

American Heritage Protective Services

“A Guide to Cyber Security”

Information system attacks on the small to medium-size business communities are on the rise. Currently, it is estimated that up to one-third of these enterprises have been affected or victimized by computer viruses.

Over the past decade, the frequency of computer virus attacks and the monetary losses associated with these events have dramatically escalated. In the mid-1990's it was estimated that the business community lost slightly less than one billion dollars to cyber security breaches. Business losses to cyber events now exceed several billion dollars each week. Even though larger enterprises can lose more in total dollars, the loss to small and medium-sized businesses can be more severe due to the smaller profit margins these businesses typically operate under.

Smaller businesses can implement proactive measures to decrease their vulnerability that are not necessarily costly in terms of dollars. Business owners and managers should be aware that the consequences of a cyber attack can run the gamut from minor inconveniences to financial devastation. Be mindful that while a burglar can break into only one business at a time, a computer hacker can simultaneously damage an infinite number of computers and networks. If your business uses the Internet, you are vulnerable

to cyber attack. However, by implementing the following recommendations, your enterprise can significantly reduce the risk of a cyber event.

Anti-virus Software

Anti-virus programs are typically the least costly means to protect your computer or system from cyber threats. Although a virus can infect a computer in a number of ways, presently the most common method is through e-mail attachments, which infect a computer or system when they are opened. Once a computer is infected with a virus, not only can it disable and/or destroy data, the affected machine will probably attempt to infect other machines and systems.

Installation of an anti-virus program, on every machine, kept up-to-date through supplier provided updates, is one of the best defenses that can be employed. A computer that is not loaded with anti-virus software should never be connected to the Internet.

Equally important is training all computer users within a business on how to remove or destroy infected files discovered by the anti-virus software. If your enterprise is networked, all computer users should be familiar with the procedures to isolate a machine from the remainder of the system. To limit the chances of a virus being set free within the

network, computer users should also be instructed not to open any e-mail attachments from unknown sources. If there is ANY doubt as to the authenticity of an e-mail, the message and any accompanying attachments should be deleted and the deleted items file on the machine emptied as well.

Lastly, to discover any problems that may have been overlooked at other check-points, a procedure should be implemented to require anti-virus examinations of all files on a periodic basis.

Firewalls

In essence, a computer firewall serves as a security guard for the computer. It examines both the messages that enter the machine from the Internet and messages that are sent from the computer. Firewalls determine what messages should continue from their origin point into the computer or be stopped. They can also be valuable in limiting the volume of potentially malicious messages that enter a computer while preventing unwanted access to a network.

A computer or network that is connected to the Internet should not be operated without a firewall in place. Without this safeguard, potential attackers can easily analyze a machine and locate its vulnerabilities. With nothing in place to monitor the information entering or

exiting the computer or network, the machines are completely reliant on individual users to exercise caution and good habits in their opening of e-mail messages or downloading of information.

When selecting a firewall, the most desirable products on the market are those that offer the option of easily reviewing each piece of information attempting to enter the computer or network. Once in place, company management can use the product to enforce an acceptable use policy. Subsequently, they can block access to websites that may be considered inappropriate for business use, such as shopping, gambling or pornography.

It is imperative that all employees are educated about the importance of a firewall. Additionally, employees should be given the opportunity to assist owners/managers in refining the company policy relative to the firewall. This will discourage the intentional disabling of the product. Employees should be trained on how to respond if a computer or network becomes infected and have a working knowledge of how to download security patches from software vendors, update virus protection and create appropriate passwords. Individual passwords should not be shared amongst employees and should be changed on a regular basis.

Just as an owner/manager would not provide keys to the business to a stranger, access to the computers should not be shared either. Computer operating systems should be checked to ascertain whether or not they permit outsiders to access the hard-drive. As a best practice, unless there is a need for a business to have the ability to share computer files, this capability should be eliminated.

Computer Security Practices

As a general rule of thumb, when clocks are changed to reflect Daylight Savings Time, an evaluation of computer security should be conducted. Security settings for the programs and operating systems should be adjusted based on experiences during the preceding six months.

Just as most businesses use multiple security systems for the physical protection of their facilities, in today's day and age, computer security systems should also be increased or tightened. Anyone with access to an enterprises' computer equipment, in essence, has the opportunity to bypass security measures, as well as to observe, change or destroy stored data. If not already in place, employee policies should be implemented and/or updated to require:

- *Users leaving computers unattended should log-off the system or all machines should have a screen lock system installed*
- *Direct assignment of accountability to employees for access to company computers and any equipment taken off-site*
- *Restriction of an employee's personal use of a company computer*
- *Establishment of procedures for corrective action when employees fail to abide by company computer use policies.*

In the course of evaluating the security of an enterprise's computers, a review of data back-up procedures should also be conducted semi-annually. Virtually all computer users, at one time or another, have experienced the pain of losing valuable data. Consequently, consideration

should be given to implementing procedures that require the back-up of all data, on at least a semi-annual basis. When data back-ups are completed, it is recommended that a separate copy of the data be securely maintained at an off-site location. In the event of an in-office catastrophe, the back-up data will not be lost. Corporate insurance policies should also be reviewed to determine whether intellectual property, data and information systems, as well as the computer hardware are covered for loss.

Cyber Security Alerts

To stay aware of the latest developments in cyber security, all small and mid-size business owners and managers should subscribe to the free U.S. Department of Homeland Security National Cyber Alert System. It offers time sensitive information relative to cyber threats and provides valuable tips on how a business can protect itself in cyber space. The National Cyber Alert System can be reached through the United States Computer Emergency Readiness Team (US-CERT) website at www.us-cert.gov.



Contributed by
Stephen J. Pollak
Executive Vice
President

AHPS Can Help

For assistance in the creation of a crisis plan for your business call American Heritage Protective Services toll free at 866-830-1800. Visit our website at www.ahpservices.com.