Asset Protection through Security Awareness

Protective Measures

Both physical and informational assets need to be protected from internal and external threats. It is interesting to note that regardless of which type of asset an organization is trying to protect, the approach to protecting them is very similar. Because we live in a physical world, everything, even data, will exist in its most basic form at a physical level. Engineering designs, human resource records, customer service notes, production methods and procedures, all exist in the physical realm. Therefore, it is important to implement technical protective measures, physical protective measures, and personnel protective measures (see Figure 1.1).

Technical Protective Measures

First on the list of means for protecting networks and data are technical protective measures. Let us consider technical protective measures to include any measure directly dealing with the transfer of digital data, including digital firewalls, network intrusion detection systems, antivirus programs, network traffic sniffers, penetration testing,
Ten Steps for Promoting Security Awareness

ACKNOWLEDGE SECURITY ISSUES
Analyze the current state of the organization to determine and make a list of what security issues currently face the organization.

ACCEPT RESPONSIBILITY
Organization’s cannot simply ignore security issues, but must accept responsibility and own the process from the beginning to the fruition of a Security Plan and provide proper training.

ASSESS RISK
Without performance of a clear risk analysis, the creation of Security Policies will have no good foundation.

CRAFT SECURITY POLICIES
Using the Risk Assessment as a guide, the organization should build appropriate security policies to protect the organization while safeguarding the organization’s finances.

TRAIN AT ALL LEVELS
Make sure all employees are aware of the expectations and requirements for their position in the organization.

CREATE BENCHMARKS
These benchmarks will be central to appropriately monitoring the successes and opportunities for improvement within the organization, and should be clearly established before any audits are performed.

PERFORM SECURITY AUDITS
Auditing the security functions of an organization are key to staying on track.

ENCOURAGE SECURE OPERATIONS
Don’t simply provide negative consequences for employees who breach established security protocols, but also be sure to provide incentives for those personnel who appropriately implement the required security procedures.

ASSEMBLE A SECURITY TEAM
The organization’s Security Team should be inclusive of people from all portions of the organization, but everyone on the team should have a solid understanding of network security operations.

PLAN FOR DISASTER
Have backups and contingency plans in place for major systems to ensure minimal down time in the event of a disaster.

Figure 1.2 Promoting Security Awareness

backup media, cryptographic measures, forensic software applications used to retrieve deleted or destroyed data, and wireless encryption, just to name some of the measures a company can implement. These are all necessary, but are inadequate without their cousins, physical protective measures and personnel protective measures (see Figure 1.2).

Some information technology (IT) professionals are excellent at making certain their networks have the latest technical protective measures in place. These technicians pride themselves on how few
viruses have successfully invaded the network, and are gurus of network security. Security patches are regularly installed, and networks are constantly monitored. There is no activity on the networks that goes unnoticed by the eyes of these IT professionals.

Although these IT professionals are excellent at keeping digital data secure from would-be cyber criminals, there is sometimes a dearth of actual physical security. So great can the lack of physical and personnel security be, that sometimes all of the digital fortress buttressing accomplished by the IT personnel only serves to provide an illusion of security, when in reality the networks are wide open to attack by internal threats.

*Physical Protective Measures*

When we stop to remember stored data are simply ones and zeros, it is quickly understood that all data are physical. These ones and zeros are all stored on physical hard drives, which need to be physically protected from external and internal attacks. Sensitive company records must be kept on databases, which will usually reside in a physical server room. Secure walls, ventilation, fire suppression systems, doors, and locks are among some of the requirements for properly securing an organization’s server room. Without proper physical security in place to stop unauthorized individuals from accessing the server room, the databases contained on the server hard drives are as good as public knowledge. The same goes for the computers, routers, monitors, and other physical parts of the network infrastructure. It doesn’t matter how good the firewall installed at a network’s gateway to the Internet is; if a computer’s disk drive is not physically protected, an unauthorized user can easily upload malicious software directly onto any one of the computers from inside the gateway, and all data contained therein will be compromised.

*Personnel Protective Measures*

Personnel protective measures deal with what can sometimes be the greatest risk to an organization’s network, the end users of the network and computers. Whether through incompetence, poor training,
genuine mistakes, or truly malicious intent, end users wield an amazing amount of power over the networks on which they work. Through the design and implementation of good policy, many of the threats posed by end users can be mitigated, managed, transferred, and, in isolated cases, completely eliminated.

**Mitigating Risks Associated with Personnel** There will always be a level of risk associated with hiring someone and allowing him or her access to an organization’s network. Accepting this risk is a part of doing business, however, managers can mitigate some of this risk by requiring employees to complete a thorough pre-employment process. This process should include several items to improve the chances of success. First, the interview should include a skills assessment test, to make certain the incoming employee has mastered at least the minimum skillset required for employment. In addition, if the employee has achieved that minimum level of skill, it can be safely assumed she will be able to learn more, and further training as required by her job will not be in vain.

In addition to a skills test, a background check is a good idea for anyone who could possibly come into contact with a computer. A background check should be considered an absolute must for any employee who will be handling money, employee health records, or customer credit card information. There are many companies specializing in providing low-cost background checks with near immediate results, so cost and time should not be a consideration when deciding to implement this step of the hiring process.

Another frequently forgotten and neglected aspect of hiring is the checking of references. If references are listed by an incoming employee, call them. If references are not given, ask for at least three, and then follow up by checking them out. If references are not provided when requested, don’t hire the person. It is better to regret not hiring someone who “felt” like a good fit, than to hire someone and find out later he has seriously jeopardized the security of your organization. Many security issues can be avoided by thoroughly vetting incoming employees, so whatever other security choices are made at your organization, make absolutely sure these are strictly adhered to, without exception.
**Managing Risks Associated With Personnel**  Managing threats includes proper security training, implementing continual reviews of processes, and regularly scheduled auditing of security systems.

Once an incoming employee is properly vetted, the next step in her process as a newcomer to your organization should be training. Training should not only include how to perform the requirements of a job, but should also include a complete review of the organization’s security policies. Wherever appropriate, security should be discussed and woven into each facet of an employee’s job.

**Transferring Risks Associated with Personnel**  One of the options when managing risk is the transference to another entity. This transference of risk usually occurs in one of two ways. Either the authority over and responsibility for key processes are given to another entity, or insurance is purchased. For instance, third-party firms specializing in customer service can handle incoming calls and issues from customers. Human Resource consultants can be hired to handle many of the HR concerns of corporations, such as providing HIPAA-compliant health record management for employees. Accounting firms are available to provide fiscally responsible and security compliant handling of company financials. Manufacturing companies hire third-party vendors to build components and subcomponents of products to lower overhead costs, but they also realize security benefits associated with having fewer internal employees directly interfacing with the company networks.

**Eliminating Risks Associated with Personnel**  Firing an employee who is known to present a specific threat to the security of a company and its assets is one method of eliminating a single threat. However, because people are dynamic, the requirements for dealing with personnel-related risks will vary from day to day, but cannot ever be fully eliminated.

**A Culture of Security Awareness**

It is the belief of the author that if true security is to be realized in any organization, a culture of security awareness must be encouraged at all levels, from the top down. Regardless of the industry in which an
organization operates, there are trade secrets, personnel information, customer information, and proprietary data that must be protected. At virtually every level of operation, people must be careful to protect the assets and interests of the organization they serve. This care will most effectively be derived from a workforce whose culture includes an awareness of security issues.

Creating or altering a work culture is not as difficult as it may seem. Knowledge is at the core of building a workforce aware of security issues. The facts regarding organizational assets and the potential risks facing them should be known by employees using and interfacing with those assets. Once this knowledge and care pervades every facet of the organization, employees will find themselves immersed in a culture of security awareness.

Education Is Key

Perhaps the most effective security measure one can put into place is simply educating employees about the inherent risks associated with any given activity. Making the workforce aware of information security issues is an essential cornerstone of a holistic approach to securing an organization’s data. Similar to educating production workers about machinery and processes that may cause damage to the product or harm employees when misused, educating today’s workforce about the inherent risks of simply using a computer will give employees the necessary tools to keep company and personal information from harm. Once aware of these risks, people will be more mindful of the potential harm, and will be forced to change their habits in order to be more circumspect.

Creating the Culture

Every organization has its own unique culture, language, and methods of operation. In order to infuse every level of an organization with security, the culture must adapt to embrace new and potentially difficult ideas and policies. There are several steps and layers necessary to create and maintain a culture of security awareness through the ranks of an organization. These steps include:
1. Acknowledging security issues
2. Accepting responsibility
3. Assessing risk
4. Crafting security policies
5. Training at all levels
6. Creating benchmarks for success
7. Security audits
8. Encouraging secure operations
9. Building a security team
10. Planning for disaster

Acknowledging Security Issues

Part and parcel of fostering a culture of security awareness is the acceptance of the real dangers facing anyone whose computer is connected to the Internet. It is no secret that the simple act of connecting a computer to the Internet immediately places all of its contents in peril of being compromised. Every computer that has a connection to the Internet is already sitting on the front lines of our cyber defenses. Our world will only continue to become increasingly interconnected via the Internet as time marches onward. The vast majority of businesses will eventually suffer considerable financial loss due to a cyber attack. This financial loss will be realized in costs associated with sidelining labor into fixing inoperative software applications, filtering e-mails, and reformatting systems, among many other reactive measures. The reality of being attacked by a cyber criminal is a very real and present threat that faces any network today.

The recognition of this threat is evidenced by the birth of entirely new industries dedicated to the protection of data. Several billions of dollars a year, in fact, are spent on securing networks and protecting proprietary information contained within company networks. Entire corporate departments are dedicated to securing data; academic programs that focus on computer protection have been created; and books such as this one have been written; all toward the end of helping organizations, end users, programmers, and anyone who otherwise comes into contact with the Internet keep their digital assets safe. The sooner we all accept the fact that the responsibility of protecting these assets lays within our own hands, the sooner
our information will be secure from the myriad threats that face us whenever we interact with the Internet.

Accepting Responsibility

At first blush, it may seem self-evident that protecting the data on our own computers does and should fall within our own realm of responsibility. Although some may see accepting this responsibility as a foregone conclusion of owning a computer, the world of information security is such an abstract and unique phenomenon that it deserves a bit more attention and thought.

Physical Security Versus Information Security  If we stop and think about the physical world, we will quickly realize that we really play a much smaller role in protecting ourselves there than we do in the digital world. Police officers, military personnel, and the entire combination of societal and governmental assistance are at our sides whenever we step outside our homes. We usually don’t worry about being attacked while in public because we live in a generally lawful society, which does not allow for rampant violence and physical intrusion into each other’s lives. If we are ever unlucky enough to be the victim of a physical assault, our court systems are designed around and capable of understanding and dealing with physical crime. In addition to the structures of laws and the executive enforcement of those laws, there is a strong social aversion to such unlawful physical behavior. In most cases, if someone accosted you at a grocery store without cause, strangers would rush to your aid in some form or another. They might assist by trying to stop the attacker; they might follow the attacker to his or her car and write down a license plate number for the police to handle later; or they may simply offer you condolences and assistance in getting things together after the attack.

The Unseen Digital World  This same societal structure within which we can feel relatively secure in the physical world simply does not exist in the digital world. This is primarily because the digital world is essentially unseen. Attackers can attack at random and with anonymity. The technology used to attack is fairly new and always changing, so there is even a chance laws may not exist to prosecute digital criminals
when and if they are caught. Even if the criminal is caught, which is highly unlikely, and even if there are laws on the books that apply to the crime committed, the criminal may not be in the same country as the victim, and could avoid prosecution altogether. This is the elusive, anonymous, and frustrating world of digital crime. Organizations and individuals cannot rely upon social structures, laws, or other existing barriers to protect their data. Instead, the responsibility for protecting data must be accepted by the owners of the data. Once responsibility of protecting assets in the digital world is fully accepted, the data owner must assess the risk associated with the data being protected.

Assessing Risk

In order to provide proper and reasonable protection of the data in question, the data owner must first figure out exactly what he is trying to protect. Archived files, personnel information, customer information, and proprietary processes all need to be protected. Of course, depending upon the type of organization you are in, you may be charged with protecting different types of assets. Deciding exactly what will be protected, and how, involves creating a list of assets, identifying the risks posed against those assets, and deciding how best to deal with those risks. See the chapter on risk management for more details on this process.

Crafting Security Policies

Once the assets and risks are documented, policies designed to protect organizational assets must be created and put into action. Successful policies cannot be arrived at quickly and with little thought. The policies must be thorough, but not so mired in minutiae as to create an environment so burdened with details that the “real work” of the organization cannot occur. When designing security policies, be sure to make every reasonable effort to make the policies easy to apply and practical. Remember to craft your security with the appropriate attention paid to each level of security. For instance, don’t try to reproduce the security of Fort Knox if you are in charge of a small company and want to protect a certain manufacturing process from your competition. It cannot be stressed enough that policies should flow with the
workflow, not bring it to a screeching halt in the name of security. Instead, make sure the policies complement the existing procedures. If policies are forced upon employees and don’t feel like a natural part of their daily processes, they will be far less likely to adopt them into their normal operations. More on creating security policy can be found in the chapter about crafting a security policy.

Training at All Levels

Once policies are created, employees at every level of the organization must be trained on the policies. A thorough training program will educate employees on the reasons why certain policies are being put into place. By trusting employees with the full picture, they will not only feel valued, but they will have a deeper understanding of how best to protect the assets they are charged with in their daily operations.

It is important not to forget that everyone in the organization must be trained on the policies of their departments and individual roles in the organization. Everyone from the CEO to the customer service representative must be properly trained on how his or her individual position in the company affects the bottom line in terms of security. If one person fails to perform the steps necessary to secure the assets with which he works, a hole in the organization’s security will open, and a successful attack upon the organization’s data will be far more likely. For this reason, seniority and position within an organization should never be allowed to override the security measures put into place. A good training program will take this into account and will provide an organization with a solid framework of security throughout the corporation.

Creating Benchmarks for Success

Before an organization can determine if policies are actually working, benchmarks to measure against must be put into place. These metrics and benchmarks can be used later during audits to determine successful policies as well as problem areas needing further attention and improvement. It is critical for organizations to quantify success in an accurate and meaningful way. Otherwise, the efforts your
information security team are making may not be making an impact where it is most needed. See the chapters on metrics and auditing for more information.

Security Audits

Like water, people like to follow the path of least resistance. Over time, if a policy is not enforced, it may or may not be followed depending upon how easily and naturally it fits into daily operations. Using benchmarks created in the preceding step, audits can be performed, which will build a good picture of the state of security within an organization. After this picture is formed, areas for improvement can be clearly seen and appropriate measures may be taken to remedy any problems affecting security. See the chapter on security audits for more details.

Encouraging Secure Operations

It is important to create an environment where employees feel both empowered and encouraged to implement security measures. Individuals will respond far better to rewards and recognition for success rather than being scared into compliance with the threat of losing their jobs. Be sure managers acknowledge employees who are keeping the organization safe and saving money by successfully implementing security policies.

Building a Security Team

A security team should be made up of representatives from all portions of the company who are properly trained in information technology and information security (IS) in general. These don’t necessarily have to be IT or IS professionals, but may be people from anywhere in the organization who have a passion and talent for keeping data safe. See the chapter on security teams for more details.

Planning for Disaster

No matter how thorough policies are and no matter what steps are taken to mitigate risk and train employees, organizations should be
ready for disaster to strike. Disaster may come in the form of a successful software virus that takes down a main server, or it may be a natural disaster that strikes the campus of the organization. All sorts of events might qualify as disasters, and all reasonable steps should be taken to plan for such events. See the chapter about disaster planning for more details.

Remaining Dynamic

One of the main factors pertaining to the creation of a successful culture of security awareness is the ability of an organization to remain dynamic in the face of changing industries and technologies. An organization should not simply put policies into place and put the issue of security to rest. Instead, a continual review of policies and their effectiveness should be instituted. If a policy isn’t working, or if a piece of technology is not providing the operations your organization requires, change it! This goes for functionality as well as security.

Security is worthless if it prohibits employees from performing their job functions. An extreme example is an unplugged computer without wireless access. Sure, the computer would be secure from attacks over the Internet, but it would not allow the user to actually use the computer in any meaningful way. In an effort to stay dynamic and improve productivity while maintaining the best possible security, be sure to listen to employees on the “front lines.” The end user, or the person who is actually using the computer, knows what security policy does to productivity. You may have created Fort Knox in the server room, but if you cannot service any computers because of all the physical security, you have lost the fight and the cyber criminals have won. Whether you are a service-related nonprofit or a for-profit business, make sure that whatever policies are put into place, they do not hurt your organization’s bottom line. Staying dynamic in your approach will allow your organization to adapt to security needs while protecting that bottom line.