# Regional Governments must take cybersecurity seriously

Guest Column

By Edward Millington

Risks due to cyber-attacks are not very well understood in many sectors, especially sectors that are not very heavily regulated by digital standards, laws and regulations.

In the last two years, digital structures and services of Caribbean and Latin American Governments have been critically affected by damaging and targeted cyber-attacks from well-funded and established cybercriminal gangs. These major cybercriminal gangs operate globally, taking on well-known names known to many that have been attacked or through threat intelligence as Conti, ALPHV (BlackCat), LockBit 2.0, and BlackByt, etc., and recently Rhysida - which has tremendously affected Martinique since May 16, 2023.

The following are some of the Caribbean hemispherical countries to be critically affected by cyber-attacks over this period: Martinique, Barbados, Guadeloupe, St. Kitts & Nevis, Brazil, Mexico, Colombia, Argentina, Chile, Costa Rica, Peru, Jamaica, Ecuador.

There are many factors (global political affiliations and agreement due to global issues, the country's reputation, financial well-being, etc) driving cyber-warfare atmospheres from these cybercriminal gangs. In essence, ineffective and inefficient cybersecurity programmes posturing to the current global cyber-warfare atmosphere, makes them at high-level risk to cyber-attacks from these extortionist cyber-criminal gangs. In fact, alluding to the World Economic Forum 2023 Global Risks Report, cybersecurity is one of the top ten risks to businesses, governments and people. In addition, it could be the number one ranking risk due to under-reporting and careful and meaningful studies.

If you are connected, you are at a very high risk to be attacked and ransomed! Just to note, cyber risks can cause many types of business risks: operational, financial, reputational, compliance, legal.

Risks due to cyber-attacks are not very well understood in many sectors, especially sectors that are not very heavily regulated by digital standards, laws and regulations. Cyber-attacks are causing too many governments and government structures and services to go offline for long periods, due to little or no cyber resilience posturing programmes building business continuity. In essence, cyber-attacks carried out by cybercriminals spread throughout networks and operations, affecting too many businesses' operating points - nullifying business continuity – halting operations and services until it can be determined that the cybercriminals have no presence and control within systems. This can take a very long time. In fact, it is a very tedious process and with limited resources and tools, extended times are expected.

The effects of cyber-attacks can last for many years (the aim of many cybercriminal gangs) as highlighted by the recently concluded CariSec Global Cybersecurity Event 2023 Virtual Conference: Reducing Cyber Risks through Cyber Resilience where esteemed speakers: the Secretary-General of the Caribbean Telecommunication Union (CTU), Rodney Taylor and the Associate of Caribbean Commissioners of Police (ACCP) representative - Acting Assistant Police Commissioner, Sidney Elskoe discussed effects from cybercriminal activities.

The following are some recommendations on how governments can be effective and efficient in the management and operation of the Culture-of-Cybersecurity as highlighted in a recent ICT Pulse cybersecurity interview - https://www.ict-pulse.com/2023/05/ictp-250-2023-expert- insight-update-on-cyber-threats-and-security-in-the-caribbean-with-edward-millington-of-carisec-global/

Create partnerships with cyber and information communities to appreciate cyber risk management, while aiming and building cyber resilience for government business continuity programmes. This can come through Cyber Advisory and Professional Services.

Implement a vibrant and sustainable cybersecurity awareness programme covering all of Government to create and grow the culture of security.

Undertake a comprehensive cybersecurity and IT/OT risk assessment and compliance programme to understand the current security and risk posture and the gaps to be addressed.

Acquire a range of Managed Security Services – Penetration Testing, Security Technology Management, Managed Detection and Response, Email Security, Data Risk Management, to name a few.

Implement certified security training programmes to increase competent security resources in the management of government assets and critical infrastructures. Such programmes will address the implementation and operations of standards like the NIST, ISO throughout governing, people, process, and technology systems.

Governments must have a true cultural understanding of the risks digital transformation incurs with respect to cybersecurity and to build cyber resilience programmes against cyber-attacks from cybercriminals, while working in close partnership with cyber and information security communities in cyber risk management for business continuity.

**Edward MILLINGTON, (BSc, CISSP, ISSA, MCIIS, MIET, PAN-ACE) is the Founder and Managing Director of CariSec Global Inc., a Caribbean (Barbados) based company and a Lead Security Consultant focused on providing Security & ICT Governance and Services to organisations operating in several sectors.**