Global Information Assurance Certification Paper

Tim Tope
GSEC Practical Assignment (v.1.2e)

Security and the New Millennia

Historically, security has always been considered overhead; a cost center. The security staff was pigeonholed and typecast as throwaways or regarded as a temporary location to place personnel that for one reason or other, the company did not wish to dismiss. Security was primarily concerned and focused on the physical control and accountability of company facilities and assets. You know, the typical issues: access control, authentication of visitors and staff in restricted areas, internal pilferage, and theft. These "old age" security concerns should seem strikingly familiar to what today's information security professional has to deal with: access control, intruders, and authentication. The more things change the more they stay the same.

But things have changed in one fashion for business. We are literally and figuratively in a new era: the reliance of business on the Internet and computing systems to achieve their business objectives. The dawning of this new era came and went sometime before the new millennia, but many have failed to come to terms with the change. How unusual. Inflexibility and resistance to change. So, age-old causes continue to haunt new age times. According to a survey of 1,500 European and US executives released in January 2000 by St Paul, a Minnesota-based global insurer, businesses do not adequately understand the risks posed by technology, are having difficulty identifying these risks and lack the tools to manage them. The Number Two on the SANS Institute's "The 7 Top Management Errors that Lead to Computer Security Vulnerabilities", is clear when it states that "[management] fails to understand the relationship of information security to the business problem – they understand physical security but do not see the consequences of poor information security" (SANS Institute).

So, what's new you might ask. Simply, security management. The responsibility for security must be a professional security staff, not a pigeonholed staff of cast-offs, or IT engineers. The leader of this staff must be as astute at the inner workings of business as that of information security. This individual must be able to co-opt the IT engineering staff, corporate employees and executives, as well as coordinate and manage security issues across corporate boundaries. Today's security environment is no longer limited to securing the warehouse, or just protecting the data, but crosses all lines from the technical physical security systems that protect the physical facility to the IDS, firewalls, and auditing programs that protect the crown jewels of the organization: the network and systems.

These changes have forced today's security staffs to be active on three fronts: information security, physical security, and business acumen. Your security staff may now look more like your IT staff where in the past it looked more like an office full of football players. A quick study of history clearly demonstrates that nothing really has changed for security other than adjusting for the same threat from a different direction. Human nature is human nature. As trails became byways for travel, highwaymen emerged to relieve weary travelers of their worldly possessions. As the banking and merchant industries grew, so did the criminal elements focused on redistributing their wealth. As railroads expanded and commerce and business relied on this

means of transport, the train-robbers specialized in boarding and robbing the iron machines. As the Internet expands and business and commerce come to rely more and more on this new technology for their very life-blood, hackers will be lurking around every corner. Actually – they already are. Highwaymen are thieves, thieves are hackers, and hackers are criminals. Nothing has changed but the method used to relieve the weary traveler of what the criminal wants: anything that they do not already possess.

Okay. Point taken. Crime is around every corner. So, how do you deal with this threat? Sorry, there is no definitive solution or in the security vernacular, there is no silver bullet to security. But, there are countermeasures that can be taken. As Marshall Ferdinand Foch (the commander of French forces during World War I) reported: "Hard pressed on my right. My center is yielding. Impossible to maneuver. Situation excellent. I am attacking." Offensive action is the best defense and this offensive action should initially be focused at your own organization by managing a change in the security culture. This can only be accomplished by a comprehensive approach to the problem. In other words, plan, plan, and plan.

Take your action by first looking at your Risk Management Program and insert yourself squarely in the middle of your organization's Business Continuity Process; a good information security professional must be just as savvy in business as in information or physical security. How can you use this to leverage your plan? It is somewhat of a general idea, but you must find some way to insert security and business continuity is the logical tie in. Next, determine:

- What do you have concerning backups and disaster recovery? Is it accurate and complied with?
- Do you have a basic Auditing Program for all your systems and devices?
- What about a Change Control Program?
- Do you have an Enterprise Service Management solution?
- Are you managing and monitoring your network and systems?

Amazingly, simple network monitoring tools (and many are freeware) are key for indicating what is happening on your systems and network. Today's commercial and freeware security software (read IDS) are nothing more than higher versions of these tools on steroids.

Now the meat and potatoes. The following is a structured, twelve-step approach (yeah, another 12-step!) to securing your information infrastructure. First, go back to your risk management. The trend in the courts is that companies must be accomplishing their "due care" or "best practices" in order to not be held liable for security compromises. Basic stuff. So, what is your current policy? How do you mitigate or transfer your information security threat? Or have you consciously or unconsciously decided to ignore it? If you do any of the aforementioned, you may wish to rethink that outdated decision. Be forward thinking. With that said, the next steps are a piece of cake. This stepped approach allows you to focus your effort by defining and implementing the most important and basic of tasks without having to immediately purchase a proactive IDS and possibly staff a security operations center or outsource for this service.

Step (1) Security Plan. This is the first and most important step to take. The "Plan" must be all encompassing and must involve buy-in from all entities from the user to the top executives. Take a top down approach. Sell the plan to the executives demonstrating the economics of sound security. This is were the business end of security comes into play. It's a tough one, but find an advocate and sell, sell, sell. Once you have executive buy-in that is supporting and pushing from the top down, you are half way home. Just as important as buy-in, is a defense in depth approach to security. Layer your security from the outside, in.

Step (2) Inventory. Basic Asset Management and Inventory Control with a twist. Take a complete inventory of your assets:

- What is on your network?
- What is it doing?
- What is its location?
- How is it configured?

Step (3) Classification. Classify systems by what services they offer into four groups based on the level of security they require: high (highest security specific to your "crown jewels"), medium (for important assets), minimum (for broad based assets such as desktops), and foundation/infrastructure (security is impossible without a clear understanding of your assets and goals). Initially focus on those assets that are the most important.

Step (4) Audit Program. Establish an Audit Program, if you do not already have one. But, take heed! Ensure that this program has teeth. System Administrators must adhere to the program. Security Engineers should not supplant the admins; make the admins part of the security process. Buy-in is the critical piece of the program. Establish a routine where the admins must accomplish set audits of your web servers, DNS, mail, routers, firewalls, and other networked devices (do not forget about the network printers and faxes!).

Step (5) Harden your systems and establish a security baseline. Determine the vulnerabilities to each specific asset, assess the potential impact on your environment, classify the vulnerabilities into fix, no action, or further research, and conduct your "due care/ best practices" of configuration management via an established, formal Change Control process. This step will eliminate over sixty percent of the threat to your company. Simple enough? Good. Once the system has been hardened, document it and establish this as a security baseline.

Step (6) Disaster Recovery. Once your systems have been baselined, make a backup of the configuration and update your DR Plan to reflect your "new" security program.

Step (7) Maintain the security baseline. If you do not maintain the security baseline by periodically assessing your systems for vulnerabilities, your systems and network will soon be as wide-open as when you began. This is a cycle or process; ever evolving, so evolve with it.

Step (8) Automate. Automation, the salve of the new age! Consider implementing a SysLog Server that is the remote repository of all syslog events from your networked systems and devices. It is also possible to have these events filtered through an IDS protected system that uses the IDS sensor to recognize the signature of the event and display an alert on your security-monitoring monitor. Pretty cool. It could limit your cost of ownership to cover all your systems with IDS agents and you can have real syslog monitoring of your network devices without wearing out your System Admins.

Step (9) Intrusion Detection Systems. Consider an Intrusion Detection System (IDS). Once your baseline is complete, or even prior to doing any of the above, consider an intrusion detection system.

Step (10) Training. Security Awareness for users is a start, but comprehensive, more specialized training for your complete IT staff is also what you will need for buy-in. Your IT staff is your frontline of defense. Train them to make up for your lack of security engineers in the importance of their assistance. Security should not be seen as the bad guys that are out to inflict pain and suffering on the IT and corporate masses. A team effort is what is required for a successful security program.

Step (11) Re-assessment. Security is a process. It is not difficult, only evolutionary. Not only should you have a standard practice of auditing your systems and devices, but also you must have a standard that forces you to constantly reevaluate and update your security plan/program. Technology changes rapidly, business objectives evolve and new ones rise from seemly nowhere. Staying current on the ever-changing security issues should be only half your focus, keeping abreast of the organization's mission and goals is the other half.

Step (12) Policy and Procedures. Documentation is the bane of all, but it is an absolute necessity. The newly adopted *ISO 17799-Code of Practice for Information Security Management* is disliked by some, and wholly welcomed by others. Use it to outline your plan, document what policies and procedures to promulgate to support your activities, and ensure best practices. Make your processes and procedures user friendly. Develop checklists that require your System Admins to simply fill in the blanks and check the necessary blocks. Modify and bring in your Change Control process into security; this is your checks and balances process, so use it as check.

An Intrusion Detection System can do pieces of what was outlined in the steps above, but do you want to rely on complete automation? I hope not. A combination of good systems administration and IDS assessment tools will be your keys to success as far as reacting to security events. Hand and hand with the IDS is real time monitoring of the system itself in order to be proactive to attacks and intrusions. Of course, it depends on your environment and business goals as to whether or not you need a complete system or should outsource the monitoring piece to facilitate a 24/7 response. As mentioned above, monitoring and management tools will also provide your company with what is necessary to manage your network and systems. Don't just buy the systems and applications and believe that you are finished! Would you be concerned if you found out that the pilot flying the plane in which you are sitting so comfortably in first-class, did not have the instrumentation and systems to provide the information required to safely pilot the aircraft? Then why is your business any different? Use all resources available and integrate your security plan to reflect this all-encompassing approach. Large amounts of money do not necessarily need to be justified, budgeted, allocated, and then expended to secure your organization. Assess what you already have in place, improve your processes and administration, identify your deficiencies and vulnerabilities and then improvise, overcome and adapt!

By far there is one thing that has not changed in regard to security in the new millennia, and that is the resistance of management to deal with security change until something happens that instigates their sudden concern. In the past it was…"we have been robbed!" Or "what happened to that widget?" In the new millennia, that has normally become…"we've been hacked!" Security must be involved in all aspects of today's business world and the proper management of the security effort is the only true answer that will ensure that this happens. The focus should be security driving, or at the very least, security being intimately involved with business/IT operations, not the other way around. Security must be given more visibility and brought in at the beginning, not at the end as an after thought. Any business venture or activity is analyzed for financial risk, why is security not generally involved? That is because security has always been considered overhead. Today's businesses cannot afford to continue seeing security in an old age light. Get with the times; organizations must secure themselves before they are shown their insecurities.

References

(1) The St Paul Companies, Inc. "Cyberrisk Survey." January 2000. URL: http://www.stpaul.com/www-cyberrisk-survey/content/index.htm.

(2) SANS Institute. "The 7 Top Management Errors that Lead to Computer Security Vulnerabilities." URL: http://www.sans.org/newlook/resources/errors.htm.

(3) Vijayan, Jaikumar. "IT security destined for the Courtroom." Computerworld. 21 May 2001. URL: http://www.idg.net/crd_idgsearch_2.html?url=http://www.computerworld.com/cwi/story/0,1199,nav47_sto60729,00.html.html

(4) ISO/IEC 17799:2000 – Information Technology -- Code of Practice for Information Security Management. International Organization for Standardization, 2000.

(5) Information Security Magazine. "Security Focused." September 2000. URL: http://www.infosecuritymag.com/sep2000/Survey1_9.00.pdf.

(6) Forrester Research, Inc. "Economics Of Security.' Volume Twelve, Number Three, February 1998 (no longer archived at www.forrester.com).

(7) Wood, Charles Cresson. Information Security Policies Made Easy Version 7. Baseline Software, Inc., 2000.

(8) CERT Coordination Center. "CERT System and Network Security Practices: June 6, 2001." URL: http://www.cert.org/archive/pdf/NCISSE_practices.pdf.