DIGITAL TRANSFORMATION: BEGIN WITH CYBERSECURITY IN MIND

All too often companies move to digitally transform data without a strategic or proactive approach to cybersecurity and data privacy. As a result of the COVID-19 pandemic, there has been a dramatic, sudden, and unexpected increase in people working, learning, teaching, and consulting from home. This largely unplanned transition from office-based and school-based network access to remote/home access has created some unique capacity, operational, and cybersecurity challenges. Many organizations who conduct digital transformations have realized gains in digital productivity, via increased speed and access to data, more rapid data analysis, and related data storage cost savings, especially when cloud-based data storage is included. However, increasingly these same organizations have encountered costly cyber-attacks in the form of socially-engineered spear-phishing attacks, business email compromise (BEC) or spoofing attacks, and/or ransomware attacks, because they did not adequately or proactively begin their digital transformation with cybersecurity in mind.

Frequently, organizations of all sizes, and from every industry, consider cybersecurity to be an afterthought. However, these organizations are learning this leads to costly lessons on cyber fraud and/or data breaches. In 2019, the estimated global damages from cyber fraud and data breaches exceeded $4 trillion, according to the Gartner Group. Rather, cybersecurity should be at the forefront of strategic business planning for all digital projects. IBM Security reported the average cost of a cyber data breach now exceeds $8.2 million.

As both the level of sophistication and the number of cyber-attacks increases every year, it has become painfully evident that the benefits of digital information including: speed, easy data access, rapid data analysis, data visualization, and related cost savings, can be completely lost or stolen as a result of damages. The damages can come from many forms such as: cyber-attacks, cyber fraud, cyber data breaches, cyber-related law suits for cybersecurity negligence, federal and/or state regulatory penalties for cybersecurity/data privacy compliance failures, and negative impacts to an organization's reputation due to inadequate information security. In addition, the global cybersecurity and data privacy regulatory landscape is increasingly complex. This leaves the door open to potential massive class-action lawsuits for cyber data breaches disclosing consumers' personal identifiable information, such as the new California Consumer Privacy Act (CCPA) enacted in January 2020. The CCPA clearly states an organization cannot ensure data privacy without "reasonable security."

BDO DIGITAL

BEGIN WITH CYBERSECURITY IN MIND

So, what exactly does it mean to begin a digital project or digital transformation of an organization with cybersecurity in mind? Simply said, it means to start all digital project planning by asking the right cybersecurity related questions up-front, including the following:

20 Key Cybersecurity Questions To Consider:

1. Will this project and/or the organization require access to any of the following types of data or information, including:
   - Personal Identifiable Information (PII) of employees, partners, or consumers Protected Health Information (PHI)
   - Payment Card Information (PCI)
   - Intellectual Property (IP)
   - Controlled Unclassified Information (CUI)
   - Covered Defense Information (CDI)
   - Classified Information (CI)
   - Company Sensitive Information (CSI)
2. Who will need access to the project and organization data?
3. How will information access be controlled, internally and with vendors/subcontractors/clients?
4. Where will the project and organization information reside/be stored and how will it be secured?
5. Who will develop and manage the organization's information governance plan, information system security plan, and data resilience or back-up plan?
6. Does the organization have the right people/resources to effectively lead cybersecurity and data privacy strategic planning and implementation?
7. What project and organization data segmentation or compartmentalization (i.e. zero trust data architecture) is needed to protect the information?
8. What identity, access, and data control procedures should be implemented, including: encryption, biometrics, multi-factor authentication, etc.?
9. Does the project or the organization's data need to be compliant with one or more specific industry cybersecurity or data privacy regulatory or contractual requirements? If so, which specific requirements (i.e. National Institute of Standards & Technology [NIST] Special Procedure 800-171,ISO 27001, Payment Card Industry Data Security Standard [DSS], New York Department of Financial Services [NYDFS] Cybersecurity, Health Insurance Portability & Accountability Act [HIPAA] Cybersecurity, HITRUST – Common Security Framework [CSF], the new U.S. Department of Defense [DOD] Cybersecurity Maturity Model Certification [CMMC], European Union General Data Protection Regulation [GDPR], and/or the California Consumer Privacy Act [CCPA], etc.)?
10. What cybersecurity vulnerabilities currently exist within the organizations email system, network/information system, software applications, and endpoints?
11. Does the organization currently conduct 24/7/365 data monitoring, cyber intrusion detection, and cyber incident response for all information? If not, are these services provided by a highly qualified Managed Security Services Provider (MSSP)?
12. Has the organization developed, documented, implemented, and tested effective cybersecurity policies, plans, and procedures for project information, including:
    - Incident Response Plan (IRP)
    - Business Continuity Plan (BCP)
    - Disaster Recovery Plan (DRP)

13. Which cyber threat actors (nation-state cyber-attack groups, organized criminal cyber-attack groups, and/or hackavists) would be most interested in the information involved with this project, the organization, the leadership, and the supply-chain?
14. What cyber threat vectors would cyber-attackers most likely exploit within the organization in order to gain access to valuable information?
15. How susceptible are the organization's employees from top to bottom to socially-engineered spear-phishing cyber-attacks and business email compromise (BEC) attacks?
16. Does the organization currently outsource the Information Technology (IT) services to a Managed Services Provider (MSP) or outsource the cybersecurity to a Managed Security Services Provider (MSSP)? Is the C-suite of the organization satisfied with the outsourced IT or cybersecurity services?
17. When did the organization most recently conduct a cyber-attack simulation or tabletop exercise with the C-suite and board of directors?
18. What percent of the organization's annual IT budget is spent on cybersecurity?
19. Does the organization have adequate cyber liability insurance coverage?
20. How effective is the organization's cybersecurity education and training program?

The twenty (20) key cybersecurity questions to consider are just a starting point for a deeper discussion about developing and implementing a strategic, proactive, and comprehensive cybersecurity program. An organization's responses to the above stated questions will certainly help paint a picture of their current level of cyber defense, potential cyber threats, and known cyber vulnerabilities, which will help cybersecurity experts to build a customized road-map for enhanced cybersecurity and data privacy.

SUMMARY

Too many organizations make critical mistakes when embarking on large-scale digital transformation for their organization. Many fail to develop a strategic, proactive, and threat-based cybersecurity program and under-investing in the following five (5) key elements of cybersecurity:

- Provide cybersecurity education/training for all members of the organization from the top to the bottom.
- Hire the right people to lead the organization's cybersecurity and data privacy strategic planning and implementation from the start.
- Engage independent firms to conduct periodic cybersecurity diagnostic testing, including: computer vulnerability scanning, penetration testing, email system cyber-attack assessments, spear-phishing campaigns, and dark web analysis, to understand the organization's cyber vulnerabilities and threats.
- Ensure continuous 24/7/365 information monitoring, intrusion detection, and rapid cyber incident response services either internally or via outsourced Managed Security Services Providers (MSSP).
- Implement and test appropriate information resilience plans and procedures via cyber incident response plans, cyber business continuity plans, and disaster recovery plans.

The key to success is to begin all digital transformation projects with cybersecurity in mind. By engaging with cybersecurity experts from the start of a project, or new business venture, an organization can ask the right questions then develop a proactive and threat-based cybersecurity program. Remember, in the digital age an organization can only achieve information integrity and data privacy through effective cybersecurity.

CONTACTS:

GREGORY GARRETT
Head of US &
International Cybersecurity
703-893-0600
ggarrett@bdo.com