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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

NOTICE: Secure Your Network

Responsibilities of Management, Information Technology Personnel and the Consumer.

© SANS Institute 2004, Author retains full rights.

Philippa Anne Lawton
GSEC Practical version 1.4b
January 2004

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Introduction

As technology continues to be an integral part of our lives it is also becoming commonplace in our business community. Companies are moving toward becoming "paperless" and our personal and private information lies somewhere between the office walls and the Cat5 cabling in a form that many average people do not understand: servers, databases, directories, files, clusters, and sectors. They do not need to understand this mysterious environment - they rely on the IT folks to do what they do. The reality is that many IT personnel, are great at building servers, connecting workstations to the network, installing software, and fixing the daily printer problems. Security breaches have become a frequent problem nationwide. Our government saw the problems of the organizational inconsistency between management and information technology and started to act.

According to the United States Postal Service, identity theft is the fastest growing crime in America.[1] Imagine some 20 year old, sitting in his basement with your bank account number and home address printing checks with your name and a fancy design – laughing his way to the bank. Our government witnessed this first hand as they raided home after home of hackers gazing at our information on their computer screens. While others inside the organization taking our credit card numbers with them as we conveniently purchased gifts over the Internet. We have to secure our networks and keep them secure, meanwhile the government is doing their best to ensure our privacy through the development of information technology laws.

In this paper we are going to take a look at just some of the various laws that have been enacted to secure our privacy and our nations' computer networks where that data is stored. We are going to consider the responsibilities of management, the IT department, and ourselves as informed citizens.

Health Insurance Portability & Accountability Act

In 1996, the U.S. Congress passed the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was enacted because congress saw a need to ensure that our private health information was secure as the electronic transmission of documents became more prominent. After three years, the Act was turned over to the Department of Health and Human Services to draft the specific regulations. This act is broad-based and includes: verbal discussions, paper documents, sign in sheets, and electronic data transmissions. HIPAA states, "the confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception

[1] USPS. "Identity theft is America's fastest growing crime."
URL:http://www.usps.com/postalinspectors/idthft_ncpw.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

during electronic transmission of the information."[2] Since HIPAA's inauguration, more medical facilities have found the financial resources in their budgets to add additional computers, more staff for data entry, and even wireless technology for many of the leading doctors to work from one facility to another. The electronic data security portion of HIPAA moves up the list of importance of HIPAA compliance. HIPAA contains three parts: Privacy, Code Sets, and Security. The security portion is then divided into four parts: Administrative Procedures, Physical Safeguards, Technical Security Services, and Technical Security Methods.

HIPAA establishes deadlines for compliance, allowing healthcare institutions time to reorganize the necessary funding for training and testing. Many healthcare employees find HIPAA a governmental hoop to jump through. They do not understand the irreparable damage that could be caused if a database of cancer patients' information were in the hands of our basement dweller hacker. Let's imagine a worst-case scenario and put this into better perspective.

- John D. Hacker finds a backdoor into a small cancer research facility computer network.
- There he gets access of to up-to-date information regarding the patient's treatment plan along with their address, date of birth, and social security number.
- J. D. Hacker notices that the record of Patient A indicates that he is losing a long battle with leukemia.
- Patient A dies and the nurse updates the database, closing Patient A's file.
- J. D. Hacker decides to take the name, social security number, and address and become Patient A for a while. Getting credit cards under his newly assumed name and spending everything he can.
- A month or two down the road the patient's estate is settled. J. D. Hacker has already moved on. He has acquired a database of 200 cancer patients and currently there is no cure for cancer.
- The medical facility does not realize the existence of J. D. Hacker on their network for months.

HIPAA points out that the medical facility is responsible for protecting people like Patient A. If the facility does not, they will pay, and in many cases their employees will pay. Who would ignore this warning? Many smaller facilities have the mindset, "That will not happen to us, we are a small rural family practice…we have a firewall…I think." It is a frightening statement, and I heard it first hand. They continued by saying, "We can not afford a $3,000 vulnerability assessment. I will check with our computer guy next week when he comes in to see if we do have a firewall." Eventually they will pay the $3,000 and it may end

[2] Department of Health and Human Services, Office of the Secretary, "45 CFR Parts 160, 162, and 164." P.2 URL: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

up in the form of penalties. Hopefully nobody's personal information is compromised in the meantime.

Gramm-Leach-Bliley Act

Enacted on November 12, 1999, the Gramm-Leach-Bliley Act (GLBA) was intended to allow and regulate the mergers of financial institutions. Public polls indicated a rise in citizen privacy awareness resulting in unhappiness with the banking industry's lack of protection for privacy issues and demanded change. These unfavorable feelings toward the financial industry became more pronounced after several high profile cases revealed credit fraud and identity theft.[3]

Effective May 23, 2003, the final "Safeguards Rule" of the GLBA intended to ensure the security of private customer records, to include the threat of unauthorized access. It is this Rule that emphasizes the information technology portion of financial security. Section 314.4 of GLBA says that a specific employee(s) must coordinate the institution's information security program. This individual(s) would then identify possible security and confidentiality risks, and any risks associated with integrity of customer information that could result in unauthorized use and access. This individual(s) would also evaluate the adequacy of the controls in place to manage these risks.[3]

The Safeguards Rule requires that vulnerability/risk assessments should include: employee training, network administration, data processing, storage backups, electronic data transmission, and intrusion prevention/detection. The Rule adds the statement, "Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program." [3] Not only does the Safeguards Rule require these security measures but frequently updating these procedures.

Penalties of the GLBA are severe for noncompliance. Fines and even imprisonment can be anticipated for the officers and directors of financial institutions. The civil penalties can reach a maximum of $100,000 per violation for the financial institution, $10,000 per violation for the officers and directors, and imprisonment of up to five years. If a violation occurs in conjunction with the violation of another Federal law the violator is subject to a fine of up to twice the amount.[4] In accordance with section 8 of the Federal Deposit Insurance Act (FDIA), financial institutions are subject to termination of FDIC insurance,

---

[3] Federal Trade Commission, "16 CFR Part 314, Standards for Safeguarding Customer Information." P.7 URL: http://www.ftc.gov/os/2002/05/67fr36585.pdf

[4] KentTrust Security Solutions. "Gramm-Leach-Bliley: What Does it Mean For You." P.3. URL: http://www.kenttrust.com/Kent_GLBA_Whitepaper.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

removal of management, officers, and directors - potentially barring them from working in the banking industry. [5]

I got chills when I heard this statement from the Vice President of a small bank: "We are a small credit union…. I do not understand all of this technical jargon. Let me check with my son, he's learning computers in college." The following week, after talking with her son "they" decided that her son could secure their network for a lot less than $5,000. You ask, where is that bank? Unfortunately, I found more small banks with the same attitude.

Federal Deposit Insurance Corporation

On October 3, 2000, the Federal Deposit Insurance Corporation (FDIC) released an official letter regarding the Security Monitoring of Computer Networks.[6] This letter released from the director to the CEO explains that computer networks connected to the Internet have increased vulnerabilities and provides some guidelines as to how to secure the institution's information assets. This letter of recommendations provides the financial institutions insured by the FDIC a helpful guide for securing their networks. At his time the FDIC is put the responsibility of information security into the hands of the individual institutions.

On February 1, 2001 the FDIC enacted the Interagency Guidelines Establishing Standards for Safeguarding Customer Information. This law, in essence formalizes the Security Monitoring of Computer Networks[6] letter regarding information security where the FDIC is involved. The law defaults to many of the rules of the Gramm-Leach-Bliley Act. Appendix B to Part 364 of the FDIC law states that it can be enforced in conjunction with the GLBA at financial institutions where violations occur. This law requires written policies and plans for information security and explains that each financial institution must evaluate their own complexity and risks. [7]

The FDIC clearly states that it is the responsibility of the financial institution's management to ensure that the information technology department will complete regular reviews of the security settings on the routers, firewalls, and servers. Added emphasis is placed on doing this following the installation of updates to the OS or any applications. These procedures attempt to make certain that all revisions and patches are updated on the system to prevent vulnerabilities from being reintroduced if a system backup were needed. They also recommend that automated logging be built into any firewall system or router because this is

[5] KentTrust Security Solutions. "Gramm-Leach-Bliley: What Does it Mean For You." P.3.
URL: http://www.kenttrust.com/Kent_GLBA_Whitepaper.pdf

[6] Federal Deposit Insurance Corporation, "FIL-67-2000."
URL: http://www.fdic.gov/news/news/financial/2000/fil0067.html

[7] Federal Deposit Insurance Corporation. "Appendix B to Part 364—Interagency Guidelines Establishing Standards for Safeguarding Customer Information."
URL: http://www.fdic.gov/regulations/laws/rules/2000-8600.html - 2000part364.101

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

essential if any forensic investigation were required. It continues to explain that an incident response team should be put into place if there were a system compromise and have the team regularly test the systems' backup for reliability.

National Credit Union Administration

In many instances the National Credit Union Administration (NCUA) defaults to the Gramm-Leach-Bliley Act as guidance standards for Federally Insured Credit Unions (FICU). NCUA guidelines require that the individual credit unions' Board of Directors oversee the development and implementation of the Information Security Program, assess the risks, manage and control these risks, oversee service provider arrangements, adjust the program according to the changes in technology, and report to the board their progress, status, and any security breaches or violations.[8]

This is definitely one regulation that provides the customer with a voice. If dissatisfied with the Board's supervision, the credit union member can make a more knowledgeable vote in future Board elections. This should encourage the Board, the institution, and the members' to take an active part in the security of their assets.

Sarbanes-Oxley Act

On July 30, 2002, President Bush signed into law the Sarbanes-Oxley Act. This Act was prompted by the scandals with Enron, WorldCom, and other large corporations. In January 2003, the Securities and Exchange Commission (SEC) had adopted and implemented the rules of the Sarbanes-Oxley Act, making it one of the most reformation times of its history. The goals of the Sarbanes-Oxley Act include reforming corporate public accounting as well as public governance, increasing personal responsibility of CEO's and CFO's regarding financial statements and securities filings, having investors make financial disclosure more understandable, and increasing the objectivity of financial analysts.

Section 805, Subsection I of the Sarbanes-Oxley Act states, "..including the destruction, alteration, or fabrication of physical evidence, the amount of evidence destroyed, the number of participants, or otherwise extensive nature of the destruction, the selection of evidence that is particularly probative or essential to the investigation, and whether the offense involved more than minimal planning or the abuse of a special skill or position of trust"[9]. It is obvious that this

[8] National Credit Union Administration, "Rules and Regulations." Pages 316, 317.
URL: http://www.ncua.gov/ref/rules_and_regs/NCUA_rules_regs.pdf

[9] U.S. Department of Labor, Office of Administrative Law Judges. "Legislative History of The Sarbanes-Oxley Act of 2002."
URL: http://www.oalj.dol.gov/public/wblower/refrnc/Sarbanes_Oxley_Act_Legislative_History.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

speaks to network administrators - they hold the ultimate control over the welfare of organizations data with their technological skills and level of trust.

California Senate Bill 1386

On July 1, 2003, the State of California introduced Senate Bill 1386 (SB 1386), one of the most serious bills ever written regarding computer security breaches. SB 1386 began when California saw their annual incidents of identity theft on the rise. "The Los Angeles County Sheriff's Department reports that the 1,932 identity theft cases it received in the year 2000 represented a 108 percent increase over the previous year's caseload."[10] These regulations are accompanied by various penalties, but not until SB 1386 did the penalties include notifying its customers that there had been a security breach. This law takes a bold stand and tells organizations that if they cannot or do not secure their systems and there is a security breach they need to tell everyone about it. This may actually work by having have companies publicly announce their inadequacy of securing their systems' and then people can go elsewhere for their services – survival of the fittest in a manner of speaking.

According to the Attorney General of California, "victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." SB 1386 defines personal information as, "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.
(2) Driver's license number or California Identification Card number.
(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." [10]

While organizations are beginning to take computer security more seriously they have not completed the implementation process by providing the resources for staff and budgets to make it possible. There are a couple of questions you can ask:

1) Does your company have one client in California?, or
2) Is there one employee working in California?

The company can be small or very large and SB 1386 will affect it. The law states, "Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California

[10] State of California, "SB 1386 Senate Bill – Chaptered."
URL: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. "[11]

The interpretation of the law remains broad-based yet powerful in getting businesses to secure their systems and encrypt their data - for the California residents. An unauthorized person can include not only outsiders but insiders as well that are not allowed access to the data. Who can be trusted? It is becoming more common that security breaches are occurring from corporate insiders, therefore it is becoming increasingly more important that organizations determine levels of security amongst their staff, and run background checks on those individuals.

Downstream Liability

This brings us to the topic of downstream liability, sometimes referred to as CyberLiability. "Downstream liability is a theory that companies who negligently fail to secure their networks or design-flawed software from security vulnerabilities could be held liable by third-party victims who are injured economically as a result of their negligence."[12] "Downstream liability is based on negligence. With negligence having four parts: duty, breach, causation, and damages. Duty is defined as a reasonable and prudent person's obligation to use reasonable care."[13] If the Information Security industry's best practice rules would be the guidelines for duty, it would be in the best interest of all parties involved to follow them to avoid any potential civil lawsuits.

These laws surrounding information technology and security are essentially formalizing IT best practice rules in business. Ignorance will no longer hold up as a defense. Without the security measures in place and best practice rules being implemented the healthcare industry, financial institutions and corporations are at risk of breaking the law. I am certain we will be seeing more issues of downstream liability in the near future.

Hypothetical Scenario

We are going to take a moment to think about these laws and illustrate their intent with a hypothetical scenario. The purpose of this scenario is to become aware of the big picture involved with corporate management, and network security - remembering who the victims really are.

---

[11] State of California, "SB 1386 Senate Bill – Chaptered." URL: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[12] Patzakis, John. "A Real Form of 'CyberLiability' Emerges." URL: http://www.infosecnews.com/opinion/2002/05/29_04.htm

[13] Zimmerman, Scott C., Plesco, Ron, Rosenberg, Tim. "Downstream Liability for Attack Relay and Amplification." P.3, URL: http://www.cert.org/archive/pdf/Downstream_Liability.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Background: Many large insurance companies issue home, automobile, and life insurance policies and have an option for automatic premium deduction from your bank account. This makes our lives much less complicated because we know that each month we do not have to remember to put a check in the mail.

- In order for the automatic deduction to occur the insurance company needs our bank routing number and personal account number. The insurance company also has our full name, current address, and social security number. In the case of homeowners insurance they have our property value, and value of our home's content. Automobile insurance includes our car's VIN number, make, and model. Let's include our life insurance policy for the sake of this argument, and add our age, date of birth, beneficiary's' dates of birth, and their social security numbers as well.

- The insurance company is large, they have customers all over the United States – including California. Each branch office has access to the corporate headquarters network as well as the Internet.

- A branch office in Kansas gets hacked and all of the customers' information is accessed.

What laws have been violated? Law enforcement investigates and the insurance company is forced to provide notice to it's customers in accordance with SB 1386, right? Let's review the law, "This bill, operative July 1, 2003, would require a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[14]

- Our insurance company does business in California but the hacked network was in Kansas. Would we need to determine if the hacker was able to get access into corporate headquarters?

- We are obligated under SB 1386 to notify the California customers (only) of the breach because their personal information was believed to have been accessed.

- Are any of the customer's beneficiary's California resident(s)? Do we need to inform them as well? Most likely, because we also have their names in conjunction with their DOB's and social security numbers.

[14] State of California, "SB 1386 Senate Bill – Chaptered."
URL:http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Do not forget that there are many customers enjoying the convenience of automatic deduction. Financial institutions as defined by the GLBA are "…businesses that are engaged in banking, insuring, stocks and bonds, financial advice, and investing." GLBA continues, "… banks, brokerage companies, and insurance companies must securely store personal financial information."[15] The insurance company has our name and social security number along with our bank name, routing number, and account number. Penalties of GLBA would be enforced.

While wondering if this insurance company's reputation could survive this event, this scenario leaves us with more questions than answers. How many companies do we deal with on a daily basis have our personal information inside insecure networks. A hacker could answer this question a lot quicker than we could. What about companies like the lenders of student loans, that use our social security number as our account numbers? It would not take long for a desperate hacker to put it all together. "The problem with identity theft is that it can happen to you before you know it, and it can take a long time to correct."[16]

Conclusion

Can you imagine an overworked yet confident network administrator admitting to management that they are only providing temporary fixes to vulnerabilities and problems? They may not even know what vulnerabilities exist. They simply install a firewall, never configure it correctly, check for a weekly Operating System update, virus updates, and hope that is enough. A survey conducted by Computer Weekly in June 2003 finds that despite security measures that were already in place, financial institutions remain vulnerable to security breaches. It says, "Four in 10 financial institutions worldwide have suffered at least one security breach within the last year." [17] These numbers are bad enough, remember though they are the institutions that reported the breach.

While visiting a well-known medical facility IT department, I gave the Director information regarding third-party vulnerability assessments, a requirement of HIPAA. He replied, "I can do my job just fine, I do not need someone else telling me they can do it better." Well, that statement alone tells me that he really has no idea what a third-party vulnerability assessment is and that it is required by HIPAA. Could it be that his defensive posture is a symptom of his fear of job security rather than his concern for the interests of the private data he is in

[15] Electronic Privacy Information Center. "Gramm-Leach-Bliley Act." URL: http://www.epic.org/privacy/glba/
[16] Federal Deposit Insurance Corporation. "When a Criminal's Cover is Your Identity." URL: http://www.fdic.gov/consumers/privacy/criminalscover/index.html
[17] Huber, Nick. Computer Weekly. "Financial institutions remain vulnerable to security breaches, says survey article." URL: http://www.computerweekly.com/Article122743.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

charge of securing? If the network was compromised imagine the reaction of the hospital's legal department if they knew he was presented with the information of a third-party vulnerability assessment.

Corporate management many times believe that the IT department should be able to secure the systems with the limited resources available to them. When a security breach has occurred, will management be pointing the finger? Let's say they hire an Information Security professional that implements the industry best practice rules. That would be one individual with the sole responsibility of administering the network, securing it, and the occasional demand, "Can you come fix the printer?" If management has chosen to invest in hiring this Information Security individual there is usually no additional funding for much more than their salary. This individual would be forced to work with no additional training or resources. Although management has made an important step in the right direction I cannot imagine anyone would want that responsibility and corresponding ulcer! That is why these laws frequently recommended that management implement a security team in conjunction with the IT department.

It would behoove any individual working in management, information technology, or average consumer to start evaluating their assets. Corporate management needs to become more aware of technology issues and begin to allocate the budgeting necessary for an information security team, training, equipment, and third-party auditing and assessments. Information technology personnel need to educate themselves on up-to-date security issues, the application of those security measures, and ask for assistance if it is needed.

Finally, consumers need to inquire into the security policies of the businesses they choose and ask if these policies are being monitored on a regular basis. The future of security breaches, identity theft, and network security administration is leaving our nation's businesses scrambling for resources, answers, and assistance.

© SANS Institute 2004, As part of GIAC practical repository.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

[1] USPS. "Identity Theft is America's Fastest Growing Crime." URL: http://www.usps.com/postalinspectors/idthft_ncpw.htm (27 January 2004)

[2] Department of Health and Human Services, Office of the Secretary. "45 CFR Parts 160, 162, and 164." Page 2. URL:http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf (10 December 2003)

[3] Federal Trade Commission. "16 CFR Part 314, Standards for Safeguarding Customer Information." Page 7. URL: http://www.ftc.gov/os/2002/05/67fr36585.pdf (21 January 2004)

[4,5] KentTrust Security Solutions. "Gramm-Leach-Bliley: What Does it Mean For You." Page 3. URL: http://www.kenttrust.com/Kent_GLBA_Whitepaper.pdf (27 January 2004)

[6] Federal Deposit Insurance Corporation. "FIL-67-2000." 3 October 2000. URL:http://www.fdic.gov/news/news/financial/2000/fil0067.html (23 January 2004)

[7] Federal Deposit Insurance Corporation. "Appendix B to Part 364—Interagency Guidelines Establishing Standards for Safeguarding Customer Information." 1 February 2001. URL: http://www.fdic.gov/regulations/laws/rules/2000-8600.html - 2000part364.101 (27 January 2004)

[8] National Credit Union Administration. "Rules and Regulations." Sept 2002. Pages 316, 317. URL: http://www.ncua.gov/ref/rules_and_regs/NCUA_rules_regs.pdf (20 January 2004)

[9] U.S. Department of Labor, Office of Administrative Law Judges. "Legislative History of The Sarbanes-Oxley Act of 2002." URL:http://www.oalj.dol.gov/public/wblower/refrnc/Sarbanes_Oxley_Act_Legislative_History.htm

[10,11,14] State of California. "SB 1386 Senate Bill – Chaptered." 2002. URL:http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html (20 January 2004)

[12] Patzakis, John. "A Real Form of 'CyberLiability' Emerges." 29 May 2002. URL: http://www.infosecnews.com/opinion/2002/05/29_04.htm (22 January 2004)

[13] Zimmerman, Scott C.; Plesco, Ron; Rosenberg, Tim. "Downstream Liability for Attack Relay and Amplification." Page 3. URL:http://www.cert.org/archive/pdf/Downstream_Liability.pdf (25 August 2003)

[15] Electronic Privacy Information Center. "Gramm-Leach-Bliley Act." 14 October 2002. URL: http://www.epic.org/privacy/glba/ (22 January 2004)

[16] Federal Deposit Insurance Corporation. "When a Criminal's Cover is Your Identity." 27 August 2003. URL: http://www.fdic.gov/consumers/privacy/criminalscover/index.html (27 January 2004)

[17] Huber, Nick. Computer Weekly. "Financial institutions remain vulnerable to security breaches, says survey article." June 2003. URL:http://www.computerweekly.com/Article122743.htm (26 September 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.