Digital anthropologist Daren Dhoray:

'Cybercrime likely to keep surging'

Andrea Perez-Sobers
andrea.perez-sobers@guardian.co.tt

Cybercrime is expected to surge in the next four years, rising from US$9.22 trillion this year to US$13.82 trillion by 2028, according to a report by Statista's Market Insights that tracks such attacks worldwide.

It's against this background that emphasized how important it is to have proper cybersecurity awareness training in the workplace to minimise the risk of attacks.

Dhoray told the Business Guardian that based on these figures, cybercrime seems to be a lucrative criminal activity, and some of the major breaches are conducted in a very sophisticated manner with payment/ransom being requested in untraceable cryptocurrency (bitcoin) transactions. As such, Dhoray said it leaves little reason to doubt why the projected figures are so high.

He said cyber-attacks result in financial impact to the organisation, which include ransomware attacks where companies are faced with paying a ransom to the cybercriminal to regain access to their systems.

Dhoray said ransomware attacks may also come in the form of phishing attacks where employees themselves may end up being tricked into paying for a (fake) service or product, which often results in credit cards being compromised.

He noted that a 2021 report from PCH Technologies provided an estimate of the average loss per company based on size:

- Small companies (1-49 employees) lost an average of US$24,000;
- Medium-sized companies (50-249) lost an average of US$50,000;
- Large companies (250-999) lost an average of US$133,000; and
- Enterprise Level (1000+ employees) lost an average of US$504,00.

These figures he said would have only increased over the years.

Asked how many companies and agencies within the region have fallen victim to cyberattackers between 2020 to now, Dhoray said unlike the United States and the United Kingdom, there isn't any legislation that mandates critical infrastructure companies such as energy, financial, communications, government etc. to report cybersecurity incidents.

In March 2022, he said the US Securities and Exchange Commission proposed a rule to require publicly listed companies to also report their cybersecurity incidents.

"For the Caribbean, a manual curation of a few incidents that have been published would be the only way to acquire such figures."

Dhoray said this tedious work was recently completed by Shiva Parasram and Alex Samm of Computer Forensics and Security Institute (CFSI) and Tier 10 Technologies respectively who compiled and launched the Ransomware Warehouse publication on February 18, 2024.

He disclosed that this document provided a regional overview of cyberattacks within Caricom and the wider Caribbean. Of the data shared, the report indicated that in 2022 there were 32 reported cyberattacks and data-leaks coming from Dominica, Puerto Rico, Dominican Republic, Trinidad and Tobago, Jamaica, Martinique, Antigua and Barbuda, Aruba, Belize, Curacao, Guyana, Haiti and the Bahamas.

Digital anthropologist Daren Dhoray

As it pertains to some of the industries that were attacked in 2023, Dhoray said Shiva and his team were also able to document some of the 2023 attacks that happened in T&T, such as manufacturing-food beverage, telecommunications, insurance, oil and gas and retail.

On what could have been done differently with respect to the Telecommunications Services of Trinidad and Tobago (TSTT) cyberbreach the digital anthropologist said, based on the interim report filed with the Parliament's Joint Select Committee investigating TSTT's handling of the breach, there are a few things to note:

- Passwords to a user account were not redacted when uploaded to an external platform. This external platform (GitLab) seems to have been a key source of information that aided in the hackers' attempt to gain access to a TSTT file server. Redacting passwords or sanitizing or removal of passwords is often a common practice when backing up or storing documentation or source code, particularly on an external or cloud-based provider;
- This user account had elevated privileges and was used to initiate a wider attack on TSTT's systems. While information is limited about what systems or applications the account was used to access, one possible mitigation strategy would be to have alerts in the form of email messages or being written to a log (that is regularly reviewed) notifying an admin or account owner when a certain type of activities is executed by that account. In this case, it was reported that the account attempted to create multiple rogue accounts on the network. This could have been one of the flags that could be used to alert other admins within TSTT, which could have led to preventing or reducing the overall impact of the breach; and
- Lastly, it was also reported that another user account from a dealer store may have attempted to gain access to the GitLab repository. Satellite locations may often be left behind when it comes to the adoption of the core company cybersecurity policies. If this is the case, then it would be the responsibility of TSTT to ensure that all 'external' vendors are forced to meet a minimum cybersecurity posture before being allowed to interact with the main company's systems.

With the cyberattacks on the increase, Dhoray was asked to estimate how much money was lost by the companies preyed upon. He said there isn't a figure that can be quoted which provides a proper estimate to all companies. But he said some recent stats which would help to provide some insight include international IBM Security, which reported that the average cost of a data breach globally in 2020 was US$3.86 million. This would be mostly attributed to phishing and ransomware type of attacks.

"The range for these types of breaches is quite wide and varies by industry. Hackers often do their homework and know their victims well enough to decide on what aspect of their systems or data is most valuable and also know well in advance how much they think a client would be willing to pay to recover that data," he revealed.

However, he said this varies depending on the industry and one example from the 2020 IBM Security report highlighted Amazon.com which was down for just under an hour in 2020 due to a denial-of-service attack and lost somewhere in the vicinity of US$75 million in sales.

Asked to provide advice to social media persons, companies, and agencies to protect themselves from hacks, Dhoray said: "Guard access to your online accounts in the same way you guard access to your physical assets eg vehicle, apartment, or house. We would often go to extra lengths to ensure our physical safety but often just stay with the basics when it comes to online safety. No longer is just having a strong password sufficient to stay safe online."

He stated in the same way people invest in security cameras and remote monitoring services to protect one's home and persons.

"Also, one needs to employ additional steps in protecting their online assets. This would include setting up multi-factor authentication on all your online accounts. Having a password refresh policy means changing your password on a scheduled basis - for some types of accounts eg online banking you may want to consider a quarterly refresh.

"Conducting security audits on your accounts e.g. review login activity and see if you notice any strange logins. Review and limit access - this should no longer be based on convenience but on need. Backups and recovery accounts are critical in the event anything goes wrong," Dhoray added.