Global Information Assurance Certification Paper

A Management Perspective: The Enabler:

Name: Trudy Morse
Date: 11/24/03
Certification: GSEC
Version 1.4b

Table of Contents

Introduction

The current economy dictates that many organizations must run lean and mean to survive. Within an organization many entities continue to compete for funding, and the competition is fierce. The Information Technology security director or manager of today is no exception in the competitive game and must catch the ear of executive management to successfully obtain adequate funding. This means the manager must have a keen awareness of executive management business objectives, triggers, and priorities; a keen perception of the business needs; and the ability to speak in "business-eez". In fact, analysis of business requirements is the foundation for providing successful security solutions. Finally, the security manager must search for ways to accomplish security objectives without adequate funding, as it is very likely security will continue to operate within a limited budget. The budget could result in an increase that does not allow all security concerns to be addressed adequately, could include no increase, or it could include a reduction in spending.

From another perspective, the successful security manager must also have a basic awareness or understanding of the key components of security that are critical to effectively managing the ongoing security requirements of the organization. The old adage, "The more things change, the more they remain the same." points to some basic principles on which the organization must focus, and on which Information Technology must refocus. This focus will allow security to be effective and takes its place as "The Enabler" allowing organizations and businesses to successfully compete, produce competitive products, and provide valued services in a safe environment.

Management Perspective

The Computer security director or manager must develop awareness of effective ways to communicate with execute management, in particular the CIO. At the recent Security Decisions Conference in Chicago, October 15-17, Thornton May, as Sheriff of the CIO Posse, presented four key subjects, or triggers, to consider in communicating with CIOs:

- Time versus work to be done
- Money - how smart you spend
- How long should it take to do things? Should things stay the same?
- Stakeholder Analysis - understanding and managing the political situation

Security has recently caught the attention of executive management and the public with strong focus on terrorist activities, illegal activities, loss of life, loss of reputation, loss of trust, downturn of the economy with loss of business and loss of jobs, loss of tax monies, increase in government debt, and rising insurance rates. At the recent Security Decisions Conference, Michael Rasmussen, Director of Forrester Research, presented three major events that have caused significant change to Information Security:

- Code Red Nimda Attacks
- September 11
- Oversight - Legal Liability, i.e., Enron, WorldCom, Global Crossing, K-Mart

Thornton May indicated that although 91 percent of executives who were asked if they should play a more active role in shaping and deploying information security programs responded with a yes. Yet, three months later 94 percent of these same executives, when asked if their behavior or involvement had changed, responded with a no (38).

What triggers catch the ear of the CIO? Return-on-Investment (ROI), Total Cost of Ownership (TCO), Risk, Value, Benefit, Compliance. Rasmussen recommends that emphasis from the security manager should be placed on customer value: Rasmussen emphasizes focus should be on seeking the benefit, not security. He states, "Security is about what you get by using it, not what you lose without it" (52). Understanding how the security effort improves efficiency and effectiveness are key:

- Revitalized sales
- Relevant value propositions
- Successful business justifications
- A safer and more productive company (52).

Security managers must consider ROI as an important method to obtain funds. Yet this is not an easy task in many instances. Caution in analyzing costs and benefits is a wise consideration. Take, for example, an ROI for Centralized Management and Single Signon. The cost of the new software may be high and the criteria for getting there even higher if the existing software with which the new software is interfacing is not at the appropriate levels. The criteria for implementation must be carefully investigated, i.e., the potential roadblocks must be identified and thoroughly analyzed to avoid bad surprises. Additionally, the benefits may not be quite as they appear from the vendor marketing staff presentation.

For example, Single Signon may provide benefits in access administration in terms of time, effort, and cost by eliminating many ids and passwords and allowing easier access, but how many customers or employees will actually benefit from it? Perhaps many or perhaps only a small portion of the customers or users use more than one or two access IDs. Required software interfaces to various operating system platforms and applications existing in the environment may or may not be available or working. The costs associated with benefits, on the other hand, may be high. Another business consideration is how long it will take to implement. The bottom line is to identify *all* the costs related to full implementation against costs of keeping the current process and ensure that all the benefits are *real*.

Some ROI endeavors are relatively easy to document. Yet others are much more difficult and rely on other functions within the organization such as asset management. TCO implies that the organization is keeping accurate inventory. Without effective change control procedures, this may be a false presumption. Then, what about the intangible assets and their value? The road to communication with the CIO may be a challenge. Yet, to be effective, security directors and managers must establish ongoing communication paths and be aware of what the CIO is looking for. The Information Technology security manager must have a business sense and awareness that allows justification of the business benefits that security can bring to the table.

Another trigger is risk. A vulnerability assessment is a must. However, it doesn't stop there. With limited budgets, risk analysis is a critical component of the security endeavor. For those who say that before the vulnerability assessment they need to start on those vulnerabilities they are aware of, and address tasks they know they must; the potential dilemma is that the limited dollars available are applied to the low risks rather than the more critical ones. Lipson and Fisher report that survivability is an emerging discipline in security with focus related to availability of information and continuity of services (1). This objective justifies the strong requirement for a risk management approach. The risks, once known, must be accepted, mitigated, or insured.

Lean and Mean

Many organizations and businesses have budget limits that do not allow security to address all security requirements. Many governments are finding themselves in debt and are cutting budgets. The economy has taken a downturn, affecting businesses and employment. A business understanding of the CIO's focus, previously presented, is important, as well as an understanding of the stakeholders. Competing for budget dollars by focusing on what security can enable in terms of business benefits is a wise strategy.

The Security Manager must work smarter, not harder. Working-smarter is imperative in accomplishing security objectives when funding is not adequate. One possible solution to accomplish security objectives is to use freeware. Free software tools are available and can often be downloaded from the Internet (with caution). Although the use of these products may not be entirely satisfactory, these products can provide some security benefits worth considering. Another working-smarter endeavor is to utilize vendor marketing staff to accomplish ROI justification, followed up with appropriate internal analysis of the information. Still another working-smarter alternative is to invite vendor in for presentations to gain insight into what is being offered and what security gaps can be decreased or eliminated.

If an outside vulnerability assessment is temporarily on hold, an alternative, as a start, is to use Best Practices documented by highly reputable organizations. See References section for some of these Internet sites: Morenet, NASA, P-Synch, Cisco, Avolio, Sans Top20. A recommended start is to develop an internal assessment list and hold an internal review referencing Best Practices for guidelines. Of course, when possible, an outside assessment and risk analysis is very valuable in prioritizing where limited budget dollars should go. Purchase of a few good guides is relatively inexpensive, and some can be found free on the Internet. One book for purchase that has excellent guidelines, including incident response, is: The Cert Guide to System and Network Security Practices by Julia Allen. Alerts for software vulnerabilities and viruses and worms are easily found by visiting vendor websites such as NAI, Symantec, and TrendMicro; and the websites of highly reputable security organizations such as CERT and Sans provide valuable alert information. Many of the vendors and organizations provide free email alert notification. There are many vendor sites that provide white papers for free. In fact, the wide wealth of information on the Internet precludes any attempt to fairly cover them all.

The Enabler

Traditionally the role of Information Security has been as "The Enforcer". Other names come to mind such as protector, disabler, impeder: all with a negative connotation to those who are trying to get work done. Security has been seen as competing with business "customer friendly" or "ease of use" operations. There is

a perceived pendulum with security on the one end and user-friendly operations and productivity on the other. Norton and Stockman point out that:

> There's an inverse relationship between "secure" and "convenient". Absolute security means an absolute pain for users and complete ease of use for your users means tossing security out the window (10).

In fact, an interesting paradox occurs because on the one extreme, the security end of the pendulum, the more secure the password rules are, the more subject they are to security breach. This paradox exists because the more difficult a password is to remember, the more likely it is that the user will write it down somewhere. Firewalls face the same challenge. The choice falls to the organization or business as to where they will place the pendulum.

As technology changes occur, new ways of doing business evolve. Security has now taken on a different look due to two major changes: the development of the Internet and the fast developing wireless and mobility market. The advent of the Internet has opened the door to electronic business and has changed business in some very significant ways. Networks that were once privately managed with costly leased lines and limited connectivity have given way to Internet connectivity, opening the door to electronic business and customer access with less costly connections. Those businesses that want the competitive advantage have embraced ebusiness. The electronic economy also includes egovernment and ecommunities. Therefore, security, keeping in tune with the changing business environment, has taken on a new look as "The Enabler". Robinson indicates that security, taking on the role of enabler, is now embracing business objectives based on trusted relationships. These trusted relationships evolve to facilitate the business need and involve partners, suppliers, employees, and customers (3). Trusted relationships continue to be based on roles and allow, enable, business processes.

Robinson states:

> esecurity should be viewed as enabling business to grow and as a catalyst to increase revenue; it is about living in an era of accessibility, trusted relationships, open communication, certified information, and proactive systems (3).

While security is now an enabler of the connectivity realized through the Internet, this technology change has resulted in significant increased risks to any organization or business using the Internet. To enable business processes, security has developed to a new status of "letting the 'good guys' in" (Robinson, 2). To state this another way, security must let *only* the "good guys" in. The Internet has significantly increased the complexities of security, B2C and B2B, and the resulting efforts required to allow, enable, business advantage.

The second major change currently underway is the explosion of wireless connectivity and mobile devices with continuously developing, enhanced technical capabilities. John Pescatore reported in 2001 that a Gartner survey predicted that 50 percent of enterprises plan to procure or deploy wireless LANs based on 802.11 standards. Since then predictions for use of wireless have increased dramatically. Wireless expands ebusiness by allowing easy connectivity to anywhere, from anywhere, by anyone, anytime. The new devices being introduced are again opening the door for more effective ways of doing business, cutting costs and time, and improving work efforts by allowing connectivity to resources from anywhere at any time. Security must keep in tune with the evolving business environment that is using wireless as a competitive advantage.

The Security Manager must understand the benefits of wireless from a business perspective and the challenges. The CIO's Guide to Wireless lists five business benefits and five challenges (4).
Benefits are:

- Increased sales
- Decreased costs
- Improved customer service
- Competitive advantage
- Rapid ROI

Challenges are:

- Coverage
- Reliability
- Standards
- Speed
- Costs

The Security Manager must weigh the pros and cons of a wireless versus a wired solution. There are many issues regarding security effectiveness for wireless and awareness of these issues is critical. The Security Manager must be involved in the architectural design for wireless. The Security Manager must understand the potential risks and address them. The manager must also be sensitive to customer or user ease-of-use business objectives. For example, if the manager promotes a solution that forces the user to reauthenticate when moving from one access point to the next, the ease-of-use benefit will not be realized. Security must understand the ability for attackers to use rogue access points, and that broadcasting from an Access Point can reveal the SSID. Security must understand the difference between infrared and radio frequency in terms of solutions to fit the business need and the security issues involved. Security must understand the standards for wireless and the various pros and cons of 802.11x. Security must understand the weaknesses of WEP and the pros and cons of alternatives such as TKIP/WPA or AES. Where can Virtual Private Lans (VPNs) be effective? What advantages does VOIP offer to business? How does security

effectively handle two different technologies that have merged? What will be the impact of the recent legislative change to allow cellular phones to use your wired phone number? When privacy of data is an issue, which encryption solutions work best? Security plays an important part in enabling the business advantage.

Mobile computing is also evolving fast from laptops and cellular phones to enhanced technology changes in devices such as smart phones, PDAs, Pocket PC phones, tablets, and continuously developing new mobile devices. These new technology advances place security once again in a position of enabler but challenge security to effectively enable the trusted parties only. Is the data secure? What happens if the device is lost? Is information backed up? Enablement of wireless results in a business advantage that opens the door for increasing security risks and at the same time places security in a powerful position for requesting funds to meet the business advantage.

Security Management Model

The Security Manager must focus on providing the following well-known security requirements:

- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Privacy
- Authentication
- Authorization

To provide a layered defense, or "Defense in Depth", the security manager, at a minimum, must focus on the following current security elements that comprise operating system or platform management, network management, and applications.

- Business Objectives and Requirements
- Vulnerability Assessment
- Risk Analysis
- Documented Policies and Procedures
- Standards
- Physical Security
- Change Management
- Asset Management
- Disaster Recovery or Business Continuity Plan
- Sound Network Design: DMZs, placement of firewalls, routers, switches, bridges, web servers, email server, proxy servers, application servers, etc.
- Sound Configuration Management
- Authentication Management - 2-3 factor identification
- Authorization Access – principle of least privilege
- RFxs, and Contract Management

- Firewalls
- Anti-virus Management
- Wired Lan-Wan, Wireless, and Mobile Security
- Virtual Private Networks
- Confidentiality: Encryption, Certificate Management and PKI
- Legal Compliance
- Continuous Monitoring, Assessment, Response, Improvement
- Network Management; Network Control - centralized
- Hardware and software support
- Patch Management
- Lock-down of Network Components
- Alert Notification
- Incident Response
- Intrusion Detection and Intrusion Prevention
- Sound Project Management – includes security
- Auditing

Although this model will not be explored, focus will concentrate on some key components of this model. Some of the components have traditionally been a basic part of security such as physical security, disaster recovery, business continuity, change management and change control, asset management, policies and procedures, and audits. Some have developed or become stronger issues as a result of the Internet and the increase of risks such as firewalls, VPNS, anti-virus protection, intrusion detection and intrusion prevention, vulnerability assessment, risk analysis, software support, patch management, sound network design, configuration management, alert notification, incident response, and encryption

Back to Information Technology Basics – but Include Security!

The Software Development Life-Cycle (sound project management) is an important part of the security environment and, in particular, the software vendor's environment. Vendors seem to be remiss in improving on software development as evidenced by the massive volume of security code vulnerabilities. While there will always be human error, vendors' strategies are not working well. Microsoft is a prime example of failure to follow sound development methodologies. Although recently at the Security Decisions Conference; Scott Charney, Microsoft Chief Security Strategist, proudly spent a great deal of time presenting the improved Microsoft patch methodology and technician-friendly processes, he fails to understand that customers are tired of patching and unable to keep up. The time, effort, and cost dictate that Microsoft has expended tremendous effort on the symptoms but not the root cause of the problem.

To claim that Microsoft is guilty in general of poor security design would not be fair. In fact, on the pendulum of security versus software user friendliness, vendor security has changed from off to on-by-default (the pendulum has moved), and installation lock-down procedures are provided to the customer. New security designs with new options have been developed. There is a serious effort to improve server and workstation security. Yet, in the arena of software development, security guidelines are seriously missing evidenced by the high volume of patches.

Security requirements definition should be a key requirement in any project for software development or changes to the current software, whether they are enhancements or corrections. Where are the security guidelines for code developers? While Microsoft is addressing some aspects of security such as default security on its servers and workstations and new security options, it fails to address a key problem for customers: security guidelines/requirements in the development of software. This is evidenced by the large volume of repeating problems with Microsoft code vulnerabilities. Scott Berinato's name for it is "Franken Patch". He aptly states the customer issue when he says:

> The more you patch, the more you need to patch, and the more monstrously kludgy and terrifyingly unpredictable your systems and applications become. Is there any way to escape this horror (100)?

How many buffer overrun or overflow alerts requiring patches does the customer have to endure along with internet attackers with their viruses or worms before Microsoft will go back to basics: Where are the security requirements definitions for code, code reviews, testing requirements? How difficult is it to set security guidelines that must be met? A 'move truncate' would not allow any overruns. Edit checks on lengths of source and receiving areas could be considered. Object oriented code with parameter passing could address this. There are many ways to address the resolution of this problem by setting some guidelines and standards for Microsoft code at the developers level at the requirements definition stage and design of any software life-cycle.

Taking this a step further, organizations and businesses that buy software packages for applications or develop their own code must include security in the requirements definition stage. For example, it is unacceptable for software such as Peoplesoft to fail to meet basic security standards such as providing for a password expiration date, then allowing the user to key in the same password.

The development cycle presents some basic concepts and knowledge that should not be lost in Information Technology security. Requirements definition and design are key initial tasks that, if done well, reduce cost, time, and effort for any project or software life-cycle. This means that all projects should include in the initial stage security requirements definition. Too often security is an afterthought or is ignored until production turnover. There is no time to address it

at the end of a project and it is inadequate if not planned for in the requirements definition and design phases. Any requirement that is not addressed upfront at the beginning of a project cannot be implemented at the end without additional cost, time, and effort. If security is not part of requirements and design, it can be a costly adventure at the end, if it is addressed at all.

Security requirements and design are very important factors in implementing network security. Again, if not considered in the initial phases of requirements and design, the resulting network can be unacceptable from a security perspective. Additionally, it is very difficult and may be impossible to address it at the end of a project.

From another perspective the Carnegie Mellon Capability Maturity Model (CMM) for Software Engineering is a recommended security management methodology. It defines where an organization is in the software engineering process. There are five levels of process maturity. This process model can be used not only to develop software, but it offers relevant methodologies to developing a mature organization and a mature security organization that can effectively address security. The CMM model consists of five stages (Capers Jones, 26)

- Initial: ad hoc, occasionally chaotic, few defined processes, depends on individual effort
- Repeatable: disciplined process; basic project management processes are established to track cost, schedule, and functionality
- Defined Software process for both management and engineering activities is documented, standardized, and integrated into a standard process for the organization
- Managed Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and measured
- Optimizing. Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies

These processes can be applied to the management of security. Are policies and procedures defined? Are they working? Is there compliance? How does anyone know? Are the processes defined, documented, and measured? What audits are defined, documented, and executed? Are vulnerability assessments being performed? What risk analysis has been or is being performed? How often? Are incident response teams and plans defined and documented? Is there an alert procedure defined, documented, and being executed? Is there configuration management? Is the network design reviewed for security periodically? Are there any intrusion detection or prevention software and procedures in place? Are they documented? Are there any security reports? What responsibilities are documented for security staff? What measurements are occurring? What efforts

are being assessed for optimizations? Are all required policies identified, published, and communicated?

Another important process that cannot be overlooked in the Information Technology department addresses Requests for Proposals and Contracts. They both must include security as a basic requirement and provide for meeting security standards. Failure to do this can result in the inability of businesses and organizations to meet security requirements and results in vulnerabilities that cannot be addressed. There is no legal way to enforce security requirements with an organization or individual under contract unless security requirements and standards are accounted for in the contract.

Compliance with new legislation at the federal, state, and local level are very important to avoid large penalties and lawsuits. Executive management is very sensitive to these issues and security must be continually diligent in addressing them and taking appropriate action. HIPAA penalties can be very high. News media can be very damaging and loss of reputation and trust can destroy a business.

Conclusion

Security is an ongoing endeavor that is continuously affected by changing technologies and the resulting business requirements to achieve the competitive edge or to provide the services the public demands. Recent tragic events and serious Internet security attacks have increased the visibility of security.

To be successful, the security director or manager must have two basic talents. One is the ability to understand the business requirements and be politically adept, assessing the stakeholders. The ability to communicate with the CIO in terms of ROI, TCO, risk, value, benefit, and compliance are strong potential success factors for the manager and open the door to successful competition for budget dollars.

On the other hand, a factor equally important for the security manager's success is a basic understanding of the key components of security critical to effectively managing ongoing security requirements of the organization. Although a component model has been presented, focus has been placed on specific components that deserve emphasis. Security must be a basic component of organizational processes such as projects and software development at the beginning stages. Carnegie Mellon's CMM points to defined and repeatable processes that are measured for optimization. Continuous assessment, measurement, and improvement are key factors in determining success. Contracts must include security requirements. The security manager must continuously address legislation such as HIPAA or Sarbanes-Oxley and be aware of consequences for non-compliance. Finally, security managers must

have a basic technical understanding of the security environment including technological changes and their impact on the business and security.

In summary, security management must be politically adept and able to communicate with the CIO and other top-level executives to enable business objectives. Security management must also be fully aware of the key components of security that are critical for survival of the organization or business. Finally, security's role has changed from the negative perception of being "The Enforcer". Security must promote its role of enabling new ways of doing business that provide the business advantage. Meet "The Enabler".

References

Allen, Julia. The CERT Guide to System and Network Security Practices. Addison-Wesley. 2001.

Avolio, Frederick A. "Best Practices in Network Security." 2000. URL: http://www.networkcomputing.com/1105/1105f2.html/

Berinato, Scott. "Franken Patch." CIO Magazine (2003): 100-110.

Cisco. "Network Security Policy: Best Practices White Paper." 2003. URL: http://www.cisco.com/warp/public/126/secpol.html

Jones, Capers. Assessment and Control of Software Risks**.** Englewood Cliffs: PTR Prentice Hall: 1994. 23-25.

Lipson, Howard and David A. Fisher. "Survivability – A New Technical Business Perspective on Security." URL: http://www.cert.org/archive/pdf/busperspec.pdf

MOREnet Missouri Research and Education Network: "Internet Security Best Practices." 2001. URL: http://www.more.net/security/best/index.html/

MOREnet: "Internet Engineering Task Force (IETF) Documents." URL: http://www.more.net/security/best/other.html

Olsen, Dave. "NASA World Wide Web Best Practices." 2.0 URL: http://nasa-wbp.larc.nasa.gov/toc.html

Pescatore, John. "Security on the Run." 2001. URL: http://www3.gartner.com/DisplayDocument?id=338818&acsFlg=accessBought

Peteanu, Razvan. "Best Practices for Secure Development." 2001. URL: http://members.rogers.com/razvan.peteanu

P-Synch. “Password Management Best Practices.” 2001. URL: http://www.psynch.com/docs/best_practices.html

Norton, Peter; and Mike Stockman. Network Security Fundamentals. Indianapolis. SAMS. 1999.

Robinson, Richard. “Managing Secure eBusiness; an IDC White Paper sponsored by Novell”. 2000. URL: http://www.novell.com/news/press/net_security_whitepaper.pdf

Synchrologic. “The CIO’s Guide to Wireless.” 2003. URL: http://www.synchrologic.com/images/whitepapers/cio_wireless_main.html

Sans. The Twenty Most Critical Internet Security Vulnerabilities (Updated) – The Experts Consensus. 4. 2003 URL: http://www.sans.org/top20/

TechTarget. Conference Proceedings and Program Guide. Information Security Magazine’s Security Decisions Conference. 2003.