CORPORATE BOARD MEMBER®

THIRD QUARTER 2019
VOLUME 22, NUMBER 3

MICHAEL O'NEILL
RETIRED CHAIRMAN
CITIGROUP

2019 BOARD LEADERSHIP AWARDS

DIRECTOR OF THE YEAR

CYBER RISK: A BOARDROOM PRIORITY

Integrated layers of defense can help protect companies from attacks.

By Akshay Bhargava

Boardrooms have traditionally focused on improving two metrics: increasing revenue and lowering costs. More recently, risk reduction has become just as important to the overall success of an organization.

In addition to inherent business risks, such as legal liability, and attracting talent, "cyber attacks" and "business interruptions" are now the top two risks facing organizations (Allianz Risk Barometer, 2019). In fact, the World Economic Forum's *Global Risks Report* examines the top risks based on overall *likelihood* and *impact* to the world. Both cyber attacks and "data fraud or theft" made it into the top five likely global risks, on par with "natural disasters" and "extreme weather."

The world's rising dependence on technology has increased risk due to cyber attacks. The executives I have consulted are very concerned and tell me quite frankly that they and their colleagues are unprepared. Attackers are increasingly sophisticated and successful in compromising the majority of organizations. The second half of 2018 saw cyber criminals pivot from attacks on consumers to more aggressive attacks on enterprise targets. According to the Malwarebytes' *State of Malware Report*, attacks on business increased 79 percent over the previous year.

A proven and optimal strategy is to place integrated layers of defense across technology, people and processes to protect your organization from attacks and mistakes. Here are a few critical points I advise board members to be aware of and ask their CEOs about.

Technology

New technologies like cloud computing, Big Data, and machine learning create new market opportunities; however, they can also introduce risk. Organizations can leverage these same technologies to detect, prevent, respond and even predict tomorrow's cyber attacks. For example, new system and user behavior technologies are being used to determine whether systems or people are acting more differently than usual. Anomalous behaviors can be detected more easily using modern machine learning algorithms.

Begin by protecting sensitive data with encryption, masking and appropriate key management. Then, limit access only to authorized systems and users for business-appropriate operations according to pre-defined policies that are aligned to overall business goals. This means breaking up powerful administrative tasks into more than one action so that no one person has too much power (separation of duties). As well, never give someone more privilege than necessary to do their job (least privilege).

With the explosion of Software as a Service (SaaS) and mobile applications, devices have more access to sensitive data. It's proven that one of the most common ways to compromise an organization is to compromise a specific individual in the company. A key technique uses phishing attacks where criminals send well-crafted emails to entice users to click and download files that include malware. This malware can then exploit the device so that the criminal can further penetrate the organization. To prevent this, deploy protection capabilities (i.e., endpoint detection and response) on all employee computers and devices. Whether they are in the office or on the road, or they bring their own devices into the work environment, prevent malicious software from compromising these entry points.

People

A critical component to an organization's security is the security awareness and knowledge of its employees. Educating and training employees on good security hygiene practices is increasingly important. For example, conduct regular simulated phishing exercises that train them to look for telltale phishing attack signs.

Another area of vulnerability is login information. The average employee must keep track of 191 passwords (LastPass, 2017). I suggest using a secure password manager to create and store secure passwords. Additionally, reduce the number of passwords to remember by using identity management and single sign-on. Add multifactor authentication so that a criminal would require the login username, password and the device that was used to set up the secondary factor of authentication in order for an attack to be successful.

Ultimately, the people must align with corporate security policies that are driven and enforced at the board level.

Process

Effective process ensures that the organization implements strategies to proactively prevent threats and respond quickly and effectively in the event of a cybersecurity incident.

Information security teams should begin with a cyber incident response plan with repeatable procedures. The plan should help to address security incidents with the goal to recover business processes as fast as possible. You want to minimize downtime and increase the chances of data recovery.

As well, processes should be implemented effectively to collect threat data, detect anomalous behaviors and respond to the real threats. Data might reveal an attack on a system vulnerability or devices that are being attacked by a software virus. By having visibility into the entire environment, security teams can leverage technology, people and process to respond intelligently.

Discussing cyber risk is undeniably an important conversation that should be taking place in every boardroom. Framing the approach around the important best practices related to technology, people and process can ensure you are covering the most critical topics.

Akshay Bhargava is senior vice president of products at Malwarebytes. You may reach Akshay at abhargava@malwarebytes.com. To read the 2019 State of Malware Report *referenced in the article, visit malwarebytes.com/malware19*

Malwarebytes