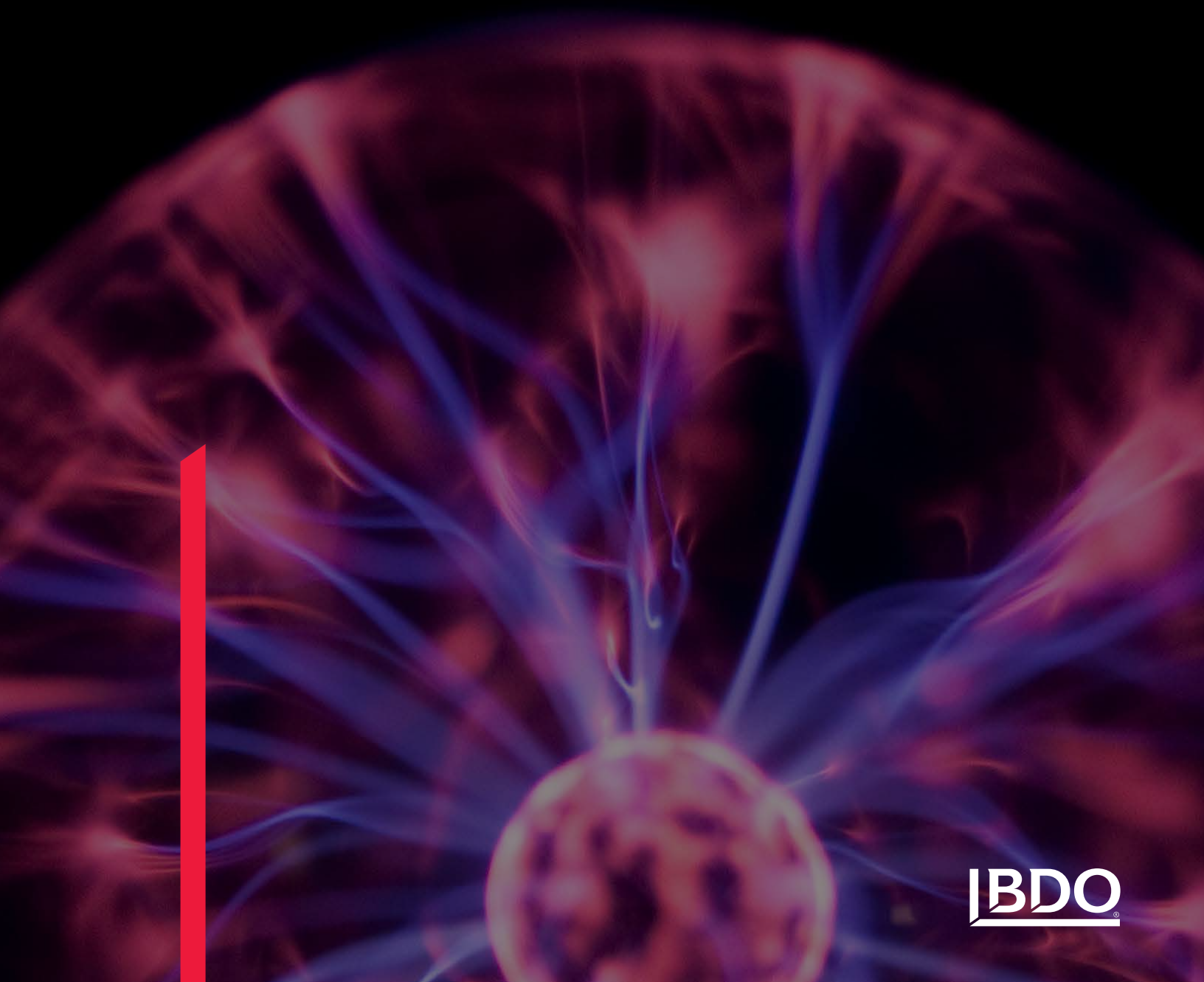
CYBERSECURITY IN 2020: TOP TEN PREDICTIONS AND RECOMMENDATIONS



BDO

THE WORLD WE LIVE IN!

According to EY's 2018-2019 Global Information Security Survey, over 6.4 billion fake emails are sent everyday by nation-state cyber-attack groups, criminal cyber-attack groups, and hackers worldwide. This results in the theft of over 2 billion private identities and $3.5 billion in cyber damages daily. To combat the ever-growing global cyber-attacks in both the public and private sectors, the cybersecurity marketplace has expanded to $100 billion in annual purchases of software, hardware, and related cybersecurity professional services with a 12% Compounded Annual Growth Rate (CAGR), as reported by the Gartner Group. Despite the growing investments in cybersecurity, the public and private sectors are not keeping up with an estimated $4.2 trillion in annual global fraud, theft, and data breach damages caused by cyber-attackers, which is predicted to exceed $6 trillion in cyber-attack related damages by 2021.

Forester Research estimates less than 2% of all information technology professionals globally are educated, trained, certified, and actively working as cybersecurity professionals. Clearly, government organizations, publicly traded companies, and privately-owned companies need to take the threat of cyber-attacks more seriously by investing more resources in creating an effective cyber defense. Realizing that 40% or more of cyber vulnerabilities are directly linked to employee behavior, per the Gartner Group's latest studies, it is vital that organizations focus more on their employees via cybersecurity awareness, education, training, and use of simulations to create a stronger human firewall to protect their vital digital assets.

CYBERSECURITY IN 2020: TOP TEN PREDICTIONS

The following are BDO's top data and cybersecurity predictions for 2020, as we enter a new digital decade.

1. **Continued Global Shortage of Cybersecurity Talent**
   There continues to be an on-going under-investment in cybersecurity education, training, and certification programs at the undergraduate, graduate, and continuing education levels. Combined with the incredible increase in cyber-attacks globally, this has resulted in a significant shortage of cybersecurity professionals and related data scientists required to meet the increased cybersecurity demands worldwide.

2. **Growth of Zero Trust Cyber Data Architecture**
   Increasingly, organizations are adopting the Zero Trust software architecture approach to thwart the damages of cyber-attacks. The Zero Trust Architecture method is designed to create micro-perimeters within information systems to increase data segmentation and establish micro-firewalls within the network to reduce the ease of lateral movements by cyber-attackers within an information system once an intrusion has occurred.

3. **Rise of Insider Threat Cyber-Attacks**
   As organizations improve their overall integrated cyber defense via enhanced investments in: cybersecurity training, encryption, multi-factor authentication, zero trust architecture, advanced data analytics, continuous diagnostics, monitoring, detection, and incident response; often using machine learning and/or leveraging new blockchain technologies; then cyber-attackers will seek to by-pass all of the security measures by bribing employees who have restricted-access to valuable intellectual property and key data assets in order to steal the data.

4. **Expansion of IoT Cyber-Attacks**
   According to Symantec, the number of Internet of Things (IoT) connected devices is estimated to rapidly increase from 10 billion devices in 2017 to over 26 billion devices by the end of 2020. With the tremendous increase in the number of internet connected devices, it is anticipated that there will be a dramatic increase in the number of cyber-attacks on IoT connected devices, especially medical devices.

5. **Growth of Distributed Denial of Service (DDoS) Cyber-Attacks**
   The significant success of Distributed Denial of Service (DDoS) cyber-attacks in the past few years suggests that these cyber-attacks will continue to increase worldwide, especially in the retail, consumer products, and critical infrastructure industries, where they have experienced the greatest impact.

6. **Increase in Cyber-Impersonation Attacks and Business Email Compromise (BEC) Attacks**
   During the past 18 months, the use of socially-engineered cyber impersonation attacks and Business Email Compromise (BEC) attacks have grown exponentially in both number and sophistication. Specifically targeting senior executives in both government agencies and the private sector to re-direct payments to cyber-attackers, usually intended for business partners or suppliers.

7. **Explosion in the Use of Machine Learning or Artificial Intelligence to Combat Cyber-Attacks**
   Organizations worldwide are exploring numerous use cases to implement machine learning and/or artificial intelligence, to enhance proactive cyber defense tactics and optimize cyber-attack monitoring, intrusion detection, and incident response capabilities.

8. **Exploitation of Cyber Weakest Link Attacks on Supply-Chains**
   With the success of cyber-attacks on global supply-chains across numerous industries, including: oil, gas, energy, defense, aerospace, healthcare, manufacturing, retail, and consumer products; expect an increase of cyber-attacks targeting the most vulnerable organizations in supply-chain networks, which are usually small business vendors/third-party suppliers, in order to gain access to the intellectual property of larger organizations.

9. **Lack of Empowerment in CISO Role**
Too many organizations have not adequately empowered and supported their Chief Information Security Officer (CISO) with the funding, resources, and senior executive commitment to ensure an appropriate level of cyber defense. Most organizations continue to care far more about the organization's network data capacity, ease of data access, and software applications than the protection of the data assets and the resilience of the information system from damaging cyber-attacks.

10. **Increasingly Complex Cybersecurity and Data Privacy Regulatory Landscape**
As companies all strive to protect themselves and their personal identifiable information from the growing number of cyber fraud cases and cyber data breaches, the number and complexity of new cybersecurity and data privacy laws, regulations, standards, and contractual requirements, are rapidly increasing. This results in the rise of potential civil and criminal penalties for non-compliance, including: European Union (EU) General Data Privacy Regulation (GDPR), ISO 27001 Information Security Standard, National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework (RMF), the Payment Card Industry (PCI) Data Security Standard (DSS), the New York Department of Financial Services (NYDFS) Cybersecurity requirements for financial institutions, and the California Consumer Privacy Act (CCPA), just to name a few.

CYBERSECURITY RECOMMENDATIONS

To reduce either the probability of a cyber fraud incident or a significant data breach, and to mitigate the negative financial and reputational impacts of cyber-attacks, we offer the following recommendations:

1. **Create an Organizational Culture of Cybersecurity**
   Ensure the C-Suite consistently promotes and supports all employees practicing effective cybersecurity policies, processes, and procedures, via a comprehensive cybersecurity awareness, education, and training program.

2. **Hire a Highly Qualified Chief Information Security Officer (CISO)**
   Provide the CISO with adequate resources and funding to take necessary strategic and tactical actions, allowing the CISO to develop and implement a comprehensive cybersecurity risk management program for the entire organization.

3. **Implement Advanced Cyber Diagnostic Assessments, on a Regular Basis, Including:**
   - Email Cyber-Attack Assessments
   - Network & Endpoint Cyber-Attack Assessments
   - Vulnerability Scanning Assessments
   - Penetration Testing
   - Security Software Assessments
   - Spear-Phishing Campaigns

4. **Encrypt All Data**

5. **Verify All Identities and Credentials**
   Require the use of multi-factor authentication (MFA), including biometrics (fingerprint, voice, or facial recognition).

6. **Secure Information Systems**
   Implement Zero Trust Architecture designed to compartmentalize data and restrict data access, thus reducing the potential damages from unauthorized access to sensitive information.

7. **Establish a Rapid Cyber-Attack Incident Response Plan**
   Develop and periodically test an enterprise-wide, well-coordinated information system incident response plan to quickly identify, contain, eradicate, and recover from cyber-attacks.

8. **Conduct 24 X 7 X 365 Monitoring, Detection & Response (MDR)**
   It is essential to continually monitor, detect, and respond to all cyber incidents including: email system, network, software applications, and all information system endpoints; using advanced security information event management (SIEM) software, data visualization tools, automation, and artificial intelligence (AI) capabilities.

9. **Protect the Information System by Ensuring a Timely and Effective Software Patch Management Program**

10. **Ensure Information System Resilience**
    Implement and periodically test an enterprise-wide business continuity plan (BCP) and disaster recovery plan (DRP), including an off-line and fully redundant data back-up system.

SUMMARY

In retrospect, we have provided our top ten predictions for cybersecurity challenges in 2020 and given our top ten cybersecurity recommendations for improvement actions. We hope you will heed our advice, so you can see the challenges ahead, make well-informed business decisions to maximize your business opportunities, and minimize the negative impacts of cyber fraud and costly data breaches.

CONTACT

GREGORY GARRETT
Head of U.S. and International Cybersecurity Advisory Services
703-770-1019
ggarrett@bdo.com

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

MIKE STIGLIANESE
Managing Director, Head of Cyber Risk Assessments
212-817-1782
mstiglianese@bdo.com

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