Defending Your Networks

Whether it's from overseas governments, disgruntled employees or poor security, cyberattacks and data breaches continue to harm businesses.

By Brian Branner

In the battle against cyberattacks, an ounce of prevention is worth a pound of cure.

Businesses large and small have been under a near-constant onslaught of attacks on their computer systems, which has put their intellectual property, trade secrets, confidential customer information and their operations at risk.

Many of these attacks have been emanating from China. In February, U.S. cybersecurity company Mandiant released a report that linked China's military to cyberattacks on more than 140 U.S. and other foreign corporations and entities.

Some of the most recent targets of cyberattacks from China have been major U.S. news organizations. The New York Times, Wall Street Journal and Washington Post revealed earlier this year that hackers from China had infiltrated their systems in repeated attacks.

While attacks from China are obviously a significant threat, data breaches may be the work of other hackers, such as the group known as Anonymous, or simply the result of human error. Recent high-profile data breaches have included companies such as Sony and Zappos. Retailers are often a prime target for cyberattacks, but even sophisticated network security providers such as RSA, Symantec, Barracuda Networks and VeriSign have suffered data breaches.

If even the world's biggest security providers can't protect their own networks, that doesn't offer much encouragement to companies that rely on their products and have fewer resources.

While even sophisticated IT companies have had problems defending their networks, businesses can reduce the risk of being victimized by taking a comprehensive approach to defend against an attack. That will also set themselves apart in the eyes of insurers as good risks, resulting in the ability to obtain more insurance coverage at better prices.

In addition, such businesses will be in a much better position to defend themselves in court in the event a data breach or network intrusion does occur. The burden of proof is on the organization to prove it was diligent and not negligent in its security efforts. Companies that are found negligent can expect significant out-of-pocket costs.

The Cost of Cybercrime

Cyberattacks are a serious and pervasive problem, and companies have been suffering significant losses.

In its 2012 U.S. Cost of Cyber Crime Study released in October, the Ponemon Institute found that the average annualized cost of cybercrime was $8.9 million a year, with a range from $1.4 million to $46 million.

The 56 companies in the study experienced a total of 102 successful attacks per week. This represented an increase of 42 percent from last year's successful attack experience, according to Ponemon.

Losses can arise from the loss of intellectual property through economic espionage and from business interruptions arising from denial-of-service attacks. Losses also can arise from the cost of compliance with data breach regulations and the cost of managing the crisis itself.

A total of 46 states currently require businesses to notify individuals when a breach has occurred. Compliance with notification laws includes the cost of drafting letters, mailing them out, setting up call centers and credit monitoring, as well as offering legal advice.

As authorities try to protect data, the burden of compliance is growing, with a wide array of regulations being pushed by multiple regulating bodies, including the federal government.

The White House plans to renew efforts to push cybersecurity legislation through Congress, according to Reuters.

The White House cybersecurity coordinator told Reuters that the White House has begun drafting "key legislative principles" for a new bill that it believes can pass both the House and Senate. Similar legislation backed by the Obama administration died in the Senate in November, after fierce opposition from businesses that complained about over-regulation.

In Minnesota, meanwhile, a new version of a bill to curb data breaches is working its way through the senate, while a data breach disclosure bill is under consideration in Maine's legislature.

Health care organizations are also facing new requirements under the final omnibus Health Information Patient Protection Act rule released earlier this year.

Strong Prevention Programs

In spite of the growing risk and media attention to this issue, too many businesses remain complacent.

Antivirus company Kaspersky Lab late last year said the cybersecurity measures being taken by businesses are "woefully inadequate." Its research showed that only 25 percent of IT specialists thought their companies were completely protected from cyberthreats such as malware, spam and hacking, and 16 percent admitted to being more reactive -- solving problems after they occurred.

At large companies, the risk is often from persistent targeted attacks as well as from insider -- either malicious or disgruntled employees who steal information or disrupt systems to harm their employers, or employees who simply lose files or get tricked by phishing scams.

At small businesses, the risk tends to arise mainly from malware and viruses.

Most businesses rely on firewalls and antivirus programs. While these serve as a valuable first line of defense, they should form just one part of an overall cyberwellness prevention program.

Cyberattacks are constant and constantly evolving. But many companies rely on security systems that are not up to the task. A good security program should provide layers of protection to address the risks arising from a company's own employees as well as from hackers and malware.

Even when a company purchases the best technology, the human element can play a vital role in its effectiveness. In many cases, people want to do the right thing, but don't have the knowledge or training to make the right decisions. As a result, they can easily fall victim to scams or inadvertently open the door to intruders.

If not already mandated by industry-specific regulations, a company should establish good corporate security policies and ensure all employees -- and even most vendors -- are made aware of the rules. Moreover, employees who touch sensitive data should be trained to understand the cybersecurity issues they will encounter.

Shunning is another key element in a strong prevention program. Most security technologies reactively focus on neutralizing threats that are already inside a corporate network, much like taking medicine after you become sick. Shunning, however, proactively "immunizes" networks by preventing communication with known hostile IP addresses.

Most firewalls can shun only about 1,000 hostile IP addresses, which must be manually uploaded. But new cutting-edge technology is available that blocks communication with more than 3 million known hostile sites around the world and updates its hostile IP list every 10 minutes. These advances have made shunning a very effective weapon in the fight against cyberattacks.

Better Insurance Benefits

Because no security program is foolproof, insurance is a smart way to complement an overall cyberprotection program. Surprisingly, companies still often believe that cyberlosses will be covered under their general liability or their property policies. This is not so. These losses are typically excluded from these policies and covered under separate cyber or network security policies.

When it comes to insuring companies for cyberlosses, insurers often have a hard time differentiating between companies that are good risks and those that are not. Businesses that take concrete steps to strengthen their network security will be seen as better risks. Good underwriters are looking for signs of a strong security culture that includes not just security technology but good behaviors as well.

Some insurance providers are now seeking to help their insureds build this strong security culture as a proactive form of cyberrisk management. These insurers are taking steps to help companies address information security exposures by offering new tools to help them manage their risk.

In addition to demonstrating a strong security culture, companies that implement a good security program also show they were not negligent, but were diligent about their security obligations. This then helps to create a strong legal defense should a breach occur.

The business world today has become wired and wireless, with information stored in the cloud and operations run by computer networks. It has changed the workplace, made employees mobile and has made vast amounts of information available instantly.

All of this connectivity and reliance on all things digital has come with its down side. Hackers, disgruntled insiders and cyberspies have broken through corporate security, disrupted systems, stolen customer information and are now targeting other valuable intellectual property.

Businesses need to raise the bar and implement a program that can help to prevent a cyberattack from ever happening. Insurers, meanwhile, can play a role by helping their clients develop a stronger security culture.

By following a well-designed prevention program, companies not only reduce the risk of a loss, they differentiate themselves from other companies, providing evidence to insurers, plaintiffs and regulators that they are a good and prudent risk.

BRIAN J. BRANNER *is executive vice president at RiskAnalytics, LLC. He can be reached at riskletters@lrp.com.*

April 12, 2013