BDO KNOWS:

CYBERSECURITY

STANDING GUARD AGAINST EVOLVING CYBER RISKS

By Gregory A. Garrett

2017 has ushered in a new era of massive cyberattacks. An elusive cyber group called the "Shadow Brokers" leaked National Security Agency (NSA) hacking tools, including highly sophisticated software exploits. Trouble soon followed.

THE LATEST EVOLUTION OF CYBERATTACKS

The "WannaCry" ransomware program was the first to hit in May, infecting 153 countries with more than 75,000 ransomware attacks; 3,300 infections were reported in the U.S. The attack affected several major institutions including FedEx, Nissan and the Russian Interior Ministry. The program held data files for ransom and demanded the equivalent of $300 in Bitcoin to restore user access. One infected computer on a network possessing administrative credentials could quickly spread the program to all other network computers. WannaCry targeted a vulnerability in Microsoft Windows, and users who hadn't updated their systems with a security update that Microsoft had issued in March were put at risk.

Just one month later, the Petya virus made its presence known around the globe, infecting more than 12,500 machines across 64 countries. Similar to WannaCry, the attack used malicious software to prevent users from accessing their data until a $300 Bitcoin payment was made. The program targeted several attack vectors, including vulnerabilities in Microsoft's Server Message Block (SMB), known as MS17-010 SMB. However, it quickly distinguished itself as a more dangerous "wiper" virus, not only locking files but potentially destroying them; the program crippled devices by overwriting and encrypting the machine's master boot record, according to Symantec.

And most recently, in one of the largest single cyber attacks on record, the Equifax data breach exposed confidential and highly sensitive personal information of more than 143 million consumers.

CONTACT

GREGORY GARRETT
Head of International Cybersecurity
703-893-0600
ggarrett@bdo.com

CLEAR STANDARDS EMERGING

Even before these mega attacks were launched, pressure had been building both in the U.S. abroad to implement more rigid cybersecurity. Earlier this year, New York's Department of Financial Services (DFS) issued a "first-in-the-nation" cybersecurity regulation that went into effect on March 1, 2017, developed to protect customer data and ensure the safety and soundness of the state's financial services industry. It requires all financial institutions doing business in New York state, regardless of their domicile, to conduct a risk assessment and maintain a risk-based cybersecurity program. Organizations must also adopt a written cybersecurity policy (including third-party risks), designate a qualified chief information security officer (CISO), establish a written incident response plan and submit an annual certification of compliance, among other requirements.

In April, the American Institute of CPAs (AICPA) announced SOC for Cybersecurity, a cybersecurity risk management reporting framework that provides a standard method for organizations to report enterprise-wide cybersecurity risk management. Stakeholders and prospective investors look at SOC attestations as a measure of corporate health and the effectiveness of enterprise risk management programs. The framework is designed to help ensure that everyone inside and outside of an organization - regardless of size or industry - speaks a common language and helps to standardize policies, procedures and controls around cybersecurity.

Abroad, the EU General Data Protection Regulation (GDPR) comes into force in May 2018 and significantly expands the scope and enforceability of the European Union's data privacy regime. Companies are required to inventory all personal data, incorporate risk-based cybersecurity measures, and report any data breach to the supervisory authority within 72 hours. Non-compliant organizations may be fined up to four percent of annual global turnover or €20 Million (whichever is greater).

And most recently, a series of congressional hearings focused on the Equifax data breach came with a call from the head of the US House of Representatives Financial Services Committee for a consistent national standard for both data security and breach notification in order to better protect consumers and hold companies accountable.

These are just a few of the latest moves that industry groups and government regulators are taking to ensure organizations are actively assessing and protecting themselves against the vulnerabilities seized by cyber criminals.

TAKING ACTION

Companies must maintain constant vigilance of evolving cyber risks, not only looking ahead to what's next, but ensuring a strong foundation exists to manage and mitigate the risks. Among the most critical elements of a successful cyber risk management program include:

- **Employee education:** Human negligence is often the biggest risk to organizations. Many attacks are entirely preventable. For example, some organizations could have avoided Petya if users had simply installed a months-old security patch to their computer. Designing training programs around various organizational roles can help employees practice good cyber hygiene and better understand the consequences.
- **Active monitoring:** Threat monitoring and analytical tools are critical weapons in an organization's defense arsenal to detect and prevent attacks. Early detection can make a world of difference when it comes to rescuing critical data and preventing further damage.
- **Incident response plan:** When an issue emerges, time is of the essence. Developing a plan that details breach notification protocols and identifies the critical stakeholders involved in containing, removing and communicating the threat can ensure the organization's response is immediate and comprehensive.
- **Security patch management program:** Keeping operating systems and software updated with the latest security patches can reduce the number of exploitable entry points for cyberattacks. Organizations must develop a solid understanding of the vulnerabilities that exist and the degree of risk they present and ensure they take appropriate measures to address them.

Cyber criminals are getting smarter and more sophisticated, and cyber-related compliance demands will only grow. Organizations can't afford to get comfortable. Developing a proactive cyber risk management framework may seem daunting, but the severity of the consequences promises to invite greater complications.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.