Global Information Assurance Certification Paper

Explaining Security Needs To Management

GSEC 1.3 & GIAC 1.2

Steve O'Brien

ABSTRACT

Although they are critical to corporate operations, network security needs are frequently ignored by corporate management. However, this lack of security is not because senior managers actually believe that there is no need for a more secure network. It is because they haven't been educated about the need for improving their network security and convinced of the steps they need to take in order to make their network secure. In this paper, I will describe the information required by corporate managers to make informed decisions regarding network security as well as techniques for conveying this information to them.

As network security professionals, we all face challenges on a daily basis. We each must keep up with the latest technologies, the latest exploits of those very same technologies, deal with user demands, and perhaps most importantly, deal with management: both their demands upon us, and ours upon them. Being watchful and stingy of corporate resources (both budgetary and otherwise) is the job of corporate management. Ours, in turn, is to provide them with a compelling argument as to why the security of the corporate network deserves a share of those resources. While I will be the first to concede that no two managers will behave the same, my goal is to provide a helpful guide to getting the resources you need.

I feel that I must point out from the outset of this discussion that my intent is not to provide for specific solutions to problems, nor is it an attempt to point out all possible vulnerabilities. Each of these specific problems and solutions, are entirely worthy of their own paper. I will use a number of examples, both general and specific to make my point, and would recommend that you do the same when making your argument to your manager. As obvious as it sounds, having solid, real world examples goes a long way.

Unfortunately for us, most of us don't work in a technology-focused industry. If we did, there would be a much higher percentage of senior management with technical backgrounds. Given the hand that we are dealt, most of us are left trying to explain technical matters to non-technical managers, or at least non-technical senior management in control of the budget.

Most businesses are, by their very nature, hierarchical. What this means in the context of this document is that you need to determine where you fall in that hierarchy, and where the person you need to talk to in order to get actions approved and taken is. In large organizations this may mean a number of middle-management layers before you reach someone who can give you the authorization you need, in small organizations it

may mean you go have coffee with the owner of the company and your project and budget are finalized. We'll talk more later about determining the correct person or persons to talk to, however as you're reading this document, I'd suggest that you picture the process you will be faced with when you're ready to take action.

What managers do care about (that is to say, what we need to make them care about) is knowing and understanding the relationship between three important concepts. First, the manager must have some understanding of the current IT security environment, and its impact on the financial health of the company and the business need for a solid plan. Then, they need to be able to evaluate the sources of threat to their specific organization. Finally, in order to make an informed decision, they must be made aware of the actions we as IT staff can take.

If this relationship is not presented well, managers will probably only be willing to provide network security reactively instead of proactively. This would be a grave mistake, both for your company, and your career in an industry where network security requirements changes on a daily basis. Traditional security says that once you've built a fortress, dug a moat and put archers on the fortress walls, that the princess is safe from the savages outside of the fortress. When it comes to IT security, the possibility exists that you may wake up tomorrow, discover that the savages have developed a Star Trek transporter and have simply beamed the beloved princess away, avoiding the moat, archers, and 40 foot walls entirely.

What management almost never needs to know is all of the technical information behind your recommendations. That's why they hire us: to know the technical mumbo-jumbo, be able to do the technical work to maintain corporate assets, and to be able to report in a clear and concise manner what they, as managers, need to know. Of course, there are exceptions to this rule, which can be both beneficial and detrimental to productivity.

Business Need

Just as good IT managers look for sound technical data before making system decisions (i.e. upgrading to a new operating system) a good business manager will look to a sound corporate strategy in making their decisions. For every large business decision made, a good business manager will want to analyze a written business case that clearly states the objective of the project, tactical steps to be taken and budgetary projections. Most importantly, we need to convince them why they should spend money on our security projects. Four security vulnerabilities are widely applicable to most organizations. They are technological defacement, the violation of confidential customer data, malicious code and the loss of proprietary information. As a network security professional working in the interest of the company, it is your job to educate the business manager of these vulnerabilities and show her how her business will be affected by these weaknesses if adequate budgetary allocations are not made proactively.

Defacements or other types of vandalism accounted for 70% of all website security breaches (CSI, p.4). Website defacements can take on a number of different aspects. Most frequently, hackers target random websites simply to leave their mark on them so that they can show off to their friends. Others may delete files or a company's entire website with malicious intent. Perhaps the most damaging attack on a website however, is simply replacing legitimate content with illegitimate content. Take, for example, the case of Adrian Lamo's attack on the Yahoo News website on September 18, 2001 (Poulsen). Lamo, a white-hat hacker, was able to use a proxy server on Yahoo's network to impersonate an internal computer and modify news stories at will. While he chose to modify an old story (about Dmitry Sklyarov) and only to add sarcastic comments about the pending case, it's easy to imagine what could have happened had someone more nefariously minded gained access to modify news stories just one week after September 11th - a time period during which Yahoo News reported it's traffic as being twice that of the entire month of August. The immediate monetary losses of website defacement is most likely low to moderate, depending on the type of damage done, the time elapsed before repairs are completed and, of course, the business model. However, the long-term effect due to the loss of consumer confidence in your company could be devastating if you are in the business of providing information.

When working in the e-business environment, the theft or publication of your customers' personal data however, is probably a far more dangerous threat to your company. According to the CSI (Computer Security Institute) annual report on 2001, 18% of companies that reported website security breaches said those breaches lead to financial fraud or transaction information theft. What your customers see when this occurs is that you are either unwilling or unable to maintain the integrity of your customer database. A classic example of this comes from early 2000 when cduniverse.com and an unknown number of other online vendors were hacked by an individual calling himself Maxis (Carrington). Maxis demanded a ransom, threatening to go public. When cduniverse refused, his version of going public was to begin publishing stolen credit card numbers on the Internet. It's believed that as many as 25,000 credit card numbers were stolen by Maxis. More recently, Adrian Lamo again breached the network of a major news organization, the New York Times (Hulme). This time Lamo was able to gain access to the Social Security numbers and other personal information of 3,000 Times employees as well as those of contributors to the paper including Jimmy Carter, Rush Limbaugh, and Robert Redford. Given that the loss of such data causes both a direct financial loss as well as a loss of consumer confidence, the business losses will be both immediate and long term.

Malicious code is both the most publicly visible network security issue and, in fact, is the primary cause of productivity losses due to security breaches. While the general public knows it simply as computer viruses, malicious code includes viruses, worms, trojans, and a number of other not-so-pleasant pieces of code. Due to the fact that the payload of malicious code can range from changing you screen saver, duplicating itself to other systems, deleting the contents of your hard drive or simply popping up and saying it's there, it's difficult to put a specific cost on a single virus outbreak. However, it's estimated that global economic losses due to malicious code for the year 2000 neared

$17.1 billion (US), and as of September of 2001, the cost for the year 2001 was approaching $12 billion (eFlash). Companies around the world reeled in the wake of viruses such as SirCam, CodeRed, and Nimda. Entire offices (including my own) were shut- down and employees sent home in an attempt to slow the spread of these viruses and allow for repairs to be made. Having seen the damage that viruses can wreak on a company, most managers are now well aware of the economic cost of not implementing an anti-virus system of some kind, making our job of convincing them to fund one much easier.

The theft of proprietary corporate information has quickly risen to the top of the list when it comes to security breaches that result in financial losses. Almost every company has proprietary information, from the corner burger-stand's secret sauce on up to the federal government's secret plans for invading Canada. While it is probably the most difficult to judge accurately the losses due to intellectual property theft, the potential for loss is enormous and, as such, has drawn a great deal of attention. In the CSI survey for 2001, of those companies willing to both admit to having lost proprietary information and to quantify their losses, the average loss was $6.5 million dollars, with the highest single loss being $50 million. The Office of the National Counterintelligence Executive reported in October 2001 that Internet exploits were one of the collection methods being used by foreign governments and companies to conduct espionage on the United States (and US businesses). They estimated lost sales in the year 2000 due to economic espionage as being between $100 and $250 billion dollars (NCIX). My personal opinion when introducing this topic is that for most organizations these numbers are meaningless. After all, most companies don't deal in matters of national security and have foreign nations trying to steal their secrets. Instead, to put things more in perspective, you should explain the situation to management in a manner that better fits your organization. Have them imagine that they now have to do business in an environment where you must share all of your information and plans with the competition. Your new product blueprints, cost cutting plans, whom you've had meetings with, and the minutes of those meetings. What would an environment such as this do to your competitive edge?

Sources of Threat: Our Vulnerabilities

After demonstrating that there is a financial-business need to defend the network from the outside world, you must further determine what protective measures the company can, and should, take. Securing your systems involves two major steps, identifying possible sources of threat, and then identifying possible actionable options that can be taken to mitigate the threat posed.

The first and most obvious security threat to any network that is connected to the Internet is of course the Internet itself. Of respondents to last years CSI/FBI survey, 74% reported some sort of attack stemming from their Internet connection. Due to the size, anonymity and ease of access (both to the network and to hacking tools) the Internet has become the latest battleground for corporate war games.

While use of the Internet as a battleground has steadily been growing, it's slower, more traditional cousin has also seen an increase in [reported] hacking activity. Vulnerability through dial-up access to corporate intranets has been moved to most network managers' back burners during recent years as the number of Internet attacks has skyrocketed. Although the use of modems to hack into networks has been around for years, with more energy being spent putting up high profile defenses, such as firewalls, to protect Internet connections, corporate backdoors have been left open for patient hackers who have not moved on to more glamorous hacking techniques. By using a war dialer, hackers can set their computer to automatically dial thousands of numbers until finding a modem. All too frequently, such modems will be enabled to answer incoming calls, and the computer they are connected to also happens to be connected to, and trusted by, the corporate intranet. This is such a problem and security risk that it is reported that any Sun Microsystems employee that is caught dialing up the Internet on a modem will be fired immediately (Williams).

Local network users may also be a security risk. This risk can be both malicious and benevolent on the part of the employee. The most obvious risk is that of a disgruntled employee intentionally damaging the integrity of your network. The not-so-obvious risk is the employee who is the victim of social engineering. Employees may fall victim to hackers in many different ways, from a "repair man" walking into the office and telling the receptionist he needs access to the server closet, a phone call from Joe in IT needing to have you reset your password, or convincing them to run malicious software due to its cuteness factor.

As previously mentioned, malicious code can be devastating to network security. A few examples include SirCam, which emails random documents (and itself) to contacts in your address list; Nimda, which creates anonymous shares with administrative level access. As described by Nick Del Grosso in his article *It's Time to Rethink your Corporate Malware Strategy*, one of the newer trends in malicious software makes use of ActiveX, Java, JavaScript and browser plug-ins to distribute malicious scripts to unsuspecting Internet users.

Regardless of how many different possible weaknesses we identify on our networks, we must next determine what actions we can take the shore up our defenses because, hopefully, after hearing of all of the things that could go wrong, the question that is now on the tip of your managers tongue is: What can we do to protect our corporate assets? Thankfully, there are many preventative measures we can take, and you can have a great answer for your manager.

- Firewalls are great. They are not however an all-in-one fix. Firewalls are placed between the Internet and your company's internal assets. The hope is that by using rules to filter the traffic that is allowed between the two networks, the odds of malicious traffic from the outside reaching its destination on the inside are greatly diminished.

- In a computing world where there are over 60,000 viruses known to exist, any

company running any computer that is connected to any other computer by any means (including sneaker-net) is running the risk of being infected: having some kind of anti-virus software is a must. A great selling point for an anti-virus solution is centralization. To managers centralization means less time is needed to get things done. To those of us in IT it means not having to run around and touch every computer in the office. Either way the end result is a savings in time and money.

- Although it should not be a high priority, a honeypot can be an excellent tool in network security. While a honeypot is not directly a defensive system, it can be of great benefit. First, a good honeypot will attract a hacker's attention away from your other 'real' systems. A honeypot will also allow for an excellent method of determining what attacks are being performed on your systems, and logging the attack as it is occurring without actually having to use cycles on production servers to log these events. Also, by tweaking the difficulty of your security systems on your honeypot, you can test the vulnerability of security measures that are normally buried several layers deep. For example, by removing a firewall and NAT from the equation, you can see where your mail server's vulnerabilities lie.

- Depending on the nature of your business, the encryption of some or perhaps all of your corporate records is in order. Encryption can take place at many different levels: VPN's, secure LAN's via the use of hardware encryption, encrypted e-mail, or the encryption of single files. Any of these, or some combination thereof, may be called for depending on your individual circumstances.

- User authentication provides for one of the most important elements of any transaction, be it business or computing, which is knowing who the other party involved is. When granting access to computer resources in a business environment this problem is compounded all the further. By using proper user validation, an appropriate level of assuredness can be reached guaranteeing that a user is who they say they are and that no man-in-the-middle attack or other identity theft is occurring.

- Network-based Intrusion Detection Systems (IDS) provide a method for detecting unauthorized or suspicious network traffic on a particular network segment. Network IDS works by putting a network card into promiscuous mode and analyzing the contents of the network traffic for known suspicious patterns.

- Host-based IDS takes a similar approach to monitoring the activity on a single system. Host IDS examine both network and non-network components of the computer, such as modem use, and the replacement or modification of important system files.

- The most important component to any network security solution is not hardware or software based - it's the personnel that are left in charge of managing their operation. In order for any security manager to be effective they must have time to perform routine monitoring and maintenance of the security systems. They must also have enough power in the organization to be able to take action regarding the operation of the network should action become necessary. Additionally, it's important that it's understood from the outset that just as the security software will need upgrades, the security manager will need ongoing training in order to keep up with security issues.

  These important requirements may mean that someone new has to be hired, or existing responsibilities need to be juggled. The first thought management will have about this idea is that it means an increase in fixed costs. Of course, the manager is correct; adding staff always increases fixed costs. However, if you've presented your case well, you could remind your manager that by staffing your security team appropriately, you will save a lot of money in the long run by preventing major security breaches. There will of course be cases in which getting the adequate manpower simply isn't an option for management. In this case, there's unfortunately not a lot you can do. Given that, I would strongly recommend noting the impact not having the proper staff has when writing your recommendations. This is mainly for your personal protection in the future should your network be attacked and you find yourself understaffed. Additionally, it will help you in the future to justify additional expenditures. If you have hard documentation that a technician had to work overtime, that a security breach could have been detected, or that users had a longer wait to be helped, you'll be in a much better place when the staffing budget is again re-evaluated.

Presentation

Ok, so you've read all of this, thought of a list of potential vulnerabilities your company could face and how to demonstrate the need to management when you're ready to present your plans. You've got some recommendations for possible actions to take, so now what do you do? Simple: peer review. Do you have a coworker capable of reviewing your documentation? Ask them to. Have them look for anything you overlooked, misstated, or just plain forgot about. Make sure they know who your target audience is, and ask for any examples or explanations they think might work better. If possible, after your peer review, give yourself a couple of days and then come back to it - you're bound to discover something you missed the first time around.

Managing and presenting the concept of risk management is a rather foreign concept to most IT security staff, and I know certainly was to me. More than likely, the budget you'll be given will require compromising your ideal network security plan in favor of decreasing capitol expenditures. The concept that there is a middle ground between success (avoiding all breaches) and failure (experiencing a significant security

breach) is a rather odd one. Sure, there are varying degrees of a breach: it's not nearly as bad to catch someone stealing the service of a proxy server as it is to find them stealing confidential documents, but is that's not what we're talking about. We're talking about it being ok (at some level) that the security of those documents has been breached. Business managers must deal with similar questions on a far more regular basis and therefore are more comfortable dealing with the compromise required. As an example, The SANS GSEC Book 1.1 presents three different techniques to dealing with a risk as it is presented to you (Northcutt). The risk can simply be accepted as is (no change), mitigated or completely eliminated (install a firewall), or transferred to another (buy an insurance policy). As your manager decides how much budget can be spent on security, your job is to help him understand how much risk he can and wants to afford. When it comes to deciding which of these paths to follow, several key questions must be answered.

- What is "it" that could happen? We looked at this earlier, so this should be a known factor.
- How bad could "it" be? We looked at some of the costs associated with past attacks; it's up to you to do customized research on this to fit the vulnerabilities in your organization.
- How often could "it" happen? This is very important to note, and it's easy to see why. We all lived through Nimda. Once. But could we live through a virus with the voracity of Nimda once a week every week with no protection from "it"?
- How reliable are the answers to the previous questions? Be prepared to supply hard financial data, and then more financial data to senior management. While you shouldn't overload non-tech managers with tech mumbo-jumbo, you should plan on presenting detailed, organized and well researched financial recommendations - the mumbo-jumbo they understand.

When presenting to management and asking for a decision, you must be prepared with this critical information. Don't wait to be asked for this information - be proactive and include the answers in your proposal. If you don't provide the answers, managers will frequently make up the answers in their head, giving you no input or insight into their deliberations.

Even if you've got everything else perfected, you've still got to be able to sell it. So what's the best way to go about it? Again, I'm going to fall back on "it depends on the company." The SANS GSEC Book 1.1 recommends demonstrating to management what the tools you're trying to get them to buy can do (Northcutt). While I certainly have no problem with this approach, and would in fact encourage it in some environments, I believe that a different tactic may be far more beneficial in many cases. Instead of presenting management with demonstrations of the solutions they'll be buying, present them with what the hackers see when attacking your network. For example, if you're trying to sell them on a policy enforcing tough passwords, generate some fake accounts with a variety of passwords and demonstrate in real time how long it takes to crack them using tools such as LC3 (formerly L0phtCrack) from @Stake (www.atstake.com

<http://www.atstake.com>). Trying to get a firewall implemented or upgraded? Put an unprotected machine on the Internet for 24 hours and log how many scans are made. Of course you should always be sure you know what's going to happen when you try something like this - I'm not saying to fix the results, just to run a practice run or two before hand so you know what the results are probably going to be for your presentation.

Other, perhaps more obvious, recommendations include making sure to keep your target audience in mind when deciding what you're going to say. If no one in the group understands techno-babble, you're wasting your breath spewing off endless jargon and your proposal will automatically be tossed out. Instead put your efforts into translating applicable case studies into business language that they will understand. Use specific numbers such as the fact that 90% of those surveyed by CSI reported security breaches, and 80% of them acknowledged financial loss of some kind due to computer security breaches. This sells far better than 'a lot of people got viruses last year.' However, don't give too many statistics. If you do, your audience is simply going to zone out and you'll again be wasting your breath.

Now that you know what the message that that must be conveyed is, the background information that may be requested, and some possible methods for portraying them are, you should think about whom you will actually be trying to convince of this. While it would likely be very easy to sell your plan to your coworkers in the IT department, it would be of very little benefit. Due to the budget vs. security trade-off that must occur in this process, it's very important that the person or group you're asking to make decisions have the organizational power to enforce such decisions. In many companies this means you're going to be selling to the 'C' crowd - the CTO, the CIO, the CFO, and perhaps the CEO.

Once again, I'll fall back on the fact all companies are different, and the command hierarchy is never the same. Thus, part of the research you need to do, and make sure you do correctly, is determining how high up the corporate ladder you need to yell before you reach someone that can provide you with the backing you need.

There is, however, one truth among all organizations. When a network security breach occurs, the first person everyone looks to is the person that implemented (or failed to implement) the network security policy that is in place. What happens after that depends on the implementation. If you implemented a poor plan on your own with no technical or managerial approval, you'll likely be walking the plank all by yourself. If however, you had a well documented, well thought out plan, that was reviewed and approved my your peers, IT management, corporate management and (ideally) the breach that occurred was not something foreseeable, or at least was not something you should have been prepared for, you'll most likely weather the storm alright. Even if the breach that occurred was foreseeable, its preventable solution had been suggested, but turned down by management; you'll again be in a good position. In this case, your course of action will be to move quickly: show senior management why you weren't protected, explain how you'll recover, and after the problem is solved make a new presentation asking to secure the area that was breached.

With luck, this document has given you a few more tools to help in the ongoing battle, which is our existence as IT professionals. By learning more about the decision-making needs of managers we can all help our respective organizations to be more effective. And by being prepared with the appropriate examples, demonstrations, facts and figures regarding the technology in question, you can help guide management to make proper assessments of their corporate risk.

REFERENCES

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 2001. The Office of the National Counterintelligence Executive. 10-Apr-2002. <<http://www.ncix.gov/pubs/reports/fy01.htm>>.

Carrington, Damian "Net thief grabs credit cards." *BBC News Online.* (10-Jan-2000). 11-Apr-2002. <http://news.bbc.co.uk/hi/english/sci/tech/newsid_597000/597828.stm>>.

Computer Security: Issues & Trends. CSI/FBI. (Spring 2002). 8-Apr-2002. <<http://www.gocsi.com/pdfs/fbi/FBI2002.pdf>>.

Del Grosso, Nick. *It's Time to Rethink your Corporate Malware Strategy. 9-Apr-2002*. <<http://rr.sans.org/malicious/corp_malware.php>>.

eFlash. Computer Economics. (4-Oct-2001). 9-Apr-2002. <<http://www.computereconomics.com/cei/01/eflash/100401.html>>.

Hulme, George V. "Hacker Adds *New York Times* To Long List Of Targets." *Information Week*. (27-Feb-2002). 12-Apr-2002. <<http://www.informationweek.com/story/IWK20020227S0003>>.

Northcutt, Stephen, et all. *SANS Security Essentials I: Information Security, The Big Picture. 2002 edition.*

Poulsen, Kevin. "Yahoo! News hacked." Security Focus Online. (18-Sept-2001). 10-Apr-2002. <<http://online.securityfocus.com/news/254>>.

Williams, Jim. "The Downside of Network Security." About.com. 11-Apr-2002. <<http://netsecurity.about.com/library/weekly/aa122999b.htm>>.