DIGITAL TRANSFORMATION: BEGIN WITH CYBER SECURITY IN MIND

More people are now starting to work, learn, teach and consult from home. This transition from office-based and school-based network access to remote/home access has created unique capacity, operational and cyber security challenges.

All too often companies move to digitally transform processes and data without a strategic or proactive approach to cyber security and data privacy. Many organisations who conduct digital transformations have realised gains in digital productivity, via increased speed and access to data, more rapid data analysis, and related data storage cost savings. This is especially true when cloud- based data storage is included. However, 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. This is a symptom of the inadequate or reactive approach to cyber security during their digital transformation.

All too often we see organisations of all sizes, across every industry, consider cyber security as an afterthought, which leads to costly lessons on cyber fraud and/or data breaches. In 2019, the Gartner Group reported the estimated global damages from cyber fraud and data breaches exceeded USD$4 trillion. This sharp increase in estimated cost is echoed by IBM Security who reported the average cost of a cyber data breach now exceeds AUD$5.6 million. From this, is it evident cyber security 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 the benefits of digital information – which include speed, easy data access, rapid data analysis, data visualisation 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 cyber security negligence
- Federal and/or state regulatory penalties for cyber security/data privacy compliance failures
- Negative impacts to an organisation's reputation due to inadequate information security.

Compounding these potential damages, the global cyber security and data privacy regulatory landscape is becoming increasingly complex. This opens the door to potential class-action lawsuits for cyber data breaches disclosing consumers' personal identifiable information. Legislation such as the Notifiable Data Breach (NDB) Scheme associated with the Privacy Act 1988 means victims of a data breach are better positioned to identify breaches where more could have been done to protect their information.

BDO

BEGIN WITH CYBER SECURITY IN MIND

So, what exactly does it mean to begin a digital project or digital transformation of an organisation with cyber security in mind? Simply said, it means to start all digital project planning by asking the right cyber security related questions up-front.

20 key cyber security questions to consider:

Access to information

1. Will this project and/or the organisation require access to any of the following types of data or information, including:
   - Personal Identifiable Information (PII) of employees, partners, or consumers
   - Government identifiers
   - Health and medical information
   - Payment Card Information (PCI)
   - Intellectual Property (IP)
   - Security classified information
   - Company sensitive information.
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?

Current capability

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 cyber security and data privacy strategic planning and implementation?
7. Does the organisation currently outsource the Information Technology (IT) services to a Managed Services Provider (MSP) or outsource the cyber security to a MSSP? Is the C-suite of the organisation satisfied with the outsourced IT or cyber security services?
8. What percent of the organisation's annual IT budget is spent on cyber security?
9. How effective is the organisation's cyber security education and training program?

Infrastructure

10. What project and organisation data segmentation or compartmentalisation (i.e. zero trust data architecture) is needed to protect the information?
11. What identity, access and data control procedures should be implemented, including: encryption, biometrics, multi-factor authentication, etc?
12. What cyber security vulnerabilities currently exist within the organisations email system, network/information system, software applications and endpoints?

Policy and procedures

13. Does the project or the organisation's data need to be compliant with one or more specific industry cyber security or data privacy regulatory or contractual requirements? If so, which specific requirements (i.e. National Institute of Standards and Technology [NIST] Special Procedure 800-171,ISO 27001, Payment Card Industry Data Security Standard [DSS], The Privacy Act 1988, The NDB Scheme, Australian Information Security Manual [ISM], European Union General Data Protection Regulation [GDPR], Australian Prudential Regulation Authority's [APRA's] Prudential Standard CPS 234, The Australian Energy Sector Cyber Security Framework
14. 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)?
15. Has the organisation developed, documented, implemented and tested effective cyber security policies, plans and procedures for project information, including:
    - Incident response planning
    - Business continuity planning
    - Disaster recovery planning.

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

Risk assessment

17. Which cyber threat actors (nation-state cyber attack groups, organised criminal cyber attack groups, insiders and/or hackavists) would be most interested in the information involved with this project, the organisation, the leadership and the supply-chain?

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

19. How susceptible are the organisation's employees from top to bottom to socially-engineered spear-phishing cyber attacks and BEC attacks?

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

The twenty key cyber security questions to consider are just a starting point for a deeper discussion about developing and implementing a strategic, proactive and comprehensive cyber security program. An organisation's responses to the above stated questions will begin to paint a picture of their current level of cyber defense capabilities and threat profile. Both elements form the base from which cyber security experts can begin to build a customised roadmap for enhanced cyber security and data privacy.

SUMMARY

Too many organisations make critical mistakes when embarking on large-scale digital transformation for their organisation. This is because many fail to develop a strategic, proactive and threat-based cyber security program. Additionally, these organisations are under-investing in the following five key elements of a cyber security program:

- Providing cyber security education/training for all members of the organisation from the top to the bottom
- Hiring the right people to lead the organisation's cyber security and data privacy strategic planning and implementation from the start
- Engaging independent firms to conduct periodic cyber security 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 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 cyber security in mind. By engaging with cyber security experts from the start of a project, or new business venture, an organisation can ask the right questions and develop a proactive and threat-based cyber security program.

Remember, in the digital age an organisation can only achieve information integrity and data privacy through effective cyber security.

CONTACTS:

LEON FOUCHE
National Leader, Cyber Security
BDO Australia
+61 7 3237 5688
leon.fouche@bdo.com.au

NICK KERVIN
National Leader, Technology
BDO Australia
+61 8 7324 6145
nick.kervin@bdo.com.au