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 Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

The Search for the Elusive Information Security Dollar… and What To Do When You Find It…

Jack E. Obert

February 20, 2001

© SANS Institute 2000 - 2005 Author retains full rights.

Case Study (Fictitious)

John is a system administrator for a medium-sized hospital in the Midwest. John has completed his Novell CNA and Microsoft MCSE certifications and feels capable of taking on most of his organizations system administration issues. Like most system administrators, John performs a number of duties. Just a few of John's responsibilities include creating user accounts, maintaining the hospital's SQL databases, administering e-mail, and managing system backups. John is also responsible for his companies Internet connection. John's company is preparing to buy several of the small clinics in his community, but only the top echelon in his corporation know this. John doesn't even know this.

John's workday had been pretty uneventful. He helped a few users reset their forgotten passwords. He created new Novell and NT accounts for a new receptionist that was just hired. He cleaned a couple of pesky word macro viruses off of a physician's computer. It had been a pretty routine day. John had completed everything that couldn't wait until tomorrow and besides it was 8:00 pm, so John went home. Later that night, as John was settling down into his favorite recliner with a fresh glass of iced tea (with lemon) and a new book, the phone rang.

"Hello, you have reached the Doe residence…", said John.
"This is Mr. Bigg." This made John a little nervous since Mr. Bigg is the Chief Financial Officer of the hospital that John works for. "Did you see the Channel 3 News this evening?"
"Well… Uh, no I haven't Sir", stammered John.
"They just ran a story about the clinics that we intend to purchase here in town."
"I didn't know we were purchasing any clinics", questioned John.
"That's why I'm talking to you now. Nobody was supposed to know. They had dates and dollar amounts. It was like they had been reading my e-mail."
"Oh…" was all that John could muster.
"I need to know how they got this information, and I need to know tomorrow."
"Yes Sir, I will do my best Sir…"

John told Mr. Bigg that he would do his best, but what can he really do. He hasn't been trained to do this sort of research. He could look at e-mail logs, he could look at his firewall log, but what would that tell him? Maybe the problem was that somebody in the hospital who knew of the purchase talked to the press. Or maybe it was one of those e-mail worms that he had read about.

© SANS Institute 2000 - 2005 Author retains full rights.

"Where do I start?" John mumbled to himself.

"Where do I start?"

The Problem

Does this story sound familiar? It sounds more familiar than most IT professionals would like to admit. How did John get himself into this situation? Even more important than that, how can John keep from getting into the same situation in the future?

Most information technology departments are being consumed by the very technologies that they are supposed to be implementing and supporting. More and more often IT professionals are being forced to manage and maintain systems on which they have little or no expertise. Many organizations rush to generate web presences, hurry to start processing e-commerce transactions, or rush to provide remote access for their employees while the training and funding to secure these endeavors is overlooked. It is estimated that while information security staffing has doubled in the last seven years, only .06% of a company's work force is dedicated to information security. When you do the math, this equates to three security professionals for a company of 5000 employees. That coupled with the fact that only an estimated 5.83% of current information security activities are outsourced, you see that the majority of information security activities are performed within an organization by its own staff.[1]

How did we get here, you ask? We are still trying to remove ourselves, as an industry, from the old attitudes surrounding information security. I'm sure that John has heard many times in his career: "Why would someone attack us? We don't have anything that anybody wants", or "We don't have any enemies". Attitudes like these have kept us in the information security dark ages until just recently.

Every corporation has information that needs to be protected. Nearly all human resource departments have employee demographics online, as do nearly all payroll departments. The customers that our organizations service have information security needs also. Corporate databases may contain credit card information, medical information, billing addresses, cellular telephone numbers, etc. all of which they would like to keep private. Sensitive data aside, nearly every corporation has an Internet home page that needs to be secured. What damages could result if a corporation's image or reputation were damaged due to electronic vandalism? The losses could be immeasurable.

According to the Computer Security Institute (CSI) Computer Crime and Security Survey, ninety percent of its 643 respondents have detected computer security breaches in the last year, while seventy percent reported those breaches as serious. Seventy-four percent of the CSI survey respondents acknowledged financial loss due to those breaches. The total loss among the 273 survey participants who were willing to qualify their losses was $265,589,940. This equates to over $970,000 in annual loss for each organization

© SANS Institute 2000 - 2005 Author retains full rights.

surveyed.[2]

It would not be realistic to expect zero loss if each of the above companies had budgeted an extra $970,000 for computer security, but the number of companies suffering serious loss and the seriousness of those losses could surely have been reduced.

The Solution

Our fictitious friend John from the example above is in a bit above his head now, but what would have helped him? What will help him in the future?

Would effective information security policies have helped?

Information security policies are important. Policies give organizations recourse when their employees do bad things. They are also a means of communicating an organization's expectations with its employees. But are policies really an effective means to prevent computer security incidents? Research done by Information Security Magazine says "no". In fact, the magazine's research shows just the opposite. Companies who have security policies in place report more security incidents than their non-policied counterparts.[3] There may be a number of reasons that this is true, with organization size probably playing the biggest roll, but it is obvious that security policies alone do not work. Security policies may have made John's superiors more aware of their risks, and offered some guidance toward industry standards, but probably would not have solved all of John's computer security problems.

Would an increased information security budget have helped?

An increased information security budget would almost certainly have helped John in his security endeavors. With an increased budget, John could have bought the latest virus scanning software, upgraded his firewall, implemented VPN, bought intrusion detection systems, etc. With an increased budget, John could have hired security consultants to come in and install these new systems. This would most certainly have helped John, right? It probably would not have helped John as much as he would have hoped. Adding these systems and tools to his arsenal would have potentially alerted John to some major problems, but they wouldn't have solved John's fundamental problem… Training. John probably wouldn't have known how to interpret all of his new data or what to do with the data that he could interpret.

Would Information security training have helped John better protect his organizations information?

Absolutely! I cannot stress the importance of information security training enough. Like most information technology professionals, John has to work overtime just to get his work done. Sure, John has been to training classes on some of the applications and systems that he is supposed to support. He can register a patient with his eyes closed. He can tell you how information moves from the blood gas analyzer to the

© SANS Institute 2000 - 2005 Author retains full rights.

> laboratory information system and John has managed to keep current with his two certifications, but he hasn't had time for any formal security training. Concepts like layered security, defense in depth, PKI, man in the middle attack, penetration testing, SYN flooding, etc. have little meaning to John. One has to look only as far as the SANS Institutes own web site to find evidence that this is true. In a group of 1850 security managers and experts meeting in Baltimore, MD in 1999, it was discerned that the number one management error that leads to computer security vulnerabilities is assigning untrained staff to maintain security without giving them the time or training to succeed.[4]

The true solution here, of course, is a combination of all three. No single solution will solve every security issue that a company will be faced with, or even a majority of them. It is mandatory for John's company to have a thorough set of information security policies in place. John's company needs e-mail content policies, acceptable use policies, physical access policies, remote access policies, etc. Having these policies in place will give the employees in John's organization a firm understanding of what is expected of them in regards to information security. It also gives John's organization the ability to take disciplinary action against employees misusing information resources. These policies also set a baseline from which John's organization can measure itself in terms of compliance and industry standards. Without an information security budget and buy-in from senior management, though, John's company may not be able to enforce its own policies. It does no good, for instance, for John's company to have an e-mail content policy, if the company is unable or unwilling to inspect e-mail content. It is necessary for John's organization to provide the funding and support to purchase and implement technology to aid in the furtherance of its own security initiatives. More important than any policy and any budget is to have trained knowledgeable information security professionals on staff. Training, experience and more importantly, time is required to develop a mere mortal into an information security professional. Doctors aren't made overnight and neither are security professionals. You don't give a scalpel to a respiratory therapist and you don't give a penetration-testing tool to a novice. Both lead to more harm than good.

The Cost

The costs associated with providing information security can be high. And the costs are high not just in terms of dollars, but also in terms of time. Security training such as that offered by The SANS Institute can cost as little as $550 for a one-day course, or as much as $3600 dollars for an eight-day Microsoft Windows security course.[5] Even with IT training budgets on the rise, and nearly doubling between 1999 and 2000, the average IT training budget for companies who have more than 100 employees is between $1000 and $1500 per employee annually.[6] When you add in transportation, hotel, etc. IT training budgets don't come close to covering the costs of comprehensive information security training programs. But, the real roadblock to providing IT professionals security training

© SANS Institute 2000 - 2005 Author retains full rights.

is time. If John, the character from our example, were to take a one-week leave of absence to attend information security training, his organization would be lost by the time he returned. It would take him two or three weeks just to catch back up which also represents a great cost to his corporation. Neither he, nor his company, can afford his time off, but then again they can't afford for him not to go either. Some companies try to solve this dilemma by outsourcing their computer security needs. But those costs are also high. It is not uncommon for an information security consulting firm to charge $250 or more per hour. The problem with these companies is that many times the "professionals" that they have employed have little more training or experience than the staff that they are being hired to augment. And even worse, when they leave, many times the knowledge leaves with them.

As shown, the costs associated with information security training can be high. But are the costs of not providing training any less? I don't think so. Just one sexual harassment lawsuit prompted by inappropriate e-mail or Internet use could easily cost a corporation its entire IT training budget. It is estimated that in 1999, malicious virus attacks alone cost organizations over $12 Billion.[7] This number doesn't take into account the monetary and reputation damage inflicted upon corporations by the theft of credit card and personal identity information. With continually increasing consumer and corporate Internet activity, and the increasing numbers and severity of attacks, this amount may well be growing.

It is almost certain that if organizations were to increase their investment in the quantity and quality of training, and provide their employees with adequate time to complete their training, severe information security breaches would become the exception rather than the norm.

Case Study (Fictitious) Continued…

Would John have solved his problems without all of this? Probably. After John's efforts to discover the source of the breach failed, John would recommend that his corporation hire an information security consulting firm to investigate the suspected security breach. It would have probably been found that a hole had been configured through the hospital's firewall to allow the vendor of the hospital's medical records system remote access capabilities to all medical records workstations in order to support their application. And it would have also been found that one of the workstations in the medical records department at the hospital that John works for had been remotely accessed several times each day for the last month. Upon further investigation, it would have been found that packet capturing software had been installed on the frequently accessed workstation. Looking at some network diagrams would have shown investigators that the compromised workstation happened to be connected to the same network hub that the CFO's computer was connected to and thus the mystery and all of John's problems are solved…

© SANS Institute 2000 - 2005 Author retains full rights.

Yeah right!

---

[1] Violino, Bob. "Information Security Spending Rising, But Still Inadequate, Study Says." February 14, 2001 URL: http://www.informationweek.com/newsflash/nf617/0214_st2.htm (February 19,2001).

[2] Computer Security Institute – Patrice Rapalus, Director. "CSI Press Release." 2000 Computer Crime and Security Survey. March 22, 2000 URL: http://www.igocsi.com/prelea_000321.htm (February 10,2001).

[3] Birney, Andy. "Security Focused." September 2000 URL: http://www.infosecuritymag.com/articles/september00/pdfs/Survey1_9.00.pdf (February 18,2001)

[4] The SANS Institute. "The 7 Top Management Errors that Lead to Computer Security Vulnerabilities." 1999 URL: http://www.sans.org/newlook/resources/errors.htm (February 16, 2001).

[5] The SANS Institute. "SANS 2001 Conference Registration." 2001 URL: http://www.sans.org/SANS2001register (February 17, 2001).

[6] Dash, Julekha. "Workload, Stress Rise for IT; Firms Respond." June 19, 2000 URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO45939,00.html (February 20, 2001).

[7] Bhavnani, Samir. "Malicious Virus Attacks Cost Organizations More Than $12 Billion in 1999." January 14, 2000 URL: http://www.info-sec.com/viruses/00/viruses_011400a_i.shtml (February 20, 2001).

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

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event