2020 CYBERSECURITY GUIDELINES FOR C-SUITE EXECUTIVES

THE BRAVE NEW WORLD OF CYBER-ATTACKS

Cyber-attacks arguably pose the single biggest modern threat to businesses. The number of cyber-attacks, their level of sophistication, and the financial and reputational impact they have all continue to increase at an alarming rate. The research firm Cybersecurity Ventures predicts that cybercrime will cost $6 trillion globally by 2021. Inside actors, nation-state groups, and criminal organizations now often work together to deploy an ever-expanding array of social-engineered cyber-attacks. Common tactics include: spear-phishing, business email compromises (BEC), ransomware, distributed denial-of-service (DDoS) and Trojan horse malware.

The impact on both the public and private sectors is significant, creating unprecedented financial, operational and reputational risk factors for organizations worldwide. According to the SEC, the average cost of a cyber data breach is now $7.5 million. And the average cost of cyber liability insurance coverage has increased by 30% or more each year for the past several years. Worse still, with the growing popularity of the Internet of Things (IoT), there has been a 600% increase in the number of cyber-attacks on IoT-connected devices in the past year, especially those focused on medical devices.

The expanding use of the Internet and software applications has dramatically increased the number of vulnerabilities within information systems, networks, software and their respective endpoints, exposing each to the potential for fraudulent actions such as identity theft, identity fraud, business email scams and data breaches. The types of information that hackers consider most valuable include: intellectual property (IP), personally identifiable information (PII), protected health information (PHI) and payment card information (PCI).

From a regulatory standpoint, the continually evolving cybersecurity and data privacy requirements in the U.S. and abroad create significant liabilities for companies. The pending January 2020 implementation of the California Consumer Privacy Act (CCPA) is of significant concern to organizations who do business in California, and could open a Pandora's box of potential litigation related to data breaches involving the personal information of California residents.

As a result, C-suite executives are struggling to determine the right strategy and investments to secure their vital data assets, ensure business operations meet evolving regulatory compliance requirements, and reduce the impact of data breach litigation. The best practice to address each of these concerns is to implement a threat-based cybersecurity program, which takes steps to safeguard against the most likely threats an organization will face, juxtaposing internal vulnerabilities against the evolving external threat environment.

BDO

THE GROWTH OF THE CYBERSECURITY MARKETPLACE

The cybersecurity marketplace has rapidly grown to a $100 billion industry, offering a wide range of cybersecurity hardware, software and professional services. There are now an incredible number of companies offering cybersecurity technologies, products and services, often claiming to have the solution to many of your cybersecurity needs. Unfortunately, no single product or service can provide a magic solution to this multifaceted, ever-evolving, and highly complex set of global information security challenges.

Thus, many C-suite executives are trying to make the right investment decisions, but often they are not well informed regarding the cyber threats facing their organization and all the potential cyber liabilities. Rather than investing valuable resources in protecting specific types of high-value data, a threat-based approach to cybersecurity identifies the vulnerabilities that a cyber-attack would likely try to exploit, and outlines measures to secure those vulnerabilities.

CYBERSECURITY FOR C-SUITE EXECUTIVES – TOP TEN CHALLENGES

Based upon our experience with hundreds of companies worldwide, across all industries, the following questions capture the most significant cybersecurity and data privacy challenges faced by the C-suite in most organizations:

1. What are the best methods and tools to identify, track and maintain all data/information assets with appropriate information governance, data mapping and cybersecurity?

2. How can the C-suite efficiently and cost-effectively verify identities and control information access?

3. What are the best tools and practices to ensure compliance of third parties and supply chain partners with evolving cybersecurity and data privacy regulatory requirements in the U.S. and internationally?

4. What is the best method to effectively deliver timely cybersecurity and data privacy education and training?

5. Should the C-suite invest in acquiring new information security hardware, software and resources to enhance cybersecurity, or is it better to outsource to a proven managed security services provider (MSSP)?

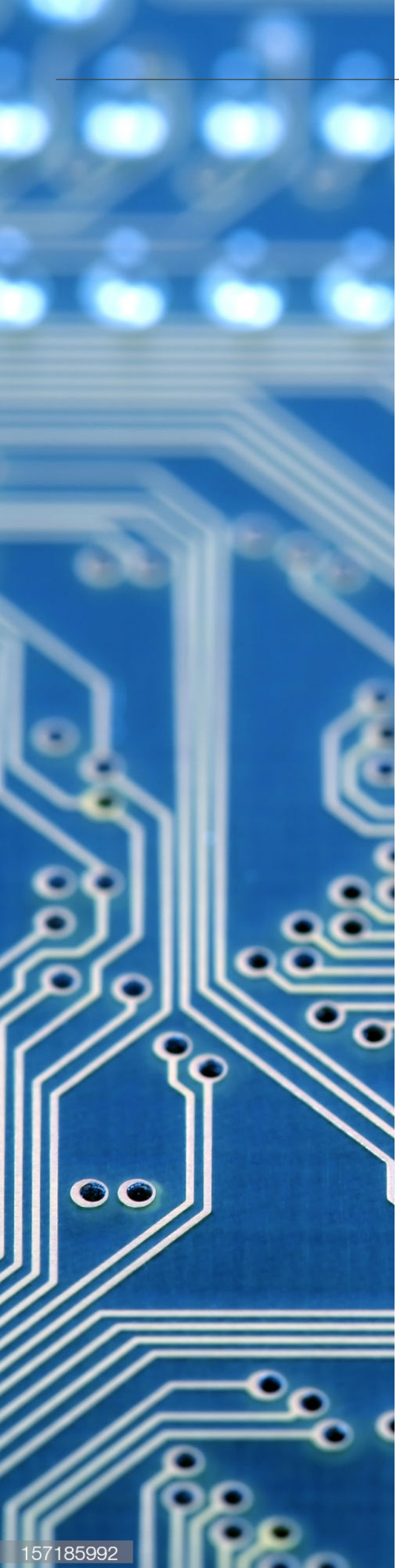
6. Who should the C-suite turn to for advice after a major cyber data breach occurs within an organization?

7. What actions should the C-suite take to ensure they are compliant with all current regulatory requirements for their industry and geographic location, as well as all customer contractual requirements?

8. What proactive actions can the C-suite take to mitigate insider threats and fraud?

9. What is the best approach to ensure an organization has developed an appropriate business continuity plan (BCP)?

10. How much cyber liability insurance coverage is sufficient?



THREAT-BASED CYBERSECURITY – GUIDELINES FOR IMPROVED BUSINESS RESULTS

BDO recommends a threat-based cybersecurity approach to combat cyber-attacks and mitigate costly cyber data breaches. Threat-based cybersecurity is forward-looking and uses analysis of a company's unique threat profile to identify at-risk areas and protect against the most likely types of cyber-attacks that could occur. This requires a multipronged strategy and a range of proactive steps, including:

1. Hire an independent firm to conduct some or all of the following advanced diagnostics:
   - Email threat assessment
   - Network and endpoint threat assessment
   - Vulnerability assessment
   - Penetration testing
   - Spear-phishing test campaign
   - Red-team security assessment
   - Security software tools assessment
2. Hire a dedicated Chief Information Security Officer (CISO) who reports to the CEO or General Counsel to develop a sound cybersecurity and data privacy risk management program tailored to the specific cyber threats facing your organization
3. Implement advanced software encryption with multi-factor authentication, including biometrics
4. Provide timely and effective cybersecurity education and training programs for the entire organization, top to bottom
5. Implement a timely and effective software security patch management program
6. Ensure the organization has developed and implemented a robust information governance program to map, track and secure all data assets
7. Review and periodically test the organization's Incident Response Plan
8. Review and periodically test the organization's Business Continuity Plan and Disaster Recovery Plan
9. Conduct or outsource 24x7x365 managed detection and response (MDR) of the organization's information systems, networks, endpoints, software applications, and email systems using the most advanced machine learning and artificial intelligence applications
10. Verify the compliance of the organization and all supply chain partners with all cybersecurity and data privacy regulatory requirements by using independent compliance and risk assessments conducted by qualified firms

SUMMARY

The C-suite worldwide is increasingly concerned about the growing risk of a massive cyber data breach, like those encountered by Capital One, Facebook, Equifax, and numerous government agencies. Thus, C-level executives within all organizations need to understand the value of the information assets they possess, the cybersecurity and privacy related risks, and then factor the benefits of cybersecurity investments and risk variables into their respective business equation.

Simply put, it is vital that C-suite executives adopt a threat-based cybersecurity strategy to understand the cyber threats they are facing, and then make the right investments to mitigate identified vulnerabilities, thereby reducing their cyber liability while also maximizing resources.

CONTACT

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

GREG SCHU
Partner, Governance, Risk & Compliance Services
gschu@bdo.com

MIKE STIGLIANESE
Managing Director, Head of Cyber Risk Assessments
mstiglianese@bdo.com

ERIC CHUANG
Managing Director, Head of Incident Response
echuang@bdo.com