Daily Express
Trinidad Express Newspapers

Week after chairman's resignation...

# TSTT board gets cyberattack report

LESS than a week after Sean Roach resigned as chairman of the Telecommunications Services of Trinidad and Tobago (TSTT), the board received the long-awaited final report on the 2023 cyberattack against the majority State-owned company.

Roach resigned as a director and chairman of the TSTT board, effective January 15, according to a material change notice filed with the T& T Securities and Exchange Commission.

He had been serving as TSTT's chairman since February 7, 2020, and was in the midst of his third successive term in the role.

On Tuesday, the TSTT board received the final report of the investigation into the 2023 cybersecurity breach and the circumstances surrounding the incident. And yesterday the board submitted the report to Gonzales.

Gonzales yesterday confirmed receipt of the report.

And after reviewing it, Gonzales stated that he will submit the report to the country's National Security Council, as well as the appropriate Joint Select Committee of Parliament.

'In accepting the report, Gonzales said he was looking forward to reviewing the findings of the investigation and was confident that the learnings would be used to improve and strengthen cybersecurity and crisis communications protocols, not just at TSTT, but across the State sector,' a release from the Public Utilities ministry stated.

'In the digital environment in which we now operate, cyber incursions pose a constant and persistent threat to business continuity and information security. It is imperative that we all remain vigilant and that we learn from past shortcomings,' Gonzales said.

Gonzales stated that every company is vulner-n able to cyberattacks.

'No organisation is fully immune to cyber incursion and a key protocol in managing such breaches is clear, sincere and honest communications with all stakeholders, especially customers and members of the public,' Gonzales said.

Gonzales said after reviewing the document, he planned to submit the report and its findings to the National Security Council and to the appropriate Joint Select Committee of the Parliament for their consideration.

Two years ago, TSTT confirmed that its systems had been hacked by the ransomware group Ransomexx after the international hackers announced that they infected TSTT with ransomware and stole as many as six gigabytes of its data, including names, e-mail addresses, national ID numbers, phone numbers and 'a lot of other sensitive data'.

**CWU: Don't make entire report public** Secretary-general of the Communications Workers' Union Joanne Ogeer said she believes the entire investigation would be in vain if no one is held accountable.

'So the accountability has to be from who would have been the person tasked with the responsibility to guard the network-that is one. And two, the CEO would not get information just like that to divulge to the minister. Information was prepared by the former PR personnel Khamal Georges, who has since demitted the organisation. It was approved by Gerard Cooper, and then passed to Lisa Agard. So in her position as the CEO she would have relied on information passed to her and then she would have passed the information to the minister. So Lisa Agard may have been just a fall guy,' Ogeer said.

The cyberattack on TSTT occurred on October 9, 2023, but was only disclosed on October 27 after Falcon Feeds, an India- based technology security company, revealed on X that TSTT was among the victims of the ransomware group RansomExx.

TSTT's perceived mishandling of communication following the cyberattack eventually led to the dismissal of Lisa Agard, its chief executive officer.

In June, Georges resigned as the senior manager of environmental, social and reputation management at TSTT.

On January 26 last year, Cooper was appointed the acting chief financial officer (CFO) of TSTT.

He had been serving as TSTT's general manager of Operations and Administration since May 2019.

Ogeer said the administrator whose credentials were used to gain access to the organisation and execute the cyberattack is still employed at TSTT.

Ogeer is calling for the report not to be made public in its entirety due to the sensitive information it may contain.

'We have criminal elements or rogue elements and we also have persons that will do a lot of mischief in the IT (Information Technology) world. So all I am saying is: if we release certain parts of the information, especially the root cause, then it could also show our vulnerabilities and what would have brought us into that space,' Ogeer said.

'So all I am saying is: we have to be careful. And I am saying 'we' because I know the company would be in receipt of the document; but all I am saying is that we need to be careful in what we disclose,' she said.

Ogeer has also questioned the independence of the company that was tasked with the investigation.