosphere
- Employees should be reminded of their responsibilities on a regular basis
- Be careful when an employee is discharged. Such employees should not be allowed access into business critical systems. Do not be overly distrustful with departing employees. They do not wish to harm their former employer, but only take advantage of a better job possibility
- Protect trade secret in a properly manner

Basically it is important to have intelligent restrictions to sensitive information. Sensitive information should only be given to employees on a need-to-know basis. Audit trails should record who accessed what information, at what times, and for how long. If proper care is given to these measures, it will reduce the chance of unauthorized access or unintentional disclosure.

[12] GAO. Federal Information System Control Audit Manual, chapter 3
[13] Kraus, Tipton. Handbook of Information Security management, chapter 10

© SANS Institute 2002, Author retains full rights.

3.4 Location access control

As mentioned earlier there are a number of possible natural disasters that can affect the business. In order to minimize the risks associated with possible natural disasters there are some preventive measures that could be taken.

Minimize risks to IT-systems by choosing facility locations with due regard for such treats as flood, earthquake and electromagnetic interference. It is not a good idea to place the facility near a river that tends to flood every year. Make sure that areas in the facility containing sensitive IT-systems, information or assets are situated so as to minimize exposure to threats such as fire, flooding, water damage, corrosive agents or externally generated electromagnetic radiation. If the facility in fact is placed near a river that tends to flood, do not place the computer room in an underground basement!

Part 4 Logical Access Exposures and Controls

Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by e.g. requiring users to input user identification number, passwords or other identifiers that are linked to predetermined access privileges. Logical controls should be designed to restrict legitimate users to the specific systems, programs and files that they need and prevent others, such as hackers, from entering the system at all.

Logical security controls enable the business to[14]:

- Identify individual users or computers that are authorized access to computer networks, data and resources
- Restrict access to specific sets of data or resources
- Produce and analyze audit trails of system and user activity
- Take defensive measures against intrusion

Logical controls are used to prevent unauthorized personnel from gaining access to computing resources. Logical controls can e.g. include[15]:

- Access control software
- Antivirus software
- Passwords
- Smart cards
- Encryption
- Dial-up access control and callback systems
- Audit trails

[14] GAO. Federal Information System Control Audit Manual, chapter 3
[15] Krause, Tipton. Handbook of Information Security Management, section 1-1

© SANS Institute 2002, Author retains full rights.

- Intrusion detection programs

Access control software

The purpose of access control software is to limit and control access to resources of a computer system. Access control software provide the ability to control access to the system by establishing that only registered users with an authorized user ID and password can gain access to the computer system or specific data, e.g. Computer Associates eTrust CA-ACF2 Security for mainframes. Access control software is very important to the information security.

Antivirus software

Viruses are a significant and a very real logical access issue. According to the NIST Handbook[16] virus is a code segment that replicates by attaching copies of itself to existing executables. The new copy of the virus is executed when a user executes the new host program. Users can e.g. get a virus from the Internet by downloading files to their computers, or from a local area network. A virus is in general a variety of malicious computer programs and can seriously affect the business by damaging files or crashing networks. In the recent last year there have been numerous virus attacks like Melissa-virus and W32.SirCam, which have caused a lot of havoc and major costs to the attacked businesses. The best way to protect the business from viruses is to install antivirus software. An example of antivirus software in Norman's NVC which supports platforms like Windows and OS2. Antivirus software is applications that detect, prevent and possibly remove all known viruses from files located in a computer hard drive. In conjunction with antivirus software it is imperative for the business to have an antivirus policy and procedure controls. The policy and procedure controls should be a how, when, what and who concerning dealing with malicious computer programs and should be a part of the company's contingency plan. The Bundesamt für Sicherheit in der Informationstechnik's IT Baseline Protection Manual gives suggestion of how this could be done.

Passwords

A password is a protected, generally computer encrypted string of characters that authenticate a computer user to the computer system. A password is usually used as a second authentication after the user has entered the user ID. Most access control systems have different criteria's when setting up a password guideline. Typical controls for protecting the confidentiality of password should as a minimum include the following[17]:

- Passwords should be five to eight characters in length

[16] NIST. An Introduction to Computer Securi ty: The NIST Handbook, chapter 4
[17] CISA. Manual chapter 4 and GAO. Federal Information Sy stems Control Audit Manual, chapter 3

© SANS Institute 2002, Author retains full rights.

- Allow for a combination of alpha, numeric, upper and lower case and special characters
- Not be particularly identifiable with the user, such as name and date of birth
- The system should not permit previous passwords within five to ten generations to be used after being changed
- Passwords should be changed periodically, about every 60 to 90 days depending how sensitive data are.
- Password are not displayed when entered
- Vendor-supplied passwords must be replaced immediately after implementation
- Password should be personal to each user, not shared by a group

Enforcing a strict password policy is important. The SANS Institute[18] talks about password as the first line of defense against outside attacks. Weak passwords are easy to break using tools like e.g. L0phtCrack (LC3) or John the Ripper. Enforcing strong password will not make it impossible to crack passwords, but it will be harder and take more time. The article "The Simplest Security: A Guide To Better Password Practices" by S. Granger gives some very useful tips on password practices.

Smart cards

A smart card is an intelligent credit card sized device with a chip e.g. used for user authentication. A smart card is an object that the user has to authenticate identity. The purpose is to validate the user to a system. Smart card require the user to enter a personal code (PIN) along with the card to gain access. This increases security because it involves both something you must have (the card) and something personal you must remember (the PIN). Smart cards can e.g. be used on doors to restricted areas as the computer room. The use of smart cards will probably increase in the future as new technology and areas of use increase. The PC/SC Working Group has defined a standard for interface between programming and PC hardware in a smart card. Members of this group are companies like Microsoft, Toshiba and Intel[19].

Encryption

Encryption is a technique used to protect the plaintext by coding the data such that it is unintelligible to the reader. Encryption is generally used to protect data stored on computers, or in transit over networks, from unauthorized interception and manipulation. But encryption has its limitations. It can't prevent loss of data and encryption programs can be compromised. Encryption should be regarded as an essential but incomplete form of access control that should be a part of the businesses overall computer security.

[18] SANS. Security Essentials. Password Assessment and Management, section 10.2.3
[19] PC/SC Working Group Web Page

© SANS Institute, Author retains full rights.

Dial-up access control and callback systems

If users connect to the system by remote via a dial-up line (e.g. from home), access should be restricted by a dial-up access control. Dial-up access controls prevent unauthorized access from remote users that attempt to access a secured environment. These controls range from dial-back controls to remote user authentication. Dial-back controls are used over dial-up telecommunication lines. The telecommunication link established through dial-up into the computer from a remote location is interrupted so the computer can dial back to the caller. The link is permitted only if the caller is from a valid phone number. It is important that these phone numbers are changed regularly. If your system is not secured by dial-up access controls, you will be very vulnerable against e.g. war dialers like ToneLoc, which are used to sweep the company's extensions, hoping to stumble on an open modem to answer the call.

Audit trails

An audit trail is a visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source. For example, a corporate employee might have access to a section of a network in a corporation such as billing but be unauthorized to access all other sections. If that employee attempts to access an unauthorized section by typing in passwords, this improper activity is recorded in the audit trail. Audit trails are essential to the system security. Security officers should regularly review violation reports to identify successful or unsuccessful unauthorized access.

Intrusion detection systems

Intrusion detection systems gather and analyze information from various areas within a computer or a network to identify possible security breaches. These security breaches could include both attacks from outside and inside the organization. Intrusion detection functions generally include[20]:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

There are a lot of types of intrusion detection systems e.g. host based, network based, hybrids, honeypots etc[21]. This paper will only focus on host based and network based intrusion detection systems. Host based intrusion detection systems aim is to detect

[20] A searchSecurity definition
[21] Taliskers Network Security Tools

© SANS Institute 2002, As the Author Retains full rights.

suspicious activity on the host it is installed on, but not on the network. They are very valuable e.g. in finding unsecured modems and insider attack that don't cross the network and thus will not be caught by the network based intrusion detection. Enterasys's product Dragon Squire is an example of a host based intrusion detection system that supports windows 2000/NT among others. TCP Wrapper and Syslog are examples of Unix host based intrusion detection.[22].

Network based intrusion detection[23] monitors both inbound and outbound network traffic in order to flag and sometimes stop an attack before it accesses information assets or damages the network. Basically it is checking the packets and analyzing every packet for attack signatures. Examples of network intrusion detection systems include Cisco Systems inc. product Cisco Secure IDS (formerly NetRanger) and the open source intrusion detection system Snort.

The intrusion detection systems are used in response to the increasingly number of attack on major sites and networks. Intrusion detection systems should be a part of the organizations overall computer security. But which should we choose, host based or network based? Basically one is not good without the other because their strength is complementary.

Part 5 Conclusions

There are an unlimited number of human or natural made disasters that cause risk to business continuity in an organization. Organizations should analyze these risks and take necessary precautions. Maintaining a good physical security is at least as important as a logical security, but basically one is not good without the other. There are a number of ways to maintain both of them, and some of them have been mentioned in this paper. As stated in the previous parts there are a number of ways to control-, authorize- and monitor access to a facility or computer system, both physically and logically. The real challenge is to find the right level of physical and logical security that exactly fits your organization. Hopefully these previous pages have given you some ideas of the aspects to consider.

[22] SANS Institute. Security Essentials. The Big Picture, part 3
[23] A. Cliff. IDS Terminology, Part Two: H-Z

© SANS Institute, Author retains full rights.

References

1. United States General Accounting Office. "Federal Information Systems Control Audit Manual – Volume 1: Financial statements audit", GAO/AIMD-12.19.6 January 1999
URL: http://www.gao.gov/special.pubs/ai12.19.6.pdf (6 March 2002)

2. Bundesamt für Sicherheit in der Informationstechnik. "IT Baseline Protections Manual", July 2001
URL: http://secinf.net/info/misc/gshb/etc/inhalt.htm (6 March 2002)

3. Krause, Micki. Tipton, Harold F. "Handbook of Information Security Management" 1997
URL: http://secinf.net/info/misc/handbook/ (6 March 2002)

4. Royal Canadian Mounted Police. Technical Security Standard for Information Technology (TSSIT), August 1997

5. Boran, Sean. "The IT Security Cookbook", 1999
URL: http://secinf.net/info/misc/boran/ (6 March 2002)

6. A. Cliff. "IDS Terminology, Part Two: H-Z". 19 July 2001
URL: http://online.securityfocus.com/infocus/1214 (15 March 2002)

7. Information Systems Audit and Control Association (ISACA). CISA Review Technical Information Manuals 2001. Rolling Meadows: ISACA, Inc, 2000.

8. National Institute of Standards and Technology, "An Introduction to Computer Security: The NIST Handbook" - Special Publication 800-12

9. SearchSecurity.com, a TechTarget site for Security professionals. A search for the definition of "Intrusion detection"
URL:http://searchsecurity.techtarget.com/ (6 March 2002)

10. Whatis.com. A search for the definition of "Intrusion detection"
URL: http://whatis.techtarget.com/ (6 March 2002)

11 PC/SC Working Group. Web Page
URL: http://www.pcscworkgroup.com/ (15 March 2002)

12. Sarah Granger. "The Simplest Security: A Guide to Better Password Practices". 17 January 2002
URL: http://online.securityfocus.com/infocus/1537 (15 March 2002)

13. SANS Institute. Security Essentials, Section 10.2.3 Password Assessment and Management. v1.9. 12 February 2002

© SANS Institute 2000 - Author retains full rights.

14. Computer Associates eTrust CA-ACF2 Security. Web page
URL: http://www3.ca.com/Solutions/ProductFamily.asp?ID=111
(16 march 2002)

15. Norman. Norman's NVC. Web page
URL: http://www.norman.no (16 march 2002)

16. John the Ripper – password cracker. Web page
URL: http://www.openwal.com/john (16 march 2002)

17. L0phtCrack (LC3). Web page
URL: http://www.l0pht.com/research/lc3/index.html (16 march 2002)

18. Enterasys Networks. Dragon Squire – Host Intrusion Detection. Web Page
URL: http://www.enterasys.com/ids/squire/ (16 March 2002)

19. Cisco Systems inc. product Cisco Secure IDS. Web Page
URL: http://www.wheelgroup.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml
(16 March 2002)

20. Talisker's Network Security Tools. Web page
URL: http://www.networkintrusion.co.uk/ids.htm (16 March 2002)

21. SearchSecurity.com. Survey: Corporate security policies. 4 April 2001
URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci539143.html
(16 March 2002)

22. The W32.SirCam virus – additional information
URL:
http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html
(17 March 2002)

23. The Melissa Virus – additional information
URL:
http://securityresponse.symantec.com/avcenter/venc/data/w97m.melissa.u.gen1.html (17 march 2002)

24. Snort. The open source network intrusion detection system. Web page
URL: http://www.snort.org/ (17 March 2002)

© SANS Institute 2002, Author retains full rights.