Global Information Assurance Certification Paper

Making the Case for Managed Security

GSEC Practical Assignment
Version 1.4b (Option 1)

James Weissman
April 13, 2004

Table of Contents

Abstract

Corporate networks are under increasing electronic attack, from external and internal sources. The cost of containment and financial damage from these incidents is enormous — and on the rise. This has forced security to be a major concern for companies of all sizes. Further pressure to respond comes from several laws, including HIPAA, GLBA, Sarbanes-Oxley, and the California Security Breach Information Act. Collectively, these require companies to either implement effective security or suffer criminal and/or civil penalties.

Existing security staffs often do not have the time or training to meet the current demands of a solid perimeter defense. Because throwing people at the problem is very expensive, many companies are looking at Managed Security Services. A Managed Security Service Provider (MSSP) offers many advantages over in-house solutions including economies of scale and the ability leverage knowledge gained by serving multiple clients. Choosing an MSSP involves several key factors but, however decided, the time is right for outsourcing security.

Introduction: Attacks are on the rise

As Bob Dylan said, "the times they are a-changin'." In these days of spam filled* mailboxes, we've grown accustomed to reading about new security vulnerabilities nearly every day. You'll find few information technology professionals who would not agree that security is a growing concern. Let's examine some actual statistics from some trusted security sources to get a handle on the scope of the problem.

Created in 1998 in the wake of the infamous Morris Worm, the CERT Coordination Center (CERT/CC) is the nation's first computer security emergency response team. CERT, a federally funded R&D center operated by Carnegie Mellon University, has been maintaining security statistics since 1988.

Here are the growth trends in the last four full years' data[1]:

	2000	*2001*	*2002*	*2003*
Incidents	21,756	52,658	82,094	137,529
Vulnerabilities	1,090	2,437	4,129	3,784

Since 2000, that's an astounding 532% increase in incidents and corresponding 247% growth in vulnerabilities!

According the 2003 CSI/FBI Computer Crime and Security Survey[2], despite the use of firewalls (in 98% of sites) and access controls (92%), 56% of the surveyed organizations still reported unauthorized access. Theft of proprietary information was the number one source of financial lost, immediately followed by denial of services.

* 63% of all email with a rising trend, according to statistics for March 2004 collected by Brightmail, Inc; see http://www.brightmail.com/spamstats.html for the latest numbers.

Disgruntled employees were almost as likely as hackers to be the source of an attack with 30% of sites reporting an internal compromise. But across the board, 78% reported an Internet-based attack.

For those organizations that experienced a computer intrusion within the previous year, half of those affected filed no report either with law enforcement or their own legal counsel. This is puzzling until the primary reason for non-reporting is considered: fear of negative publicity. Because of the cost resulting from public exposure, even in face of potentially recovering damages, companies are choosing to be silent.

Symantec, a leading Internet Security vendor, in its latest "Internet Security Threat Report"[3] reports that in 2003, on average, 7.2 new vulnerabilities were announced each day. The report also reveals that while only 16.6% of companies reported a serious breach in the first half of the year, the number had grown to 50% in the second half.

So not only are breaches increasing, but, worse, 70% of the 2003 were categorized as "easy to exploit." Making matters worse is that exploits that were previously difficult to accomplish are now being performed by an increasing population of “script kiddies” — computer novices running canned scripts that often performing complex operations beyond the understanding of the person running them.

Finally, the report affirms the ongoing observation that the time between a vulnerability announcement and subsequent exploitation is shrinking. The implication is that companies need to be active in online security forums and email lists in order to gain access to the latest announcements. Consider what happens if a vulnerability is discovered on a Saturday. Do you even have staff on duty to monitor, yet alone react to the news? Can your anti-virus system reliably comb through your incoming spam and pick off the latest virus?

So, the picture is rather grim. What about the resultant damages from these attacks?

Financial Costs are Enormous

A Toronto "Globe and Mail" story[4] quotes data from a mi2g Intelligence Unit report that estimates dollar damages from Distributed Denial-of-Service (DDoS) attacks of 3.4 - 4.1 *billion* in the first three months of 2004. The previous year’s *total* was about a third of that: $1.3 - 1.6 billion. At first glance, the numbers seem astronomical. But consider that in a DDoS attack, typically your connection is so thoroughly saturated that you are effectively cut-off from the Internet. If any component of your business relies on e-commerce, lost revenue can quickly mount up. Worse, customers who perceive your website as “down” may spend their dollars with a competitor.

In considering all attacks, the numbers get scarier: Trend Micro estimated[5] the total 2003 damage costs of virus attacks around the world at $55 billion. This is an amount that has roughly doubled each year since 2001. Trend Micro, naturally, predicts a rising trend in 2004. And, this does not even factor in the cost of dealing with SPAM (estimated globally at $20.5 billion in 2003 by the Radicati Group[6]).

Statistics like this are easy to come by, but justifying the numbers can be difficult. Alinean, a company specializing in return on investment (ROI) analysis and management tools, provides[7] a foundation for doing loss calculation. For example, its data suggests that a single DDoS attack on average will cause $122,000 in business and collateral damage.

To assess your own containment costs, beyond the actual costs of lost business, you need to compute staff costs by tallying the specific people and hours involved. When incidents arise, accurately recording the time spent in resolution will assist in better estimates of future costs allowing you to more intelligently budget for security. Additionally, if legal recovery of damages is attempted, this information can be the foundation for a judgment.

Indirect costs arising from negative publicity and reputation damage can easily exceed the direct costs of battling and containing the attack. This is especially true for financial institutions where customer trust is critical. In a study[8] by the University of Maryland's Smith School of Business, the stock-market value of breached companies was tracked. In those cases where confidential data was leaked, they saw an average market valuation decline of 5%. So, the *type* of data you are securing is an important consideration in deciding on the degree and extent of protective measures.

Information Security as an Obligation

Given the threat level and the potential cost of a breach, one would think that there is incentive enough for companies to deploy advanced security measures. However, there is a new element on the table that is actually *compelling* organizations to act: the law. Depending on the nature of the business, and the geography, and of the following four new legal regulations may apply:

1. HIPAA
2. GLBA
3. Sarbanes-Oxley
4. California Security Breach Information Act SB-1386

In a recent poll[9] by PricewaterhouseCoopers and CIO magazine, 62 percent of companies surveyed indicated that they will be increasing spending on security with the #1 reason to satisfy legislation. So, let's briefly survey these laws and see why they are commanding so much attention:

1. HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), also known as the Kennedy-Kassebaum bill, was passed in 1996. Various aspects of it have only recently taken effect with some compliance deadlines still on the horizon. This complex legislation covers several discrete areas of health policy:

Portability: The "portability" components provide mechanisms that make it simpler to replace employer sponsored health insurance coverage if you lose your job. More generally, protections are offered that ensure your ability to maintain continuous coverage in almost all circumstances.

Privacy: The law gives new powers to consumers over the use of their "protected health information" (PHI) which includes all medical records. Consumers now have the legal right to both inspect and amend their records and, within limits, control the dissemination of this information. Providers must follow new rules regarding use and disclosure of PHI and create procedures that limit information exchange to the minimum necessary amount for proper care. These are the steps detailed in the "Notice of Privacy Practices" that most of us have been required to sign by our healthcare providers.

Administrative Simplification: In an effort to streamline the electronic processes that are involved in the transmission of healthcare information, HIPAA both attempts to both encourage and standardize the electronic data exchange (EDI) of medical (and related billing) information. Standards are set for both data content and format ("transaction and code sets" in HIPAA jargon).

Security: Under the rules set by the Department of Health and Human Services (HHS), healthcare organizations must implement administrative, physical, and technical safeguards to guard data integrity, confidentiality, and availability. Additionally there are policy and procedure, and documentation requirements.

The requirements are rather detailed and cover a broad array of security methodologies including: access controls, audits, training, workstation usage policy, remote access, automatic logoff, disaster recovery, and digital signatures. These rules, which take effect in April 2005 (or a year later for smaller health plans) have both civil and criminal penalties for non-compliance. While many of the mandated aspects are often extant as part of best practices, compliance will still entail a huge effort for most entities.

The rules, while vast and comprehensive, do provide a bit of flexibility. HIPAA security implementation specifications can either be "required" or "addressable." Required measures are just that; addressable ones can be evaluated by an organization and selectively implemented based on their own assessment of the reasonability and effectiveness within their particular environment. The bottom line is that healthcare organizations are now mandated to ensure the security of health information. And, if a violation occurs, penalties start at $100 per violation but can balloon to up to $250,000 or ten years imprisonment for knowingly, with malicious intent, disclosing PHI.

2. GLBA

While HIPAA targets healthcare organizations, the Gramm-Leach-Bliley Act (GLBA), or Financial Services Modernization Act of 1999, focuses on financial institutions. And, the GLBA's regulation compliance enforcement date has already been in place almost 3 years.

While Banks and Credit Unions are obviously subject to the act, it also extends to any business that engages in "financial activities." This would include, for example, a check cashing company, a collection agency, or even an auto dealer that provides leasing.

Because of the increasing consolidation (by merger and acquisitions) of financial institutions, consumers found that so called "nonpublic personal information" (eg; bank account balances, health records, investments) was increasingly being centralized. GLBA attempts to prevent the abuse of this information with restrictions detailed in its Title V, Privacy section. In addition to requiring the security of information and methods to control the release of it, institutions must provide a notice of privacy practices and give consumers the ability to opt-out of information sharing.

Beyond privacy, GLBA speaks specifically to financial institution safeguards that governing agencies (at the Federal and state level) must enact. These steps are designed to protect both the security and integrity of customer data.

With regard to Banks, the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" come into play. These guidelines require the development and implementation of security programs that:

- Involves the Board of Directors
- Assesses risk
- Manages and controls risk
- Oversees service provider arrangements
- Adjusts the program
- Reports to the Board
- Implements the standards

Section "C" requires, among other things, access controls, encryption, and "monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems." The most obvious implementation method for this is an intrusion detection system (IDS) that incorporates good logging. Whatever security measures are taken; they are all subject to audit during regular examinations.

Enforcement of GLBA is serious: violations may incur penalties ranging from $5,000 to $1,000,000 per *day*.

3. Sarbanes-Oxley

In the wake of public outrage following the accounting scandals at WorldCom and Enron, Congress enacted the Sarbanes-Oxley Act (SOA) in 2002. It enforces strict accounting controls on publicly traded companies to facilitate the creation of more accurate and complete financial reports. SOA requires that the CEO and

CFO certify all financial reports of the company and also makes directors and officers personally liable (as in fines and imprisonment) for financial violations such as fraud. The first round of enforcement deadlines arrives in June with complete compliance by April 2005.

From an information technology perspective, the portion of the act that is commanding the most attention is section 404, "Management's Reports on Internal Control Over Financial Reporting." This section obligates management to assess and report on the effectiveness of these internal controls. As part of this, management must identify the framework† used to make this assessment. Further, the reports themselves are must be audited by the company's outside auditors.

While the definition of “internal controls” (to monitor financial reporting) is subject to some debate, the SEC rules specifically define internal controls to include policies and procedures that "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition"[10] of data. They go on to emphasize that "the safeguarding of assets is one of the elements of internal control over financial reporting.” Therefore, appropriate security measures are, necessarily, a significant component of implementation.

4. California Security Breach Information Act; SB-1386

As a means to combat identify theft, in July of 2003, California enacted a law that requires any business that licenses or owns computerized “personal information” to notify the individual if the data has been breached. *Personal information* is considered to be a name in combination with a social security or drivers license number, or combined with an account or credit card number along with a PIN. *Breach* is defined as the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.”[11]

The law actually has some meat due the corresponding civil code 1798.29 which uses similar language. The bottom line is that if a company has a breach and does not report it to the affected individuals, it can be sued in civil court. As previously noted, 50% of companies don’t report successful intrusions to authorities, so SB-1386 now forces their hand. It also provides a significant impetus to shore up existing security efforts.

California is often considered a sort of cultural bellwether, so we can anticipate future action in other states. In fact, the senator from California has already introduced similar legislation to the Senate.

† A “framework” is an extensive set of processes used as a guide to achieving compliance. The framework itself can be a massive document along with associated templates, flowcharts, and tracking software. Some frameworks have been developed by industry associations, others created by consulting companies who sell them to clients.

Security Staffing

Faced with the hostile environment of the Internet and the various legal imperatives, security has become an essential responsibility of any IT organization. The problem is that the increased level of malicious activity is requiring the consumption of more and more internal resources.

For example, an organization may already have purchased and deployed firewalls and intrusion detections systems. But these devices generate a steady stream of log and/or alert data. If no one is able to analyze and respond in a timely fashion to the data, the value of the information is severely reduced. As the number of incidents increase, so does the volume of information that must be analyzed, generating even more time pressure.

Another time-related concern is the fact that network scans, attacks, and other invasive activities do not occur only during normal business hours; "hackers never sleep." Obvious responses to this state of affairs are either placing your engineers on call or adding staff for round-the-clock coverage. But this is not always practical and besides, information security expertise is not cheap.

According to the 2003 Computerworld Salary Survey[12], the average salary of a Network Engineer is $70,579. Add 25% to get the "fully burdened" (that includes benefits and taxes) for a total of $88K. The total cost of an Information Security Specialist is even higher, almost $94K. And that's before factoring in any training. Noted security expert Bruce Schneier, CTO of a Managed Security Services company, says [13] it takes at least *five* full-time employees to staff appropriately for security expertise.

Especially in smaller organizations, even a single trained security professional may not be on staff; instead the security functions are spread across several IT staffers. Cost savings can be great but there comes a point where the available time, or more commonly, the expertise of the staff is exhausted. With attacks becoming both more sophisticated and more frequent, the need for security specialists has never been greater.

At this juncture, it is time for management to consider outsourcing security, or more specifically engaging a Managed Security Service Provider (MSSP). Larger companies with fuller security staffing come to this same decision, when they recognize that more of its IT efforts are going into protecting and managing the perimeter than focusing on the core business. This trend towards MSSPs is so strong that industry analyst Gartner is predicting[14] a 31% compound annual growth rate (CAGR) through 2005.

Why a MSSP?

A generic MSSP will likely offer some combination of the following services: managed firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), external monitoring, managed virtual private networks (VPN),

anti-virus and SPAM screening, log and alert analysis, reporting, hardware support, ongoing maintenance, and full documentation.

A typical MSSP has at its core a fully staffed network operations center (NOC) which can have varying degrees of redundancy. At the very least, it will have strict backup procedures and the ability to withstand an extended power outage.

The NOC houses the Network Security Engineers (NSEs) who become the watchguards over your network. Monitoring and control of your firewalls is all performed remotely from the NOC. Because client systems are always connected to the Internet, NOCs are staffed 24/7/365.

The key to any MSSP is its people. You can go to any consumer electronics website and order a firewall which will probably function perfectly well. However, first it must be configured correctly. Second it must be monitored to ensure that the access rules are achieving the desired result. And finally, violations of policy must be handled. A MSSP's engineers take over these tasks for you. Ultimately the service you are buying is the human intelligence of a trained engineer. When an IDS sensor triggers an alert, it is the NSE who interprets it and determines whether it is a false positive or a bona fide attack.

Thus, for an NSE, a solid foundation in security is essential. While this can be established by various credentialing organizations, due to the rapid rate of change in the field, a certification today needs to be coupled with ongoing training tomorrow. Most important is real experience in analysis and incident handling. This is one legitimate instance where "been there, done that" is of high value.

The NSEs become a virtual extension of your own staff, performing configuration changes and handling incident responses as well as being a general resource for your security concerns. A successful NSE will have the ability to communicate clearly and, as the person responsible for implementing your security policy, have a full understanding of your network.

In between analysis of logs and incident handling, NSEs will immerse themselves in the daily onslaught of security related information: alerts, virus announcements, vulnerability reports from CERT, SANS, BugTraq, etc. Keeping current is one of the necessities of being a security provider and it also one of the biggest challenges to an in-house staff.

Advantages of a MSSP

MSSPs offer many advantages over in-house solutions. Among these are economies of scale and shared knowledge across client systems.

Your own network may be relatively stable and suffer attacks only occasionally. But, at the occurrence of an attack, everyone springs to full alert and you deal with it. It is sort of like the way a municipal fire department works. A MSSP, on

the other hand, by handling multiple clients, and varying networks, is dealing with threats and attacks on a daily, if not hourly basis. When an attack arises, they are likely to have seen it before and, if not, have a well-defined method for responding to it including, if requested by the client, involving the client's technical staff.

Beyond having the effect of better "load balancing" of people, when an attack is seen at one client, the MSSP can use this information to push out preventative changes to other client sites. For example, if a variant on an existing worm is discovered, an IDS signature can be developed and quickly deployed to all the MSSP's clients' sensors even before an official signature is released.

That implies another advantage: the MSSP is a member of a trusted community of "white hats." These are the folks who are proactively working to discover and disarm the latest vulnerabilities and exposures. As part of this group, your MSSP may be privy to exploits and fixes or patches before they are released to the general public.

Some MSSPs offer remote vulnerability assessments (RVA). An RVA report details the weaknesses of your network as perceived by an unprivileged outsider. To perform these tests, the MSSP uses the very same tools that are employed by hackers to get into your network. As the NSEs become expert in the use of these hacker tools they then gain the experience to better recognize the attack signatures when they are seen on any of their monitored client systems.

A fully managed MSSP solution will include the hardware. That means that you actually do not own, for example, your firewall. You are paying for a service — security — that happens to include this hardware. Because the MSSP owns the equipment it is their responsibility to maintain it, monitor it, patch it, upgrade it, and, when the time comes, replace it.

Remote monitoring tools allow the MSSP to securely track the status of the box and collect reports that can include disk errors. Therefore, if hardware is showing signs of failure, it can be proactively replaced. When there is critical connectivity, a MSSP can provide a spare firewall that sits on the shelf until it is needed. Then, with a brief out-of-band dial-up connection, backup firewall configurations can be quickly loaded onto the new box and make it live.

In cases where even a few minutes of offline time is unacceptable, a MSSP will utilize a high availability (HA) firewall setup, where both machines are live but one remains passive without traffic flowing through it. When the active firewall's configuration changes, they are mirrored on the backup. The NOC then monitors the active firewall and, when it fails, switches it over to the backup, which becomes the new primary.

Conclusion: Making the Decision

Unless your organization is extremely small or extremely large, at some point you will likely consider the utility of a MSSP. In selecting a provider, here are a few factors to consider:

- Longevity and financial stability of the company — What is its track record? How is it funded?
- External Audits — How secure is your provider itself? They will have the "keys" to your network; make sure they are worthy of them.
- Service Level Agreements (SLA) — What is the guaranteed response time for an incident? How long does it take to configure a simple change?
- Staff Credentials — What certifications/degrees do the NSE's hold? The CTO? How many years in the trenches are represented?
- Scalability — With increasing MSSP growth rates, is the provider well positioned for expansion?
- References — Try to solicit a company reference with a similar network configuration and complexity and, if possible, one for whom the provider has handled a successful attack.

Choosing to use a MSSP is the first hurdle. Having looked at the severity of today's threat level, the legal mandates to be secure, and some of the costs of a penetration, whether to ramp up your security efforts is no longer a question of if, but how. The cost of effectively providing the level of security that today's environment demands has become prohibitive. For these reasons, now is the time to consider Managed Security Services.

References (by Subject Area)

HIPAA

American Management Systems. "What is HIPAA?" August 5, 2002.
http://www.cms.hhs.gov/hipaa/hipaa1/content/more.asp

Department of Health and Human Services. "Health Insurance Reform: Security Standards." February 20, 2003.
http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf

Nachimson, Stanley. "HIPAA Security Standards Final Rule."
http://www.urac.org/documents/URACPresentationCMS.ppt

Suarez, Walter "Overview of the legislation." January 30, 2003.
http://www.wedi.org/snip/public/articles/details%7E6.htm

"HIPAA Administrative Simplification - Security." December 10, 2003.
http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp

"HIPAA Administrative Simplification Compliance Deadlines." February 12, 2004.
http://www.cms.hhs.gov/hipaa/hipaa2/general/deadlines.asp

Gramm-Leach-Bliley

Electronic Privacy Information Center. "Gramm-Leach-Bliley Act." March 30, 2004.
http://www.epic.org/privacy/glba/

Federal Trade Commission. "The Gramm-Leach-Bliley Act Privacy of Consumer Financial Information." June 19, 2001.
http://www.ftc.gov/privacy/glbact/glboutline.htm

Langin, Daniel. "Gramm-Leach-Bliley Security Requirements: Keeping Robbers and Regulators from the Door." June 23, 2002.
http://www.itsecurity.com/papers/recourse1.htm

"Gramm-Leach-Bliley; Summary of Provisions."
http://banking.senate.gov/conf/grmleach.htm

"Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Final Rule." February 1, 2001.
http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf

Sarbanes-Oxley

Beaver, Kevin. "Ask the Expert: Law, Public Policy, and Standards." January 18, 2004.
http://searchsecurity.techtarget.com/ateQuestionNResponse/0,289625,sid14_cid570990_tax295652,00.html

Entrust, "The Sarbanes-Oxley (SOX) Act and the Impacts of Non-Compliance."
http://www.entrust.com/governance/sox.htm

Ernst & Young, "An Overview of the Sarbanes-Oxley Act of 2002." September 2002.
http://www.ernst-young.de/global/download.nsf/Russia_E/EY_Sarbanes_9_12_02e/$file/EY_Sarbanes_9_12_02e.pdf

Hurley, Edward. "Security and Sarbanes-Oxley." September 25, 2003.
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929451,00.html

Jefferson Wells International. "Sarbanes-Oxley Section 404 Deadlines." March 1, 2004.
http://www.jeffersonwells.com/inet/sarbanes/Sarbanes-Oxley404Extension.pdf

Nagel, Karl. "Sarbanes-Oxley Act of 2002."
http://www.sarbanes-oxley.com/pcaob.php?level=1&pub_id=Sarbanes-Oxley

University of Cincinnati College of Law, "Section 404 -- Management Assessment of Internal Controls."
http://www.law.uc.edu/CCL/SOact/sec404.html

SB 1386

Decru. "Data Security Requirements for California's SB1386." August 7, 2003.
http://www.decru.com/solutions/pdf/sb1386.pdf

Lemos, Robert. "Law aims to reduce identity theft." June 30, 2003.
http://zdnet.com.com/2100-1105-1022341.html?tag=nl

MSSP

Allen, Julia et al. "Outsourcing Managed Security Services." January 21, 2003.
http://www.cert.org/security-improvement/modules/omss/a.html#toc

Gartner, "Guidelines for choosing to outsource security management." October 31, 2003.
http://techrepublic.com.com/5100-6264-5093691.html

Hamblen, Matt. "10 Questions to Ask a Managed Security Service Provider." January 19, 2004
http://www.computerworld.com/securitytopics/security/story/0,10801,89101,00.html

Hameed, Imran. "Successful Managed Security Services (MSS)." July 16, 2003.
http://internet.about.com/library/aa_mss_082902.htm

James, Natalie. "How to Pick an MSSP." August 2002.
http://infosecuritymag.techtarget.com/2002/aug/pickmssp.shtml

Citations

[1] "CERT®/CC Statistics 1988-2003."
http://www.cert.org/stats/

[2] Richardson, Robert. "2003 CSI/FBI Computer Crime and Security Survey." 2003.
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

[3] Friedrichs, Oliver. "Symantec Internet Security Threat Report Trends for July 1, 2003 - December 31, 2003." March 2004.
http://enterprisesecurity.symantec.com/Content/displaypdf.cfm?pdfid=665&EID=0

[4] Kapica, Jack. "Computer virus damage shatters records." April 2, 2004.
http://www.globetechnology.com/servlet/story/RTGAM.20040402.gtjackvirusapr2/BNPrint/

[5] Reuters, "$55bn virus damage costs for businesses last year." January 19, 2004.
http://www.silicon.com/software/security/0,39024655,39117842,00.htm

[6] Fogarty, Kevin. "Block Spam! Save Millions! Feel Better!" April 5, 2004.
http://www.eweek.com/article2/0,1759,1561892,00.asp

[7] Robinet, Judy. "The Alinean ROI Report - March 2004."
http://www.alinean.com/Newsletters/2004-3-March.asp

[8] Loeb, Martin. "Cybercrimes' True Price: Crime May Not Pay, But Someone Has To Pick Up The Cost." March 29, 2004.
http://www.informationweek.com/shared/printableArticle.jhtml?articleID=18402607

[9] Lemos, Robert. "Study: Regulations driving security spending." September 29, 2003.
http://zdnet.com.com/2100-1105-5083758.html

[10] Securities and Exchange Commission. "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports." June 11, 2003.
http://www.sec.gov/rules/final/33-8238.htm#ia

[11] Peace, Steve. "SB 1386 Senate Bill - CHAPTERED." October 02, 2002.
http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[12] Computerworld. "2003 Computerworld Salary Survey." 2003.
http://www.computerworld.com/careertopics/careers/exclusive/salarysurvey2003/entry

[13] Schneier, Bruce. "The Case for Outsourcing Security." June 20, 2002
http://www.computer.org/computer/sp/articles/sch/index.htm

[14] Symantec, "Key considerations for outsourcing security." January 6, 2004.
http://www.symantec.com/symadvantage/020/mss.html