TABB FORUM

WHERE CAPITAL MARKETS SPEAK

TIME TO GET SERIOUS ABOUT CYBERSECURITY

To respond to the growing number of attacks, as well as to newly emerging threats, companies must reevaluate their approaches to prevention and mitigation. The bare minimum is no longer sufficient. Here are tips for thwarting the latest cyber threats.

In October 2017, Richard F. Smith, then-Chief Executive of the credit reporting agency Equifax, testified before the House Energy and Commerce Committee. The subject was an insidious security breach at Equifax that compromised the Social Security numbers of more than 145 million Americans. Under pointed questioning from lawmakers, Smith said a single Equifax employee had facilitated the breach.

One slipshod employee. Millions of sensitive personal records compromised.

Just as one employee can put an entire organization at risk, it only takes one to spot and contain a threat. In 1986, a young German programmer named Markus Hess hacked hundreds of U.S. government computers with the intention of selling American military secrets to the KGB. Hess would have achieved his goal if not for an attentive systems administrator named Cliff Stoll, who detected the intrusion based on a 75-cent accounting error. Stoll later went on to write a book about the experience called "The Cuckoo's Egg," which became a cult classic in the field. Today's cybersecurity professionals must be every bit as vigilant and responsive as Stoll, alert to the slightest sign that something is amiss.

New Risks

Despite the industry's best efforts to prevent them, cyber threats are becoming more numerous and more sophisticated, and state actors with tremendous resources have become major backers of such attacks. Three types of threats are becoming increasingly common.

Phishing

Phishing targets a company's users by using email, phone calls and text messages to trick them into compromising their own systems. This is sometimes part of a synchronized attack, which appears to be coming from a trusted source. If hackers manage to infect someone's computer, then their malicious code can travel laterally across the network, and once inside, infect additional systems. Technical controls and continuous awareness programs for employees are crucial to circumventing these threats.

Ransomware

Ransomware has become the most popular method for monetizing cyberattacks. Here, hackers encrypt a computer's data and then demand a ransom to decrypt it. Owing to social engineering advances, malicious actors can now launch multiple attacks within the same company, so training for employees who have data access must be a top priority. Also, a machine compromised by ransomware can only spread the malware to what it has access to, so having strong access controls ruled by a 'least access' concept can help reduce the spread of ransomware within an organization.

ABOUT THE AUTHOR

Baba Gurjeet S. Bedi is Senior Vice President & Chief Information Security Officer at AST, one of the largest transfer agents on Wall Street. Mr. Bedi has almost 30 years of professional experience in the IT sector, both in the U.S. and India.

AST

Zero-Day Threats

Zero-Day threats, the target of Google's Project Zero, include unpublished, ignored or new vulnerabilities in products such as software, hardware and firmware. They are called zero-day because they have not yet been exploited – and there is no known solution readily available. Subscribing to a reputable threat intelligence service and participating in industry peer groups like Information Sharing and Analysis Centers (ISACs) are keys to sharing and receiving early information.

TACKLING THE LATEST CYBER THREATS

To respond to the growing number of attacks, as well as to newly emerging threats, companies must reevaluate their approaches to prevention and mitigation. The bare minimum is no longer sufficient.

Throwing Away the Checklist Approach

Senior executives and technology professionals are moving away from the check-the-box approach to cybersecurity. In 2018, company-specific risk assessments will shape preventive measures as never before. Different organizations, even within the same industry, may have different risks. A trading firm, for example, could have more transactional risk than an asset management company because of the volume of its transactions. Through custom risk assessments, businesses will determine where their greatest cyber risks exist, so they can allocate resources appropriately.

Getting Ahead of Regulations

The New York State Department of Financial Services (DFS) launched broad, sweeping cybersecurity regulations effective March 1, 2017, which are being phased in over 24 months. Already, DFS-regulated companies must have a written cybersecurity program, a qualified Chief Information Security Officer, a tested incident-response plan and a trained cybersecurity staff. As of March 1, 2018, additional technical controls, such as multi-factor authentication for data and applications, will be required. Other requirements will kick in this fall and next spring. As financial services firms adapt to this more stringent regulatory framework, they will also need to be vigilant about the penalties for non-compliance.

Utilizing Next-Generation Emerging Technologies

While expensive and difficult to implement, companies are increasingly investing in newly emerging technologies for the improved security they provide. Behavioral analytics, for example, employs data analysis, machine learning and artificial intelligence to build profiles of devices, networks and users and then flag any deviations from expected behavior. These tools are especially useful in monitoring for the exploitation of zero-day flaws, such as the Meltdown and Spectre chip-level vulnerabilities discovered last June by security researchers at Google and made public last month once patches had been developed. Behavioral analytics with higher sensitivity settings could have been used in the interim to monitor corporate networks for such intrusions until vendors came up with fixes and the company could deploy them across the enterprise.

Can new technologies like behavioral analytics prevent the next Equifax-level breach? The next Markus Hess? Maybe, maybe not. But the takeaway is clear: As hacking evolves, cybersecurity techniques must evolve with it. The bad news is that one negligent employee can still inflict a lot of damage. And the good news is that it still only takes one Cliff Stoll, armed with the right tools, to prevent it.

http://tabbforum.com/opinions/time-to-get-serious-about-cybersecurity
Reprinted with the permission of Tabb Forum.

AST