BDO

CYBERSECURITY

DIGITAL TRANSFORMATION: BEGIN WITH CYBERSECURITY IN MIND

AUDIT • ADVISORY • TAX

INTRODUCTION

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 organisations transformed digitally have realised gains in digital productivity via increased speed and access to data, faster data analysis and related data storage cost savings, especially when cloud-based data storage is included. However, increasingly these same organisations 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. They did not adequately or proactively begin their digital transformation with cybersecurity in mind.

Frequently, organisations of all sizes and from every industry consider cybersecurity to be an afterthought. However, these organisations 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. IBM Security reported the average cost of a cyber data breach now exceeds $8.2 million. Cybersecurity should be at the forefront of strategic business planning for all digital projects.

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, namely speed, easy data access, rapid data analysis, data visualization, and related cost savings, can be completely lost or stolen as a result of damages. These damages can come in the form of cyber-attacks, cyber fraud, cyber data breaches, cyber-related law suits for cybersecurity negligence, state regulatory penalties for cybersecurity/ data privacy compliance failures, and negative impacts to an organisation'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 lawsuits for cyber data breaches disclosing consumers' personal identifiable information, such as the Protection of Personal Information (POPI) Act. POPI clearly states an organisation must ensure data privacy.

BEGIN WITH CYBERSECURITY IN MIND

So, what exactly does it mean to begin a digital project or digital transformation of an organisation 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 organisation require access to any of the following types of data or information.

- Personal Identifiable Information (PII) of employees, partners, or consumers
- Payment Card Information (PCI)
- Intellectual Property (IP)
- Controlled Unclassified Information (CUI)
- Classified Information (CI)
- Company sensitive information (CSI)

2. Who will need access to the project and organisation data?

3. How will information access be controlled, internally and with vendors/subcontractors/clients?

4. Where will the project and organisation information reside/be stored and how will it be secured?

5. Who will develop and manage the organisation's information governance plan, information system security plan, and data resilience or back-up plan?

6. Does the organisation have the right people/resources to effectively lead cybersecurity and data privacy strategic planning and implementation?

7. What project and organisation data segmentation or compartmentalisation (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 organisation'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? For example: European Union (EU) General Data Privacy Regulation (GDPR), South Africa's Protection of Personal Information (POPI) Act, 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), just to name a few.

10. What cybersecurity vulnerabilities currently exist within the organisation's email system, network/information system, software applications, and endpoints?

11. Does the organisation 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 organisation 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, organised criminal cyber-attack groups, and/or hackavists) would be most interested in the information involved with this project, the organisation, the leadership, and the supply-chain?

14. What cyber threat vectors would cyber-attackers most likely exploit within the organisation in order to gain access to valuable information?

15. How susceptible are the organisation's employees from top to bottom to socially-engineered spear-phishing cyber-attacks and business email compromise (BEC) attacks?

16. Does the organisation 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 organisation satisfied with the outsourced IT or cybersecurity services?

17. When did the organisation most recently conduct a cyber-attack simulation or tabletop exercise with the C-suite and board of directors?

18. What percentage of the organisation's annual IT budget is spent on cybersecurity?

19. Does the organisation have adequate cyber liability insurance coverage?

20. How effective is the organisation's cybersecurity education and training program?

These 20 key cybersecurity questions are just a starting point for a deeper discussion about developing and implementing a strategic, proactive and comprehensive cybersecurity programme. An organisation's responses will 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 customised road-map for enhanced cybersecurity and data privacy.

SUMMARY

Too many organisations make critical mistakes when embarking on large-scale digital transformation. Many fail to develop a strategic, proactive and threat-based cybersecurity programme and under-invest in five key areas of cybersecurity:

- Providing cybersecurity education/training for all members of the organisation from the top to the bottom.
- Hiring the right people to lead the organisation's cybersecurity and data privacy strategic planning and implementation.
- Engaging 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 organisation's cyber vulnerabilities and threats.
- Ensuring continuous 24/7/365 information monitoring, intrusion detection and rapid cyber incident response services either internally or via outsourced Managed Security Services Providers (MSSP).
- Implementing and testing 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 organisation can ask the right questions then develop a proactive and threat-based cybersecurity programme. An organisation can only achieve information integrity and data privacy through effective cybersecurity.

BDO

FOR A CLEAR PERSPECTIVE, PLEASE CONTACT US:

MICHIEL JONKER
Director
BDO Global Cybersecurity Leadership Board Member
+27(0)82 570 9478
mjonker@bdo.co.za

SADIKA MAHARAJ
Associate Director
Cybersecurity Leader
+27(0)66 488 4196
samaharaj@bdo.co.za

/BDOSouthAfrica /bdoafrica /bdo_sa /company/bdo-south-africa

www.bdo.co.za

BDO Advisory Services (Pty) Ltd, a South African company, is an affiliated company of BDO South Africa Inc, a South African company, which in turn is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the Member Firms. For more information, please visit: https://www.bdo.co.za/en-za/services/advisory/cyber-innovation-assurance-and-analytics-ciaa/cybersecurity-and-digital-forensics Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2020 BDO South Africa. All rights reserved.