BACKGROUND ON BUSINESS

Beefing Up Your Company's Security "Playbook"

by Manny Novoa

(NAPSA)—The shift to a digital, mobile and virtual world means that even the smallest businesses are increasingly at risk from cyber threats.

Other factors that motivate companies to deploy IT security solutions include SPAM prevention, desire to reduce the risks associated with Web-based business operations and regulatory compliance.

The Sarbanes-Oxley Act, for instance, has a provision mandating that CEOs and CFOs attest to their companies having proper "internal controls." If a company's IT system is not secure, then management is at risk signing off on internal controls, so it becomes necessary to ensure auditable security measures are in place.

While many smaller business owners now understand the need for increased IT security measures, it may be confusing trying to determine where to begin. The following are four critical areas to help small and medium businesses (SMBs) beef up their security "playbooks."

1. Build your offense.

The most crucial component of securing your business is to develop a security program that educates you and any employees on the vulnerabilities of technology, and puts in place processes to help avoid risk. No matter how much secure technology you have in place, you can't be safe without support from your technology users. A robust security governance policy, including basic IT security training for all new employees and strict user access policies, is also key.

Your governance policy should cover the basics such as "thou shall not post your password next to your monitor, open suspicious looking e-mail or give *anyone* your password, or thou shall be fired," to ongoing education about the latest external threats. It's also wise to set specific access rights to help prevent employees from inadvertently giving outsiders access to sensitive information, and to potentially protect from malicious insiders.

2. Block and tackle.

The key to protection from external threats is to have several layers of defense. As the magnitude of e-mail virus damage has proven, humans are fallible, so barriers such as firewalls and virus software are a must.

Additional hardware-based solutions can provide added data protection—especially important for portable devices. In the case of theft, it's the DATA on the system that becomes the clear concern, not so much the loss of the actual device.

For example, HP's ProtectTools portfolio includes Embedded Security and Smart Card solutions for select HP business desktop and notebook PCs. HP's ProtectTools Embedded Security solution can protect user data and access to the system by using an embedded chip for added data encryption. The HP Smart Card security solution uses a credit-card-like security device to make system access more secure, by combining something the user has (a Smart Card) with something only the user knows (a password/PIN).

3. Keep on your toes.

Sometimes glitches are discovered in software that may leave a system or network vulnerable to attack, so ensuring timely patch management is critical. Even a virus utility or personal firewall is only as good as the last update for "known" attacks. Proactive policies must be put in place to "force" users to update these periodically or automate that update process. IT vendors offer technology patch management solutions, such as HP's Client Management Solutions, to facilitate this process and help automate IT systems updates.

4. Have a strong second string waiting to take the field.

A final recommendation is to have a consistent data backup program. Daily data backup to an onsite, or preferably off-site, storage solution can protect a company from losing significant portions of its critical financial data and intellectual property in the event of a security breach.

Look for PCs that offer local recovery, like that provided by Altiris on HP desktops, to prevent loss of individual user data in the event that an employee opens an infected e-mail that destroys information on his or her system. A company can usually recover from loss of one day's data, but loss or damage of all electronic company information can be devastating for a small business.

Manny Novoa is a distinguished technologist in HP's Personal Systems Group.