Education counts in the cyber wars: prevention begins on the home front

By Konrad Martin

News of global cyber attacks have businesses, institutions and individuals on edge. People understand just how serious a threat it is. The percentage of middle market businesses now carrying some form of cyber liability insurance has jumped dramatically in the last decade.

Yet, while insurance is important, prevention is preferable. Businesses should do everything possible not to find themselves in the position where they need to use the insurance they have very wisely purchased.

Famous last words: If you have anti-virus and anti-malware, the last thing you need to worry about is a virus infecting your computer, right? Wrong. Hackers don't sit at home thinking they can't get around the latest virus and anti-virus protection and give up. They are extremely sophisticated and clever criminals that continue to create new ways to trick you. They make a fortune by stealing your information. So even though you have the latest anti-virus protection (which you should!), they are already figuring out ways to trick you into inviting new viruses and malware into your system.

The strongest, and best anti-virus protection is only as good as the team using it.

Two specific threats are widespread in the business world: ransomware and spear phishing. By staying educated on these technological scourges, you should be able to identify and avoid them.

Ransomware is just as it sounds: a virus that infects a system through an unsuspecting user clicking on an attachment will start looking for data to encrypt. Once it does, that data can only be unencrypted with a private key, held by the hacker who holds that information ransom. Typically the hacker will request the ransom payment in bitcoins (a form of cybercurrency), and because the payments are usually a relatively small amount, it tends to be easier to pay the ransom than restore all the files from backup.

Spear phishing is a new twist on an old trick. A phishing email tends to ask questions that seem okay to answer, or tries to entice you into clicking on an attachment because it says it includes information about an IRS refund or package tracking. Spear phishing is a technique where the email appears to come from someone you know, usually in an authoritative position, telling you to transfer funds or click on an attachment. To the recipient of the email, the email looks legitimate. However, the email is actually coming from criminals using a technique to capture the boss's email and then, for example, request that tens of thousands of dollars be transferred to fictitious bank accounts. Once that money is transferred, it is almost always gone. Or the case where "the boss" asks an employee to send him several dozen W2s. Then, once done, that opens a Pandora's Box of legal and financial problems for the company and the people whose information has been breached.

There is no magic anti-virus protection that can cover all dangers. The best protection a business can seek is through education, supported by awareness, training, and policies. End users must know that even the most harmless-seeming email, website, FaceBook post, or article can contain a virus or malware. Read carefully before clicking – and if there is the slightest doubt, don't do it! Usually, there is something that seems out of place. The grammar is a little off, you were not expecting a refund from the IRS, or you haven't ordered anything that you need to track. With awareness, training, and effective policies, something in a hacker's attempt will usually jump out at you. That is how to prevent these nasty viruses and malwares from locking up your systems and costing you thousands and thousands of dollars in downtime and ransom money.

When in doubt, call the person you believe the email is from and ask "Did you send this?"

Here are a few steps that you can take as a business owner to lower the risk of being hacked.

1. Tell your employees that if an email looks even mildly suspicious, do not open. Forward to y our IT department for evaluation.
2. Develop strong passwords for your company. So many times people use passwords like "123456" or "letmein" or "password." Hackers know the common ones; yours should have a variety of characters, including symbols.
3. Consider a cloud-based data protection system to supplement a strong password policy. There are companies which will do this for you for a reasonable monthly amount.
4. Avoid "free" offers. They are potential trouble.
5. Develop and enforce a strong policy regarding employees using their personal devices. Whether that's a tablet, a home computer, an iPhone, every device connected to the company infrastructure offers hackers yet another opportunity to get inside. If you do allow employees to use their own devices, you have the right, and the obligation, as an employer, to tell them what they can and cannot visit and access.
6. Train your employees. Partner with a strong IT consultant who is knowledgeable and can spend time with your employees to help them identify and avoid threats to your infrastructure.
7. Consider running vulnerability assessments against servers, workstations, and networking equipment to ensure risks from vulnerabilities are mitigated.
8. Have a strong backup system for data, in the cloud.
9. Be sure that your Written Information Security Plan (WISP) is up to date and that your employees are familiar with what they can and cannot do.

Education is key. Knowing that there are threats out there and how to recognize them will save your company both time and money – and help you to do what you do best, running your business without interruption.

(Konrad Martin is CEO of Tech Advisors, http://tech-adv.com, with offices in Medfield and Boston).