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

The Rule of Law vs. Issues of Privacy and Public Security

Charles Hart

February 4, 2003

Practical Assignment Version 1.4b

Abstract

In 1934 when Haven Gillespie and J. Fred Coots first wrote the lyrics to "*Santa Claus is Comin' To Town"* I doubt they seriously considered the privacy aspects of their words: "He sees you when you're sleepin', He knows when you're awake, He knows if you've been bad or good, So be good for goodness sake." If these words, which children happily accept without question, were applied to the adult reality they would inspire paranoia suitable for George Orwell's novel 1984. Yet, as the capabilities of technology expand and the digitalization of the culture continues, many are increasingly concerned about the gradual development of such an Orwellian society. As a result, the laws of our nation are being forced to address and precariously balance the issues of public security, consumer privacy, and business interests.

Although information security arena today is comprised of a labyrinthine of legal issues, few subjects are more pertinent to both the information security and legal professions than the topic of privacy. This paper will attempt to outline the scope of the privacy issues that are being encountered by both professions. To accomplish this, the paper will provide an overview of the core issues influencing privacy concerns including Federal and State regulatory trends, technology advancements in the field of electronic discovery, and finally an examination of the impact of computer forensics on litigation. Computer forensics is important from the standpoint that privacy issues are increasingly arising as a result of information stored on various electronic media.

Federal Regulations and Standards

One of the primary methods in addressing privacy concerns has been the creation of new legislation, which is impacting diverse economic sectors from financial services to medical records, and the overall category of electronic communications.

Electronic Communications Privacy Act (ECPA) of 1986

The ECPA of 1986 is actually an expanded version of an earlier law, the ECPA of 1968. The original 1968 version was part of a crime bill that had been largely inspired by the 1967 case Katz vs. the U.S., which dealt with the improper use of FBI wiretaps. In this case the U.S. Supreme Court ruled that the use of wiretaps by the FBI without a warrant violated the Fourth Amendment of the Constitution, which prohibits unreasonable search and seizures. As a result, the U.S. Supreme Court outlined procedures for electronic surveillance by government agencies, such as the need to demonstrate probable cause and the issuance of a search warrant. In an attempt to prevent blanket searches by the government, the Court's procedures also called for authorities to be specific in regard to the exact telephone number to be monitored.

However, since passage of the 1968, the concept of electronic communications has expanded well beyond the law's initial focus of wired telephone conversations. The 1986 version emerged as an attempt to rectify both the technological changes that had

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

occurred over the years, and the new privacy issues being encountered within the society from the introduction of several new electronic communication devices and formats. At this juncture it is important to understand the definition of electronic communication. Title 18, Part 1, Chapter 119, Sec.2510 of the U.S. Code defines electronic communication as:

> "Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include -
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds."[1]

Just as its predecessor, the 1986 law established criteria for the interception and use of electronic communications during surveillance activities by government agencies. However, the newer version deviated in one important aspect from the earlier 1968 version. In addition to identifying what the Fourth Amendment protected, the ECPA of 1986 also specified circumstances where the Fourth Amendment did not protect electronic communications. One such circumstance occurs when corporations monitor email within their own internal networks. This provision is particularly important when considering an employer's responsibility and potential liability on issues involving employee misconduct in the workplace. This law is one of the key drivers, which enables employers to conduct investigations when necessary into employee behavior without the fear of invasion of privacy allegations if the case were to proceed to litigation (see Garrity v. John Hancock Mutual Life Insurance Co., 2002 U.S. Dist. LEXIS 8343 (D. Mass.)).

Health Information Portability and Accountability Act (HIPAA) of 1996

Another regulation from the federal government that has significantly impacted business considerations and consumer privacy issues is the Health Information Portability and Accountability Act (HIPAA) of 1996. This legislation was initially drafted to address concerns with 1) insurance reform, and 2) administrative simplification. However, HIPAA should primarily be thought of as a law that governs the privacy of medical records. While HIPAA defines specific regulatory guidelines that "covered entities" and any of their third party services contractors must adhere to, the law also contains a more general HIPAA Safeguard Statute under 42 U.S.C. Sec. 1320d-2(d): security standards for health information which state that the various safeguards are designed to:

> (A) to ensure the integrity and confidentiality of the information
>
> (B) to protect against any reasonably anticipated
>
> (i) threats or hazards to the security or integrity of the information; and
>
> (ii) unauthorized uses or disclosures of the information; and
>
> (C) otherwise to ensure compliance with this part by the officers and employees of such person.

As defined in Subchapter C - Administrative Data Standards And Related Requirements, Part 160 – General Administrative Requirements, Subpart A - General Provisions, § 160.103 Definitions "covered entity" means one of the following: (1) a health plan, (2) a health care clearinghouse, or (3) a health care provider. The focus of HIPAA has been to secure the medical records from both an information security and personnel viewpoint, in an effort to protect the privacy of an individual's medical history.

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

The Financial Services Modernization Act of 1999, also known as Gramm-Leach-Bliley Act (GLBA) Privacy Rule – 15 USC 6801-6827

Where HIPAA is designed to address privacy issues of an individual's medical records, Gramm-Leach-Bliley focuses on the security and privacy of consumer information maintained by financial institutions. The financial services sector had enthusiastically rallied behind the development of Gramm-Leach-Bliley that was intended to repeal certain sections of the Banking Act of 1933, known also as the Glass-Steagall Act. Glass-Steagall's core sections of 16, 20, 21 and 32 had created an operational divide between the activities of "commercial banking" and "investment banking." This resulted in the effective separation of banking and insurance services within the United States. Glass-Steagall had been the Congressional solution to the numerous bank failures that occurred during the Great Depression.

In its final draft Gramm-Leach-Bliley proved to be a significant piece of privacy legislation that imposed several security and privacy responsibilities upon the financial services industry; such as those outlined in Title V which address preventing the disclosure of non-public personal information by the financial institutions to their affiliates. Gramm-Leach-Bliley also focuses heavily on physical security procedures implemented within corporations. Specifically, there are physical guidelines regarding the location of where customer information is stored, and limits access to such areas to only authorized personnel.

From a legal perspective, Gramm-Leach-Bliley created both a potential liability issue, and an effective paper trail to pursue litigation against the Board of Directors of a financial services firm. This liability originates from the Board's responsibility to develop and maintain a written security policy for the enterprise. Under this directive the Board essentially serves as a focal point for all major security initiatives and status updates. Such a structure does not readily permit the Board to deny knowledge of the enterprise security procedures or vulnerabilities in the case of a security breach.
Further information regarding the Gramm-Leach-Bliley Act Privacy Rule can be obtained at www.ftc.gov/privacy/glbact/index.html

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001

The most recent addition, and probably the most controversial from a security and privacy viewpoint is the USA PATRIOT Act. This legislation signed into law on October 26, 2001 by President George W. Bush was intended to address security threats posed to the United States by international terrorists. The USA PATRIOT Act gives considerable attention to the issue of international money laundering, in an attempt to deprive terrorists of financial resources. As stated by Director James E. Gilleran for the Office of Thrift Supervision (OTS) "the USA Patriot enhanced our ability to cut off the financing of terrorism by strengthening the tools we have to prevent, detect, and prosecute international money laundering."[2] Beyond privacy issues that have emerged as a result of regulations outlined in Title III designed to deter money laundering, the PATRIOT Act also impacts areas in immigration, provides government agencies with

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

enhanced capabilities to share information, and greater authority to deal with computer fraud and abuse. It is this issue of computer fraud and abuse that will most likely have the greatest impact on privacy agendas and information security.

While volumes have already been written about the benefits and potential pitfalls of the 300 plus page PATRIOT Act as they relate to government operations, little attention has been given to how this omnibus law could impact or shape privacy and security litigation in the future. One incident that may have illustrated the dilemma developing between First Amendment rights and the increased need for public security occurred in April 2002. During this time the German national railway – Deutsche Bahn AG had threaten to file suit against Google Inc. if the company failed to remove specific hyperlinks from its servers. These links contained articles that provided detailed information on how to sabotage railway systems from Radikal, currently a banned publication in Germany. Prior to this event, Deutsche Bahn had already won a similar case in an Amsterdam District Court against another Internet service provider. Although Google eventually agreed to remove the hyperlinks this incident raised several interesting questions, which have increasingly become commonplace in our society since the events of September 11, 2001. Questions such as the conflicts between the First Amendment and new antiterrorism laws such as the PATRIOT Act that give a new level of importance to the prevention of cyber terrorism. This example also reveals liability issues associated with the posting of potentially dangerous information on a corporate Web server. While in this case the material was obviously malicious in nature, future problems will be posed by situations where the circumstances are less black and white when relating to the materials posted though the Internet and potential acts of cyber terrorism. Further information regarding the USA PATRIOT Act can be obtained at http://news.findlaw.com/cnn/docs/terrorism/hr3162.pdf

State Regulations and Standards

While the scope and complexity of federal standards, regulations and legislation which address issues of privacy and information security have proliferated in recent years; individual states from California to Vermont have seen their legislatures take an active stance on privacy concerns that occasionally exceed the standards outlined in legislation such as Gramm-Leach-Bliley.

It is often stated that "as California goes, so goes the nation." While that remains to be seen in all endeavors, there can be little debate on California's leadership role in drafting legislation on a broad range of information privacy issues. From bills that detail the obligations of commercial Internet site operators in maintaining the privacy of consumers (AB 68-Simitian), to bills that establish a minimal level of responsibility for loan operators in verify an applicant's identity (SB 25-Bowen); the California Assembly and Senate have aggressively sought answers to various privacy weaknesses in the digital age. However of all the proposed bills and laws that California has considered or implemented over the last few years; there are three laws that effectively demonstrate the impact this legislation will have in the public arena. The first involves the Social Security Number Confidentiality law, which will require financial institutions as of July 1, 2003 not to print Social Security Numbers on statements or similar documents that are

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

normally distributed through the public mail system. The idea is to prevent the possible intercept of sensitive information, such as an individual's Social Security Number through the mail that could then be used to conduct identity theft.

The second peace of legislation addresses the protection of computerized personal information that may have been accessed during a security breach of computer systems. The Security Breach Notification Law (SB 1386 – Peace) was signed into law on September 25, 2002 by California's Governor Grey Davis, and becomes effective July 1, 2003. This law will require individuals to be notified when their personal information may have been compromised due to a breach of security. The Act applies to both state agencies and businesses that conduct business in California. As stated in the October 2002 edition of the Truste Advocate newsletter, the Security Breach Notification Law:

> "Applies to computerized data consisting of 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:
> - Social security number,
> - Driver's license number or California Identification Card number,
> - 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."[3]

As stated on California's Office of Privacy Protection Internet site:

> "This bill gives consumers notice that unauthorized individuals have acquired their personal and/or financial information, thereby giving them the opportunity to take proactive steps to ensure that they do not become victims of identity theft."[4]

The final piece of privacy legislation to be examined, which was enacted by Senator Debra Bowen (SB 168 of 2001) permits California consumers to "freeze" and "thaw" their credit files that are maintained by the three credit reporting agencies: Equifax, Experian and Trans Union. The program works through the use of a PIN that is created by the individual in combination with the various credit agencies. This concept is an important and unique attempt to stem the rising number of identity theft cases, and provides the individual consumer with greater control over who is able to access their credit reports. Even though the service will be available to all residents of California, it will only be provided free of charge for individuals currently listed as victims of identity theft.

Electronic Discovery Defined

In addition to Federal and State regulatory trends, the growth in the use of computer forensics has contributed significantly to addressing the legitimacy of certain privacy issues through the introduction of modern forensic handling capabilities. The reason for its relevance can be witnessed in virtual every home and office during a typical day. The utilization of computers and electronic communication by the general public and companies has dramatically increased over the past decade. "With as much as 90% of all business records now created and stored electronically, it is rapidly becoming the rule rather than the exception that discovery opponents will seek production of electronic records."[5]

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

The second reason centers on the development of new computer forensic technology such as Guidance Software's EnCase product that has significantly reduced the expense associated with acquiring, recovering, and authenticating electronic evidence for an investigation. EnCase is a software program that is capable of both acquiring a hard drive and performing analysis on that drive; thereby fulfilling many of the tasks required by forensics examiners during the course of a typical computer investigation. These tasks include the ability to analyze files for modification and creation dates, verify the file extensions of files, recover deleted or partially overwritten files, and examine data located in the file slack. Slack space represents "the space on a hard disk between the end of a file and the end of the cluster that the file occupies."[6] This reduction in cost has facilitated the use of computer forensic examination, in incidents that would have just a few years ago been considered prohibitively expensive for small businesses or law firms.

While many may perceive this topic as nothing more than the collection and analysis of electronic data from a computer or related device, it is the issue of admissible evidence that is actually the dominant consideration during the entire process. Without the proper management and preservation of electronic evidence, the whole reason behind conducting an investigation would rapidly become irrelevant. These investigations are increasingly important from both an information security perspective, and from a legal perspective, which are utilizing this technology in litigation proceedings. These cases often produce charges of "invasion of privacy", which must be proper addressed during a trial.

Procedurally, once a computer forensics investigation has been requested or approved by a company's internal Human Resources department, it is essential that the forensic examiners responsible for the case adhere to certain core steps designed to ensure the validity and admissibility of evidence. First, all information pertaining to the recovery of computer evidence must be properly recorded and maintained. Second, an unbroken chain of custody for the evidence must be properly documented, and the electronic evidence stored in manner such as a secured room to prevent potential allegations of physical damage or tampering. Chain of custody is defined in Black's Law Dictionary as "the movement and location of real evidence from the time it is obtained to the time it is presented in court."[7] Finally, and perhaps most significant from an admissibility viewpoint, analysis of the data must never be conducted directly from the original source. In fact, a suspect system should not even be powered on since "simply booting up a computer can alter date and time stamps on files, and may overwrite portions of deleted information residing in the 'free space' of the hard drive, resulting in irretrievable loss of this information."[8] This means that for the examiner to maintain the authentication of computer data, all analysis of the data obtained from evidence such as hard drives must be conducted from an exact bit-by-bit duplicate often referred to as a "mirror image" of the original. The authentication of evidence gathered from such mirror images of hard drives has been upheld in court cases such as *Ohio v. Cook, 2002 Ohio 4812, 2002 Ohio App. LEXIS 560 (October 22, 2002).*

The Role of Litigation

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

At first a discussion on email or computer forensics may appear to simply represent a highly specialized segment of the law, and not a topic that has much significance to the rest of the legal community. However, the reality is that both these topics and their applicability to the traditional law and issues of privacy are rapidly impacting all segments from the law firm attorney to corporate counsel. The following case examples are intended to provide insight into the influence of email in privacy related issues, and reveal some of the legal issues within corporate environments that are increasingly reliant on the capabilities of electronic discovery.

Bryant v. Aventis Pharmaceuticals, Inc., 2002 U.S. District Court WestLaw 31427434, LEXIS 21070 (S.D. Indiana October 21, 2002)
This suit exemplified the meaning of flawed logic. It dealt with an Aventis Pharmaceutical sales representative that had been terminated for generating false sales activity reports. Following the termination the employee filed suit against Aventis for age discrimination. Now, it is this point where the presence of flawed logic enters the story. The plaintiff's rational behind the allegation of age discrimination was based upon the following facts:

1. That the former employee freely admitted to the charges of falsifying sales reports, and
2. She had retrieved emails from her computer that had been written by four former colleagues, which indicated that these Aventis employees were also in the habit of producing false documentation regarding their own sales activity.

Therefore, the terminated employee concluded that she could not have been terminated for her sales reports since other employees within the organization were also engaged in similar practices. However, the court did not quite see the case as cut and dry as the plaintiff, and ruled in favor of Aventis. The court's ruling was based upon the fact that the emails did not demonstrate that Aventis had prior knowledge or had given corporate consent for the misconduct of these other employees.

Garrity v. John Hancock Mutual Life Insurance Co., 2002 U.S. District Court WestLaw 974676, LEXIS 8343 (D. Massachusetts May 7, 2002)
This case is of particular importance when examining the issue of individual privacy while at work, and the responsibilities that organizations have to protect their employees as mandated by various federal and state regulations and standards. The case dealt with a John Hancock employee that had been terminated for essentially a code of conduct violation involving the receipt and distribution of sexually explicit emails while at work. Hancock had begun an investigation into employee's conduct only after receiving complaints from other employees inside the company. After termination the former employee filed suit against John Hancock for wrongful discharge and invasion of privacy. These charges the plaintiff contended were supported by Hancock's own internal email policy, which required employees to establish their own passwords. The plaintiff's case rested in the belief that this procedure, in addition to other features of the email system had lead to a belief that the corporate email system was individually private. In the final ruling the court disagreed with this assessment of the situation, and added that even if such an expectation had been present at the company, John Hancock still had a duty to investigate possible sexual harassment.

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

Wall Street and The Blodget Emails

During the course of my research into this topic, I have often recalled a story that former U.S. President Ronald Reagan would tell about a little boy digging through a pile of manure, saying, "I know there's a pony in here somewhere." Well, fewer cases could be more suitable for this type of imagery than the one involving former Merrill Lynch stock analyst Henry Blodget. However, in this tale the little boy would represent Eliot Spitzer, New York's Attorney General, while the pile of manure would be analogous to Henry Blodget's internal emails.

When Spitzer released these emails to the public in early 2002, they gave credence to the long held suspicions that a conflict of interest had developed between the research and investment banking units of several Wall Street firms. In addition, the use of these internal emails by the Attorney General's office gave credibility to rulings such as SEC rule 17a-4 and NASD rules 3010 and 3110[9] that specifically deal with the retention policy of electronic documents held by financial services companies. Ultimately, Spitzer's office would issue additional subpoenas in 2002 to several Wall Street firms including Bear Stearns, Credit Suisse First Boston, Goldman Sachs, Morgan Stanley, Saloman Smith Barney, and UBS PaineWebber.

In Blodget's own case, one of the more publicized e-mails from October 2000, which Spitzer used as an example of Blodget's true feelings and the degree of conflict involved in the case emerged from an email that a financial consultant had sent Blodget requesting further information on Infospace's handwritten Annual Report. This email was reprinted from the New York Times, Late Edition as follows:

> "Would you or someone in you office please respond to the Dow Jones News Service article by Michael R. Sesit October 20 discussing a new study analyzing annual reports of new companies? In that article, Infospace's is held up as a "horror story" due to its 'high school exam format' and 'some pages that are handwritten."...A handwritten annual report for a company you have a buy rating on with a price target of $100 is disconcerting to me to say the least. Tell me article is wrong..."[10]

Blodget who still had a high rating on the stock forwarded this email onto an internal colleague, and in the response referred to Infospace as a "piece of junk." Spitzer's office utilized this "piece of junk" comment in one of its press releases that stated:

> "These communications show analysts privately disparaging companies while publicly recommending their stocks. For example, one analyst made highly disparaging remarks about the management of an internet company and called the company's stock 'a piece of junk,' yet gave the company, which was a major investment backing client, the firm's highest stock rating."[11]

This case illuminated the fact that there is absolutely nothing private about emails, and the fact that government regulations are actually mandating the specific retention periods for electronic communications. In fact, in many respects the electronic communication trail of today is far easier to follow than the traditional "paper trail" notion that many have become accustomed to over the years. The Blodget case may seem like an interesting story with no real long-term significance. However, this case has implications for both the information security and legal professions. From a security perspective, there is a mandated necessity to ensure the retention and protection from alteration or destruction of such electronic documents. Although from a legal

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

perspective, the case demonstrates the growing necessity of lawyers to be fully conscious of the various standards and regulations required to successfully navigate the enormous volumes of electronic data being created and stored by businesses and individuals.

Conclusion

In conclusion, as technology has continued to advance so has the legal definition of what can be considered private information and under what circumstances. This consideration has often been clouded by public security concerns, the rapid proliferation of technology in the form of new communication tools typified by email, and the increased utilization of computers in our work environments.

While businesses have struggled with compliance and potential liability exposure to various situations, individuals have struggled with the concept of what is classified as private. As recent litigation has demonstrated, emails cannot be considered to be truly private communications, and especially not within the business environment. Even those that have been stored on personal computer hard drives outside the office are subject to retrieval by modern computer forensics programs. As consumer privacy concerns continue to grow with the propagation of issues such as identity theft, government regulations and standards will also continue to change and grow in response. The role of information security in this dynamic environment is to assist in providing direction to legal elements and government regulatory institutions.

© SANS Institute 2003, Author retains full rights.

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

Endnote References

[1] Legal Information Institute. U.S. Code Collection. Title 18, Part I, Chapter 119, Section 2510 – Definitions. URL: http://www4.law.cornell.edu/uscode/18/2510.html
[2] "OTS Will Examine for USA PATRIOT Act Compliance." Office of Thrift Supervision, Press Release. March 20, 2002. URL:http://www.ots.treas.gov/docs/77213.html
[3] Hacket, Emily and Caldwell, Kaye. "California Enacts Privacy Legislation", TrustE Advocate Newsletter. October 2002, Volume 6, Number 9. URL:http://www.truste.org/partners/newsletter/october2002.html#politics
[4] California Legislation "SB 1386" (Peace). URL: http://www.privacy.ca.gov/leg2002.htm
[5] "The Impact of Electronic Records in Litigation and Criminal Investigations." Electronic Evidence Services – PriceWaterhouseCoopers. URL:http://www.pwcglobal.com/extweb/service.nsf/docid/4f8a496392798c1a8525697c00677dc4
[6] Definition of Slack Space. Itsecurity.com Dictionary. 2002. URL:http://www.itsecurity.com/dictionary/slack.htm
[7] Garner, Bryan A., Editor In Chief, Black's Law Dictionary, Seventh Edition, 1999, West Group; Page 222.
[8] Papazian, William and Spinelli, George. "Using Forensics to Investigate Staff Wrongdoing." New York Law Journal. September 10, 2002 Vol. 228; Page 5, Column 1.
[9] "SEC Approves Rules Regarding Supervision, Review, And Record Retention Of Correspondence." Effective February 15, 1998. URL:http://www.nasdr.com/pdf-text/9811ntm.txt
[10] Cohen, Noam. "Word for Word / Mixed Messages; Swimming With Stock Analysts, or Sell Low and Buy High…Enthusiastically." The New York Times. May 5, 2002, Sunday Late Edition-Final, Section 4, Page 7, Column 1.
[11] "Merrill Lynch Stock Rating System Found Biased By Undisclosed Conflicts Of Interest." Office of New York State Attorney General Eliot Spitzer, Press Release. April 8, 2002. URL:http://www.oag.state.ny.us/press/2002/apr/apr08b_02.html

Additional References

1. U.S. Department of Health and Human Services, Administrative Simplification, Privacy and Security. URL:http://aspe.hhs.gov/admnsimp/bannerps.htm#privacy
2. "Gramm-Leach-Bliley Act Financial Privacy and Pretexting." Federal Trade Commission. URL:http://www.ftc.gov/privacy/glbact/index.html
3. "Affidavit In Support Of Application For An Order Pursuant To General Business Law Section 354." Supreme Court of the State of New York, County of New York. URL:http://www.oag.state.ny.us/press/2002/apr/MerrillL.pdf

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