COVID-19 Is Exposing Cybersecurity Vulnerabilities

Cybersecurity

There is no widely accepted definition for cybersecurity. Broadly speaking, it can be understood to involve the protection of computer systems, networks and online data from unwarranted penetration, malicious damage and misuse.

Zoombombing

Zoombombing (zoomraiding) is a popularized term stemming from the COVID-19 pandemic, where various conferences held on zoom platforms became targets of unwanted intrusions.

Cyber-attacks

There are various types of cyberattacks.

Ransomware attacks: The use of malicious software (malware) to threaten publication of a victim's data or block access to it until a ransom is paid.

Malspams: Malicious spams delivering emails with infected documents or links.

Phishing attacks: Hackers masquerading as trusted entities to steal user data and sensitive information.

(N.B. these are just some of the numerous types of cyberattacks)

COVID-19 is shifting more activities to online platforms: from board meetings to classrooms, to church services, to local vendors, all are moving online as a result of new social and physical distancing measures. Reports indicate that since the pandemic began, web conferencing has grown by 500%, video platforms by 265%, webinars by 226% and live chats by 194%. E-commerce too has grown as shoppers are being forced to conduct transactions online. While these developments represent a win for the digital economy, a darker underbelly is also growing as cybercriminals capitalize on the increase in online activity.

Perhaps you've heard of 'zoombombing' a term recently coined to refer to unwanted intrusions of racial slurs, pornographic content and other discriminatory actions by individuals on the Zoom platform. These attacks have occurred worldwide and here in the Caribbean. We at the Shridath Ramphal Centre (UWI) were recently victims of 'zoombombing', as were the UWI's Caribbean Sociological Association and the University of the Bahamas.

Cyberattacks on a whole have increased during COVID-19. Observations show a spike in ransomware attacks, malspams and phishing attacks. Even the World Health Organization (WHO) has been a victim of such, reporting a fivefold increase in cyberattacks since the start of the pandemic. However, even prior to COVID-19 cybercrime has long been a silent threat to the Caribbean region. Reports reveal that Government websites have been hacked in Jamaica, Trinidad and Tobago, the Bahamas and a number of OECS countries; ransomware attacks were launched on some Caribbean tax authorities; ATM scam attacks were carried out in Barbados; 1.3 million files from the Bahamas Corporate Registry were leaked online; and an increasing use of crypto currencies to fund criminal activities was observed. These are just a few of the many manifestations of cybercrime occurring throughout the region. In 2018, cybercrime was estimated to be costing Latin America and the Caribbean approximately US$ 15-30 billion annually.

The Importance of Cybersecurity

The increasing incidence of online crime and attacks underscores the importance of cybersecurity. The GLACY+ joint project differentiates between cybersecurity and cybercrime strategies, noting that the first addresses technical security and infrastructure to prevent such acts, while the latter addresses the law enforcement capacities for sanctioning such acts. Both technical protection and legal sanctions are needed to effectively deter cybercrimes and attacks.

With regard to technical protection, individuals are searching for their own solutions, with reports indicating that since COVID-19, searches for antivirus software have increased by 357%. Additionally, several online platforms and networks have been ramping up cybersecurity measures. For example, since April 8, 2020 Zoom introduced a 'security' option allowing hosts to lock meetings and to remove 'zoom' bombers. At a more institutional level, organizations like Interpol are promoting protective measures by developing cybersafety checklists for both companies and individuals.

However, technical protection remains a challenging area for the Caribbean. The Caribbean Council notes that there is a lack of appropriate security particularly for government portals, while outmoded IT systems and outdated software continue to make the region vulnerable to cyberattacks. This vulnerability is exacerbated by insufficient financial resources

Computer Misuse Laws

Typically address unauthorized access to computer material, access with intent to commit or to facilitate commission of offence, unauthorized modification / use / interception of computer material / service, authorized disclosure of access code, unauthorised obstruction of use of computer, power of police to access computer and data, among other things.

Electronic Crimes Laws

Generally address various online offences, including inter alia: identify theft, electronic forgery, electronic fraud, violation of privacy, misuse of encryption, electronic terrorism, sensitive electronic system, false websites and spam, unauthorised access to code, harassment utilizing means of electronic system, child pornography, sending offensive messages through communication services, access and inference, etc. Subsequent Investigations and procedures for these offenses are also outlined by this Act.

Budapest Convention

The Budapest Convention on Cybercrime is the first International Treaty on cybercrime whose overaching objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

and local expertise to develop a reliable cybersecurity infrastructure. Too often the region finds itself relying on foreign providers for technical support to solve cybersecurity problems. However, these exposed vulnerabilities have encouraged some proactive responses. For example, in 2015 Jamaica established a National Cyber Security Strategy and Cyber Incident Response Team and St. Lucia decided to strengthen its cybersecurity after the St. Vincent and the Grenadines' cyberattack incident. At the regional level, in 2016 the CARICOM Implementation Agency for Crime and Security (IMPACS) developed the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) which identifies building sustainable capacity, technical standards and infrastructure as a priority area for addressing regional cybersecurity.

With regard to legislation, countries are developing legal frameworks to fight cybercrime and build trust in the Internet, which remains the fifth greatest strategic risk worldwide according to the World Economic Forum's Global Risks Report 2019. Presently, there is concern that the chance of successful investigation of and prosecution for a cyberattack based on existing legislation is estimated at 0.05% in the USA, with similar reports worldwide. With COVID-19 accelerating the world's transition to the digital economy, the clock is ticking for a strengthened legislative approach to cybercrime.

In the Caribbean, at least 67% of CARICOM Member States have some form of cybercrime legislation. The most popular appears to be the Computers Misuse Act and the Electronic Crimes Act. However, due to their dated nature in most cases, their adequacy in effectively prosecuting the current wave of cybercrimes remains questionable. Additionally, the GLACY+ joint project indicated the need for increased capacity building among the region's criminal justice authorities due to the technical nature of cybercrime.

Currently, there is no regional (CARICOM) legislation on cybercrime, but within the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) the legal environment was identified as a priority area of intervention for addressing cybercrime. There is also the 2010-2012 HIPCAR (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean) project which produced model legislative texts in six areas including cybercrime. This model legislation included many of the provisions of the Budapest Convention on Cybercrime and in some respects even goes further. However, to date no CARICOM Member State has signed on to this International Treaty and according to the GLACY+ joint project very few CARICOM Member States "have enacted legislations on the basis of the HIPCAR model law".

Towards Solutions

Clearly, COVID-19 is accelerating our resort to online facilities for practically everything. The region must provide the means to conduct these transactions as well as the infrastructural and legal safeguards to protect them from those with fraudulent and criminal intent.

The solutions may well start at an entrepreneurial level. Local Barbadian developer Steven Williams, Managing Director of SunIsle Technologies in Barbados, has already developed Chatterbox – a local video conferencing service with enhanced security measures.

However, governments must also ensure that they too begin to take action towards developing appropriate legal frameworks in the fight against cybercrime to make it easier for Caribbean people to take advantage of the opportunities and realities of the new emerging global online environment.

Date: May 12, 2020

Prepared by: Chelcee Brathwaite
SRC Trade Researcher