By Mary Siero

WILL SUPERIOR TECHNOLOGY WIN THE CYBERCRIME BATTLE?

We all want to believe that good will triumph over evil. If only we work harder, smarter and faster we will always win, won't we?

What we don't often think about is when Internet computing took off around 1990, malware had its beginnings too. That year, experts estimate around 1,300 different pieces of malware were released into the Internet. Fast forward to 2012, and you'll find that malware releases into the Internet have increased to a point where about every 6 seconds a new malware is released. It's pretty hard to stay in front of that curve. Industry statistics show that even the best anti-virus software will only catch between 15 percent to 30 percent of malware that is out there.

This explosive growth is the result of the cybercriminal enterprise increasing in sophistication and moving to automation. They have learned how to automate everything, from scans to find vulnerable devices or software on your network to attacks.

Unfortunately, the private industry is still working in a manual detection and prevention world creating a huge disconnect. The outcome is that most people will most likely suffer an attack at some point.

One of the more recent malware attacks was reported in May 2012. The FBI reported that cybercriminals were targeting hotel guests using a pop-up window that appeared when the hotel guest logged onto the hotel's Internet system. The window advised the traveler that he or she needed to perform a routine update to a widely used, legitimate software product. When the guest clicked to upgrade, malware was downloaded onto his or her laptop. Another well-known attack on hotel guests has the cybercriminal sitting in the hotel parking lot, broadcasting a wireless signal stronger than the property's and that has a name that sounds like your establishment. When the guest connects to that wireless network (which they think is the hotel's), he or she is taken to a fake Web page made to look like the properties Web page, where the cybercriminal can capture credit card numbers or any other personal data the guest enters through that connection.

In its 2012 Data Breach Investigation Report, Verizon reported that the most afflicted industry with regard to breaches of data, for the third year in a row, is the accommodations and food services industry. Likewise, another major 2012 Data Breach Report published by Trustwave, echoed that finding and reported that more than one-third of breaches in this industry represent franchised businesses. Cybercriminals who target franchise operations have the advantage of finding one vulnerability that they can then exploit across many locations or entities.

The question then is not if you will be breached, but rather when your data is compromised. Developing a solid incident response plan can be the difference between a minimal business disruption and a major loss of business.

An organization's plan should start with end-user security awareness training (the No. 1 recommendation by I.T. security firms) so that employees know how to recognize an incident. Rapid identification and reporting of an incident significantly increases the chances of a successful resolution and minimizes not only the data loss but also the reputational damage to an organization.

Understanding the appropriate escalation procedure and tasking a key management employee with the responsibility of decision making during a cyberemergency are two additional vital steps that can facilitate a quick, effective and orderly response.

Make sure that incident response team members are identified and that their roles and responsibilities are clearly outlined. Also, ensure that they have the required training to perform their duties in these matters. For example, turning off a PC that has been compromised may impede an investigation because vital data in the cache will be lost. Training a key technical staff member on what to do before computer forensics investigators arrive could be the difference between quickly resolving an incident and suffering from it for an extended period of time.

Finally, post-breach public relations are critical to insure that guests retain confidence and trust in an organization. It is more than just knowing and following the breach notification laws in the states of the affected customers; it is projecting to the customers or guests that the property or organization has the skills to manage the crisis. It is giving them the confidence that trust in the organization will not be misplaced, which will make your organization worthy of future business.

In every incident there are lessons learned. Use these lessons to grow the employees' skill sets and improve security awareness training.

MARY SIERO, *CISSP, CISM, CRISC, is the president of Innovative IT in Las Vegas, www.iitlasvegas.com.*

In May 2012, the FBI reported that cybercriminals were targeting hotel guests using a pop-up window that appeared when the hotel guest logged onto the hotel's Internet system.