CENTRAL BANK OF
TRINIDAD & TOBAGO

Cybersecurity in Financial Institutions: Best Practices

Dr. Alvin Hilaire, Governor
Mrs. Michelle Francis-Pantor, Deputy Inspector
Mrs. Keisha Lashley, Assistant Manager, Information & Cybersecurity

Public Seminar hosted by the Central Bank of Trinidad and Tobago
June 06, 2023

Live streaming LIVE STREAMING
www.youtube.com/c/centralbankoftrinidadandtobago

www.central-bank.org.tt; email: info@central-bank.org.tt

Cybersecurity in Financial Institutions: Best Practices* - Key Points

1. Modern financial institutions face huge cyber risks.
2. Central banks have taken steps to boost their own cybersecurity and increase financial sector supervision in this area.
3. The Central Bank of Trinidad and Tobago has cybersecurity as a major priority.
4. Technology continues to be a disruptor.
5. Financial institutions must understand the attackers they are up against...
6. …the types of attacks they face and how they are executed.
7. In the face of a major cyber attack, the consequences are therefore grave.
8. The Central Bank must also be resilient…
9. … but we cannot win alone, we must work together with the rest of the community.
10. We must therefore set a baseline for cybersecurity operations
11. The Central Bank plays a key role in providing guidance to the sector.
12. There are six key cybersecurity elements in the guideline that the Central Bank wishes to highlight for financial institutions' consideration.
13. Good governance and risk management are essential to protect the security of information systems and data and to cater for risk.
14. Security awareness and training for employees are critical in deterring many cyber attacks.
15. An incident management framework helps in discovering and dealing with threats.
16. Business continuity and recovery planning can minimize outages and disruptions to business operations.
17. Cybersecurity testing should be carried out regularly to check the robustness of systems.
18. Active sharing of threat information allows one institution's detection to become another's prevention.
19. The Central Bank will solicit comments with a view to issuing the guideline by mid-September 2023.

***Contributors: Kendall Cuffy, Shanta Dhoray-Baig, Patrice Valentine-Cato and Tanisha Mitchell**

1. Modern financial institutions face huge cyber risks.

2016

The **Central Bank of Bangladesh** was attacked by cybercriminals with losses estimated at around US$100 million.

2019

Capital One announced that it had suffered a data breach compromising the credit card applications of around 100 million individuals.

2021

A federal indictment charged three North Korean computer programmers for conducting a series of destructive cyber attacks, extorting more than US$1.3 billion of money and cryptocurrency from **financial institutions and companies**.

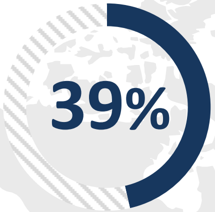
2022

Blockchain project **Ronin** lost US$615 million in ether and USD Coin tokens in the second largest cryptocurrency heist to date.

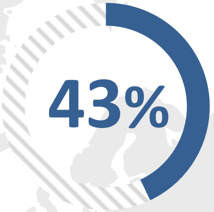
2. Central banks have taken steps to boost their own cybersecurity and increase financial sector supervision in this area.

"The rising number of cyber attacks in the financial sector poses a threat to financial stability and makes cyber risk a key concern for policy makers." - Doerr et al 2022 (Cyber risk in Central Banking)

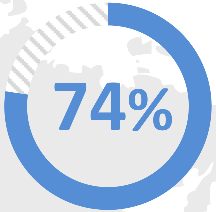
According to the **Central Banking Risk Management Benchmarks 2023**



- Central banks identified **cybersecurity** as their **top priority.**



- Participating institutions placed **cybersecurity** as the **risk that rose the most** over the previous year.



- Participating central banks identified **cybersecurity** as one of their **top three risk management concerns.**

Central banks and the **wider financial system** have:

- Assessed cyber risks

  Central banks and financial system players are **developing** a **framework** to **analyse cyber risk**.

- And are currently building defences against cyber attacks

  Since 2020, most **central banks** have **boosted** their **cybersecurity investment** budget by at least 5 per cent.

- Many central banks are **directly addressing cybersecurity** in their supervision of financial entities.

3. The Central Bank of Trinidad and Tobago has cybersecurity as a major priority.

- Cyber issues feature prominently in our **Strategic Plans** (2016/17-2020/21) and (2021/22-2025/26).

- Most recently the Bank hosted an **IMF Technical Assistance Mission** to:

  i. strengthen the **cybersecurity posture of the Central Bank**; and
  ii. build **supervisory capacity for the effective supervision of cybersecurity of its regulated institutions.**

- The **IMF Report** is available to the public on the IMF's website at https://www.imf.org/-/media/Files/Publications/CR/2023/English/1TTOEA2023002.ashx. It's recommendations are consistent with the plan of the Bank and would:

  i. Internally address weaknesses in the governance process, improve Board level discussions, increase resources, adopt security hardening baselines, and commission security reviews of payment system; and
  ii. Draft a focused cybersecurity guideline for financial institutions based on international best practices and improve supervisory intensity.

- The Central Bank intends to take things a step further by drawing up a set of **best practices** that will be relevant to all financial institutions in Trinidad and Tobago, including those not currently supervised by the Central Bank.

4. Technology continues to be a disruptor.

1. In an interconnected world, **technology has changed the way we do business**.

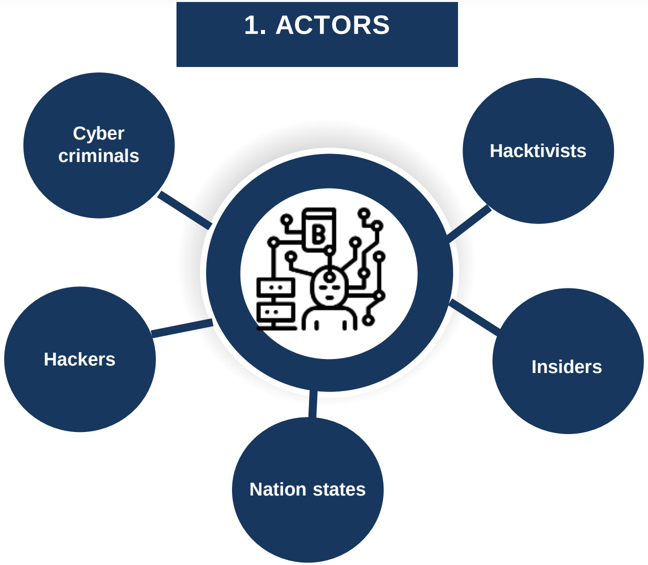
2. Demands have grown for a **more cashless society**; greater options for e-money issuers; a possible CBDC to name a few.

3. Just as technology opens new markets and enhances the way of doing things, **criminals are also not restrained to their borders**.

4. Cyber attacks have increased in **frequency and sophistication**, estimated every 39 seconds.

5. "A major cyber attack poses a threat to financial stability – not a question of ***if,*** but ***when****."* IMF, Global Cyber Threat (Spring 2021)

5. Financial institutions must understand the attackers they are up against...



1. **Threat actors** are the persons/group that are responsible for **executing** a cyber attack.

2. They continually perform **reconnaissance**, are **stealthy** and look for **vulnerable targets** with minimal controls and weaknesses in their environment.

3. Financial institutions must understand the **mindset** of those attacking them.

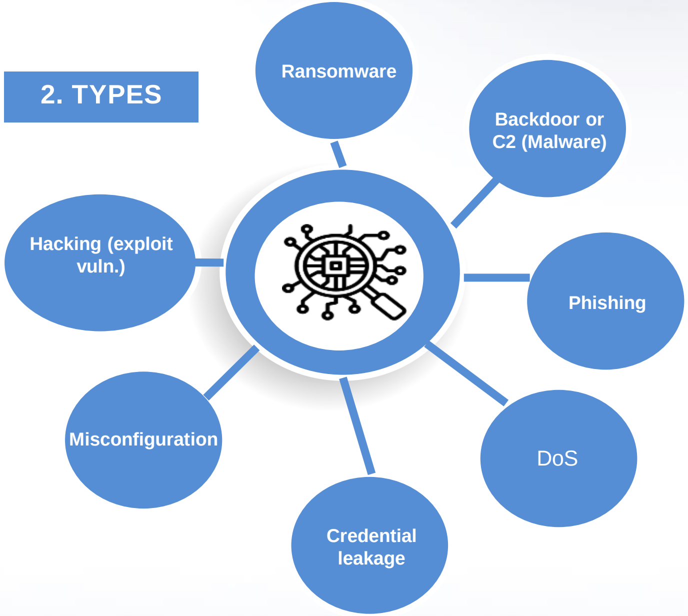
4. Malicious actors are largely **organized criminals,** who are well-resourced and skilled. Even when they’re not, **cybercrime is a service.**

6. …the types of attacks they face and how they are executed.

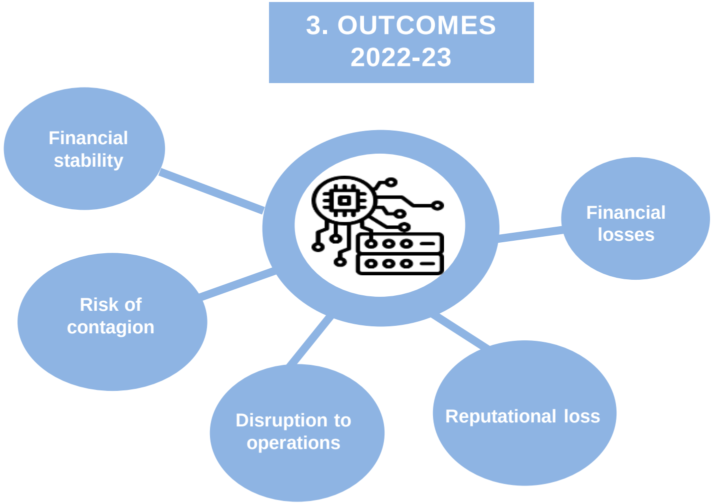
1. The major reason for successful attacks is the **human element** i.e. from stolen credentials, phishing, errors (unintentional/misconfiguration).

2. **Ransomware** accounts for one of the most common types of security attacks and organizations must **train** users; **reduce** vulnerabilities and **strengthen** controls.

3. **Insufficient safeguards** around assets, data, technology provide an environment for cyber criminals to **penetrate, blend in and then launch attacks** (disrupt operations; deny service; personal gain).



7. In the face of a major cyber attack, the consequences are therefore grave.



1. **It's all about the money**. Financial gains continue to drive organized crime i.e. from compromised payment systems; logins; data etc. E.g. stolen credit card info is worth about US$10-$15; domain admin - US$8.

2. **What is your reputation worth?** Everything**.** Clients and stakeholders must have **confidence** in the financial system i.e. service must be secure and resilient.

3. A **disruption** to the operations of one financial institution can affect not only their customers/transactions, but it introduces the risk of **contagion**.

8. The Central Bank must also be resilient…

Tools, Resources, Safeguards

- Controls must be applied to people, information, technology assets
- Multi-layered defense: network, infrastructure, data, on-premise/offsite

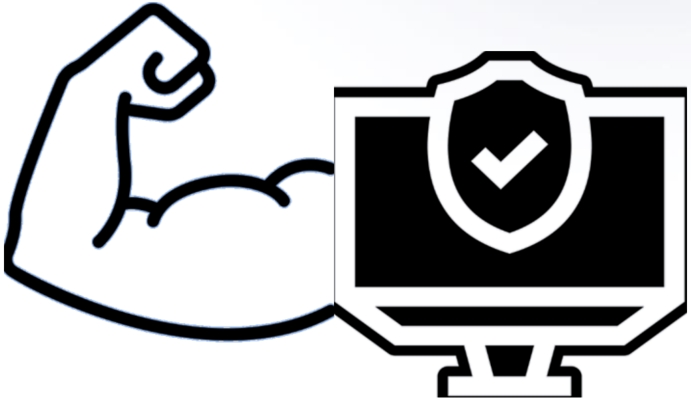
Building Capacity

- Business continuity management
- Incident response capabilities

Partnerships with International agencies

- Threat intel
- Training/staff exchanges
- Project support
- Building capacity
- Maturity of security domains

Regional Central Banks, World Bank, Bank of International Settlements



No security professional can give assurances that successful attacks won’t happen.

Instead, it will always be a journey to get better.

9. … but we cannot win alone, we must work together with the rest of the community.

1. A key aspect of a cyber-programme is **threat intelligence.**

2. Some jurisdictions perform **regulatory-led assessments**: UK, Singapore, Hong Kong, to test operational cyber-resiliency.

3. Before we get there, we need to have a better appreciation for attacks impacting the **country and region**.

4. **Partnership**: TT-CSIRT for Information Sharing and Analysis Centre (ISAC). Need support of entire community for it to be effective.

10. We must therefore set a baseline for cybersecurity operations.

Central Bank has drafted a guideline to:

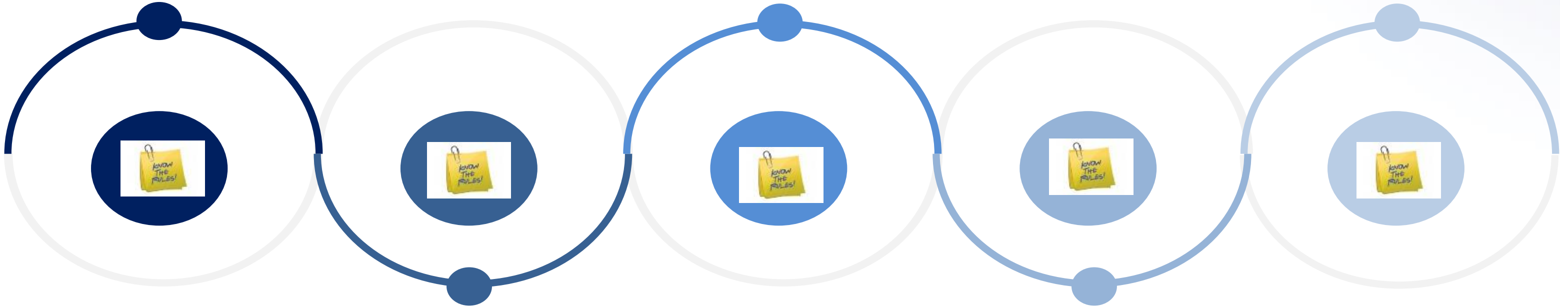
Provide a baseline of cybersecurity operations for participants in the sector

Promote compliance with cybersecurity standards

Complement international best practices (ISO 27001; NIST CSF; CIS etc.)

Strengthen and help build resilience in the sector

11. The Central Bank plays a key role in providing guidance to the sector.



Sets out the Central Bank’s expectations with respect to cybersecurity.

Strikes a balance between principles and prescription.

Provides effective guidance to institutions who are at different levels of sophistication.

Covers key areas such as governance, risk management, IT resilience, and Third Party risks.

Can be used as a guide for other financial sector participants to adopt.

12. There are six key cybersecurity elements in the guideline that the Central Bank wishes to highlight for financial institutions' consideration

1. Governance and Risk Management
2. Security Awareness and Training
3. Incident Reporting
4. Business Continuity and Recovery
5. Cybersecurity Testing
6. Information Sharing

13. Good governance and risk management are essential to protect the security of information systems and data and to cater for risk.

1: Governance and Risk Management

Board Responsibilities 1

- Approval of strategy, risk appetite and tolerance statement; and policies
- Ensuring sound and robust risk management frameworks
- Ensuring and reviewing regular reports from senior management

Role of Senior Management 2

- Implementation of cybersecurity framework
- Implementation of board approved policies including relevant procedures, and systems
- Reporting to the Board

Cyber Security Strategy 3

- Aligned to the overall business strategy
- Must have clear cybersecurity objectives

Independent Reviews 4

- Should be risk based
- Review of backup and recovery processes annually
- Establish a process for tracking and monitoring cybersecurity audit issues

Risk Management Framework 5

- Risk Identification
- Risk Analysis and Evaluation
- Risk Mitigation
- Monitoring, Review and Reporting

Policies, Procedures and Standards 6

- Must be consistent with cybersecurity strategy
- Regularly reviewed and updated

14. Security awareness and training for employees are critical in deterring many cyber attacks.

2: Security Awareness and Training

Establish a Security Awareness Programme:

- Consistent with cybersecurity policies and procedures

Training programmes should be provided at least annually to all staff

Content of Training Programme - include:

- Identification of malicious applications
- Types of attacks
- Reporting an incident to management and the Board

Provide Specific Training for High Risk or Sensitive Groups

15. An incident management framework helps in discovering and dealing with threats.

3: Incident Reporting

OBJECTIVE

To restore an affected IT service or system securely as quickly as possible.

GOAL

To minimize impact to an institution’s business and customers.

EARLY WARNING SYSTEM

Configure system events or alerts to provide an early indication of issues that impact IT systems’ performance and security.

TIMELY REPORTING

Immediate reporting of major incidents to senior management and the Board.

COMMUNICATION PLAN

Must cover process and procedures to inform customers of impact on services Timely updates to all regulators.

16. Business continuity and recovery planning can minimize outages and disruptions to business operations.

4a:Business Continuity Plan

01
IDENTIFY
02
03
04

IDENTIFY

Critical Assets and Functions

TEST

Your plan and response to ensure plan effectiveness

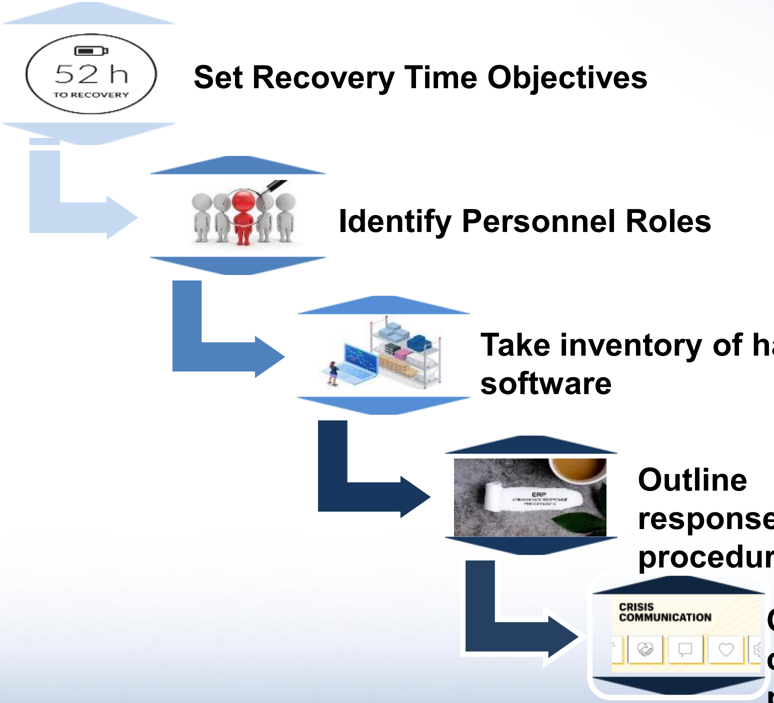
ENCRYPT

Sensitive data in transit and in storage to protect it in case of theft

TRAIN

Other business stakeholders in their responsibilities during a cyber attack

4b: Disaster Recovery Plan



Set Recovery Time Objectives

Identify Personnel Roles

Take inventory of hardware and software

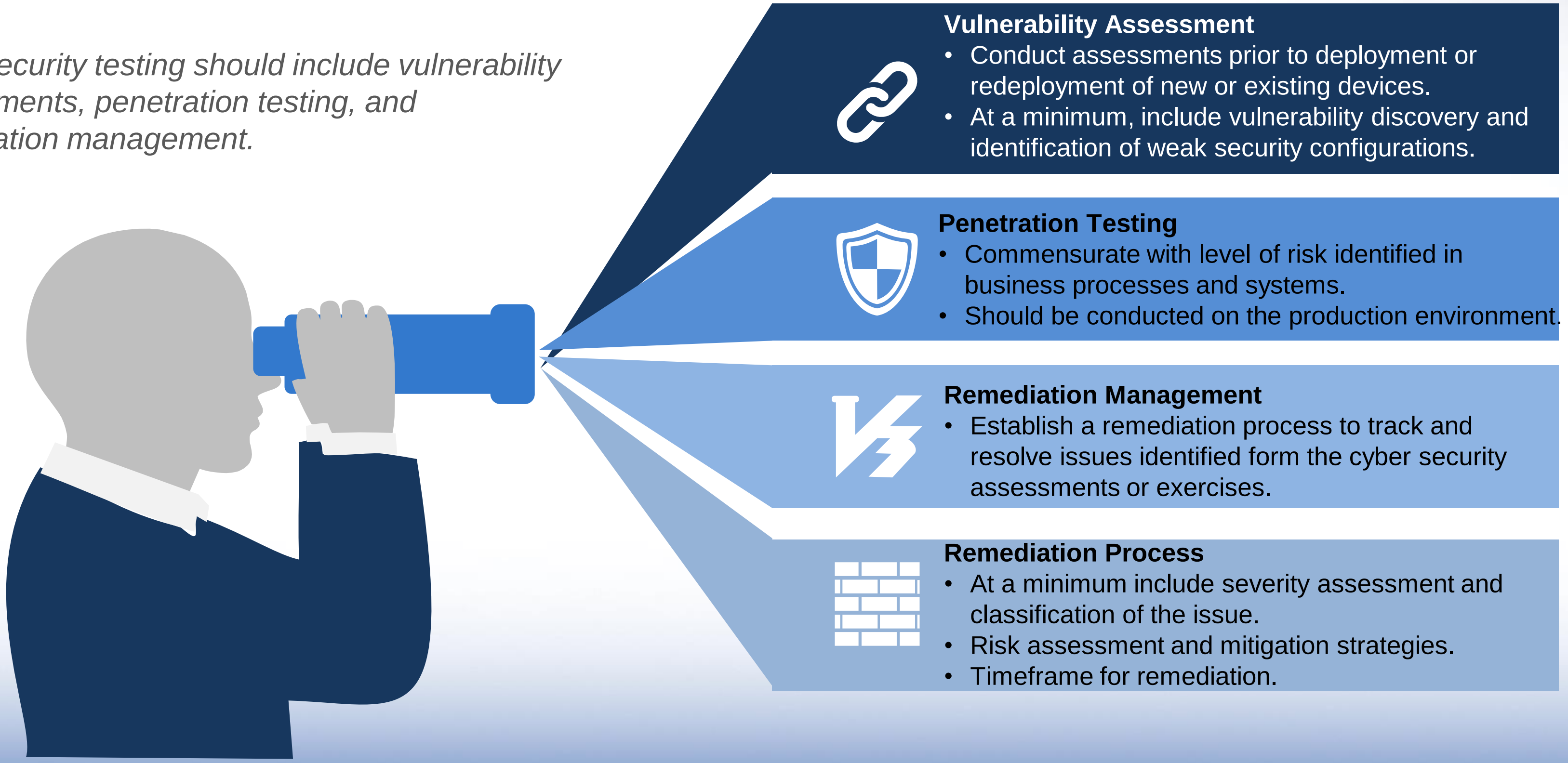
Outline response procedures

Create a crisis communication plan

17. Cybersecurity testing should be carried out regularly to check the robustness of systems.

5: Cybersecurity Testing

Cybersecurity testing should include vulnerability assessments, penetration testing, and remediation management.



Vulnerability Assessment

- Conduct assessments prior to deployment or redeployment of new or existing devices.
- At a minimum, include vulnerability discovery and identification of weak security configurations.

Penetration Testing

- Commensurate with level of risk identified in business processes and systems.
- Should be conducted on the production environment.

Remediation Management

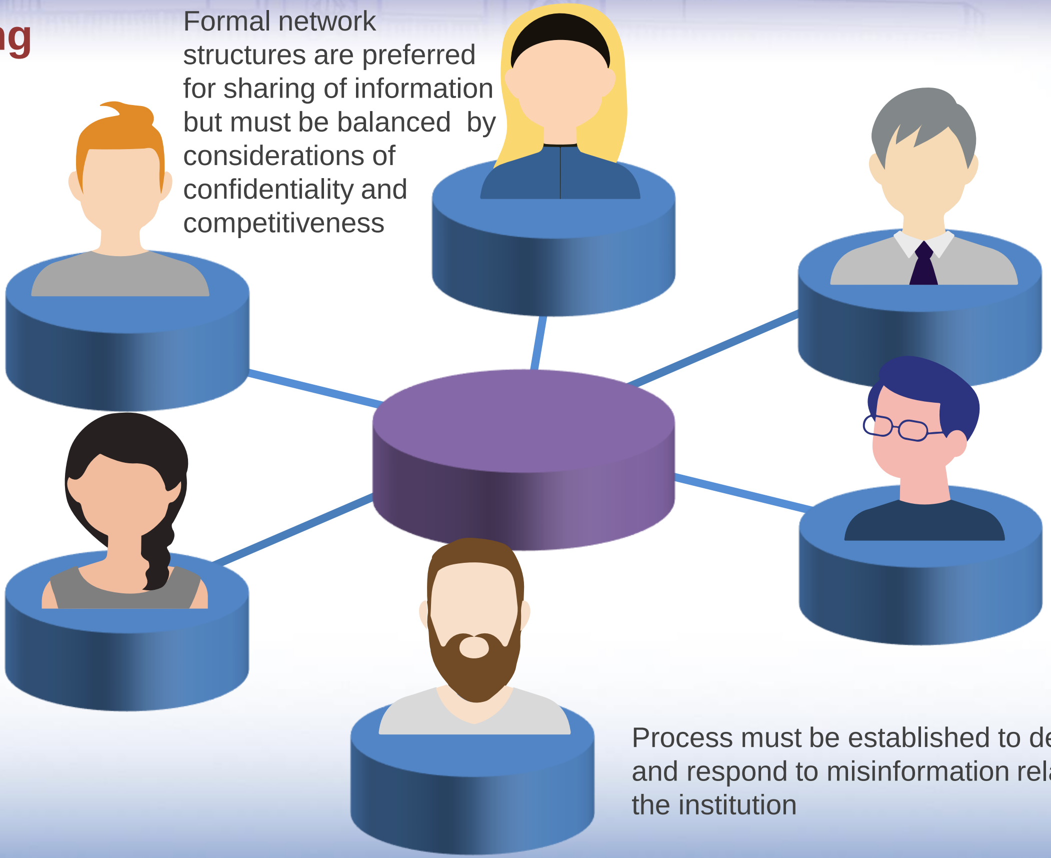
- Establish a remediation process to track and resolve issues identified form the cyber security assessments or exercises.

Remediation Process

- At a minimum include severity assessment and classification of the issue.
- Risk assessment and mitigation strategies.
- Timeframe for remediation.

18. Active sharing of threat information allows one institution’s detection to become another’s prevention.

6: Information Sharing



Formal network structures are preferred for sharing of information but must be balanced by considerations of confidentiality and competitiveness

Central hub facilitates timely threat information to facilitate prevention of cyber attacks

Types of Information to share:

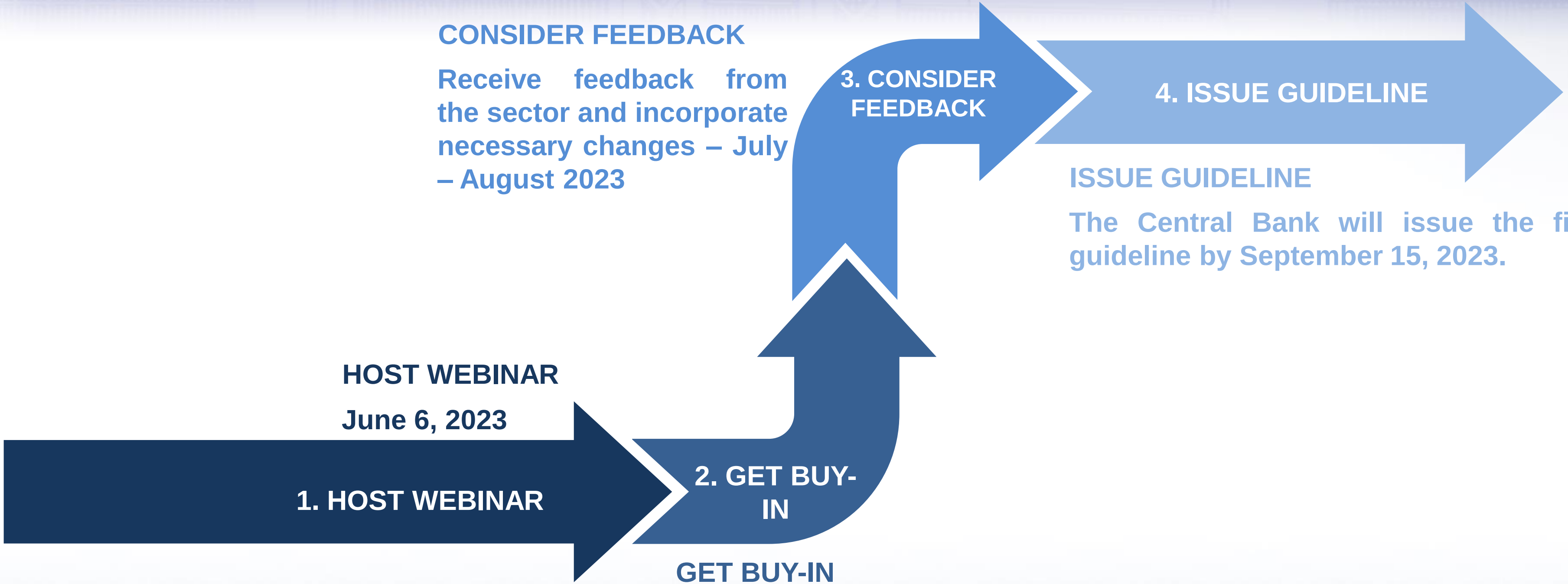
- Threat intelligence
- Incidents
- Good practices

Security threats must be shared with applicable internal employees

Consider engaging external media and brand protection services

Process must be established to detect and respond to misinformation related to the institution

19. The Central Bank will solicit comments with a view to issuing the guideline by mid-September 2023.



1. HOST WEBINAR

2. GET BUY-IN

3. CONSIDER FEEDBACK

4. ISSUE GUIDELINE

HOST WEBINAR

June 6, 2023

GET BUY-IN

Issue draft guideline for comment by June 30, 2023. Draft guideline will be placed on our website.

CONSIDER FEEDBACK

Receive feedback from the sector and incorporate necessary changes – July – August 2023

ISSUE GUIDELINE

The Central Bank will issue the final guideline by September 15, 2023.

References

- Barret, Devlin. Capital One says data breech affected million credit card applications. 2019 – https://www.washingtonpost.com/national-security/capital-one-data-breach-compromises-tens-of-millions-of-credit-card-applications-fbi-says/2019/07/29/72114cc2-b243-11e9-8f6c-7828e68cb15f_story.html

- Bouveret, Antoine. Cyber risk for the financial sector*: A framework for quantitative assessment*. International Monetary Fund. 2018 – https://www.bis.org/publ/work1039.pdf

- Central Bank of Trinidad and Tobago. Strategic Plan 2016/2017-2020/2021. 2016 – https://www.central-bank.org.tt/about/strategic-plan/strategic-plan-2016/17-2020/21

- Central Bank of Trinidad and Tobago. Strategic Plan 2021/2022-2025/2026. 2021 – https://www.central-bank.org.tt/about/strategic-plan/strategic-plan-2021/2022-2025/2026

- Central Bank of Trinidad and Tobago **Strategic Plan** 2021/22-2025/26: **Project Implementation Plan**. Year 2 : 2022/2023 − Half Year 1. https://www.central-bank.org.tt/sites/default/files/page-file-uploads/strategic-plan-project-implementation-update-2021-2026-y2-hy1-20230331_0.pdf

- Doerr, Sebastian, Leonardo Gambacorta, Thomas Leach, Bertrand Legros, and David Whyte. Cyber risk in central banking. 2022 – https://www.bis.org/publ/work1039.pdf

- European Central Bank. Cyber resilience and financial market infrastructures - https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html

- International Monetary Fund. The global cyber threat. 2021 – https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

- International Monetary Fund. Trinidad and Tobago: Strengthening cybersecurity in financial institutions. 2023 – https://www.imf.org/en/Publications/high-level-summary-technical-assistance-reports/Issues/2023/04/17/TRINIDAD-AND-TOBAGO-STRENGTHENING-CYBERSECURITY-IN-FINANCIAL-INSTITUTIONS-532437

- Mendez-Barreira, Victoria. Risk Management Benchmarks. 2023 – https://www.centralbanking.com/benchmarking/risk-management/7958596/risk-management-benchmarks-2023-presentation

- The United States Department of Justice. Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe. 2021 – https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

- Wilson, Tom and Elizabeth Howcroft. Blockchain project Ronin hit by $615 million crypto heist. 2022 – https://www.reuters.com/technology/blockchain-company-ronin-hit-by-615-million-crypto-heist-2022-03-29/

Thank You

Be safe 😷

Please send comments/suggestions on the Presentation and Guideline to info@central-bank.org.tt

Connect with us Museum Auditorium

www.central-bank.org.tt; email: info@central-bank.org.tt