

A company's proprietary information is its most valuable asset. Since the inception of commerce the protection of this asset from theft or destruction has been of the highest priority. With the advent of Information Technology, clandestine attacks on this asset have grown in sophistication and maliciousness. One method of these attacks, in the form of "viruses" and "worms", may not even be targeting your business, but can still have a devastating effect if allowed to infect your IT infrastructure.

The best defense against these attacks is a good offense. This comes in a five pronged approach. First, assess the vulnerabilities and risks. Second, create company policies designed to mitigate the vulnerabilities and risks. Third, protect your assets by strict implementation and enforcement of these policies. Fourth, institute a method for monitoring policy compliance and the detection of successful as well as failed attacks. Fifth, create a plan to recover from successful attacks and modify policies to help protect against similar attacks in the future.

IT infrastructure vulnerabilities are divided into "internal" and "external" sources. According to the SANS (SysAdmin, Audit, Network, Security) Institute, the greatest source of attacks on IT systems are "internal" (from inside your own organization). Nearly all of these are unintentional and typically work by exposing system vulnerabilities to external sources. They usually occur because policies do not exist, are insufficient, are poorly implemented, or not enforced. SANS has developed a comprehensive collection of IT policies which can be found at www.sans.org/resources/policies/. These policies provide an excellent starting point for creating policies specific to your business. **But remember, having policies in place does no good if they are not implemented properly and strictly enforced.**

The following paragraphs cover critical issues that should be covered in your corporate IT policies:

Physical Security

Servers

If anyone, be they a thief or personnel, has physical access to the servers, company data can be stolen, compromised, or destroyed. If the server or the disk drives can be removed from the site, any number of methods can be employed to access the data. Ideally, all servers should be physically located in a locked, sealed area and access should be limited to a very few key personnel. This reduces the risk of malfeasance or simple unintentional acts like unplugging or rebooting servers. This will also reduce the temptation to use the server as a workstation which beside impacting performance, could lead to inadvertent changes in the server's operation or even the infection by a virus or other malware. The most sophisticated "server rooms" use keyless or biometric entry systems with access logging; have alarms for unauthorized entry, flood, and fire; and have Halcyon based fire suppressant systems. This is extreme for most small businesses, but even so there could be business requirements demanding this level of protection.

Laptops

Laptops are great for traveling personnel, until they are lost or stolen. Laptops that connect to your internal network contain quite a bit of information that could be used to gain access to and compromise your network. Thus, consider laptops to be a high security risk and should be assigned higher protection features. If lost or stolen, the passwords of user accounts that have used the laptop should be immediately changed. Users that use laptops should have very strong passwords and they should be changed frequently. Also, the password for the local administrator should be unique for each company laptop.

Mobile devices

These devices are vulnerable from hijackers on IR or bluetooth to virus and other malware attacks sneaking back into your company network. Theft can compromise company information like your contact list that is synchronized from your CRM or Email clients like Outlook. Likewise, passwords used in the operation of mobile devices should be changed immediately if the device is lost or stolen.

Acceptable Use Policy (AUP)

The purpose of an Acceptable Use Policy is to delineate the acceptable uses of the company IT system by company personnel. The rules are in place to protect the employee as well as the company. Inappropriate use exposes the company to risks including compromises to the IT infrastructure and legal issues. The policy should contain sections on what is and is not permitted including, protection of company information and passwords, electronic communications (e.g. email), as well as monitoring by the company, enforcement, and the consequences of non-compliance. All company personnel should be required to sign a copy of this document. For an example, refer to: www.sans.org/resources/policies/acceptable_use_policy.pdf and www.sans.org/resources/policies/email_policy.pdf

Accounts, Permissions, and Passwords

Accounts are the cornerstone of IT security. They come in three flavors: system, service, and user. System accounts are used for installation of hardware and OS level software on individual servers or workstations and should never be used for other purposes. Service accounts are used by network services and applications to access other services or to do scheduled tasks (e.g. backups). User accounts are used by personnel in the performance of their tasks. Accounts are assigned "permissions" giving the account access to the resources needed to perform their assigned tasks. Best practices dictate the creation of "Security Groups" for specific functions. The principle of "Least Privilege" should then be employed and the group assigned only the minimum required permissions to perform that function. Accounts are then associated with security groups that are required for the performance of a user's or service's tasks.

Passwords are assigned to individual accounts and are stored using encrypting technology. Passwords have three properties: length, strength, and age. Length refers to the number of characters. Strength refers to the different types of characters and the complexity of the combinations of those characters. Age describes the span of time within which the password can be used before change is required. A company policy for passwords is essential for good security. For more information on passwords, refer to: www.sans.org/resources/policies/password_policy.pdf.

Protection from External Attacks

The only sure way to prevent external attacks is to never connect to the outside world (Internet). In today's business environment this is neither desirable nor practical. So as a compromise, isolating the company internal network from the Internet is accomplished through the use of "firewalls". Firewalls come in hardware and software (running on a "proxy" or ISA server) varieties. The best solutions use a combination of both to provide the most flexibility, control, and isolation. Policies for accessing the internal network through the internet are a good idea. http://www.sans.org/resources/policies/virtual_private_network.pdf, and for mobile computing, http://www.sans.org/resources/policies/remote_access.pdf, are good examples.

Last but not least, no IT system should be without an enterprise wide version of an **Anti-Malware** solution. One preventable infection could easily cost as much to remedy as several years of licensing and administrating of such products.