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

William S. Packer
GSEC, Assignment 1.3 (December 12, 2001)

Information Security Audit Processes for Financial Services Firms, the C-I-A Approach

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Abstract	**3**
Executive Summary	**3**
Introduction	**3**
GLBA	6
Risk Framework	**6**
Brief Background of SAS-70	**8**
Other Types of Assessments	**8**
Voice and Telephony Systems	**9**
Conclusion	**11**
REFERENCES:	**12**

© SANS Institute 2000 - 2005, Author retains full rights.

Abstract

This paper examines the adequacy of financial service firms' reliance on the *Statement on Auditing Standards Number 70 (SAS-70)* that was developed and is maintained by the American Institute of Certified Public Accountants (AICPA)[1]. The financial services industry has generally relied on SAS-70 audits to ascertain the relative adequacy of, among other things, the strength of the information security of their vendors. The author's opinion is that this is generally inadequate. This paper will provide an overview of the current internet-related threats that a financial service firm may face, propose a categorization framework for thinking about information security threats and, utilizing the SANS C-I-A triangle metaphor, provide a basis for advocating that merely relying on SAS-70 audits is insufficient.

Executive Summary

The Statement on Auditing Standards No. 70 (SAS-70) is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA) (About SAS 70). It is well accepted within the financial services community as a de facto representation that a firm has sufficient information safeguards to protect the information assets of the corporation. In a typical contractual arrangement between a bank or other financial services firm and a vendor the bank will generally ask for a copy of the latest SAS-70 audit and use this as a fundamental basis of its information security and financial controls due diligence. This approach, while having some merit, is simply not sufficient. Information security assessments must be combined with other assessment tools such as comprehensive penetration and vulnerability tests, a technology culture that supports treating information security as an important part of any development or integration effort as well as a well thought out internal education campaign in order to be effective. In light of the fiduciary responsibility that the Gramm-Leach-Bliley Act (GLBA) explicitly stated, a financial service firm would be well advised to look beyond the auditing statements contained in a SAS-70. The firm should assure themselves that other processes and structures are in place to support the appropriate safeguards as well as encouraging a proactive information security culture.

Introduction

The events surrounding the September 11 attack have brought renewed emphasis to issues relating to information security. The popular press brings a daily onslaught of issues to our collective consensus; see, for example, the March 25th article in Time Magazine titled "Mission: Intelligence" (Franklin). Against this backdrop there is an

[1] www.aicpa.org

© SANS Institute 2000 - 2005 Author retains full rights.

opportunity to re-evaluate our current security practices and controls and make necessary changes.

As January 1, 2000 approach, many information technology organizations found themselves in the unique positing of having resources available to inventory all systems and upgrade those systems that appeared to be non-Y2K compliant. Similar to this opportunity, the current environment has brought to many boardrooms and senior executive suites across the country a new understanding and emphasis on efforts to create a computing environment that is reliable and resilient, or, as the SANS C-I-A triangle would refer to it *available.* In addition, public scrutiny has focused its attention to the confidentiality practices of corporations. In particular, this attention has been drawn to the practices of financial services firms since they have access to our most personal financial information and health care firms.

The review of the available data shows no clear indication that the information security threat from outside the firm, that is, internet-related or web-based threats are increasing. However, it is clear that the level of sophistication is certainly increasing (Internet Security Systems). Apart from the threats posed by such things as computer viruses, spoofing and denial of service attacks, we see the power of the internet being further leveraged to provide for more complex extensions of these threats, such as distributed denial of service attacks. More alarmingly, we increasingly see the use of hybrid attacks. These hybrid attacks combine a virus or viruses with a range of automated tools that try to exploit known vulnerabilities to deposit their payload (ibid.). Against this rise in threat sophistication is our continued trend toward reliance on the Internet as a global network. It is no coincidence that some of the most useful technologies being developed today, such as web services and instant messaging, assume an open architecture and rely on such ports as 80 or 21 or 22 as being open. "Nearly 70% of all attacks in Winter 2002 exploited port 80" (Ibid. 4). I doubt that many information technology professionals would last long in their position if they closed port 80 and told their firm to find another way other than the Internet to transact business.

The message is clear; the only effective strategy is a multi-layered and multi-vendor strategy. A strategy that extends the defense-in-depths concept and applies it not only to a multi-tiered authentication process but also applies multi threat-resistant procedures, processes and technologies at each reasonable perimeter or boundary point (Ernst and Young). Our security posture must also include the realization that reliance on a single vendor's product probably leaves us exposed. A multi-vendor product set is therefore appropriate. Additionally, within-applications authentication and other threat-resistant techniques should be employed to limit the damage that an attack may cause. Finally, carefully crafted contingency operations plans should include the recognition that all parts of the C-I-A triangle may come under attack; and, worst of all, the corporate owners of the data may be unaware that an attack has taken place and resulted in harm.

© SANS Institute 2000 - 2005 Author retains full rights.

Although the current environment has helped to sensitize senior management to issues of information security, security professionals still face many obstacles in obtaining appropriate funding. One of the key difficulties with presenting recommendations stems from the difficulty in evaluating security-related solutions. Traditional measures of financial return, or return on investment (ROI), are simply inadequate to appropriately capture the real benefits. In traditional ROI measures, we estimate the costs and the resulting cash flows and using some financial techniques such as pay back period or discounted cash flow models we estimate the expected increase to corporate revenue that can be tied to the successful implementation of the proposed project. After the project is completed, we can then look back and generally tie revenue changes to our project thereby validating our original assumptions. However, in information security projects, the task is much harder. As you can quickly see, the revenue enhancement is derived by an event not happening. So, you can certainly estimate the probability of an event occurring and then estimate the loss in revenue due to the event but there is simply no way to validate these assumptions. To make matters worse, information security often deals with issues that have complete unknowns. No one would have ever imagined that on a single day two passenger jets would be flown directly into the World Trade Center. The same can be said of information security. We need to design systems that can withstand attack by forces we cannot even imagine.

There is also a perceptual issue that works against information security professionals. When we talk to the general business population about information *security* they assume that we are using this word in the general vernacular. That is, that you can be secure from threat. Or, as Merrian-Websters Collegiate Dictionary defines it, "the quality or state of being secure: as a freedom from danger" (Merriam-Webster's). However, information security professionals know that the only way to be "free from danger" [ibid.] is to close the firm, to go out of business. Short of this draconian measure, the complete elimination of danger is simply not possible. When we talk about information security, our standard is more like the one used in psychology, "A sense of confidence, safety, freedom from fear or anxiety, particularly with respect to fulfilling one's present (and future) needs…" (Penguin Dictionary of Psychology). When I discuss information security, I use the simple standard of the sleep test. That is, at what level of assurance or at what level of probability can you be sufficiently anxiety-free that you are able to sleep at night. Sleepless nights worrying about your firm's exposure to threat, means that you need to keep investing in appropriate technologies and processes until you finally get a good night sleep.

This last point is an important one, one we cannot be emphasize enough, if you fail the sleep test, then continue to invest in *appropriate technologies and processes*. Investments in information security, while critically important, must be made prudently. Although it may comfort us to hear someone report that we invested "x" million dollars

© SANS Institute 2000 - 2005 Author retains full rights.

in information security, we need to make sure that those investments actually made the firm more secure. The investments in protection, site hardening, notification, contingency, human capital et al must be aligned with the value of the asset that the technology or process is protecting.

GLBA: On November 2, 1999, then President Clinton signed into law the Gramm-Leach-Bliley Act (GLBA). This law had several provisions one of the provisions prohibited a financial service institution from sharing certain personal information without the consent of that person. Another provision held the financial service institution responsible for ensuring that its service providers, who may be outside the scope of the regulation since it only applied to financial services firms, complied with this law. That is, if a vendor not ordinarily covered by this law, provided services to a financial service provider who is covered, and the non-covered vendor violated any provisions of GLBA the financial services provider and not the vendor would be held liable [State of Massachusetts].

Risk Framework

One way to think about the kinds of threats that a firm may face, is presented in this two-by-two matrix:

		Type of Attacker	
		Insider	**Outsider**
Type of attack	**Targeted**	Evil Insider	Puposeful Outsider
	Non-targeted	Tester	Joy rider

There are two parameters, the type of attack, targeted or non-targeted and the type of attacker, insider or outsider. From a type of attack perspective, in a targeted attack, the firm has been explicitly identified as the object of the attacker's efforts. Conversely, in a non-targeted attack, the attacker doesn't identify the firm. The actual firm-victim is an afterthought. That is, the attacker's list is limited to those firms that s/he has determined is vulnerable. Next, we can look at the type of attacker. The attacker can either be an insider, such as an employee, recent ex-employee, contractor or other affiliated person. The key to this definition is that the attacker posses some sort of special knowledge of the firm. Conversely, the attacker may be an outsider, who possesses no special knowledge of the firm, its controls or activities beyond what is publicly available.

We can examine each of these quadrants. The *Evil Insider* possesses both insider

© SANS Institute 2000 - 2005, Author retains full rights.

knowledge of the firm and specifically targets the firm for attack. The clearest example is an IT worker who was recently fired from the firm and wishes to take revenge on their former employer. Since this group has both knowledge of the firms typical defenses, may know what information is most valuable and may be able to more easily employ social engineering tactics to unwittingly recruit former or present workers at the firm, these can be especially deadly attacks. For example, it isn't uncommon for many Bank accounting departments to create and store vast quantities of financial data in excel spreadsheets stored on the network. Often this data includes information that GLBA would categorize as customer confidential. It is generally stored with little or no protection other than that provided by the network and very often, they e-mail this data in an unencrypted format to their outside accounting and audit firms. Obviously, someone with knowledge, time and some commonly available tools could copy and use this data or simply modify it without the firm ever being aware that this has occurred.

An interesting variant on this quadrant is the unintentional evil insider. Here, without malice, an action is taken which causes the firm harm as if it were under attack. Recently, I was involved in such a case. Although non-disclosure limits what I can say, basically, the bank's marketing department had contracted with an outside firm to market one of its web-based products. The outside firm decided to run a direct e-mail campaign to a group of folks who would be paid a nominal fee to click on a link and be directed to the bank's website. Unfortunately, neither the marketing department nor the bank's technology group knew that the outside firm was going to do this. So, when the e-mail campaign happened, the bank's website was flooded with hits eventually bringing the website down.

The *purposeful outsider,* unlike the *evil insider* has no special knowledge of the firm. They may have determined that there is important data that can be useful if it were obtained. Or, simply be interested in attempting to cause the firm damage by bringing down the firm's web-based or non-web-based computing environment. Or, they have decided to take up what seems like a challenge, such as graffiting a popular website.

The *joy rider* is sometimes referred to as script kiddies. These individuals download tools from the web deploy them and then wait to see who or what is impacted by their efforts. Sometimes they simply scan for vulnerabilities and then plan an attack on the most interesting targets and sometimes they simply let attacks run directly and indiscriminately.

Finally, we have the *tester.* There are two variants to the tester. In the first variant they start out as a joy rider but in the course of their testing, they find out that their own firm has unprotected vulnerabilities. Imagine their surprise and joy when they find out that the firm they get to attack is their very own. Very quickly, they begin to look like *evil insiders* however, they didn't start out intending to do the firm harm, the firm just

© SANS Institute 2000 - 2005 Author retains full rights.

happened to be on their radarscope.

The second variant of the *tester* is the insider who downloads a series of publicly available internet-related vulnerability tools and then launches them against the firm either directly from their own workstation, behind the firewall, or from some place off the LAN on the public side of the firewall. If caught, when they are questioned, they will usually say something like, I was just "testing" to see if my company had this vulnerability, I didn't mean to do any harm. Of course, they do harm the firm. Either in lost productivity as desperate IT, audit and/or information security professionals spend valuable time attempting to determine what has happened, who did it and how. Or, in real impact to the firm as the weapon unleashed delivers its painful load.

Brief Background of SAS-70

The SAS-70 is an auditor report performed by a certified public accounting firm for the purpose of offering an opinion on the internal controls of the firm [About SAS 70, Ernst and Young]. There are two types of SAS-70 audits, type 1 and type 2. Type 1 comment on the control infrastructure while type 2 includes an opinion on the controls and an opinion on the actual operation of those controls. The firm defines what it is trying to protect and outlines how it is protecting it. The auditor reviews this information and provides an opinion. In type 2, the auditor will also observe these controls on a test basis to determine if they are functioning the way that management is expecting them too.

When employing a SAS-70 audit to form a basis of an opinion of a firm's information security posture, some of the audits shortcomings should be kept in mind. These include:

- It is designed to verify internal controls not to develop or enhance the information security posture of the firm.
- It is a point-in-time audit. That is, the controls could rapidly decay after the audit is performed without anyone being aware.
- They are typically performed by audit professionals not information security professionals
- Controls are assessed via policy review and interviews not by actual testing
- The control standards are by and large set by the firm and not by any objective criteria other than the guidance that the individual auditor may receive from his or her firm.

Other Types of Assessments

There are other types of assessments or examinations that may be employed.

© SANS Institute 2000 - 2005 Author retains full rights.

Since to a large extent the SAS-70 examination is subjective and is often performed by someone with limited information security domain specific knowledge. I advocate that other assessments in conjunction with the SAS-70 be utilized in order to determine the clearest picture of the firm. Since GLBA makes the financial institution responsible for the information security practices of its partners, by extension, these recommendations apply to evaluating those firms as well. As a recent Information Security Magazine article pointed out, "…when you are being asked to evaluate the state of someone's system security…. no single test is automatically always the best…" (Winkler).

These other audits and assessments should include:

- Network architecture review
- Voice systems review
- Penetration tests
- Physical access review
- Education and cultural alignment

Recommendations

Beyond the SAS-70 audit, the firm should have periodic, independent evaluations of its technology network architecture. A qualified firm should perform the evaluation and that firm should not be eligible to participate in the remediation of any issues found. Or, if they do perform the remediation, they should be precluded from being part of the assessment in subsequent time periods. Apart from this, the firm employed to perform this assessment should be replaced every 5 to 7 years and the assessment team itself should have its lead members modified every 3 to 4 years. The point of this assessment is to identify critical architectural issues that might result in less than sufficient availability of the network. This is the "A" in the C-I-A triangle.

Second, an external firm should perform a series of network scans both inside and outside the firewall in order to understand what vulnerabilities the firm has. Typically, this is referred to as a penetration test. In addition to the typical penetration test, prudence dictates that internal scanning be done as well in order to detect devices or systems that are on the network that may leave the network vulnerable.

Voice and Telephony Systems

The continuing convergence of voice and data systems as well as the remarkably rapid increase in sophistication and usage of voice systems such as voice mail, auto-dialers, predictive dialers, voice response units (VRUs), computer telephony integration (CTI) and the like, argues for the explicit inclusion of voice systems in our network

© SANS Institute 2000 - 2005, Author retains full rights.

assessment and penetration tests. Unfortunately, due to the way in which these systems have traditionally been viewed there appears to be a fundamental lack of acknowledgement that we should include these systems in our framework. Consequently, there can be some difficulty in locating appropriately skilled technicians who can design and execute the appropriate tests.

Voice systems have generally been required to be high availability systems. In the United States, we assume that like our light switch and our blenders, when we pick up the phone we will receive a dial tone and be able to make our call. As switch vendors began to introduce other voice system technologies such as voice mail, they brought that same zeal for high availability, typically what we call five-nines or 99.999% uptime to those systems. As such, they have generally relied on well-established highly available operating systems such as Unix and high quality switched-based connection systems to assure voice grade quality. Voice systems haven't had the same kind of vulnerabilities that our less mature web-based systems have experienced, nor have they been subject to the kind of attempted attacks that our web-based systems have. However, it is an interesting side note that in the United States, hacking originally started with attempts to obtain free calling from AT&T which was the only telephone carrier. We should not be surprised to find voice systems again under increased attack.

Another way to look at this trend is as an effort-reward equation. That is, as the value of the assets in web-based systems increased while at the same time the ease of penetration decreased, hackers and other ne'er do wells shifted their attention from free long distance calls to these web-based systems. Said another way; the reward increased while effort required decreased. Now however, as the equation reverses and the level of difficulty rises in penetrating web-based systems while at the same time the value of voice system assets increases and their ease of penetration decreases, attacks again shift to voice systems.

Several trends which started in the mid 1990s now force us to reconsider the relative comfort that we have with respect to voice systems. As voice over IP (VOIP) technologies have entered our common vernacular we are often taking traditional voice system services and deploying them on Wintel based platforms, abandoning our traditional, and more secure, switched networks in favor of packet based transport mechanisms. As an example, a major equipment provider, AVAYA, began selling during 2000 what they call an IP600, which is a small to mid-sized office IP enabled switch running on a Windows NT 4.0 desktop operating system. Even if you chose not to use the voice-to-IP capabilities of this switch, you had the inherent security concerns of an NT4.0 desktop, which was handling all your voice traffic and was generally enabled to handle the voice mail needs of that office as well.

Another trend prevalent in the voice space is the emergency of many niche players

© SANS Institute 2000 - 2005 Author retains full rights.

who see the voice-data convergence as an opportunity to develop and deploy products. Often, these products are priced very competitively and are typically being deployed on low-end machines that are again utilizing the Wintel platforms.

Complicating all of this, is that the individual technicians developing and deploying these systems have generally never had to wrestle with the kinds of attacks that are so prevalent in the web-based public facing systems. Yet, what system is more public and more necessary for day-to-day activities of the firm than voice systems? It is precisely over these systems that some of our most confidential matters are discussed. These systems are public facing and can contain or have access to very private information; or at the very least, allow someone to gain access to the firm's data network through an under-protected voice system.

Third, a physical assessment of controls needs to occur. That is, are doors left open allowing individuals access to the computing environment? Are sensitive documents shredded before being disposed in the trash? Are physical access devices used to control when and who can enter the firm's offices? If so, are these reviewed on a periodic basis to ensure that only appropriate folks are entering the firm at appropriate times? Are tools being used to provide behind-the-firewall remote access? If so, are these appropriately located in secure areas? What kind of access are non-employees given? Are appropriate background checks performed and should all employees be bonded?

Finally, and perhaps most importantly, both the non-IT employees of the firm and the IT employees of the firm should be regularly exposed to security awareness training. The best line of defense is the employee as s/he is performing his or her day-to-day activities. They, more than anyone else, are able to report to us anything out of the ordinary as well as things that the firm has always done a certain way but in light of new threats might need to rethink. The threats posed to us by efforts such as social engineering can only be effectively mitigated if the employees feel that security is an important aspect of their job and have been given the knowledge to understand the kinds of issues that they may face. Finally, there has to be a format in which folks can bring to light issues that appear at variance with the firm's security culture. The culture has to encourage and endorse that information security is everyone's job. In a firm where new technologies are developed, developers have to be encouraged to build-in best practice security methodologies from the outset of the project, rather than as a retrofit later.

Conclusion

In the end, for the financial services firm evaluating the relative strength of a potential vendor, we have to look beyond the methods we have used in the past to evaluate vendors. In order to reduce the risk of an information security failure, financial services firms need to ask questions that provoke provider firms to adhere to best practices in

© SANS Institute 2000 - 2005 Author retains full rights.

information security. The financial services firm should certainly read and evaluate a type 2 SAS-70. In addition, they should also look for independent assessments of the internal network. The financial service firm needs to look for a series of independent security assessments that probe for internal and external vulnerabilities both at the logical and physical layers. Perhaps most importantly, they need to look for a culture that encourages and reward forward thinking and proactive information security processes.

© SANS Institute 2000 - 2005, Author retains full rights.

REFERENCES:

About SAS 70. Http://www.sas70.com

Consumer Bankers Association, 2001 http://www.cbanet.org/issues/privacy/documents/Exam%20Guidelines%20July%2019%202002001.pdf

Disaster Recovery Journal, www.drj.com

Ernst and Young, "Service Auditor's Report (SAS70)" http://www.ey.com/global/gcr.nsf/US/SAS_70_-_eRisk_solutions_-_Ernst_&_Young_LLP

Franklin, Daniel, 2002, "Mission: Intelligence" Time Magazine, Http://www.time.com/magazine/

Frost, Allen, Porter, Bloodworth, 1999, Operational Risk and Resilience, Butterworth-Heinemann.

The Information Systems Audit and Control Association and Foundation, www.isaca.org

Internet Security Systems, "Internet Risk Impact Summary for December 22, 2001 through March 21, 2002."

Laudon and Laudon, 2002, Management Information Systems, 7th edition, Prentice Hall.

Merriam-Webster's Collegiate Dictionary (on-line) http://www.m-w.com/cgi-bin/dictionary

Penguin Dictionary of Psychology Education, Second Edition.

Shimell, Pamela, 2001, The Universe of Risk, Pearson Education.

State of Massachusetts, Securities Division, Boston, Ma. http://www.state.ma.us/sec/sct/sctgbla/gblaidx.htm

Winkler, Ira, July 2000, Information Security Magazine, http://infosecuritymag.com/articles/july00/features4.shtml

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.