QMII

10 Steps to Bolster Maritime Cyber Security

What We Will Cover Today

1 About QMII

2 Why Are We Here?

3 Bolster your cybersecurity ….

4 Q & A

About QMII

- QMII has provided best in industry process improvement services since 1986.
- Headquartered in Ashburn VA.
- Global Reach.
- ISO 9001:2015 Certified.
- SBA 8(a) & DBE certified.
- Minority owned business.
- GSA PSS and Schedule 70 Holder.

About QMII

US Coast Guard

FHWA

US Navy

NJ Transit

US Army

Amtrak

DOT

US Air Force

US Marines

GPO

DOC

Commerial

U.S.ARMY

BOEING

smsa
Seychelles Maritime Safety Authority

Holland America

Interlake
MARITIME SERVICES

Why Are We Here?

Understand what is a cyber threat

Identify the common practices that will bolster cybersecurity

Auditing the system for effectiveness

What is Cyber Security (1 of 2)

Cyber security can be defined as:

"The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."*

[*] International Telecommunications Union, "Overview of cyber security", ITU-T X.1205, 2008, Geneva, Switzerland

What is Cyber Security (2 of 2)

- Cyber security is not just about preventing hackers gaining access to systems and information, potentially resulting in loss of **confidentiality** and/or control.
- It also addresses:
  - The maintenance of **integrity** and **availability** of information and systems;
  - Ensuring business continuity; and
  - The continuing utility of digital assets and systems.

Current Problems

- Increase in data breaches
- Loss of business continuity due breaches
- Lack of response plans
- Increased reliance on automation
- Lack of awareness
- Cloud computing vulnerabilities
- Phishing/ Social engineering attacks
- Internal attacks

Maritime Cyber Security - Vulnerabilities

- Cybertechnologies are essential to the operation and management of shipping. Vulnerable systems could include, but are not limited to:
  - Bridge systems;
  - Cargo handling and management systems;
  - Propulsion and machinery management and power control systems;
  - Access control systems;
  - Passenger servicing and management systems;
  - Passenger facing public networks;
  - Administrative and crew welfare systems; and
  - Communication systems.

Control of both information technology and operational technology systems should be considered.

Step 1 – Leadership Commitment

- Gain Leadership buy-in from the outset
- ***Cyber-security cannot be buttoned on.***
  - It is a part of the business processes.
  - Measures taken to bolster cyber-security will impact the regular processes:
    - By at times slowing them down; or
    - Perhaps even making them more costly
- Leadership needs to weigh in on the risk versus reward and address accordingly

Step 2 – Use a System Framework

- **PLAN -** Establish security policy, objectives and processes relevant to managing risk and improving cybersecurity to deliver results in accordance with an organization’s overall policies and objectives
- **DO -** Implement and operate the security policy controls processes and procedures
- **CHECK -** Assess and where applicable measure process performance against security policy objectives and practical experience and report the results to management for review
- **ACT -** Take corrective and risk mitigation actions based on the results of the management review to achieve continual improvement of the system

Step 3 – Give risk a context

- Consider the context of the organization, trade patterns, cargo, technology, legislations etc.
- Identify the various stakeholders included in the operation and chartering of the vessel
- Online networks on the vessel
- Critical components / business sensitive information identified

Step 4 – Risk Assessment (a 3D framework)

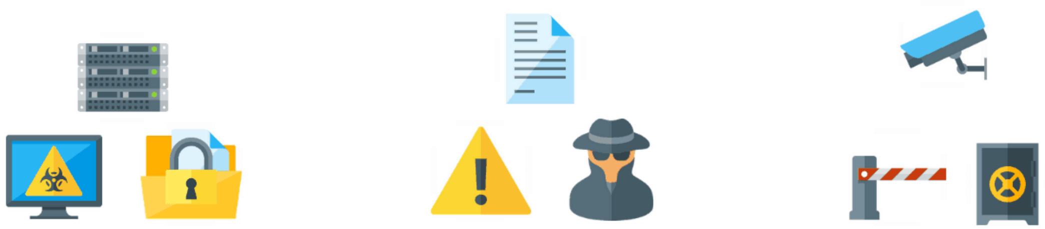
- Probability – Likelihood of occurrence
- Severity – Consequence
- Detection – Likelihood of identification

*Consider **CONFINDENTILITY, INTEGRITY** and **AVAILABILITY** of Information*

(including the assets, it is stored on)

Step 5 – Build controls into the processes

- Identified controls should be implemented basis the *feasibility rule*
- Information security should be a part of all the organization does – not an add on
- Use a layered approach to implementation of controls



TECHNICAL CONTROLS

ADMINISTRATIVE CONTROLS

PHYSICAL CONTROLS

Step 6 – Maintain basic measures

- Keep hardware and software current
- Automate antivirus and antimalware updates
- Limit Administrator privileges
- Control removable media devices
- Restrict access to assets/spaces as needed
- Do not connect to public networks unless using a VPN
- Backup information and test restore capabilities

Step 7 – Employee Awareness

36% of data breaches are caused by employee negligence. Train Personnel to:

- Identify phishing emails and malicious websites
- Use of own devices in connecting to network
- Third party personnel left to work without supervision
- Safeguarding own user information (passwords etc.)
- Identifying and reporting an incident

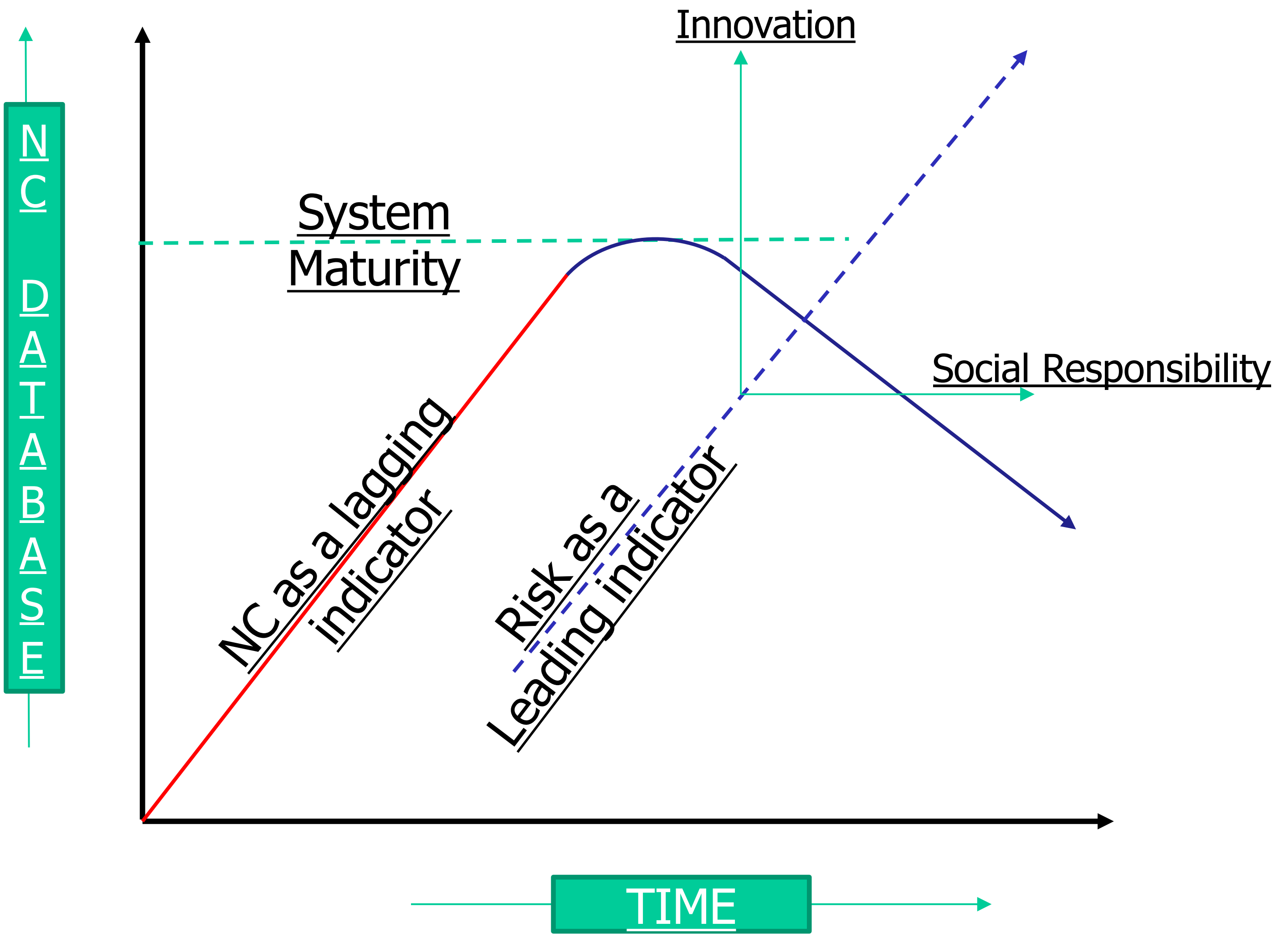
Step 8 – Emergency Preparedness

- Develop a business continuity plan
- Consider information critical to maintain supply chain and operations
- Test the plan at planned intervals and improve from lessons learned
- Test restore capabilities

Step 9 - Assess Effectiveness

- Has a cyber security assessment been conducted? Evidence:
  - Assets and vulnerabilities identified
  - Processes and inter-dependencies identified
  - Have IT/OT, physical and human vulnerabilities been considered
    - Physical access as well as access to assets (equipment, networks etc.)
    - Insider threats, contractors used
    - Malware, phishing, hacker breach potentials
  - Risk criteria in place / Control plan developed
- Consider Third-party assessment

Step 10 – Continual Improvement/MR



Maritime Cyber Security - Best Practices

- *The Guidelines on Cyber Security Onboard Ships* produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

- ***ISO/IEC 27001 standard on Information technology*** – Security techniques – Information security management systems – Requirements.

- United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (*the NIST Framework*).

Quality Management International, Inc.

Procurement Options

GSA Contract Holder
Contract GS-10F-0075N

SBA
U.S. Small Business Administration
8(a) Certified

GSA MAS (Schedule 70): 47QTCA20D0050
DUNS: 82-5610108
CAGE: 1GFC9

SDVOSB Partners
WOSB Partners
HUBZONE Partners
Other Vehicles

Thank You!!!

Inderjit Arora
iarora@qmii.com
(888) 357-9001

Assessing Effectiveness (2 of 3)

- Technical measures implemented may include:
  - Firewall
  - Anti-virus software
  - Spam-Filter
  - USB lock
  - Backup Storage
  - Blocking email attachments
  - Separation of internal and external systems
  - Stand alone solution instead of network-system
  - Access rights controls (password/key access)
  - Activation of automatic updates and patch services

Assessing Effectiveness (3 of 3)

- Operational measures implemented may include:
  - Password policy / Password management
  - Clearly defined responsibilities
  - Responsibilities of Contractor(s)
  - Backup policy
  - Monitoring of IT networks (continuous)
  - Clear screen/Clear desk policy
  - Auto patches/updates
  - Recovery plan / continuity plan /redundancy
  - Avoid single administrators
  - Remote access policy