PARLIAMENT
REPUBLIC OF TRINIDAD AND TOBAGO

Summary of Proceedings
Public Hearing
Held on **Monday December 11, 2023 from 2:15 p.m. to 5:01 p.m.**

Subject matter: An examination of the Government's ongoing response to the recent cyber-attacks on state bodies/entities, or in which the State has an interest.

1. The level of information and communication technology (ICT) support the Ministry of Digital Transformation currently provides to Ministries, Departments and the agencies of the State;
2. The level and type of cyber security systems and infrastructure that are required to more effectively protect the state assets and combat digital vulnerabilities with the public sector;
3. The human and technical resource deficits that are affecting the Government's ability to effectively prevent and /or respond to cybersecurity breaches;
4. The possible regulatory and legislative provisions that can be made to more effectively protect our State and public assets and combat digital vulnerabilities within the public sector; and
5. The state of the proposed cybersecurity strategy and the extent of protection it is intended to provide.

Venue: In person: The Linda Baboolal Meeting Room

Committee Members

The following Committee Members were present:

- Dr. Paul Richards - Chairman
- Mr. Avinash Singh
- Ms. Vandana Mohit, MP
- Mr. David Nakhid

The following Committee Members were excused:

- Mr. Roger Munroe, MP
- Ms. Pennelope Beckles, MP
- Mr. Rohan Sinanan
- Mr. Esmond Forde, MP

Witnesses who appeared

The following officials of the **Ministry of Digital Transformation** appeared:

- **Senator the Hon. Hassel Bacchus**
  Minister of Digital Transformation
- **Mr. Cory Belfon**
  Permanent Secretary
- **Mr. Devindra Ramnarine**
  Digital Transformation Adviser
- **Ms. Denyse White**
  Deputy National Chief Officer
- **Mr. Leon Wessels**
  Deputy National Chief Digital Officer

The following officials of the **Trinidad and Tobago Cyber and Social Media Unit (CSMU) (Trinidad and Tobago Police Service)** appeared:

- **Mr. Amos Sylvester**
  Head I.T.

- **Mr. Marvin Walker**
  Sgt. Cyber Crime Unit

The following officials of the **Cyber Security Incident Response Team (TT-CSIRT) (Ministry of National Security)** appeared:

- **Mr. Angus Smith**
  Manager – TT- CSIRT

- **Mr. Anish Bachu**
  ICT Security Specialist

Key Issues Discussed

The following are the main themes arising from discussions with the **Ministry of Digital Transformation:**

Potential Threats

i. Significant amounts of transactions in Government are controlled by some level of Information and Communication Technology (ICT) usage and the security component were not necessarily built in at the time when the services were being developed or expanded.
ii. In essence, Cybersecurity is not an Information Technology (IT) problem, it is an enterprise risk problem which needs to be managed at that level.
iii. Challenges to the improvement of cybersecurity readiness stems from the boardroom.
iv. As various Ministries, Divisions and Agencies move forward with their digital agendas and increase digital technologies to their portfolios, their potential risk of attack increases.
v. Current prevention and recovery methods are not at a level that is required for modern data.
vi. Analysing threats are an ongoing process because the threat actors constantly modify their modus operandi.
vii. A number of ways threat actors tend to infiltrate organizations has been identified.
viii. Generally, threat actors try to infiltrate networks to take control or/as well as exfiltrate data which they then hold for ransom.

Cybersecurity at Ministries

ix. Some Ministries are better protected than others.
x. The Ministries current cybersecurity readiness needs to be identified and based on that, the appropriate actions need to be taken to get them to where they need to be. Presently, very few Ministries are where they need to be.
xi. The absolute readiness of the State across all Ministries, divisions and agencies is that they are not where they need to be and the MDT is currently working towards assisting these entities.
xii. It was stated that there is significant resistance with staff as it relates to when more stringent security measures are added. This creates significant issues in the workplace.

Responsibility of the Ministry of Digital Transformation

xiii. Currently, the Ministry is involved with getting persons/Ministries prepared for threats by developing strategies that can be eventually implemented. However, the MDT has not yet determined how it will address incidents that occur at other Ministries, division or agency.

xiv. In terms of strategy and interventions when it comes to cyberattacks, the responsibility is shared between the Ministry of Digital Transformation and the Ministry of National Security.

Preliminary Assessments or Forensic Investigations conducted by the MDT

xv. Any cyberattack, successful or unsuccessful are assessed by the relevant team at the Ministry of Digital Transformation.

xvi. The MDT was involved in the forensic investigation of the breach at the Office of the Attorney General and Ministry of Legal Affairs as well as the breach at the South-West Regional Health Authority.

xvii. There is not a high enough understanding of personal responsibility in cybersecurity spaces. For example:

a. Persons reusing passwords for over an extended period of time;
b. Not employing strong password technology;
c. Not safeguarding their own credentials and sharing them with other people; and
d. Not having "basic tools" that should be there to protect networks EDRs, XDRs, modified firewall rules.

xviii. Credentials of officers of State have been found on the dark web.

Threat Actors

xix. There are currently a variety of threat actors at play and they are engaged in different approaches. These include, holding data at ransom, exfiltration of data that will be used as leverage for negotiation. In the event that a ransom is not paid, threat actors may engage in customer shaming to force persons to pay the ransom.

xx. Most of the threat actors are well established. They have different motivations, for example, some may be for political reasons, and others may be driven by money.

xxi. Most threat actors are international in origin.

xxii. Some of the threat actors are well known. Some of these include *Ransom X*, which executed the breach at the South West Regional Health Authority and *Lockbit*. The MDT also discovered various imitators of these threat actors.

xxiii. Ransomware for hire is a very large industry.

Capacity of the MDT

xxiv. The MDT currently has a Cabinet-approved organisational structure that is being filled. The Ministry was previously operating on a temporary structure and is now in the process of recruiting.

xxv. The Ministry has published vacancies and subsequently held interviews.

xxvi. One main challenge that was identified was that the Ministry could not find a number of qualified persons.

xxvii. Qualified persons that were identified were not willing to work for government salaries.

xxviii. The MDT has recognized that it does not employ enough cybersecurity professionals.

xxix. The MDT is actively working on filling positions through the Public Service Commission. Some permanent positions, contract positions and short-term persons are being transitioned into new roles.

xxx. There are a number of vacant cyber-security positions in other Ministries.

xxxi. It was stated that funding has never been an issue for the Ministry. The Ministry has always tailored programmes to be in alignment with the allocations that they receive and have no deficiency where funding is concerned.

Public Education and Awareness Drives

xxxii. The Ministry contends that public education and awareness requires a whole-of-government approach.

xxxiii. The Ministry collaborates with the Ministry of Public Administration to carry out sensitization initiatives. The Ministry has also conducted individual sensitization outreach initiatives with Ministries, Divisions and Agencies.

xxxiv. Similar initiatives are happening with iGovTT and the Telecommunications Authority of Trinidad and Tobago.

xxxv. The Ministry has also partnered with international agencies. The Ministry have previously worked with the Inter-American Development Bank (IDB) and is working with the Andean bank and also with the Development Bank of Latin America (CAF).

xxxvi. The MDT in collaboration with their sister agency iGovTT, has been working on developing a plan of action to strengthen current capacities and improve software quality assurance.

xxxvii. The MDT has also been trying to engage secondary schools from a cyber-security awareness standpoint.

xxxviii. While there are ICT/STEM programmes available at the secondary school level, there is a lack of programmes dealing specifically with security. The MDT, along with the MoE is in the process of attempting to showcase the opportunities in the field of cyber security.

Collaboration and Policy Development

xxxix. The international agencies the Ministry collaborates with includes the ITU, the CTU, the CTO, the IDB and the Andean Bank, all have a significant focus on cybersecurity.

xl. The Ministry signed a MoU in August 2023 with India to gain insight into the areas of expertise possessed by that country. These include:

a. Identity management;
b. The use of identity management for social benefits of distribution;
c. The use of open source software;
d. Software development; and
e. Certifying and standardizing the way software is developed.

xli. The 'India Stack' is a group of software that had been offered to the Ministry through the partnership with India. It includes a range of applications that the Ministry can utilize, customize and tailor to Trinidad and Tobago.

xlii. There is currently no policy which deals with the illegal and malicious access of the public's data.

xliii. There have been calls for the State to implement a policy that says the State will not pay any ransoms associated with exfiltration of data and ransomware attacks.

Data Centres

xliv. One of the Ministry's flagship projects is building a Tier 4 Data centre. Tier 4 is the highest level of security and operational functionality that one can have in a data centre.

xlv. There are currently 5 Tier 3 data centres in Trinidad.

xlvi. The intention is to incorporate all data centres for Government's use. The overall goal is to have Government-owned, Government-operated Tier 4 data centres to allow for the removal of a number of the stand-alone independent centres.

Implementation of the iGovTT data protection policy

xlvii. Significant changes have to be made to the Data Protection Act and the companion legislation, the Electronic Transactions Act because its current iteration is outdated.

Budapest Convention

xlviii. There has been a delay in the ratification of the Budapest Convention due to the lack of certain legislative provisions in place.

xlix. Trinidad and Tobago has made representation to accede to the Convention on October 2021 and has five years from that date to be fully ratified.

Amendments to Acts

l. There are currently a number of amendments to be made to the Telecommunications Act. Several amendments are before the Ministry for evaluation.

li. The Ministry indicated that they will be working on making significant changes to the Data Protection Act and its companion legislation, the Electronic Transactions Act.

lii. While some legislation is partially proclaimed, the Ministry stated that the General Privacy Principles are enforced and these guide how persons are to treat with personal data.

liii. Under the Data Protection Act, the Office of the Information Commissioner will be the regulatory authority.

liv. The public sector, under the Act, will be mandated to follow the certain restrictions:

a. Once installed in office, the Information Commissioner would be able to ensure compliance with the general privacy principles and the other provisions of the Data Protection Act.

b. The Information Commissioner will also work with the private sector to require them to develop their own Codes of Conduct based on the needs of that sector.

Operationalization of the Office of the Information Commissioner

lv. The Office of the Information Commissioner is still under consideration of the Cabinet.

lvi. There is currently no timeline for the establishment for the Office of the Information Commissioner, however, it is currently being discussed.

Trinidad and Tobago Cyber Security Agency

lvii. Ten years have passed since the proposal of the establishment of this agency.

lviii. It has been stated that any proposal emerging from 2012 to present day needs to be reviewed.

lix. Initial proposals that were supposed to form part of the agency were extracted and contributed to the development of TTCSIRT. One of the core functions of TTCSIRT is to be the repository of all cybersecurity incidents.

lx. The Ministry still sees value in cyber security agencies and has modern models from a number of agencies such as UK models, US models and Australian Models.

The following are the main themes arising from discussions with the **Cyber and Social Media Unit of the Trinidad and Tobago Police Service**

Responsibility

i. The CSMU is responsible for providing technological assistance to all arms of the Trinidad and Tobago Police Service in matters dealing with cybersecurity, cyber-enabled crimes and digital incidents that may occur that breaches the laws of Trinidad and Tobago.

Cyber Attacks in Trinidad and Tobago

i. There are various levels of cyber offences, however, not all categories are reported to the police service.

ii. Regarding the reported cyber-attack on TSTT, the unit stated that a report was not initially made, however, as the situation unfolded, a report was eventually made to the TTPS.

iii. The TTPS has launched its own investigation into the matter but they are not a part of the internal investigation of TSTT.

iv. As it relates to Facebook incidents (marketplace, direct messaging), there were 38 robberies in 2022 and 68 in 2023. Arrests have been made in this regard.

v. There were 58 larcenies in 2022 and 70 in 2023.

vi. There were 14 and 35 instances of fraud incidences in 2022 and 2023 respectively.

vii. There is no current legislation that covers cyberbullying.

Supporting Legislation

viii. There is a lack of supporting legislation in relation to cybersecurity. As a result, the Computer Misuse Act of 2000 is the guiding legislation. However, the Act does not address the current use of social media in terms of the current technological landscape.

ix. The current iteration of the Act deals with unauthorized access or hacking into the system and modifying data, but does not address phishing and web defacement.

x. If persons make a report, there is nothing the unit can pursue due to legislative shortcomings.

xi. Without legislation, the unit cannot use the Mutual Legal Assistance Treaty because it requires having the requisite legislation in place.

xii. The Computer Misuse Act is partially proclaimed.

Reporting Requirements

xiii. There is a great degree of underreporting of cybercrimes to the police service.

xiv. The police service cannot say the number of reports being made over the last five years.

The following are the main themes arising from discussions with the **Trinidad and Tobago Cyber Security Incident Response Team (TT-CSIRT)**

Responsibility

i. TT-CSIRT is responsible for incident response and management. They are responsible to respond to incidents on a national scale of critical infrastructure, government services and in some instances, private sector entities.

ii. The mandate of TT-CSIRT is outlined within the 2012 National Cybersecurity strategy. The mandate of the unit is to treat with national cybersecurity incidents that affect the country and protect critical infrastructure.

iii. Services offered include:
   a. Incidents response and management;
   b. Root calls and analysis;
   c. Assessments of software applications;
   d. Standard base assessments of all online payment systems for the Government;
   e. Cybersecurity control gap assessments;
   f. Server configuration review and hardening;
   g. Secure network architecture design;
   h. Vulnerability assessments and analysis; and
   i. Notifications and alerts and security solution deployments, among other services.

Engagement with Ministries/State Entities

iv. Some of the Ministries that have engaged TT-CSIRT include: Office of the Attorney General and Ministry of Legal Affairs, Registrars General Office, Civil Land and Companies, IPO, the Ministry of Works and Transport, Ministry of Trade and Industry, the SEW platform, the Ministry of Social Development and Family Services, Ministry of National Security, Ministry of Health, all regional health authorities, Point Fortin Borough Corporation, Arima Borough Corporation, the Office of the Prime Minister, Trinidad and Tobago Securities Exchange Commission, Lake Asphalt, Ministry of Education, National Helicopter Services, Environmental Management Agency, Board of Inland Revenue.

v. TSTT was not one of the agencies the TT-CSIRT has engaged with.

Statistics on Cyber Attacks in Trinidad and Tobago

vi. Various categories of cyber-attacks that have occurred included data breach and system compromise, ransomware, phishing, business email compromise, website defacements denial of service and malicious insiders.

vii. There have been 200-plus incidents over the last five years.

viii. As it pertains to the government sector, there has been approximately 80 incidents that were recorded by TT-CSIRT. Additionally in the private sector, there has been approximately 100 -105 incidents over the past five years.
ix. For 2023, there have been 22 public sector incidents and 29 private sector incidents.
x. Statistics that are provided on Cyber Attacks are those that have been reported to TT-CSIRT as incidents.

Cyber Attack at the South-West Regional Health Authority

xi. The cyberattack at the South-West Regional Health Authority was noted as an exploitation of a remote access system.
xii. Evidence suggests that a foreign party, originating out of Europe was involved in executing this attack.

Policy Guides

xiii. TT-CSIRT functions on industry standard documentation.
xiv. There is an RFC which is a 2350 which guides TT-CSIRTs' operations.
xv. TT-CSIRT is also a part of the International Organization of Incidents Response Teams (FIRST).
xvi. TT-CSIRT also considers the frameworks of the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) to guide their operations.
xvii. TT-CSIRT recently completed an industry standard base assessment of the unit which is called SIM3. This was done by US-AID programme, in conjunction with Deloitte.

Vulnerabilities at State Agencies and Entities

xviii. Identified vulnerabilities include improper configuration, lack of trained staff to suit the positions that require systems are infrastructurally secure.
xix. TT-CSIRT estimated that nine out of ten cases faced this issue.

Legislation

xx. There is an overall lack of legislation.
xxi. The TTPS and the Cybersecurity Incidents Response Team have been working with the Ministry of National Security towards the creation of legislation related to cyber-security since 2012.
xxii. TT-CSIRT have stated since 2009 they have been working together with the Ministry in getting the legislation to where it was.
xxiii. It was stated that the legislation never got off the ground for various reasons.
xxiv. The present draft legislation has been there for consideration since 2012.
xxv. Most of the region put forward a Computer Misuse Act around 2000 and subsequently developed a cybersecurity legislation a few years later, however, Trinidad and Tobago did not.

Reporting Requirements

xxvi. There is no requirement for private or public sector to report incidents to TT-CSIRT.

Cyber Attack Perpetrators

xxvii. The main actors involved in Cyber-Crime attacks would be ransomware from foreign groups.

xxviii. These are generally known ransomware groups, for example Ransom X.

xxix. There have been two cases that were repeat offenders so that the same entity got attacked twice. This has occurred twice over the last five years.

xxx. So far, it has been stated that when an entity is attacked it seems to be an isolated incident.

Collaborations

xxxi. The TT-CSIRT has collaborated with TTIFC, Ministry of Digital Transformation, Inland Revenue Division, Customs and Excise Division, TTDF, TTPS, Ministry of Health and Ministry of Finance.

xxxii. The MDT currently has an MOU with the Central Bank and they are in the process of developing an information sharing group with the financial sector.

xxxiii. TT-CSIRT also does significant work with iGovTT.

xxxiv. Based on the spread of Ministries and State Agencies, there are varying levels of cybersecurity maturity.

xxxv. TT-CSIRT collaborates with Ministries in an effort to assess the competencies of their existing infrastructure.

This public hearing can be viewed on demand via our YouTube Channel.

19th Meeting- JSC Social Services & Public Administration - Dec 11, 2023 Cyber Attacks - YouTube

Contact the Committee's Secretary

jscsspa@ttparliament.org or 624-7275 Ext. 2283/2284/2277

Committees Unit
February 19, 2024.