Port Security and Cyber Security

Port Authority of
Trinidad and Tobago

Port Security and Cyber Security

17th March 2022.

By Hugh Gibson

Head, Information Technology

About the
Port Authority of Trinidad and Tobago

is a Statutory Authority, established by the Port Authority Act 51:01 in 1961.

The Port Authority, has direct responsibility for the Ports of Port of Spain and Scarborough, which are divided into **three Strategic Business Units (SBU)**:

- Trinidad and Tobago Inter – Island Transportation Company (TTIT)
- Port of Spain Infrastructure Company (POSINCO)
- Port of Port of Spain (PPOS)

SECURITY AND CYBER SECURITY

Implications of September 2011 attacks.

Dramatic refocusing of attention on global transportation networks that the world's economies remain so dependent on.

SECURITY AND CYBER SECURITY

Port Security and Cyber Security

- Ports and security.

- At what level of impact does action need to be taken to mitigate against the obvious risks?

Physical and linear infrastructure

Superstructure

Information and Communication Systems

SAFETY AND EFFICIENCY

SECURITY AND CYBER SECURITY

Challenges to Security - Infrastructure

- Lack of Security Electronic Equipment System such as:
  - CCTV Surveillance
  - Access Control System
  - Intrusion Alarm System
  - Scanning x-ray and metal detectors
- Maintenance of adequate Lighting
- Fencing
- Physical barriers
- Back-up power supply

Challenges to Security - Operations

- Physical Disruption
- Cargo Theft (through commercial fraud and corrupt/dishonest port employees and port users)
- Movement of illicit drugs goods through the port as legitimate cargo
- Smuggling of contraband by port employees and port stakeholders
- Human Trafficking
- Terrorism
- Retention of Port Security Officers
- Security Staff Shortages
- Response to harbor incidents

SECURITY AND CYBER SECURITY

Challenges to Security - Operations

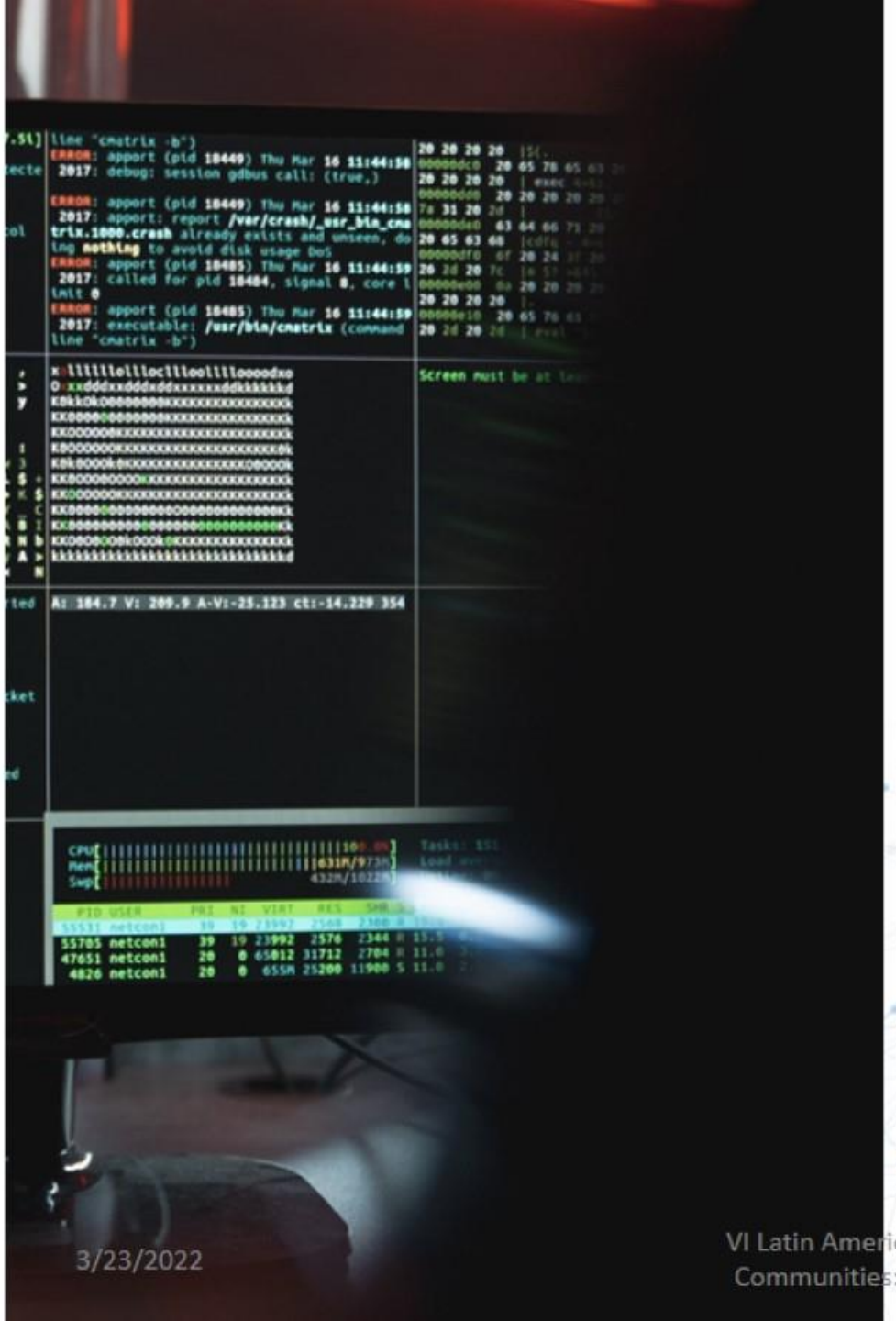
- Sabotage (Disgruntled employees or customers seeking revenge)
- Cyber Attack
- Natural Disaster
- Fire
- Explosion
- Bomb Threat

Cyber Security

- Ubiquitous broadband
- IT-centric business and society
- Social stratification of IT skills

Digital Transformation

SECURITY AND CYBER SECURITY



Cybersecurity - Vulnerabilities

- India’s Jawaharlal Nehru Port
- Shipbroking giant Clarksons,
- Chinese conglomerate Cosco and
- French container shipping line CMA CGM
- International Maritime Organization (IMO)
- Maersk

SECURITY AND CYBER SECURITY

Impact of Cyber Security Breaches

- Stoppage of operations
- Theft of data and /or cargo
- Drug and human trafficking
- Damage to systems
- Financial loss

Cyber Security – Risk Management

- Last year, the IMO introduced its first comprehensive cyber-security recommendations MSC-FAL.1/Circ.3 *Guidelines on maritime cyber risk management.*

- The container shipping sector, for example, the industry body, the Digital Container Shipping Association (DCSA) published its cyber-security implementation guide back in 2020. -Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems.

Cyber Security – Risk Management

- Confidentiality – access control and privacy protection to sensitive data.
- Possession or control.
- Integrity of system – configuration of system must be robust enough to allow for the maintenance of system integrity – secure information flow, unauthorized access through insecure network or corrupted file.
- Authenticity – ensuring that inputs to and from the port systems are genuine. Implementation of means of verification.
- Resilience – easy transformation, renewal and recovery of information and systems to normal operating state in a timely manner.
- Cloud services, a key element

Cyber Security - Challenges

- Slow use of technology within the Port's eco-system.
- Lack of training.
- Budgetary and Human Resource allocation.
- Training in the complex port operation logistics chain.
- Secure supply chain secure integration
- Infrastructure redundancy / Failover systems

Cyber Security – Mitigation of Threats

ACTION	REQUIREMENT
Training/awareness	End-user / staff awareness /training in online safety.
Keep software up to date.	All software on an update schedule to ensure the latest updates from vendors are tested then deployed to production environments.
Endpoint protection.	Endpoint protection is installed and centrally managed to ensure the latest protection signatures are applied.
Firewall	Firewall installed with robust incoming and outgoing rules
Backup of data.	Daily and weekly backup with point in time restore to ensure data and information availability utilizing online and offline mechanisms.
Control access.	Access to network, systems and data controlled by secure passwords.
Employee personal accounts.	All users have individual accounts
Access management.	Access control limited to individual work requirements
Passwords complexity.	Robust password complexity implemented through system policies
VPN.	Remote users access resources through VPN encryption.
Securing of devices and network.	Only approved devices are allowed to connect to corporate network

Re-evaluation

- Continuous re-evalution of risk mitigation strategies and appropriate accompanying action are critical in managing Port and Cyber Security.

THANK YOU

SECURITY AND CYBER SECURITY