Expert: Get serious about cyber risks

+5 Q&A

The cyber incident reported by the Barbados Revenue Authority (BRA) has rekindled debate and concern about cybersecurity and data privacy in Barbados. With October commemorated as Cybersecurity Awareness Month, Barbadian cybersecurity expert Edward Millington, founder and managing director of CariSec Global Inc., addresses cybersecurity issues, including the BRA matter.

How can we improve cybersecurity awareness in Barbados?

October, the month of cybersecurity awareness, started dramatically with the awareness of a critical breach of a Government system, reportedly affecting nationals and possibly non-nationals alike. We need to relook our development from the 1970s and 1980s to where we are now, understand the risks that have plagued first-world countries, learn from their mistakes and triumphs, and present a programme involving all stakeholders to address the deficiencies in the current operating programme, developing it to a level to enhance the nation and not discussed when a security incident occurs. Incidents are too often treated specifically but not holistically.

There is an apparent lack of understanding of cyber risks. The Government needs to have expert stakeholders with verified backgrounds and activities to develop a programme that is simple, presented in forms appropriate to the population and delivered through varying mediums. There are international standards that can help us achieve that purpose, customised to our culture, demographics and political landscape.

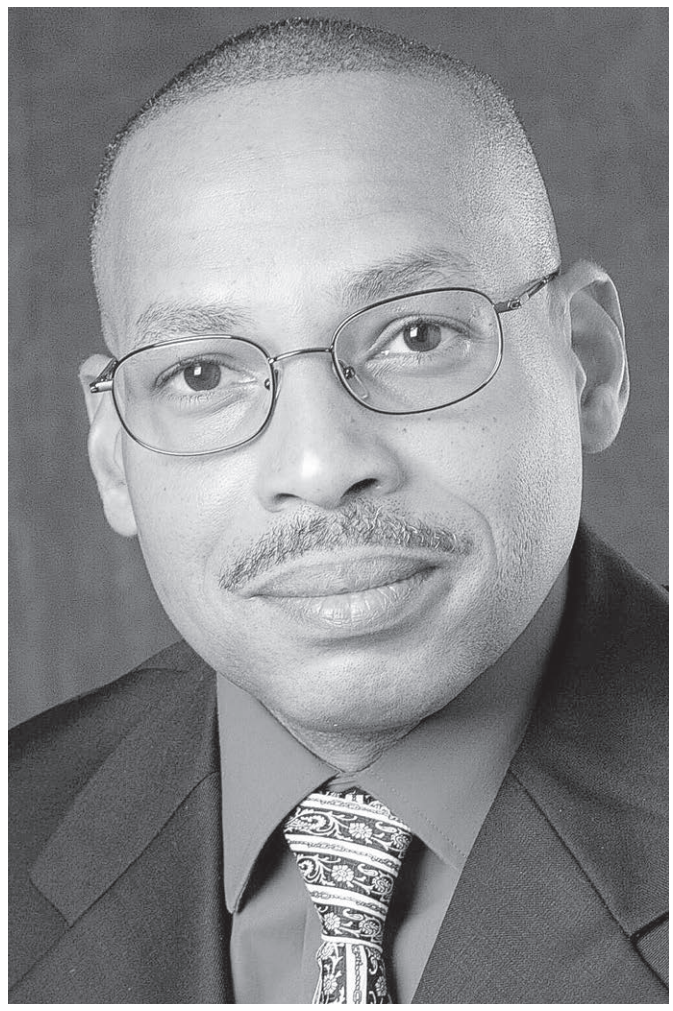
What are your main concerns as it relates to cybersecurity in Barbados?

I am concerned that too many entities offer security services and advice with an unproven track record of activity, involvement, and certifications in the security field. These service-offering entities are not pure security providers with credentials and associations to demonstrate true security capabilities and security landscape development. These services are modular, non-ecosystemic, and have low-security capabilities. Additionally, those with political will who can effect change in the security domain need to do so responsibly in the form of good governance and a conduit in building true capacity through the initiation of stakeholders – public and private.

Cyber and information security run out of information technology (IT) management structures, and in some corners of the imagination, it is believed to be all IT network security. Information security operates from the governance level into operations, making information security more involved with governance, people, process and technology.

Stating it differently, organisations must comply with international information security standards like ISO 27001 or the National Institute of Standards and Technology cybersecurity framework and not IT Security to be compliant. That should be the most significant hint to corporate governance committees when designing and implementing structures.

We must understand these two domains are different and, respecting that, initiate the governance activities and processes to build and enhance information security management systems to



CYBER SECURITY EXPERT Edward Millington. (FP)

international standards to mitigate global risks from cybercriminals.

How can the business community become more resilient and better prepared for cyber incidents?

The business community must first understand that cyber and information security are different from IT and, once understood, work to create structures in the organisations to reflect this. Building cyber resilience requires separate budgets not tied to IT. Doing so will help businesses to treat cyber resilience from a risk-based approach, thereby allowing them to monitor cyber risks effectively and efficiently, institute risk-based security controls, and continuously monitor and improve the resilience programme to meet new and emerging risks due to the business landscape and its threat landscape.

Additionally, businesses must comply with at least an international standard regarding information security. Doing so implies that cyber risk can be ingested and managed in the overall business risk management programme to build resilience. In essence, treating cyber risk in the boardroom will help the business proactively prepare for cyber incidents, lessening their effects on the business. This also builds digital trust among all stakeholders while enhancing the business's reputation and social responsibility. Risk-aware boards and directors can imply safe and secure companies through their support and involvement in building a culture of security reflected in policy, processes, procedures and guidelines.

Are there any specific sectors that are more vulnerable than others and how is data protection and privacy affected?

Based on global threat reports from the World Economic Forum, European Union Agency For Cybersecurity, managed security service providers, Palo Alto Networks, etc, the public service, professional services, healthcare, educational and financial sectors are all vulnerable and tip the scale to be the sectors that face the most significant cyber risks. Excluding commercial banks to some point, these sectors are vulnerable due to their evolving and increasing digital transformation profile to be competitive but with low maturity in security capabilities when it comes to the threat landscape they operate in. The security capability maturity model is relatively low in compliance with security standards to handle today's ever-evolving cyber risks, thereby making them very vulnerable to cyber-attacks.

The highlighted maturity also affects the level of security controls that needs to be in place to protect the confidentiality, integrity and availability of data, including privacy for all stakeholders.

In such cases, the development and operations of a privacy management system (PMS) based on the ISO Standard 27701) maybe non-existent or low in maturity, thereby affecting the security of data assets and privacy of clients, customers and other stakeholders. In essence, the business does not have a true understanding of risk to data and privacy and the governance, policies and processes in place to prevent or reduce the effects of a breach.

What are the main lessons you see from the new cyber incident involving the Barbados Revenue Authority?

Beyond that incident, businesses must be cyber-risk-aware, incorporating cyber risk into the overall business risk strategy. This will help them develop and implement controls to build business resilience through cyber and data resilience. That implies compliance with international information security standards, designing, implementing, operating, monitoring, and continuously improving their incident, business continuity, and disaster management programmes. The institution and integration of management systems will be crucial to remain competitive and resilient.

2) Boards, directors, and committees should seek cybersecurity advisory services or employ highly certified chief information security officers, or an information security officer to provide the awareness and intelligence to make informed decisions on cyber risk.

3) Privacy must be taken seriously and treasured. An individual's (data subject) loss of privacy can have undocumented effects on a person's life for years – for example, fraud, online account takeover, digital impersonation, and so on. That implies that there is a need for an international standardised-based PMS to be in compliance with data protection regulations and laws – whether locally or internationally.