Expert predicts increase in cyber attacks as businesses fail to take security seriously

Edward Millington

BY MARLON MADDEN

Founder and Managing Director of Barbados-based cyber security and management firm Carisec Global Inc.

Edward Millington is not convinced that companies here and across the region are taking cyber security seriously as threats become more sophisticated.

And he has warned that more cyberattacks will be seen in the coming months.

During an interview with Barbados TODAY, the cyber security consultant said if companies were doing all they could to protect their systems “we would not be hearing about massive breaches”.

“We do not feel that businesses, especially in the Caribbean, are doing enough to secure themselves. One way this is being shown to us is, unfortunately, through the continued cyberattacks that we suffer within the past year,” said Millington.

His concern comes on the heels of reports of several successful cyberattacks on government agencies and departments and some major private sector

operations over the past year.

Citing the Queen Elizabeth Hospital (QEH) which was recently impacted by such an incident, Millington told Barbados TODAY this was of "great concern" to cyber experts here.

He cautioned companies to be careful who they get services from, how those services are implemented and what standards they are using.

Noting that firms can expect an increase in cyber incidents in coming months, Millington said the type of attacks were getting more sophisticated and the culprits were making sure they were more far-reaching across organisations, which could easily result in weeks or months of loss of business and productivity and cost companies dearly.

"Some people might say we are speaking of doom and gloom. No, we are seeing that ramp up . . . . Because of sophistication, they are hitting the larger companies and when they do hit them it is fairly hard. What happens is that even if they do not get a ransom that company spends a long time being down [and] the reputation damage is bad," he said.

Millington explained that while cybercrime has been taking place since the advent of the Internet, it has morphed into somewhat of a "cyber criminal enterprise".

"It is all about money making. It is all about using ransomware as a service. You find that before, people had to have the art of how to get into a company but now you can use artificial intelligence tools. So that is why you are going to see more attacks because people can now [purchase this malware]," he warned.

The expert said while companies often introduce firewalls and antivirus software, that was simply not enough.

Pointing out that it can take "one slip up" by an employee to make a system more vulnerable, he argued that in addition to having proper systems in place, training of employees – the end users of the systems within firms – was necessary to ensure they were not clicking on phishing emails or visiting suspicious websites.

Millington, who has worked across several sectors in the field of cyber security and ICT, said he started his company Carisec Global in 2019 "to give back to Barbados" and to help more companies strengthen their systems through partnerships he has formed with industry stakeholders.

He was speaking with Barbados TODAY ahead of the March 7-8 cybersecurity seminar organised by his firm, entitled Reducing Cyber Risks through Cyber Resilience.

The free event, which will be held on the Zoom platform and streamed on YouTube, will address a range of topics stemming from business cybersecurity strategies and strategic response to cyberattacks, the economic impact of cybercrime, the importance of training, and data risk management, among others.

It is intended to educate business leaders and executives, government officials, security and IT managers and board members on matters relating to the business of cybersecurity, frameworks and standards.

To register, individuals are asked to visit the website carisec.global.

Stating that building cyber security and resilience was critical, Millington said too often general risk management within firms did not take into account cyber risks.

“If you think about resilience, this is really to be able to recover from something. A resilient system means then that if it is being affected it continues to operate so that is what really is some form of business continuity in the event of an incident,” he said.

marlonmadden@barbadostoday.bb