NEWS RELEASE

For Immediate Release

Cybersecurity expert advises CIBC customers and suppliers

Bridgetown, Barbados, February 22, 2024 – No one is immune; large companies have been hit by cyber attackers and small ones have also felt their heavy hands. Joe Lobiance gave this advice to a group of 20 IT professionals gathered at CIBC Caribbean for a cyber security workshop recently.

While urging them to be vigilant, he advised them to keep up to date with cybersecurity issues, regularly update software and closely monitor their protection systems. Lobiance, a Senior Vice President and Chairman of Information and Security at CIBC stressed that the cyber criminals were becoming more creative, and they are using more advance technology like ChatGPT which gives them an edge. He added that some cybercriminals are well organized while some are funded to carry out attacks.

Lobiance told the group comprising representatives of the bank's clients and the Barbados public sector as well as CIBC Caribbean officials, that the attackers were not picky and were targeting all sizes of organisations and in fact a shift downward to small and medium size companies was noticeable.

He described ransomware as a gamechanger, noting that it can be installed on any size company. Ransomware is malware used by hackers to block companies' access to their computer systems or to gain access to their data. To regain access, the victim must pay the hacker a ransom. In addition, hackers practice double extortion by threatening to expose a company's information if they are not paid.

To further explain why size was not a deterrent to hackers, he pointed out that ransomware could be installed on any size company and attackers were smart enough not to ask for sums of money a company could not afford. He said they price their ransom so that it isn't so big that it scares the company away from paying it. "If they can get back online quickly, they will pay,"

The cybersecurity specialist added that large organisations tended to invest more in security and were harder to penetrate than smaller companies that don't have the same resources. He posited that while it may appear that smaller companies don't have as much to attack or protect, getting tens of thousand dollars out of more companies, though they are small, may be more profitable that spending several more days or maybe months trying to compromise a large company. A weak company can be compromised in less time, he said, so no one is immune.

The CIBC official also said that the shift must be made away from mainly protecting sensitive data to looking at all systems - the critical ones, the heartbeat of the company's operations.

He then drew attention to the attacks of supply chains, pointing out that in one such incidence a piece of software that moved data from one place to another was compromised and so significant was it that hundreds of companies around the world were victimised and a tremendous amount of ransom was generated.

One of the lessons from that, Lobiance said, was that while outsourcing was a way of life for most companies, it also brought risks of which the organisations must be aware and he said that in recent months, hackers had breached suppliers' systems not because of who those suppliers were but who their clients were.

The question is what to do with supply chain attacks since an organisation cannot control the entire supply chain. Lobiance's advice included making sure you know with whom you are dealing. He added that sometimes going to the lowest bidder was not the best option since some companies may not have a lot of expertise in the cybersecurity space, He said it was important to ask companies about their cybersecurity programme and that can be a requirement that could be scaled to the criticality of the services they are offering, for example the difference in requirement between a key provider and a provider at a lower rung.

Using cloud technologies was the way of the future, but he advised that companies adopting the technology should carefully regard the associated risks which must be managed. They should therefore go into it intentionally making sure they understood those risks.

Despite the fact that technology is the ultimate target, Lobiance reminded participants that people were part of the chain, and any large attack had some form of social engineering.

It can be as simple as getting people to type a phishing email, he said, adding that the large attack at MGM service in the United States is believed to have been started by someone asking the calls desk to reset their accounts and the attackers used that as their initial entry to attack the organisation.

He noted that organisations give customers and employees, access to some portion of their systems, consequently organisations should treat cyber security awareness as very important, ensuring that front line staff, everyone dealing with the public, was educated on these methods which attackers use to gain access. Customers should also be made aware of the threats.

Cybersecurity threats and their potential impact should be part of the awareness for the Board of Directors and top officials including the CEO, so they will understand the importance of investing in security - research and development. Information about those top officials is often public and hackers can skilfully use this information to con top officials to do things that will help them gain access to the company's systems, for example, they can embed something in an email.

He said that attackers continued to become creative in their approaches including finding ways of getting people to give out security codes, despite IT managers issuing messages instructing not to share this code with anyone or telling customers, that the company will never ask them for specific information.

He noted that technical measures can be implanted to boost protection but if staff willingly bypass security controls that is something that cybersecurity managers should consider.

He also noted that attackers are targeting employees with high privilege and IT managers should know who these people are and should ensure that they are properly educated on the risk.

Best practices, he suggested including making sure that updates are applied; having multi-factor authentication; testing system; knowing your back-up system and how quickly you can recover from an attack; test these systems, periodically; have security awareness for staff including human resources and the finance team; get partners that can give independent advice.

He also said it was good practice to have a communication plan that included suppliers, staff, customers and regulators but he explained it as a balancing act. The longer they deny a problem, the worse it could get, yet companies must be careful in their analysis of the situation which would influence how information was dispensed to each stakeholder, the expert noted.

Lobiance said that cyber insurance policies are available, and insurers usually provide expertise that could help with ransom. They also have negotiators trained in cybersecurity forensics who can help companies analyse the extent of an attack and the restoration of services.

Ends

Joe Lobiance speaking to a group of 20 IT professionals gathered at CIBC Caribbean for the cyber security workshop.

About CIBC Caribbean

CIBC Caribbean is a relationship bank offering a full range of market leading financial services through our Corporate and Investment Banking, Personal and Business Banking and Wealth Management segments. We are located in twelve (12) countries around the Caribbean, providing the banking services through approximately 2,700 employees in 45 branches and offices. We are one of the largest regionally listed financial services institutions in the English and Dutch speaking Caribbean, with US$13 billion in assets and market capitalization of US$1 billion. We also have a representative office in Hong Kong that provides business development and relationship management for our fund administration. The face of banking is changing throughout the world and CIBC Caribbean intends to lead these changes with the expertise, integrity and knowledge gained from banking in the Caribbean since 1836.

CIBC Caribbean is a member of the CIBC Group. CIBC is a leading Canadian-based global financial institution with 11 million personal banking and business clients. Through our three major business units - Retail and Business Banking, Wealth Management and Capital Markets - CIBC offers a full range of products and services through its comprehensive electronic banking network, branches and offices across Canada with offices in the United States and around the world.

For more information about CIBC Caribbean, visit www.cibcfcib.com , Facebook, Twitter , LinkedIn, Instagram or YouTube.

Media contact:
Debra King, Director of Corporate Communications, CIBC Caribbean, Barbados Head Office
Telephone: 246 367 2248; Fax: 246 421 7148 and Email: debra.king@cibcfcib.com