More cybersecurity awareness 'needed'

MANAGING DIRECTOR of CariSec Global Inc Edward Millington. (FP)

by **EDWARD MILLINGTON**

DIGITAL TRANSFORMATION has grown tremendously regionally for governments, the private sector, and customers in general. It has made the accessibility of public services, e-commerce, investments, education, and so on, easy, including the use of innovative technological services like digital wallets – all demonstrated in 2024.

BARBADOS AND other Caribbean countries have faced increased cyber attacks. (FP)

Let us not forget the use of ChapGPT and many other artificial intelligence driven technologies, products, and services. We also have the transformation of the public health services sector and human resource management of organisations. In fact, we have become dependent on digital technologies and their functions in our lives, businesses and governance, that we are unable to do without them. If so, to many, we will be returning to the stone age.

As highlighted throughout my publications and discussions, while such developments are necessary for human index development and competitiveness, these data-centric-driven technologies have inherited risks. They are susceptible to exploitation by cybercriminals and cyberterrorists. Therefore, we must be aware of digital transformation vulnerabilities and the risks associated with cyber threats. We need to be risk-based in our approach to reducing digital transformational risks that can cause varying levels of business risks and risks to all stakeholders – partners, clients, customers, the public, etc.

As we head into 2025 in a few weeks, our approach to cybersecurity awareness must be strategic. This will make systems safer, build digital trust, and improve digital operational resilience.

A greater need for cyber risk management

In 2024, across the region, we have seen several ransomware attacks, causing data breaches and operational losses in sectors such as government, healthcare, finance, retail, manufacturing, education, etc., affecting services, products, and deliveries. Therefore, our awareness in 2025 must take an approach to recognising cyber risk as a risk that needs to be incorporated into the overall business risk discussion and programme to reduce business risks surrounding cybercriminal activities that can lead to business losses, legal ramifications, reputational damages, etc. Let us not forget the possible harm to the stakeholders.

Known Caribbean countries affected by ransomware (number of) attacks that led to breaches: Aruba (one), the Bahamas (one), Barbados (four), Bermuda (three), British Virgin Islands (one), Cayman Islands (one), Dominican Republic (four), Jamaica (two), Puerto Rico (12), St Vincent and the Grenadines (one), United States Virgin Islands (four), and Venezuela (four).

Fraud against individuals and businesses

Data breaches enhance social engineering and other techniques cybercriminals use to exploit businesses and people – like phishing through emails – not only to compromise but to commit fraud and, in some instances, to blackmail businesses and individuals to achieve their criminal objectives. It is imperative to understand how breach data can be used against you and to monitor all activity throughout business operations and personal life. That is, monitoring for funds transfer fraud, account money transfers, authorising funds, account take-overs, directive calls to perform some action surrounding financial activities, etc. With so many breaches occurring over the last few years, greater awareness and vigilance are needed throughout every aspect of our lives and business operations.

Building and enhancing cyber resilience

In today's digitally transformed world, business and operational resilience is key to reducing business risks and other future liabilities that can put the business's vision, including its well-being, at risk. Sectors such as the government, healthcare, financial services, education, etc., are all critical national infrastructure (CNI). When these CNIs become unavailable, public trust erodes, and public safety becomes a crucial topic, as long-term unavailability can create national security issues. Therefore, cyber risk management is needed to build resilience, in addition to adhering to international and industry compliance standards. To achieve this with urgency, cyber risk awareness and cyber risk management are needed at all levels of sectoral governance. That is, there needs to be responsible discussions and accountability surrounding cyber risk and its management at the strategic level.

Transparent communication of breaches

Breaches are here to stay. What is essential is reducing their impact. Therefore, the data commissioner's office must be fully involved from a visibility point of view in the transparent communication of the breach, thereby helping non-affective businesses and individuals to be more aware of cyber and information security risks and how to better enhance cyber and information security risk management from a business and professional point of view in protecting data. Like the US Security Exchange Commission (SEC) cyber incident reporting, such a system can help the public become aware of breaches with insight and be vigilant to cybercrime that can be committed against you – whether as a business or individual. Remember, cybercrime is one click away!

Creating cyber security competency

Cyber and information security (CIS) is not information technology security; CIS advice and services should be performed by competent professionals and experts who have been in the profession for over ten years and have varying certifications (Certified Information Systems Security Professional, Certified Information Security Manager, and ISO Standards), a broad background and part thereof of security associations (Chartered Institute of Information Security, Information Systems Security Association, Institute of Engineering and Technology, and BCS, The Chartered Institute For IT), including publications in varying training and security magazines and public speaking.

Companies should be ISO 27001, SOC 2 Type 2 certified (to name a few) or in partnership with companies with such certification. This partnership forms a basis for how each partner should operate, reducing risk to all stakeholders and enhancing integrity core values.

As 2025 approaches, let us all do our part, especially encouraging board chairmen, board directors, ministers, permanent secretaries, non-governmental organisations, etc., to become more risk-aware and responsible in managing cyber risks. Only then can we make society a safer place. Security starts from the top, building the security culture.

Edward Millington (BSc, CISO, SOC 2, CISSP, ISO, ISSA, MCIIS, MIET), is a principal security consultant and the founder and managing director of CariSec Global Inc. CariSec is a managed security service provider.