

How Security Policy Affects the Safety & Security of a Business

By Ravi Das, HTG Solutions

Importance of a Security Policy

Security and Safety has always been an issue in Corporate America, but it has intensified after the tragic events of September 11, 2001. These events triggered vast amounts of legislation as well as research and development of technologies to secure our organizations and businesses. However, despite all of these massive efforts, Corporate America is still finding itself literally “under the gun” of many types of Security Threats, Security Risks, and Security Vulnerabilities. These types of Threats, Vulnerabilities, and Risks occur either in a Physical or Logical manner. In terms of the former, there are still many issues with unauthorized individuals entering the physical premises of a business or organization. Very often, even when there is a Physical Access Entry Security System put in place, it can be bypassed quite easily. For example, someone can steal an Identification Card, process it through an automated Card Reader, and gain unauthorized access. Or, the Security Guard, instead of examining credentials of people entering the building, takes a cursory glance. These actions result in increased Security Threats and Risks to an organization or business critical Information and Data Infrastructure. For example, Worms, Viruses, Phishing Attacks, Denial of Service Attacks, Identity Theft, etc. all occur almost on a daily basis. In fact, trying to address Security Issues from both a Physical and Logical perspective has become “Survival of the Fittest”. As one victory is accomplished over a Security Threat or Risk, attackers come out with something new and different.

There is a mindset in Corporate America that by applying the latest Security Technologies to the infrastructure of an organization or business, all Security Threats and Risks will be resolved. While there is no doubt that Security Technologies are very much needed, they are only one part of an overall Security and Safety Solution. The other component is the Security Policy. The Security Policy defines the Security Rules that all employees must follow and abide by and spells out the consequences of not following the Security Rules. So while it is important to

have Security Technology in place, it is even more important to have a well written and documented Security Policy. This is what establishes the culture and mentality as to how employees will react to any Security Threat or Risk that they are faced with.

Developing a Security Policy is often a time consuming and complex process. You simply cannot take an existing Security Policy and implement it at another business. Every business has their own unique Security Needs. Therefore, it is not the goal of this article to go into the minute details of creating a specific Security Policy, rather, to provide the framework of a general Security Policy.

Need For Risk Assessment

Defining Security Risk

The complexity and scope of a Security Policy largely depends upon the level of Security Risk a business or organization faces. As each business has their own processes, the parameters used in assessing Security Risk will vary greatly. For example, a Financial Institution will be at a higher level of Security Risk, because they possess large amounts of confidential Financial Information and Data about their customers; their Security Policy will be very detailed and well organized. A small business owner with a smaller employee and customer base with less confidential Information and Data, will have a Security Policy that is less detailed than the Financial Institution's Security Policy. However, the bottom line is that all types of business entities no matter how large, small, or complex, all face a certain degree of Security Risk, thus underscoring further the need to have a Security Policy.

An exact definition of Security Risk involves the statistical probability that a particular Security Threat will accidentally or intentionally trigger Information System or Physical Access System vulnerabilities and subsequent impact the organization or business.

Risk Assessment Analysis and Risk Categories

The key word is “impact” -- you must measure the degree of tolerance a business or organization can handle before it starts to suffer a Negative Rate

of Return on their processes. Measuring the level of impact is usually accomplished via a Risk Assessment Analysis. There are many Risk Assessment Analysis Models available that can quantify the level of “impact”, and reviewing them in detail is out of the scope of this article. However, there are a number of Risk Categories which are utilized in a Risk Assessment Analysis Model. Some of these Risk Categories include:

- 1) Outsourcing Risk: This refers to having an Outside Vendor carry out the functions of one or more process or operation. The level of impact to be measured here is to what degree, or how much of the process or operation you are able or willing to give to an Outside Vendor without divulging confidential information about the organization or business. It's important to give the Outside Vendor just enough information, data, and resources in order to carry out that process or operation for which they were hired, but not enough to pose a Security Threat.
- 2) Business Continuity/Disaster Recovery Risk: This refers to a total shutdown of the organization or business (at the primary location), caused either by a natural disaster or some catastrophic Security Breach. The level of impact to be measured here is how much downtime the organization or business can sustain and, at the same time, how quickly operations and processes can be started at the back up, or alternate, site.
- 3) Physical Protection Risk: This refers to the guarding of the actual physical premises of the business. Although all areas of the organization or business need to be secured, to what extent should the level of protection be? What will be the impact or consequences be if a Single Layer Security System were to be implemented versus a Multi-Tiered Security System?
- 4) Data and Information Availability/Integrity/Protection Risk: Data and Information must be made available on demand and in full integrity to customers and employees. Also,

there will be times when some this Data and Information must be shared with the public. The level of impact to be measured here is how quickly Information and Data can be made available and restored to full integrity in the advent of a Security Breach, and how much and to what level that Information and Data can be shared with the public without causing any subsequent Security Risk to the organization or business.

- 5) Compliance Risk: Today there is a lot of Government Legislation and Mandates that organizations and businesses are required to comply with, resulting in a lot of time and resources being spent on being Compliant and less time and resources on other critical processes and operations. Therefore, the impact to be measured here is how much time and resources can be spent on Compliance without compromising the time and resources necessary to combat the real Security Threats which may occur on a daily basis. Also, what will the impact be by being in partial, rather than full, Compliance?

Security Policy

Defining Security Policy, Security Standards, and Security Guidelines

After the level of risk has been defined via the Risk Assessment Analysis, the next step is in the creation of the Security Policy. However, before discussing its major components, it is important to specifically define what a Security Policy is: a formal document which establishes and states the rules through which people are given access to an organization's or businesses' technology, systems and processes, as well as the information and physical assets.

The other components which support the Security Policy are the Security Standards and the Security Guidelines. A Security Standard can be defined as the specific requirements which all employees of the organization or business are required to abide by. These Security Standards can be either system or procedure specific. For example, in a system specific Security Standard, one would specify the types of Hardware or Software an employee can install on their computer, if the need arises. In a procedure specific Security Standard, one would specify the proper protocols to be followed if an employee were to download Software or any other kind of Information or Data from the Internet. A

Security Guideline can be defined as the "Best Practices" employees should follow in order to protect the tangible assets (such as computers, business documents, etc.) as well as the intangible assets (such as the Intellectual Property, Information, and Data) of the organization or business. An example of a Security Guideline would be the best ways an employee can protect their Username and Password.

Components of the Security Policy Model

The following are some major components of a Security Policy. Although a Security Policy primarily deals with rules about granting access, it should also address the types of Security Systems and Technologies utilized to protect the organization or business. These should not be Vendor Specific, but rather Security Tool Specific.

Physical Security: This part of the Security Policy deals with the Physical Protection of the organization or business, as well as the Tangible Assets. Items to consider when developing this part of the Security Policy include:

- The Perimeter Protection for the organization or business, including the types of Security Devices to be implemented. The frequency and the procedure for testing the Perimeter Protection should be also addressed. Penetration Testing techniques should also be documented here, as these types of tests reveal the strengths and weaknesses of the Perimeter Protection.
 - The Physical Access Entry Protection. This refers to the type of Security Procedure and Protocols which will be used to authorize employees and others into entering the business or organization. They include:
 - Which employees will have what levels of access to places inside the business or organization?
 - What methods will be used to check the authenticity of the Identification Credentials of the employees, and how many layers of Security will be needed (for example, will simply checking the Identification badge of the employee and others be enough, or will multiple layers of Security be required as a further and more positive means of Identification)?
 - Depending upon how large the organization or business is, will Security Guards be needed to check for employee Credentials, and if so, what is the level of training and experience that is required of the Security Guards?
 - A Classification Scheme will have to be formulated for all Tangible Assets, and rated accordingly in terms of importance. For example, confidential and proprietary Business Documents, will need to be prioritized and archived for future retrieval in the advent of a catastrophic Security Breach. Consideration should also be given to Physical Off Site Storage Locations of important Business Documents, as well as Electronic Off Site Storage Locations (scanning and storing at a server off site). Note that there will be overlap here with the Disaster Recovery and Contingency Planning component of the Security Policy.
- Logical Security:** This part of the Security Policy deals with the protection of the Intangible Assets of the organization or business, specifically the Information and Data, and the Information Technology Infrastructure on which they reside upon. Items which should be considered when developing this part of the Security Policy:
- The Security Devices and Technologies which will be used to protect the Network Structure of the organization or business, also referred to as the "Intranet". Consideration and implementation needs to be given to protecting the Information and Data from an internal and external perspective -- maintaining the integrity and confidentiality of the Information and Data from people who access it from inside and outside of the confines of the business. There are many Security Tools and Devices which are available to in order to accomplish this, such as Firewalls, Routers, and Network Intrusion Devices. Consideration also needs to be given to the Layout Topology these Security Devices (where they will be located on the Network Structure), in order to assure maximum protection to the organization or business.
 - Protection of the Computer Network Configuration. For example, Security Standards need to be developed as to when the computers need to be upgraded for Software Patches and Upgrades, in order to protect against such Security Threats as Worms, Viruses, Trojan Horses, Malicious Software Code contained in E-Mail Attachments, etc. Also, a Security Standard needs to be for-

mulated and documented as to how often and to what level of investigation is required in order to check the computers for any Security Threats or Security Vulnerabilities.

- A key component of this part of the Security Policy is addressing the access to the Information and Data -- which employees have access to which pieces of Information and Data or, establishing "Access Rights". For example, certain employees will need to have access to very confidential and proprietary Information and Data in order to accomplish their job tasks, and other employees will need to have access to only lower levels of Information and Data. The second issue to be dealt with is the method in which the Information and Data is accessed. This is known as "Authentication". The most common form of Authentication is the Username and Password. It is important to develop very specific and clear Security Standards as to how employees should create a Secure Password, and the subsequent protection of that Password. Consideration should also be given if more than one level of Authentication is required (such as using another Security Protocol in conjunction with the Password). A typical Security Solution here would be what is known as a "Single Sign On Solution", or an SSO Solution. This type of Security Solution utilizes Biometric Technology, primarily Fingerprint Recognition. In this scenario, an employee can authenticate themselves onto their computer with just one scan of the Fingerprint.
- Security Standards need to be developed for the Mobile Workforce of the organization or business -- employees who use their Laptop Computers to connect to the Intranet, often via a "Wireless Connection". The main Security Risk lies in the fact that much of the Data Transmission occurs in the open air, rather than in the confines of the Network Cable. Thus, this Data can be very easily intercepted and used to compromise the proprietary Information of the organization or business. This type of Data needs to be protected so that if it were to be intercepted, it would be rendered useless. Also, the Wireless Connection needs to

be protected and secured -- known as "Encryption". There are many Encryption Tools available, such as Secure Sockets Layer, Secure Shell, Virtual Private Networks, Digital Certificates, Public Key Infrastructure, etc.

Security Awareness, Training, and Compliance: This part of the Security Policy deals with employee training on the Security Standards and Security Guidelines set forth by the business or organization. This can be deemed to be one of the most important components of the Security Policy. Items which should be considered when developing this part of the Security Policy:

- The types and frequency of Security Training Programs to be implemented. Security Training Programs for employees can include formal Workshops, Group Sessions, Company Based Security Newsletters, One On One Training Sessions, etc. The key is to develop Security Training Programs that employees will remember the Rules and Regulations and also be proactive about Security Issues, and how to appropriately react and respond to Security Threats if they are faced with them. It is important to stress that Security Awareness is a group effort and a common goal to be reached among all employees of the organization or business.
- Compliance with the overall Security Policy, as well as the specific Security Standards and Security Guidelines. Communication between the Security Staff and the other employees of the organization or business is most important. The consequences for not abiding by the Security Policy must be clearly communicated to all of the employees, so that they can be held accountable.

Disaster Recovery and Contingency Planning: This part of the Security Policy deals with how the organization or business will recover and restore operations and processes if faced with a Natural Disaster or Catastrophic Security Breach. Items which should be considered when developing this part of the Security Policy:

- Offsite Storage and Location of Secondary Site. Develop details of

where to store Paper and Electronic Back Ups of all critical Information and Data, and who will have will have access to that Offsite Storage both during the normal times of business and in the event of a Natural Disaster or catastrophic Security Breach. Also, decide upon the location of the Back Up Site, where the processes and operations will commence if the Primary Location shuts down.

- The Logistics involved when transferring the processes and operations to the Back Up Site. Formulate the details as to how, if the Primary Site is shut down, the transfer will be made to the Back Up Site. Include which employees will be utilized at the Back Up Site (do not have all employees at the Back Up Site) how the Paper and Electronic Backups will be transported, and which processes and operations will resume at the Back Up Site. For example, which critical processes will be necessary to resume, as you will only have a limited number of employees to monitor them.

Conclusion

This article reviewed the Importance of a Security Policy; the Need for a Risk Assessment, and the Security Policy Model.

Whenever an organization or business considers an overall Security Strategy, the Security Policy is the first item which needs to be addressed and formulated. The Security Policy sets forth the level of Security Consciousness among employees, and is the first thing an organization or business will rely upon if faced with a Major Security Threat or Risk.

Ravi Das is a Consultant for HTG Solutions and launched its security solutions division in January 2003. His previous positions involved Software Configuration Management and Database Management and Administration. Das has published articles worldwide about biometric technology. He holds a MS in Agribusiness Economics from Southern Illinois University, Carbondale; and a MBA from Bowling Green State University. He can be reached at: rd@htgsolutions.com