Booz | Allen | Hamilton

10 CYBER PRIORITIES FOR BOARDS OF DIRECTORS

BILL PHELPS, EXECUTIVE VICE PRESIDENT, BOOZ ALLEN HAMILTON

INTRODUCTION

A company's board of directors is expected to drive market competitiveness by asking the tough questions—about executive performance, growth opportunities, compliance, risk, and more. In 2017, cyber risk is reaching new heights in both event likelihood and business impact. As boards and associated executive committees engage in dialogue over this ever-evolving topic, they need access to the right information to effectively challenge the security status quo and validate that the future investment strategy will address the anticipated cyber risk environment.

As we peer into how business, technology, regulatory, and cyber threat realities are evolving in the coming year, here is a reference guide for board members to use in validating their company's cybersecurity approach.

TOP 10 CYBER FOCUS AREAS FOR BOARDS IN 2017

External Forces

Key regulatory bodies are becoming increasingly prescriptive on cyber defense requirements, and the consequences of noncompliance are becoming more severe.

1. EU General Data Protection Regulation (GDPR). Sweeping EU data protection regulations, effective May 25, 2018, will affect organizations operating within 28 EU member states. The GDPR harmonizes regulations and implements significantly more prescriptive requirements, with significant fines for noncompliance. As a result, companies will need to place even greater focus on data security and privacy.
2. New York Department of Financial Services (DFS) Cybersecurity Regulation. Increased efforts to protect sensitive financial information has resulted in significant, first-in-the-nation proposed regulation focused on financial institutions conducting business in New York, effective March 1, 2017. However, these new regulations are likely to influence other industries and jurisdictions. Pragmatically, all companies can take cues from the DFS regulation's core mandates, including identifying internal and external risks, protecting sensitive information, initiating annual penetration tests of systems, and conducting routine vulnerability assessments.

Threat Landscape

Adversaries are diversifying their methods and intents—going beyond traditional theft of personally identifiable information and intellectual property. Now, disruption of business operations and destruction of key digital and physical assets are increasingly becoming part of threat actors' modus operandi. In the near term, there are several threat variants that boards need to stress test with company security leaders.

3. Fake News/Disinformation. Russia and other threat actors have demonstrated that fake news and disinformation work to drive public opinion and behaviors. Public corporations, in particular, should be ready for an increased use of disinformation against them to harm their brands. Boards must understand that fake news and disinformation extend the definition of "cyber threat" from a direct attack against a company to an indirect attack via information warfare. Organizations will need a plan of action to handle disinformation.
4. Ransomware. Originally aimed at individuals, ransomware is increasingly targeting businesses, particularly as it continues to grow in sophistication and ransom demands increase in value. Organizations must be ready for hyper-targeted ransomware against high-value digital assets (e.g., applications and databases) and individuals, including executives, officers, and board members. In addition, experts predict that we will see an increase in the diversity and volume of devices—and subsequent business processes—held for ransom. We will see ransomware beginning to infiltrate the Internet of Things (IoT), cloud infrastructure, and industrial control system (ICS) realms.
5. Data Integrity Attacks. Attacks seeking to create confusion or shape behavior by manipulating data have long been understood and demonstrated in information warfare but have seldom been seen in the commercial cyberspace. This is beginning to change, as manipulation of Internet Protocol (IP) source code, sensitive financial information, and the like become real concerns today. The challenge, of course, is that data does not move in integrity attacks; therefore, the effects of manipulation, like fraud, are difficult to detect.

6. Continued Scaling of DDoS. Threat actors will increasingly employ large-scale IoT device-based botnets to disrupt business systems, processes, and networks. The 2016 distributed denial-of-service (DDoS) attack against an Internet performance management company (Dyn), causing major commercial online services to go offline, illustrates how damaging these attacks can be. DDoS has long been a favorite tool of politically motivated attackers, but we will likely see it return to its roots as a tool for ransom.
7. More ICS/IoT Attacks. Security professionals have long understood the vulnerability of ICS and connected architectures to cyber attack, but threat actors operating in the commercial market have not exploited these vulnerabilities at great scale yet. This is changing. Board members in manufacturing, transportation, energy, oil and gas, and chemical industries should be especially aware and should press their companies for increased resilience in this space.

Key Cyber Operational Focus Areas

In spite of tremendous investment in cybersecurity, most organizations are not able to effectively scale their cyber defenses to the growing attack surface, which leaves exploitable gaps for threat actors to pursue.

8. Red Teaming and Executive Wargames. Despite growing cyber regulations, compliance assessments are simply not effective in assessing the effectiveness of an organization's cyber defense capabilities. Continued testing of operational effectiveness through "red teaming" employs expert, adversary-minded resources to expose gaps in a company's security posture. In complement, wargames test the readiness of cross-functional leaders and senior executives to respond in the face of a material cyber incident. Boards should require that they be briefed on the results of both red team and wargame exercises to understand the readiness of their companies to detect and respond to serious cyber incidents.
9. Security Beyond IT. In many organizations, responsibility for security beyond the core IT infrastructure remains unclear. It may fall under a corporate chief information security officer who does not always possess the necessary skill and authority, or in other instances, responsibility may simply not be well defined. Cybersecurity concerns have expanded to new realms, including the supply chain, product development, manufacturing, and retail operations. Boards must ensure that their organizations possess clarity on both accountability and responsibility to ensure that security coverage is appropriate across the extended enterprise.
10. Getting Cloud Security Right. Migrating applications to the cloud is an ever-increasing priority for organizations. From a security perspective, cloud providers are generally strong at protecting their own cloud infrastructure, but too few customers realize that it is their own responsibility to ensure security of their cloud-based data and applications outside of the core purview of their service provider. There are services and leading practices available, but this lack of understanding often represents the Achilles' heel of cloud security. Boards need to ensure the organization is counterbalancing the cost savings of moving to the cloud with investment in security controls and governance.

FINAL WORD

Although computing platforms are slowly becoming more resistant to cyber attack, phishing and other social engineering techniques that exploit human weakness continue to be the most effective tools used by adversaries for gaining malicious access to organizations' systems. Despite a tremendous focus on employee education, the success rates of broad phishing attacks are still in the 10-percent to 15-percent range, and very carefully targeted "spear phishing" attacks have success rates much higher than this. In spite of improvements in technical security, the weakness at the human layer continues.

About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy, technology, and engineering for more than 100 years. Booz Allen partners with private and public sector clients to solve their most difficult challenges. To learn more, visit BoozAllen.com. (NYSE: BAH)

For more information:

Bill Phelps
Executive Vice President
phelps_bill@bah.com