BDO KNOWS CYBERSECURITY

TOP TEN TRENDS AND KEY RECOMMENDATIONS FOR 2019

Cyber-attacks are increasing in sophistication and magnitude of impact across all industries globally. According to a recent report issued by the U.S. Security Exchange Commission (SEC) the average cost of a cyber data breach is $7.5 Million and is continually increasing in value year over year. While all organizations are potential targets of cyber attacks, the industries which possess the most valuable data are the biggest targets including: financial services, healthcare, government, automotive, manufacturing, and retail. All organizations possess valuable information assets, which may include: intellectual property, financial payment information, client information, supply chain partners' information, personally identifiable information (PII), protected health information (PHI), and/or payment card information (PCI).

TOP 10 CYBERSECURITY TRENDS OF 2018

1. Blurring of Cyber Threat Actors
The FBI/DHS and other law enforcement and intelligence agencies are all reporting the increased collaboration between nation-state cyber-attack groups and organized criminal cyber-attack groups worldwide, especially in China, Russia, Iran, and North Korea.

2. Rise of Business Email Compromise (BEC) Attacks
Rapid growth of social engineering based cyber spoofing attacks on companies globally, typically focused on the payment of invoices to wrongful suppliers.

3. Growth of Spear-Phishing Email Attacks
Increased number of spear-phishing attacks targeting senior company executives especially CEOs, CFOs, and Controllers for unauthorized electronic transfer of funds.

4. Expansion of Ransomware Attacks
Over the past year there has been a 350% increase in the number of ransomware attacks globally, with an ever increasing focus on the healthcare industry.

5. Exploitation of Supply Chain Network based Cyber Attacks
Significant increase in the number of cyber data breaches resulting from initial unauthorized access via third-party vendors network connections to prime contractors.

6. Recognition that Regulatory Compliance with Cybersecurity Industry Standards Does Not Ensure Real Data Security
Many companies who have invested in ensuring compliance with various industry standards for cybersecurity (i.e. PCI-DSS, NYDFS, HIPAA, ISO 27001, etc.) have experienced cyber data breaches. Thus, realizing that regulatory compliance with general information security requirements does not guarantee a company will not suffer a major cyber data breach.

7. Higher Cost of Cyber Data Breaches = Higher Cyber Liability Insurance Premiums
As the average cost of a cyber data breach has increased every year for the past five years, so has the average cost of cyber liability insurance premiums.

8. Increasingly Complex Cybersecurity Regulatory Landscape
Throughout the U.S. and internationally regulators at the multi-national, federal, state, and local levels are continually enacting new government regulations intended to protect consumers' personally identifiable information (PII), protected health information (PHI) via Electronic Health Records (EHR), and payment card information (PCI). All ultimately have a cost associated with compliance, which is passed on to the consumers.

9. Shortage of Experienced Cybersecurity Professionals
There is a global shortage of experienced, trained, and certified cybersecurity professionals to meet the ever increasing demand for cybersecurity advisory services and managed security services worldwide.

10. Cyber Attack Fatigue/Burn-out is Affecting Cybersecurity Investments
As a result of continuous news reports of massive cyber-attacks and data breaches internationally, more and more companies are becoming increasingly apathetic to the potential impact on their respective company, often assuming merely purchasing more cyber liability insurance is sufficient, rather than investing in trying to prevent an attack.

KEY CYBERSECURITY RECOMMENDATIONS FOR 2019

1. Conduct Email Threat Assessments
Given the increasing number of cyberattacks via email systems, companies are increasingly looking to conduct periodic email threat assessments, especially to detect malware that made it through their anti-virus software and firewalls which have previously gone undetected.

2. Perform Network & Endpoint Threat Assessments
With the expansion of information systems, software applications, bring your own devices, and Internet of Things (IoT), organizations are increasingly testing their network and endpoints via threat assessments using sophisticated Intrusion Detection Systems (IDS) to reduce potential vulnerabilities to cyber-attacks.

3. Conduct Spear-Phishing Campaigns
Due to the significant increase in spear-phishing attacks, organizations should periodically test the cyber awareness and susceptibility of their employees to cyber-attacks via engaging certified ethical hackers who can conduct social engineering-based spear-phishing exercises.

4. Perform Vulnerability Assessments & Penetration Testing
Most organizations either internally conduct or hire an independent firm to perform some form of vulnerability assessments, via computer malware scanning software, and penetration testing to discover potential external vulnerabilities to cyber-attacks. It is important to conduct these tests at least once a year but, twice or quarterly is better given the constant evolution of cyber-attacks.

5. Implement Effective and Timely Software Patch Management Program
The most significant cyber data breaches in the past two years all resulted from organizations not implementing an effective and timely software patch management program of Microsoft and Cisco software.

6. Establish a Cybersecurity Awareness/ Education Program
The cost effective means to improve cybersecurity is to create a human firewall by providing quality cybersecurity educational programs for all of your employees from the top of the company to the bottom.

7. Conduct Cybersecurity Risk Assessments
It is important to independently verify that an organization's cybersecurity policies, plans, and procedures are sufficient to adequately protect the organization's digital assets and to ensure regulatory compliance with the appropriate industry cybersecurity standards.

8. Implement an Incident Response (IR) Program
It is critical that every organization has a well thought through and periodically tested incident response (IR) program, including: policies, plan, process, procedures, standard forms, and periodic exercises and/or simulations.

9. Ensure Continuous Monitoring, Detection, & Response (MDR)
Every organization should invest in an appropriate level of MDR services based upon the cyber threats their organization encounters or anticipates. The key is to rapidly detect intrusions to quickly contain and eradicate the malware to reduce negative impacts upon the information system and data assets.

10. Invest in Business Continuity Planning/ Disaster Recovery to Ensure Resilience
Given the high probability of a cyber data breach, it is essential to have a reliable and secure off-line data back-up system to ensure minimal impact to the organization's operational performance, and protection of the most valuable digital assets from loss or damage.

SUMMARY

As noted by the top ten trends in cybersecurity, the risk of a massive cyber breach negatively impacting a company's reputation and market value is ever increasing. Thus, all companies need to fully understand the value of the information assets they possess, the cybersecurity related risk of a data breach, and then factor the benefits and risk variables into their respective business equation. Once all of the aforementioned actions are taken, then informed business decisions can be made by the C-Suite and company board of directors to mitigate potential negative impacts of a cyber breach and the post breach consequences.

Said simply, spending thousands of dollars on some or all of the key cybersecurity recommendations, including: conducting email and network threat assessments, performing vulnerability assessments and penetration testing, implementing spear-phishing testing, and providing cybersecurity educational programs could all serve to reduce your cyber vulnerabilities, which would significantly reduce the impact of a data breach, thus saving millions of dollars.

CONTACT

GREGORY GARRETT
Head of U.S. and International
Cybersecurity Advisory Services
ggarrett@bdo.com

MICHAEL ADDO-YOBO
Managing Director, Cybersecurity Advisory Services
maddo-yobo@bdo.com

ERIC CHUANG
Managing Director, Cybersecurity Advisory Services
echuang@bdo.com

GREG SCHU
Partner, Cybersecurity Advisory Services
gschu@bdo.com

MIKE STIGLIANESE
Managing Director, Cybersecurity Advisory Services
mstiglianese@bdo.com

www.bdo.com