CYBERSECURITY 2020: MYTHS VS. REALITY

THE WORLD WE LIVE IN

In our digitally-driven society, cybersecurity is an essential element in ensuring both data integrity and privacy. Nearly every organization is going through some form of digital transformation to enhance data access, increase the speed to market, and reduce operational expenses. Unfortunately, we also live in a time of extensive fake technology, rampant cyber fraud, increased sophistication of cyber-attacks, and costly cyber data breaches. Many organizations are struggling to separate the facts from the fiction (mis-information, hype, and fake news) in understanding the value of the growing number of cybersecurity software, hardware, insurance policies, and related professional services working to mitigate cyber fraud, cyber lawsuits, and data breach damages. To dispel some of the common myths surrounding cybersecurity, we look to research, extensive field experience, and common sense.

BDO DIGITAL

Myth #1

Most companies have significantly increased their investments in cybersecurity software, hardware, insurance policies, and related professional services in the past three years to appropriately manage cyber risks.

Reality

By 2021, global cyber fraud and cyber data breach damages are expected to reach $6 trillion, increasing from the current $4 trillion in global damages, according to Cybersecurity Ventures. The global damages from cyber fraud and cyber data breaches have been on the rise for the past ten years — largely due to a gross under-investment in global cybersecurity. Many companies have modestly increased their spending on cybersecurity tools and services. However, the average organization is currently spending/investing only 2% to 5% of their annual Information Technology budget on information security, according to studies by Forrester Research, the Gartner Group, and the Carnegie Mellon University (CMU) Software Engineering Institute (SEI).

Myth #2

Nearly all organizations are providing timely and insightful information on evolving cyber fraud and cyber-attack risks to their C-Suite executives and Board of Directors.

Reality

According to BDO's 2019 Cyber Governance Survey, less than 30% of the C-Suite and Board of Directors surveyed stated they received quarterly or more frequent updates on cyber-attack threats, cyber fraud threats, or cyber data breach risk factors.

Myth #3

Most organizations have hired a full-time, dedicated, and highly skilled Chief Information Security Officer (CISO) to manage their organization's information security strategy, people, policies, plans, systems, tools, and procedures to effectively mitigate cyber fraud and cyber data breach risks.

Reality

Less than 20% of all organizations surveyed by BDO during the past three years have hired a CISO. Of those who have been assigned the title of CISO, many lack appropriate cybersecurity education, training, and professional certification.

Myth #4

Cybersecurity specialists are capable of effectively managing the growing number of cyber threats as a direct result of technological advancements in big data analytics, data visualization, data encryption, biometrics, identity and access management, zero trust data architecture, cyber-attack simulations, computer-based training, and artificial intelligence.

Reality

The majority of small to mid-size enterprises have made relatively limited technological investments to enhance cybersecurity, due to financial reasons.

Myth #5

The use of cybersecurity education, training, simulations, and email phishing campaigns have enabled organizations to thwart all email phishing attacks.

Reality

The human factor remains the weakest link in cybersecurity. Even after conducting periodic cybersecurity awareness education, training, and spear-phishing campaigns, most organizations typically find about 5% or more of their employees as still susceptible to socially-engineered email phishing attacks. In addition, human insider-threat cyber-attacks represent a clear and present danger to nearly every organization.

Myth #6

Only large multi-billion dollar companies and government agencies are subject to significant cyber data breaches.

Reality

According to a recent Forrester Research study, nearly every industry worldwide has suffered from significant cyber data breaches and about 30% of all reported cyber data breaches occurred in companies with less than 200 employees. Furthermore, it is important to note that many cyber-attacks and data breaches are not reported.

Myth #7

Cyber liability insurance coverage can ensure organizations are financially protected from costly cyber fraud and data breaches.

Reality

There are more than 100 insurance carriers globally offering a wide-range of cyber liability insurance coverage policies, with very diverse limitations, exemptions, and related terms and conditions. Most companies find it to be difficult to substantiate some of the damages while preparing a cyber data breach claim and do not always receive full reimbursement from the insurance carriers for needed post-breach cybersecurity remediation actions.

Myth #8

The majority of prime contractors are effectively managing their supply chain partners' cybersecurity risk via vendor relationship management programs and independently conducted cyber audits.

Reality

Most prime contractors are relying primarily on vendor cyber risk self-assessments and are not conducting vendor cybersecurity risk audits or requiring independently conducted industry specific cybersecurity audits and cybersecurity compliance certifications such as ISO 27001.

Myth #9

To rapidly detect cyber intrusions and reduce the impact of a cyber data breach, most organizations have implemented an effective 24 x 7 x 365 email system and network system monitoring, detection, and incident response capability.

Reality

Many small to mid-size enterprises are vulnerable to these damages and do not conduct 24 x 7 x 365 active monitoring, detection, and incident response capability, either internally or via outsourced Managed Security Services Providers (MSSPs).

Myth #10

Most companies and government organizations have developed, documented, and implemented an effective cyber defense program.

Reality

Unfortunately, most organizations are not implementing an effective Threat-Based Cybersecurity program. Rather, some companies do not have any structured or documented cybersecurity policies, plans, and procedures. Many companies and government organizations are choosing to implement a Compliance-Based Checklist approach to cybersecurity, which is well-intended, but often does not achieve real cyber defense as the regulations are unable to keep pace with the rapid pace of cyber-attack tactics, methods, and procedures.

SUMMARY

Too often, senior executives make poor information security investment decisions based upon mis-information, short-term financial focus, and a lack of cybersecurity awareness, leaving their businesses vulnerable to the ramifications of cyber-attacks. To achieve real information security, an organization must understand key elements of and misconceptions surrounding the issue, such as: cyber-attacker's data targets and sophisticated methods, as well as the assessment of their organization's real information system attack vulnerabilities.

CONTACT

GREGORY GARRETT
Head of U.S. & International Cybersecurity
703 -70-1019
ggarrett@bdo.com

GREG SCHU
Partner, Governance, Risk & Compliance Practice
612-367-3045
gschu@bdo.com

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