NAVIGANT

GLOBAL LEGAL TECHNOLOGY SOLUTIONS (DFLT)

COMPANIES CAN COMBAT GROWING CYBERSECURITY THREATS

Cybersecurity threats are not only happening with greater frequency, they also are increasing in scope and sophistication.

Companies seeking to protect their data and information need to realize that cyberattacks are no longer limited to the stereotypical hacker on a laptop. International criminal networks and powerful nation-states are now deeply involved in trying to compromise corporate computer systems. As a result, the attacks are happening more often, they're more sophisticated, and they're causing more damage.

Businesses need to be more aware of the growing number and sources of cyber threats. They also need to take steps to increase security and better educate their employees on how to avoid falling victim to an attack. The good news is, not all security improvements need to be costly; enhanced employee education and training, and adopting cybersecurity policies and assessment plans can go a long way toward reducing a company's vulnerability.

Here is an update on the current cybersecurity landscape, and tips on how companies can reduce their exposure to attacks:

TODAY'S GREATEST THREATS

The popular image of a cyber-criminal is a troll on a laptop in his parents' basement. Unfortunately, many companies continue to deploy their cybersecurity strategies with that image in mind. The reality is, hackers no longer need to possess extensive computer skills to crack a company's computer system. Hackers can simply use the dark web, essentially a black market, and purchase off-the-shelf malware and ransomware.

But hackers should be the least of a company's concerns. There are international criminal networks that send millions of phishing and spam emails – some with malicious links or attachments – to gain access to corporate computer systems. These criminals gain access to sensitive data and either use it to drain bank accounts, sell the information, or hold it hostage in return for ransom.

The most recent example was the data breach at Equifax, the credit reporting agency, where cyber criminals extracted Social Security numbers and other sensitive information from some 143 million people. The victims are still bracing for how that information might be used.

An even more menacing threat looms from nation-states, such as China and Russia, which have the intelligence apparatus and the infrastructure to carry out massive cyberattacks. China has been accused of stealing sensitive employee data from the U.S. Office of Personnel Management and the Department of Defense, while Russia is currently being investigated for trying to influence the outcome of the 2016 presidential election. Public and private companies have been subjected to similar nation-state attacks, and more are coming.

One problem is that corporations don't build their systems in anticipation of a threat from a nation-state. Companies build systems for commercial use, for improving the speed and efficiency of doing business. These systems aren't built for defense.

Even if a company improves its security measures, it's most likely focusing on the lone-wolf hacker or the low-level criminal, not a nation-state. There is a big difference between building security to thwart a threat from a criminal on laptop, as opposed to 40,000 state workers staging an attack from China. Companies need to gear their security toward defending against nation-state attacks.

TOP CYBERSECURITY TIPS

Fortunately, there are a number of steps companies can take to combat these growing cyber threats, with some measures costing little or no money.

Education and Training: A relatively quick and inexpensive security method is to provide education and training to employees. Companies can teach employees how to identify suspicious email files that might contain a malicious link or attachment. Photos and videos also are potential breeding grounds for malware and ransomware. Through training, employees can learn how malware and ransomware work, and how to avoid opening corrupted files in email. The training can be delivered in person or online, and should take no more than 30 minutes. Offering training sessions quarterly keeps the information fresh and on the minds of employees.

Monitoring Social Media: Employees also need to be educated to understand how their mobile devices and social media can add to the vulnerability of their employer. Most mobile devices contain both work and personal email accounts. A hacker can gain access though a personal email account and use the mobile device to penetrate the user's business email or other company files. Additionally, the social media on a mobile device can serve as an entry point for hackers to invade the business accounts. Consider the 800 "friends" you have on Facebook. How many do you know really well? One might be a hacker who has gained control of your mobile device, waiting for the moment you open your business email or other company applications.

Strengthening Password Protection: Companies can easily add a layer of security by requiring employees to log in using two factor authentication. This system requires users to not only log in using their password, but also a second method to confirm the identities of the users. A familiar example would be where a user enters a password on a mobile device, and is then sent a dynamic passcode by email, which must be entered as the second form of authentication. A more sophisticated form of authentication might employ eye, voice or face recognition.

Cybersecurity Program: Firms should develop a cybersecurity program to establish a framework to govern security. The program should address procedures, personnel and training. The program establishes an organized and methodical approach for understanding the organization's risk and security, and creates a hierarchy of responsibility.

Cybersecurity Policy: The cornerstone of any cybersecurity program are the policies and procedures that govern the protection of information. Policies and procedures provide employees and customer's guidance on controls surrounding information and access to that information. Written policies provide accountability and guidance.

Risk Assessment: Companies need to regularly perform a risk assessment to ascertain the strength of their cybersecurity systems. Cyber threats are changing constantly, and the methods and tools necessary to detect and defend against attack are being updated just as fast. Therefore, a regular reassessment must occur to ensure that new and emerging threats are mitigated or identified before they cause irreparable harm.

CONTACT

ROBERT E. ANDERSON

Managing Director, Global Leader
Information Security Practice
+1.202.481.7306
bob.anderson@navigant.com

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage, and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the firm primarily serves clients in the healthcare, energy, and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

linkedin.com/company/navigant

twitter.com/navigant

BEING PROACTIVE

Cyber security threats have become a high-stakes enterprise that have quickly moved beyond the simple work of the rogue hacker to sophisticated operations involving criminal syndicates and nation-states.

Companies are vulnerable to cyberattacks because they have built their computer systems for speed and enterprise, with little thought to defense. Corporations also have underestimated the abilities of cyber criminals, still viewing them as lone hackers, while criminal networks and nation-states are becoming increasingly responsible for the attacks.

Corporations can take some quick and relatively inexpensive steps to improve their cybersecurity by educating and training their employees to identify threats; strengthening passwords; establishing cybersecurity programs and policies; and conducting frequent risk assessments. Raising awareness among corporate executives and employees is an effective method for combating cyber threats.