Global Information Assurance Certification Paper

The Business Case for an Information Security Policy

Kyle Ginney
GSEC Practical Assignment, Version 1.4b, Option 1
April 23, 2004

ABSTRACT

An information security policy is a necessary part of today's IT infrastructure. When creating or seeking approval for a policy, it is imperative that the writer keep in mind the needs of the business. Security does not exist in isolation – it must coexist with everyday business practices or it will be abandoned. This paper lays out a framework for understanding the security policy creation from a business perspective with attention to those factors that will help ensure management approval.

INTRODUCTION

With the development of the Internet in the 60's and 70's, and the subsequent adoption of the World Wide Web by business in the 80's, communication and business opportunities on a world-wide level has never been easier. While this technology has given us unparalleled access to information wherever it may reside in the world, it has also taken away our sense of personal space and the belief that access to our most private information can be easily controlled. Even to this day, there are organizations that believe they can prevent access to their information through the use of simple firewalls and routers installed out-of-the-box. Even more amazing is the fact that those organizations that do put some effort into an Internet-based security posture will also completely ignore any form of Intranet security. While the statistics vary over the amount of security breaches from the outside of an organization vs. security breaches from the inside, the main point remains clear that valuable information must be secured.

These factors have formed the basis for the emergence and rise to prominence of the information security professional. The job of any information security professional is to provide the accepted level of security for your organization. But who decides what is acceptable security? In these days of burgeoning state and federal legislation holding executive management accountable for the security of their information, it is to those people that the level of security of the organization's information should be acceptable. One of the more common methods of laying out a security framework for an organization is through the adoption of a security policy. However, while developing a security policy, it is important that the policy be constructed around the organization, for it is from the income provided to the organization that any security measures will eventually be funded. It is therefore critically important to keep any security measures in line with the continuing prosperity of the organization. Failure to pay attention to the business impact of security initiatives may doom any security policy from the start. You, as a security professional, may be called upon to justify the nature and expense of any security initiative, and if you cannot present a valid business case for said initiative, you will likely encounter resistance from those in executive management. In order for any security initiative to work, it will need to have the full support and backing of executive management, and the best way to gain their approval is to approach a security policy from the business point-of-view.

WHAT DO YOU MEAN BY "SECURITY"?

"Security" is a term that is commonly thrown around in the IT world, but it is also one of those terms that may mean different things to different people. Before you can have a discussion with executive management about security, you must make certain you are all talking about the same thing. In the IT world, "security" is a concept that embodies the three main tenets of Information Security: confidentiality, integrity, and availability. By addressing the security problems associated with these areas, you are making an effort toward making the systems in IT more secure. Notice, however, that the key here is "more secure". Sometimes executive management may have an idea that security is an absolute – you either are secure or you are not. It is important to make them understand that, due to the complexity of the systems that make up today's IT infrastructure, there is never absolute certainty that any given system will ever be 100% "secure". Security is an ongoing process that has as its' end goal the greatest possible security for IT systems with the least significant impact on daily business processes. Therefore, it follows that the main goal for a security professional is to make the IT systems as secure as possible, or, as is commonly the case in the world of corporate IT, as secure as management will let you make them.

The creation of a security policy can be seen as the negotiation process between you, as the security professional, management, and users as to the amount of security that should be in place and the best methods for providing that level of security. The policy itself – the end result of these negotiations – will therefore reflect a common ground for securing the systems of IT that management is willing to endorse. It is also important for the executive management to understand that, because the business processes that IT supports are always changing, the policy needs to be a living document that must be reviewed on a periodic basis to ensure that it is still relevant.

WHERE SHOULD I BEGIN?

Before setting out on a security policy quest, it is best to start with what you know. As in any situation where you are assigned the task of protecting something, you need to know two things: what am I protecting and from what am I protecting it? This is where the process of risk assessment comes into play. A risk assessment identifies each system in the organization according to function and criticality to the business infrastructure. According to NIST, there are 9 phases of a risk assessment:

1. **System Characterization**: establishes the scope of the risk assessment effort, delineates the operational authorization boundaries, and provides information essential to defining the risk.

2. **Threat Identification**: identify threat-sources, potential vulnerabilities, and existing controls.
3. **Vulnerability Identification**: develop a list of system vulnerabilities that could be exploited by the potential threat-sources.
4. **Control Analysis**: analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood of a threat's exercising a system vulnerability.
5. **Likelihood Determination**: derive an overall likelihood rating that indicates the probability that a potential threat vulnerability may be exercised within the construct of the associated threat environment.
6. **Impact Analysis**: determine the adverse impact resulting from a successful threat exercise of a vulnerability.
7. **Risk Determination**: assess the level of risk to the IT system by utilizing risk scales and a risk-level matrix.
8. **Control Recommendations**: recommending controls or alternative solutions that could mitigate or eliminate the identified risks, as appropriate to the organization's operations.
9. **Results Documentation**: the results of the risk assessment are documented in an official report or briefing.[1]

While this process will identify each system and its importance, this process will also identify the interrelationships between systems. This information is just as critical to security as the identity of the systems themselves. Without knowledge of the dependencies among systems, security measures could be focused on certain systems while ignoring other systems that, if compromised, would give easy access to information you thought you had already protected.

The risk assessment will also detail the amount of access to business critical information that is necessary for the organization to operate. This will tell you how much security can be placed on each system and how far you can restrict access before you will impact the ability of the organization to function. This is an important issue to be addressed. On the one hand, if you secure each system to the highest standards possible, but it negatively impacts the function of the organization, all of your efforts will have been in vain when the CxOs demand that the security measures be removed. This will also ruin whatever security momentum you had built up to that point as the CxOs will now scrutinize all of your efforts at security as possibly jeopardizing the bottom line. On the other hand, if you secure each system to the lowest possible standard, you leave the organization wide open to attacks which could cause it to spend large sums of money to repair. This is a fine line that each security professional must walk in order to get the best possible security policy in place that will not adversely affect the function of the organization or the organization's bottom line.

Risk assessment is one of the most fundamental and crucial steps that must be taken before any security policy will ever gain executive approval. Before you can

[1] Stoneburner, et al.

ever justify the expense associated with purchasing, installing, and maintaining any new security initiatives, you must first be able to catalog the information by orders of importance and have specific dollar figures associated with this catalog. This is not done just for the executive side of the house, however. Every security professional worth their certifications must have an understanding of just what is to be secured and the relative worth of that information in relation to the amount of money proposed to secure it. Management's input at this stage is crucial to its success.

There are also intangible factors in deducing the monetary value of any security incident. While it may be easy to put a dollar figure on the loss of a server, the manpower required to rebuild a database, or the lost revenue from the loss of an Internet connection, what about other, more long-term damage that is harder to quantify? This damage may include loss of reputation or of customer confidence. How do you put a dollar figure on your company's reputation? As Shon Harris points out, "The value placed on information is relative to the parties involved, what work it took to develop that information, how much it costs to maintain it, what loss it would cause if it was lost or destroyed, and what benefit would be gained if another party obtained this information."[2] This just helps to illustrate the many factors that can determine the value placed on an organization's information.

The largest hurdle you, as a security professional, may encounter occurs when you try to obtain financial backing for the latest security initiatives you require. Remember, this is a business that exists to make money, and the executives cast a disapproving eye towards anything that takes away from their net profits without a justifiable reason. Therefore, it is essential that any security measure must answer the same question that all other proposed changes must answer – how will this impact the bottom line? This question can only be answered in terms of dollars and cents. Can you justify this expense with an acceptable ROI? Or, at the very least, do the dollars associated with this project fall below the projected losses from a security incident? These questions can only be answered accurately after a thorough risk assessment has been completed.

WHAT IS A SECURITY POLICY?

Now that you have an idea of what systems exist in the organization and the worth of the information stored on them, the next step to securing these systems involves the creation of a Security Policy. A simple definition for "security policy" is "…the primary way in which management's expectations for security are translated into specific, measurable, and testable goals and objectives."[3] The policy should clearly define what management expects for a secure operating environment and list the specific requirements and procedures necessary to

[2] Harris, pp.63-64.
[3] Sun Microsystems.

achieve this goal. It is also important that the degree to which these expectations, or “goals”, have been successfully implemented must be measurable. Because security is never a black-and-white issue, it is always important to understand exactly how effective a particular initiative has been. With the advent of the recent regulations concerning public corporations, it is now financially necessary that executive management have proof that the required security processes are in place and are fulfilling the requirements.

There is a common misconception that a Security Policy is a single document that addresses all of the security requirements for the organization, outlines the practices necessary to attain regulatory compliance, and provides specific instructions for acceptable use of information resources. This is not always the case, however. In small companies where the entire staff can see each other from their desks, it is possible that one document can satisfy their security policy needs. In larger companies with entities spread throughout the country or the world, any attempt to create a blanket document that would cover all security policy requirements will inevitably prove futile. The larger the organization, the more management needs to be involved in the creation of the policy, the more compromises will be made. You must be able to design a Security Policy in such a way as to address the organization’s cultural environment, the value of the information to be protected, and the legislation and regulations that apply to your industry. Regulations differ from state to state and from country to country – it would be impossible to address all of these differences with a readable document that would not need to be moved with a forklift. In these instances, the requirements for a security policy should be broken down into three separate documents: an *Information Security Policy*, an *Information Security Standard*s document, and an *Information Security Procedures* document.

Information Security Policy

The Information Security Policy should be a document that provides a general outline of the security requirements for the company. This is the document that creates the awareness of security in the organization’s culture and becomes part of the public domain of the organization that everyone must adhere to in daily business activities. This document should address all legal and company-specific security requirements in such a general fashion that, should the company decide overnight to switch from one type of OS to another, the document still applies without any changes. It is still important that no matter how general the Policy is written, the document should be sound in-and-of itself and a document that auditors will be able to accept as the company’s official statement on information security. However, and perhaps most importantly, in most large organizations, the management that needs to sign off on this policy is usually not technically savvy. It is therefore a crucial matter that the security policy document be brief, about 1 or 2 pages, to the point, and able to be understood by anyone in the company. After all, this is a company-wide policy that will affect everyone and if a

document is created that requires a tenure in the Computer Science program at a university to understand, it will be quickly dismissed by the employees and, most importantly, by those in management who need to enforce it. Without this policy in place and supported by management, none of the other security initiatives will have the necessary foundation for acceptance into the organization's environment.

Information Security Standards

The Standards document serves as a more detailed listing of exactly which systems are to be protected and by what means. It spells out for management and auditors the main areas of focus (i.e. server security, desktop security, router/switch configuration, third-party support, etc.) along with the type of security measures that will be implemented in each area. This document depends heavily on the risk assessment process, the results of which will determine the exact nature of the security measures to be implemented. Using the sample policies on the SANS website as a template, the main features of this document should include:

- **Purpose** – the reason for the policy
- **Scope** – what systems, behavior, etc. the policy is meant to address
- **Policy** – specific statements regarding systems, security measures, and responsibilities
- **Enforcement** – the nature of the punishment for disregarding the policy – either willfully or though ignorance
- **Definitions** – definitions for any terms that may need to be explained to anyone without much technical knowledge[4]

This document also serves as the reference for the creation of the *Information Security Procedures* document in that it lists specific security requirements for certain OS, server types, and desktop environments.

Information Security Procedures

The Procedures are the actual nuts and bolts directions that state specifically what is to be done and who does it. The procedures spell out exactly how the security policies and standards are to be implemented in the organizational environment. These procedures will be specific to certain OS, machine types and programs. They will spell out how to install an OS, what services to remove, how to lock down a Web server, how to structure an FTP site, who can be part of the Domain Administrators group, etc. Since these policies will be necessarily technical in nature, these will most likely stay in the IT department and used as the official procedures for configuring machines and dealing with security

[4] The SANS Security Policy Project.

incidents. These procedures will be the bible for all techs and admins to use when setting up user accounts, machines, servers, or network equipment. Because of their highly specific nature, these procedures must be constantly tested and modified to meet the policies outlined in the Standards and Policy documents.

WHY HAVE A SECURITY POLICY?

There are several reasons for implementing a security policy for your organization, but perhaps the most important reason that exists from a business perspective is that a security policy will add to or enhance the financial stability of the organization. This is an important concept to keep in mind. According to Benjamin Wright, "the trend in law is increasingly to hold institutions accountable for IT security weaknesses."[5] For example, Berinato and Scalet point out that "experts fear personal injury lawsuits filed by customers whose personal information has been disclosed, corporate lawsuits based on damage caused by security breaches at business partners, and class-action lawsuits filed on behalf of irate stockholders."[6] The reparations demanded by the courts as a result of these lawsuits range from a mere slap on the wrist to millions of dollars. There exist cases where a penalty was severe enough to cause the business to declare bankruptcy and close their doors forever. It is by addressing these concerns that an approved and properly executed and enforced Security Policy could potentially save money.

In this perspective, a well-written and thoroughly researched security policy serves as the organization's official declaration to legal entities that they consider security a priority and are taking reasonable steps to provide security for their information and their systems. According to Benjamin Wright, "A solid IT security policy, properly enforced, shows the enterprise is thoughtful and deliberate and the records created are more reliable for liability, audit, insurance, and law enforcement purposes."[7] The key issue here, however, as illustrated by this statement, is that a security policy must be enforced – must have management backing – in order for it to be effective. Without management's support, no amount of hard work will ever generate a security policy that has any hope of safeguarding the organization from litigation. Also note that a security policy can be used in legal situations to show the validity of organizational information by proving that safeguarding procedures are in place and adhered to, with penalties in place for non-compliance.

Those who fill CxO positions in your organization are not likely to see the need to introduce more restrictions to their employee's behavior unless a valid business case can be made. If you can prove to the CxOs that the organization stands to

[5] Wright, p.7.
[6] Berinato and Scalet.
[7] Wright, p.40.

lose money over the course of time, either by regulatory penalties, lawsuits, or through wasted labor resources, then the idea of a security policy will begin to make financial sense. Basically, you would demonstrate the cost benefits of a security policy by the money the organization might have to spend if they didn't have one. The easiest way to make this case is with an ROSI (Return On Security Investment). However, while this is the best way to present the need for and merits of a security policy, actually gathering the data necessary to make an ROSI and proving that the ROSI is a valid figure can be a very difficult task.

THE ROSI

An ROSI (return on security investment) can best be described as the amount of money spent to completely deploy a security initiative vs. the costs associated with a security failure[8]. The ROSI is usually calculated by gathering information from three different areas. These areas are referred to by Dr. Larry Ponemon as "direct cost, indirect cost, and opportunity cost."[9] A direct cost is what can be described as the purchase price of the security initiatives, including all costs associated with personnel training, on-site vendor assistance, etc. This number is usually very easy to find. A more difficult area for expense estimation is the area of indirect cost. This area includes such intangible quantities as the hours spent by various staff setting up the equipment, making all of the network connections, monitoring and tweaking the product to fit your environment, sitting on hold waiting for the vendor's help desk to resolve an issue, and generating the appropriate management reports. Because your staff are the ones being tasked with making initiatives work, and these staff are on the company payroll, each minute of their time has an associated monetary value. The opportunity cost, according to Dr. Ponemon, is "the cost resulting from inefficient or ineffective compliance, including the cost of failure or non-compliance."[10] This cost includes criminal and civil lawsuits and regulatory penalties as well as such intangibles as loss of consumer confidence or business reputation resulting from a publicized incident, be it a successful intrusion or not.

However, as Scott Berinato points out in his article dealing with the issue of obtaining valid numbers from an ROSI, when they can't find the hard numbers they need for a conventional ROSI, "…information executives rely on soft ROSIs – explanations of returns that are obvious and important but impossible to verify."[11] This ties into the previous idea of intangible organizational assets such as reputation or customer loyalty. While these assets are much harder, if not impossible, to place a specific dollar amount on, they are nonetheless as much an asset to an organization as the products they produce or the services they offer. Loss of business reputation can cause more financial damage to an

[8] Ponemon.
[9] Ponemon.
[10] Ponemon.
[11] Berinato, "Finally, a Real Return on Security Spending".

organization than the actual costs of cleaning up after a security incident. As Scott Berinato suggests, “Know how the executives want the ROSI positioned – cash savings, productivity gains, increase in security – and move forward that way.”[12] Those who ultimately run the organization - the CEOs and Presidents - are best able to identify these costs. In this situation, a security policy can be justified by illustrating all of the potential ramifications from a security incident and let those in upper management decide on the appropriate level of protection based on their views of the relative worth of those intangible assets.

New research is being conducted with the goal of finding provable and verifiable methods to produce valid ROSIs. With methods that can produce solid financial numbers, security professionals may finally have the information they need in a form that upper management is more comfortable in dealing with. These numbers will now allow security professionals to see the costs and benefits of security initiatives and help them decide on the most appropriate initiatives for their organization.

WHO SHOULD BE RESPONSIBLE?

Information security is linked to every function of an organization. Therefore, the responsibility for maintaining a secure environment must distributed among the entire organization as well. Everyone with access to a desktop computer is charged with the responsibility of using common sense and adhering to organizational security standards. Security professionals are charged with evaluating, installing, configuring, and maintaining the security measures approved by management. They are also the ones responsible for measuring the success of any security process as well as accurately diagnosing security incidents and responding in an appropriate and timely fashion. Middle management is responsible for ensuring the security professionals have the equipment and training they need to be successful and the notoriety they deserve after a job well-done. Executive management is ultimately responsible for, well, everything. They are the ones tasked with categorizing all of the information by importance to the operation of the organization. They are the ones who must approve all security initiatives and attest to auditors that they are aware of the initiatives and their correct application and that the initiatives are successful in meeting their goals. They are the ones that you, as a security professional, must convince that their involvement in organizational security from the very beginning is the only way a security policy will succeed.

CONCLUSION

It is important to note that any given company will spend less money in the long term if they take a proactive stance and establish a security plan before any security-related purchases are made. Without a plan, the company will be placed

[12] Berinato, “Calculated Risk”.

into a reactive stance and will spend more money on stopgap technologies to solve the problem of the day. Having a proactive vision allows security engineers and managers to find solutions to their security issues that will form a cohesive security core by enabling them to select initiatives that best fit the environment of the organization and will work together to address the security needs. Addressing security issues in a stopgap fashion leads to the acquisition of products that may be untested, inadequate, or, at the very worst, ultimately unhelpful. This results in a larger investment by the company in security initiatives through wasted time and effort.

When designing a security policy, always keep in mind that the function of the organization must be a priority. There are always methods for securing information that can be incorporated without negatively impacting the bottom-line. It's all a matter of finding the right technology to fit the needs. Remember the adage "an ounce of prevention is worth a pound of cure"; it is especially applicable to the world of security policies.

LIST OF REFERENCES

Berinato, Scott. “Finally, a Real Return on Security Spending.” 15 Feb. 2002. URL: http://www.cio.com/archive/021502/security.htm (15 March 2004).

Berinato, Scott and Sarah Scalet. “The ABCs of Security.” 20 March 2002. URL: http://www.cio.com/security/edit/security_abc.html (15 March 2004).

Berinato, Scott. “Calculated Risk.” 12 December 2002. URL: http://www.csoonline.com/read/120902/calculate.html (21 March 2004).

Harris, Shon. All-In-One CISSP Certification Exam Guide, Second Edition. Emeryville, CA:McGraw-Hill/Osborne, ISBN 0-07-222966-7, 2003.

Ponemon, Dr. Larry. “Calculating an ROI for Data Security.” September 2003. URL: http://www.darwinmag.com/read/090103/secureroi.html (6 April 2004).

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. “Risk Management Guide for Information Technology Systems.” NIST Special Publication 800-30. January 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (7 April 2004).

Sun Microsystems. “Developing a Security Policy.” 15 March 2002. URL: http://www.informit.com/articles/article.asp?p=25934 (19 April 2004).

The SANS Security Policy Project. URL: http://www.sans.org/resources/policies/.

Wright, Benjamin. Business Law and Computer Security. SANS Institute, ISBN 0-9743727-1-4, 2003.