Security Awareness Starts in IT

Written by:

William Farrar

(GSEC Certification Practical)

Version 1.2e

Introduction

This practical defines the current state of business operations, security design function, introduction policy development, security awareness, and communicates our new found knowledge to the IT security design team. This practical was selected due to two significant driving factors, . 1) In the LevelOne SANS Security Essentials text, Stephen Northcutt states, "I have never ceased to be amazed by the fact that you can't take a class in information security without being told to do this or the other thing in accordance with 'your security policy'. But nobody ever explains what policy is or how to write or evaluate it". As an industry, we still are not in agreement with what effective security policy is all about. 2) Even worse, "How to communicate it?" Those of us who are responsible for delivering the security message are ill prepared. This practical "**Security Awareness Starts Within IT**" is one individuals attempt to provide some insight into the initial steps of delivering the security awareness message to the business, starting with the IT security design function. The practical is built upon the author's own research, career experiences and classroom instruction. Security awareness communications start at home, **"IT to IT"**. Before we deliver the "security message" to our business users, we must ensure that security management, security administration and security design teams are totally aligned with our overall security policy strategy. We must understand our working frameworks, roles we fulfill, what "IT security policy" is all about and its impact on the organization.

Practical Objective

This practical is written to provide an overall "how to" perspective of introducing concepts of good security policy and its potential impact on security design . We have to continually remind ourselves that the security design group is highly technical, and in the midst's of day to day implementations and deployment of new security informational assets. They might be reluctant to listen to, "How security policy is going to make their lives better?" Remember that we in security management are the 'new guys' on the street. Those of us in security management must work towards partnering with of our major policy and procedural stakeholders, the IT security design and administration teams.

It is not the intent of this practical to provide detailed information on the subject of security policy management or development, rather, it introduces various security management concepts and provides content and templates into delivering the security message to the IT security design group. This practical will take a brief look at the current state of affairs, a virtual security management team, security management process, security operating principles, security design framework, security policy framework, aligning with your IT security architecture group and delivering the "security management message".

Current State of affairs

"Business Operations"

The “brick and mortar” walls of our companies have disappeared. The competitive advantage forces us to open our networks for e-commerce opportunities, leading us into the future in an open network infrastructure. Trading partners are knocking at our doors, while we are knocking on our trading partners doors to develop ways to increase profit, while providing 24 * 7 operations to/from the outside world in B2B, B2C and P2P applications. Our companies have now become virtual entities that are constructed by the onslaught of developing technologies. These technologies have the potential to introduce new vulnerabilities that we in the security field have to contend with. The market place is driving and dragging IT groups into a futuristic world where there are no physical walls to the organization. In this new e-world order, the expectation from the business is that we continue to perform at the highest levels. Applications solutions will still need to provide high levels of system availability, confidentiality and integrity.

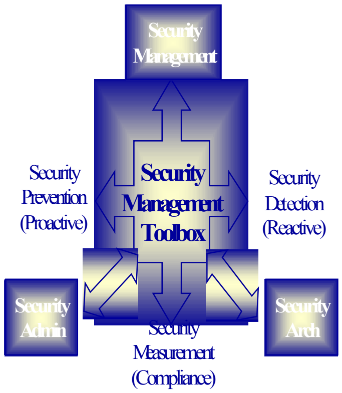
"Security Design Function"

The business units that the security design function supports have an unending appetite for more and more technology to enable an ever-growing list of business objectives. New Acquisitions, spin-offs, major ERP implementations, storage area networks, private exchanges, to mention a few. New technologies like Windows 2000 servers and clients, wireless communications, and NT server farms the size of a major airport continue to find there home within our IT environments. After a period of discovery we find many procedures written and mostly unwritten are not being guided by corporate security policies. The objective should provide for the consistent implementation of security physical assets across the enterprise.

"Security Management Group"

Yes! We can help once we have been empowered by a published “Enterprise Security Charter Policy”. We can help by developing and communicating an effective security management framework and policies driven by best practices, standards (ISO/IEC 17779), industry guiding principles, and the subsequent development and communications of security policies across the organization. The security management group must be chartered from the highest levels of the organization-Executive Senior Management. Our primary responsibility is to align us with the goals and objectives of the organization and its culture, and through a security process develop, deploy, and measure our compliance to published security policies. We must ensure that the policies that we develop are in balance with our businesses tolerance levels of risks against the vulnerabilities and threats that are internal and external to our organization. We must clearly understand what we are trying to protect, its value to the organization, and the impact if a specific informational asset is compromised. Finally, our policies must be measurable. We must be able to determine compliance through effective procedures. Without effective written procedures there are no metrics to measure compliance. Without a valid test of compliance, we have “*NO enforceable policy”!*

Information Security Management


Security Management
Security Prevention (Proactive)
Security Management Toolbox
Security Detection (Reactive)
Security Admin
Security Measurement (Compliance)
Security Arch

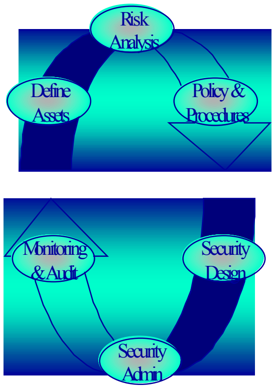
The figure on the left, developed by the author, depicts the virtual information security management organization. In some companies, this might be a centralized function, and in other companies these teams might be decentralized. There are two points to take note regardless of specific organization structures.

1) The Security management toolbox focuses on detection and prevention, and ensuring compliance to security policy.
2) The three security functions: management, design, and administration, have to work to understand each others respective roles, and how the team working collaboratively can defend attacks against our businesses.

Security policy management is a successor event to asset and risk analysis (see figure below). Policy drives security design, and security administration follows to ensure compliance through the development of effective procedures. All three elements must be present to create effective security defenses.

Security Management Process

Depending on our specific organization, we find ourselves focused on the different elements of the security management process. The MIS Training Institute provides the insight behind the graphic to the below. Security management starts with defining our information assets, concludes with monitoring and audit, and then recycles as a continuous process. Old assets are retired, and new assets are continuously being deployed**.**



***Define Assets*-**is the process of defining “what” within the organization that we are trying to protect. If it is information, what is the sensitivity level? Is it public, internal use, confidential, privilege?

***Risk Analysis*-**is the process of determining the value of the assets and what is the business impact of potential loss, manipulation or compromise. This is a process of identifying potential vulnerabilities and determining if specific threats exist that can exploit these vulnerabilities

***Policy and Procedures*-**Policies define the “What” in our business and have to be controlled, whereas the procedures define the “How to”. Policies define the expected behavior, roles of policy stakeholders, business culture and objectives. Procedures provide the steps of implementation to ensure consistent application across the enterprise. Procedures become the auditable metric that ensures our day to day business practices is in compliance with our policies.

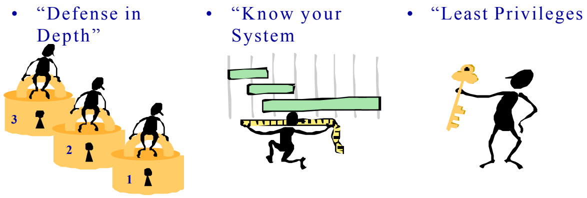
Security Design-is responsible for the design of our security design infrastructure, guided by specific published security policies. The security design infrastructure includes such items as the perimeter design, with appropriate firewalls, IDS monitoring, proxy server design, encryption**.**

***Security Administration*-**administers various security policies in the area of access control, and security configuration policies for hardware components.

*Audit and Monitoring****-is the process that ensure compliance to security policy and early detection of***

unwanted network guests, and the day to day monitoring of network events looking for anomalies in the system logs. Assuming, as mentioned below, "know your system".

Operating Principles



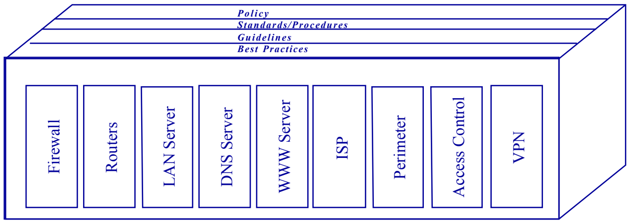
- "Defense in Depth"
- "Know your System
- "Least Privileges

Operating principles provide general guidance to our security strategies.

***Defense in Depth*-**becomes our defense- counter measures. Two walls are better than one. Two walls of different material are even better. Multiple layered firewall strategies with differing vendors, the counter measures should be a mix of prevention and detection mechanisms.

***Know your system*-**It is not enough to receive an alert when something breaks in our defense systems. If attackers are successful, we will never be able to answer the question, "Have you ever been attacked?" We must have a strategy to baseline our system as to what is normal. We have to be able to identify anomalies when they occur so that we can quickly identify and correct them. Anomalies will place us on the alert in becoming more suspicious of incoming and potential outgoing messages.

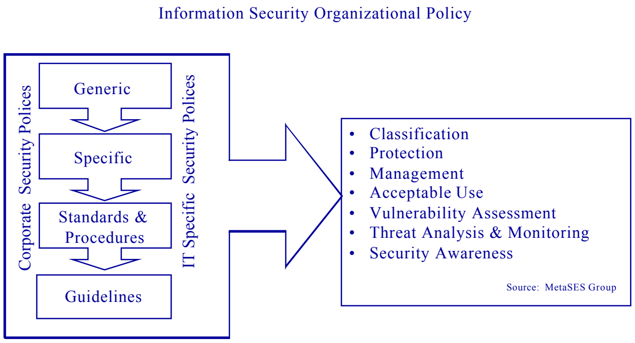
Least Privileges-This principle protects from two 1) vulnerabilities; our software/hardware vendors and 2) individual employee roles that are found in our organizations. Although software/hardware vendors are getting better, we find default settings that provide numerous vulnerabilities beyond the shrinkwrap of the products. Security holes are left wide open. It would be much easier if the products were released with "no security privileges". Privileges would be added only on an as needed basis. Another issue that is commonly found is authorization privileges to employees. How often do we see an authorization form state, "set Joe Smith up as Mary Jones". Joe is an associate and Mary is a senior associate. Or, Joe gets transferred to a new position, receives his new authorizations, however his old privileges are not terminated.



Security Design Framework

To effectively communicate with the security design team, we in security management have to obtain knowledge as it relates to our respective company's security infrastructure components. To obtain creditability within our IT ogranization, we have to complete our "due diligence" and create a security design framework to communicate to our other IT associates.

Policy Framework



Source: MetaSES Group

The figure on the left was constructed based on the readings found in "The Handbook of Information Security Management" and a White paper that was published by the METASeS Services Group**.** LevelOne SANS Essentials, Part 1 also provides the following definitions.

1) "(General) Corporate Policy: the highest level (perhaps national); consists of high level documents that provide direction to what has or thrust to be implemented at lower levels in the enterprise".

2) (General) Division-wide Policy: typically consists of an amplification of enterprise-wide policy as well as implementation guidance.

3) (Specific) Local Policy: contain information specific to the local organization or corporate element.

4) (Specific) Issue-Specific Policy: policy related to specific issues, e.g. firewall or anti-virus policy.

5) Security Procedures and Checklist: local Standard Operating Procedures (SOP's); derived from security policy.

6. Michelle Crabb-Guel, summarizies it best in her presentation on: "Policies and Procedures."

6.1. Policies Must:

6.1.1. Be implemented and enforceable

6.1.2. Be concise and easy to understand

6.1.3. Balance protection with productivity

6.1.4. Be updated regularly to reflect the evolution of the organization

6.2. Polices Should

6.2.1. State reasons why policy is needed

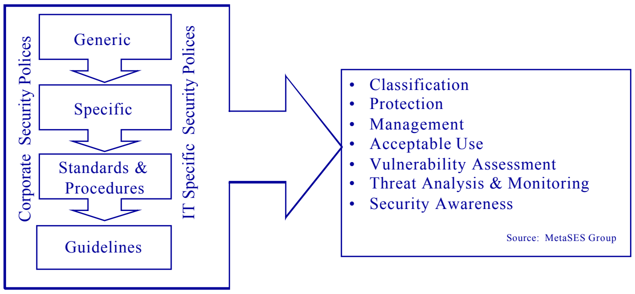
6.2.2. Describe what is covered by the policies-whom, what and where

6.2.3. Define contacts and responsibilities to outside agencies

6.2.4. Discuss how violations will be handled

The Information Security Organizational Policy or more commonly known as the Enterprise Security Charter is defined in the ISO/IEC 17779 Information Technology – Code of Practice for Information Security Management as, "a policy document that should be approved by management, published and communicated, as appropriate to all employees. It should state management's commitment and set out the organization's approach to managing information security."

Information Security Organizational Policy



Source: MetaSES Group

The METASeS Group in their white paper, provides the following definitions security policy categories**.**

Asset Classification-"Defines an organization's objective for establishing specific standards to define, identify, classify, and label information assets.

Asset Protection-"Defines an organization's objective for establishing specific standards for providing an appropriate degree of confidentiality, integrity and availability for information assets".

Asset Management-"Defines an organization's objective for properly managing its Information Technology infrastructure, including networks, systems, and applications that store, process and transmit information assets throughout the entire life cycle".

Acceptable Use-"Defines an organization's objective for ensuring the appropriate business use of information assets. The policy also states an organization's position of the right to monitor, record and audit the use of such systems and equipment, and addresses potential misuse."

Vulnerability-"Defines an organization's objective for vulnerability assessment activities and ongoing vulnerability management efforts".

Threat Assessment and Monitoring Policy-"Defines an organization's objective for threat assessment activities and ongoing threat monitoring efforts".

Security Awareness-"Defines and organization's objective for establishing a formal Security Awareness Program. This policy ensures that the Policy

Framework elements are properly communicated and accessible to new hires, employees, and third parties".

The definitions above are presented only to reflect that policy categories exist. Different companies will have different security frameworks and policy requirements. Security management must select a policy framework that works for our respective business objectives and cultures. Another good example can be found Table of Contents in the ISO/IEC 17779 Standard.

Cheryl W. Helsing, provides the following definitions in "The Handbook of Information Security Management".

Policies. "These are high level statements that indicate management's intentions. They provide broad direction or goals".
Standards. "These are more specific statements embodying control requirements suitable to achieving management's goals. Compliance with standards is expected".
Procedures. "Procedures are step-by-step ways of obtaining and end result. Procedures are often established to satisty requirements".
Guidelines. "These are suggestions about how to achieve compliance with protective standards. Guidelines are not binding".

Aligning with the Security Design Group

Due to the shortage of trained security management personnel, many of us are offered or choose to make a career change into the field of security management, with little or no security design experience. Corporate networks are and continue to get more complex each and everyday. While IT continues to reach out to our trading partners, brokers, vendors, customer and consumers. So it becomes imperative to obtain a clear understanding of our informational assets but also to obtain the knowledge in our security design components; security perimeters, border routers, firewalls, intrusion detection, and anti-virus software. This activity promotes real world experience from our respective organizations. Take this opportunity to casually begin to sell your security management program from within the IT group. There is no single answer that we can cut and paste to include in our security message delivery. Security awareness is a process that needs to be delivered throughout the organization, continuously over time.

As mentioned earlier in the "Current State of Affairs" section we need to next understand where the security design is heading. Is that group in status quo mode, or are they in the final stages of delivering a corporate private exchange with single sign on and strong authentication? Are they about to sign on the dotted line, when no policies are in place? If they are, we better catch up and put the tail behind the dog. For most of us just the opposite exists, “the tail is in front of the dog. Certainly, we must realize that this catching up will require additional effort on our parts. If we are going to communicate the *future state* of security management, we have to get ourselves in the *current state* with one of our primary stakeholders-security design team.

Delivering the "Security Message"

Communications 101-“Know your audience”. Our respective audience is listening for those magic words, “So how is security policy going to make my life easier”. Let’s first review at a couple of definitions of “security policy” and its role within the organization. LevelOne SANS Security Essentials Part One we find the following:

1) “A security policy establishes what must be done to protect information stored on computers. A well-written policy contains sufficient definition of “what” to do so that the “how” can be identified and measured or evaluated.”
2) “An effective security policy also protects people. A security policy allows people to take necessary actions without the fear of reprisal”

In his book, “Information Security Policies Made Easy”, Charles Cresson Woods defines the following elements of good security policy:

1) “…it’s very important that the policies in effect be clear, sufficient and responsive to the computing environment in question.
2) “…well defined corporate information security policy is the biggest problem with most security efforts. …Instead policies must be uniquely tailored to the needs of the organization.
3) “Policies are high-level statements that provide guidance to workers who must make present and future decisions.”
4) “…Before beginning to write a policy document, the policy writer should check with management to make sure that they are all talking about the same thing, and that they understand why a policy development effort is important.

Two more points are defined in the book, “Internet Security for Business”:

1) “Good information security policies provide the foundation for an effective information security program. In a broad sense, policies are management directives that establish the business goals of the organization, provide an implementation framework to meet the objectives of those goals, and assign responsibilities and ownership for the process”.
2) “More specifically, security policies are designed to manage the risk that the company incurs as it pursues those business objectives”.

Unfortunately, there are no magic words, nor a single silver bullet that answers all the questions of security risk that the e-internet world brings to our companies. Security elements work together with the business to “eliminate, minimize, accept or transfer the risk”, as found in the SANS Kickstart book.

Conclusion

One clear statement can be made to our partners in the security design function that enables them to be the best that they can be. This statement is found in the LevelOne SAN Essentials Part 1 book on page 5-24, “Good policy empowers people to do the right thing.” It is extremely important that we spend the time to understand the world of our targeted audience’s. This is necessary so that we can communicate from a platform of common knowledge. Our audience can assist us in understanding their perspective and we can assist our audience in understanding the role each of us has relative to “security” in our organizations. Our next step, “**Security Awareness Starts Within IT.”**

References

1) Information Security Policies Made Easy – Version 7, 1999
Charles Cresson Wood

2) Handbook of Information Security Management – 1993
Della G. Ruthberg, Harold Tipton

3) Internet Security for Business –1996
Terry Bernstein, Anish B. Bhimani, Eugene Schultz, Carol A. Siegel

4) ISO/IEC17779 Information Technology
Code of Practice for Information Security Management – 12/2000

1) SANS Institute, The. "Risk Management." Kickstart Track Book KS-1A/B (2001), Chapter 1, pp 1-23

5) SANS Institute, The. "Basic Policy." Track 1: Security Essentials Book 1.1 Version 1.35 (2000): Chapter 5, pp 1-30

5) SANS Institute, The. "GIAC Basic Security Policy." Track 1: Security Essentials Book 1.1 Version 1.4 (2001): Chapter 6, pp 1-12

5) MIS Training Institute, The. "Building An Information Security Program: Blueprint for Success." (2001) p-5

6) Network Security Library, "Internet Security Policy: A Technical Guide."
URL: http://www.secinf.net/info/policy/isptg.en/ISPTG-Contents.html

7. Michelle Crabb-Guel. "Section Three: Policies and Procedures."
URL: http://www.sans.org/newlook/resources/policies/bssi3/index.htm

8. Malcolm E. Palmer, Craig Robinson, Jody Patilla, Edward P. Moser.
METASes Information Security Policy Framework-White Paper,
"Best Practices For Security Policy and Policy Distribution in the Internet and e-commerce Age."
URL: http://www.metases.com