BDO KNOWS:

CYBERSECURITY

COMPLIANCE DOES NOT EQUAL SECURITY

Cybersecurity is a growing risk factor in all industries within the U.S. and worldwide. Cyber attacks are increasing in sophistication and magnitude of impact across all market sectors 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, Federal/State/Local government agencies, government contractors, automotive and manufacturing, and retail. All organizations possess valuable information assets, which may include: intellectual property, financial payment information, client information, supply chain partners' information, personal identifiable information (PII), protected health information (PHI), and/or payment card information (PCI) just to mention a few.

It is vital for any organization's leadership to ensure they fully understand both the value of the information assets they possess, and the level of cyber threat and vulnerability the company is facing. Plus, every organization's leadership must understand their real probability of a significant data breach, in order to determine the potential financial impact of the company's cybersecurity preparedness or lack thereof.

CONTACTS:

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

ERIC CHUANG
Managing Director, Cyber Incident Response
703-245-8687
echuang@bdo.com

MICHAEL ADDO-YOBO
Managing Director, Cybersecurity Advisory
214-243-2925
maddo-yobo@bdo.com

The reality today is many companies have relied too much on conducting just a cybersecurity compliance checklist assessment, often using either some generic cybersecurity standard, or an industry-based cybersecurity risk assessment framework, i.e. ISO 27001 (Multi-national organizations), NYDFS (NY-based Financial Services), AICPA-SOC (Accounting Services), PCI (Retail - Payment Card Industry), HIPAA (Healthcare Services), or NIST (Government/Defense/ Critical Infrastructure). While these cybersecurity compliance assessments are good tools to evaluate the current state of cybersecurity policies, plans, and procedures vs. industry standards in order to identify gaps – they alone are insufficient to ensure real cybersecurity.

The focus of this article is to highlight the appropriate actions organizations can take both before a cyber data breach and after a cyber data breach to mitigate the potential negative impacts and optimize business performance results. It is essential for all companies to take the following cybersecurity actions as appropriate for their respective industry, size, and complexity of their information systems, including:

BEFORE THE BREACH (PROACTIVE CYBERSECURITY ACTIONS):

- Hire one or two qualified independent firms with extensive cybersecurity testing capabilities to perform the following key cyber diagnostic actions:
  - Conduct an email cyber threat assessment
  - Perform a network cyber threat assessment
  - Conduct an internal vulnerabilities assessment of the enterprise network
  - Perform penetration testing services, including: Spear Phishing and Spoofing campaigns based upon social-media analysis
- Conduct a Cyber Liability Insurance Coverage adequacy evaluation to discover what is covered and what is not covered, and understand the cost of cybersecurity remediation actions vs. the cost of the cyber insurance premium
- Provide a Cybersecurity Awareness Education and Training program for all employees to develop a real cybersecurity culture
- Hire a Qualified Security Assessor (QSA) organization to conduct an appropriate Cyber Risk Compliance Assessment to evaluate all of the organization's critical Information Security policies, plans, and procedures, and compare them to the appropriate industry standard. Then identify gaps between the organization's current state of cybersecurity documentation vs. the industry stated regulatory requirements. Then develop a prioritized cybersecurity plan of action to remediate any deficiencies in the policies, plans, and procedures. Key information security plans include:
  - System Security Plan (SSP)
  - Identity and Access Management Plan
  - Incident Response (IR) Plan
  - Business Continuity Plan (BCP)
  - Disaster Recovery (DR) Plan
  - Third-Party/Vendor Management Plan
- Hire an independent company to gather cyber threat intelligence services, including:
  - Conduct a Dark Web Analysis for the company, key personnel, and selected supply chain partners
  - Conduct a Social Media Analysis of the company and key personnel
  - Conduct an extensive Internet Search of the company and key personnel
- Perform appropriate email, network, and endpoint Monitoring, Detection, and Response (MDR) services either with internal Information Technology department team members (using purchased company hardware and software) or outsourcing to a Managed Security Services Provider (MSSP) for Managed Security Operations Center (SOC) services, Security Incident & Event Management (SIEM) services, Endpoint Management Services, and Incident Response Services, or some combination of the above.

All cybersecurity actions taken should be focused on identifying potential negative or damaging information, which could lead to cyber vulnerabilities including: ransom, malware, ransomware, spear-phishing, spoofing, and other attack modes.

AFTER THE CYBER DATA BREACH (REACTIVE CYBERSECURITY ACTIONS)

Take the following cybersecurity remediation actions as necessary and appropriate:

- Conduct Incident Response necessary to contain, mitigate further damages, and eradicate malicious software
- Investigate the source(s) of the cyber attack(s) and data breach
- Replace corrupted hardware and software as required
- Scan the entire network for viruses
- Prepare a cyber insurance claim as needed
- Hire an independent firm to conduct a post-breach investigation
- Evaluate Incident Response to the data breach to identify areas for improvement
- Enhance IT technical operations and staffing
- Provide cybersecurity education and training to employees as needed
- Engage or replace the Managed Security Services Provider (MSSP) to provide managed monitoring detection & incident response services – 24x7x365
- Assess third-party vendor cyber risks
- Conduct periodic vulnerability assessments
- Perform penetration testing
- Ensure timely software patch management program
- Develop a multi-layer cyber defense program with encryption
- Implement multi-factor authentication
- Develop an Incident Response Plan
- Conduct Incident Response Exercises
- Ensure Business Continuity Plan
- Practice Disaster Recovery Plan

SUMMARY

The risk of a massive cyber breach negatively impacting a company's reputation and market value is ever increasing. Thus, every organization needs to fully understand the value of the information assets they possess, the cybersecurity related risk, and then factor in 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 organization's senior executive leadership team to mitigate potential negative impacts of a cyber breach, and the post breach consequences.

Said simply, spending thousands of dollars on cyber email and network threat assessments, vulnerability assessments, penetration testing, and threat intelligence services up-front could provide a much more valuable holistic and comprehensive understanding of the real state of the organization's level of cybersecurity vs. simply conducting a cyber risk checklist assessment of policies, plans, and procedures alone. While compliance with government and industry documentation standards is good, it is not sufficient, nor does it ensure real information security.