CBMU
The Canadian Board of Marine Underwriters

THE NEED FOR CYBER SECURITY IN THE TRANSPORT ECO-SYSTEM

May 26,2016

CBMU
The Canadian Board of Marine Underwriters

THE NEED FOR SECURITY IN THE TRANSPORT ECO-SYSTEM

- Transportation forms an integral part of a nation's critical infrastructure
- Preserving the integrity, confidentiality and availability of information and services is a leading priority for every transport organisation
- It has never been more so with the advent of intelligent transport systems and services (ITS)
- Connected cars, connected aircraft, automation of cargo journey information, self-service airports, the growing reliance of ships on technology all powered by the adoption of new technologies such as the internet of things (IoT)
- Current Cyber defenses are not adequate to address advanced threats
- The speed of attacks have increased and the ability for organizations to detect an attack will determine the impact and cost of the cyber incident on the business
- Securing the supply chain and its components parts is a balancing act between cost efficiencies, new technology and compliance organizations are discovering this with the threat of cyber increasing

CBMU
The Canadian Board of Marine Underwriters

THE TECHNOLOGY DISRUPTION OF THE SHIPPING INDUSTRY

- Increasing Digitalisation -drives Cyber Threats (e.g. ship to shore communication, e-navigation, integration technologies)
- Secondary and Tertiary uses of Technology- creates potential security issues (e.g. GPS technologies integrated with weather forecasting)
- Crew and Onshore Staff -pose the biggest risk to Cyber Security (e.g. common networks for navigation, engineering, crew)
- Physical Access to equipment (e.g. diagnostic ports on equipment)

CBMU
The Canadian Board of Marine Underwriters

ENTERPRISE MOBILITY OF DATA HAS PROVEN TO BE A MAJOR RISK

- Data and files leave enterprise firewalls everyday
- Technology that takes the data beyond the enterprise firewalls leaves the organization exposed
- The more mobility you have on the data it increases the risk of being hacked
- It is estimated that targeted attackers are on average are able to operate some 416 days within an organization prior to detection[1]

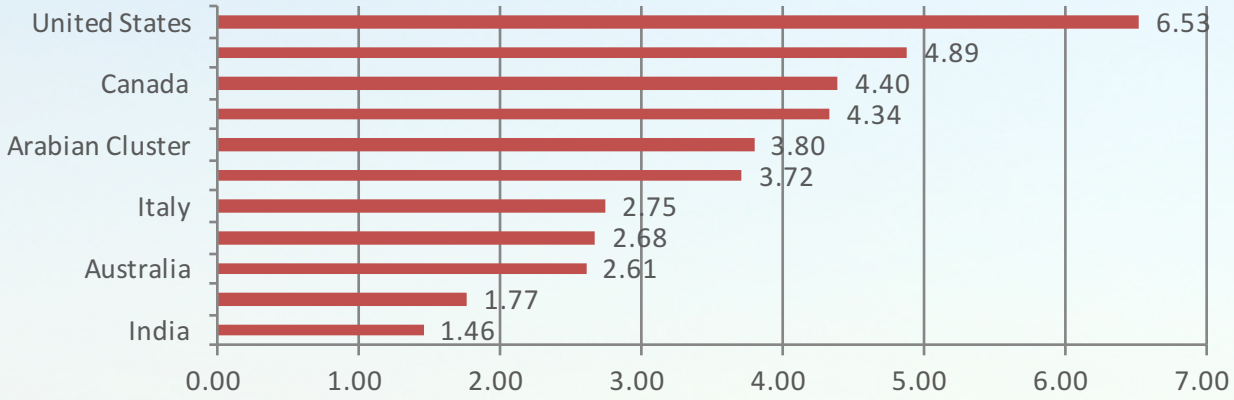
1 Mandiant-M-Trends 2012

CBMU
The Canadian Board of Marine Underwriters

CYBER RISK

As seen in the figure below, the average cost of an organizational breach is upwards of $4.4 million in Canada

Average total organizational cost of a data breach ($US mill.)



Source: Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis*

Largest data breaches in the last decade have cost … hundreds of millions of dollars

CBMU
The Canadian Board of Marine Underwriters

CLAIMS STUDY

Average cost of crisis services $500,000

Average cost of legal defense $434,000

Average cost of legal settlement $880,000

Source: NetDiligence 2015 claims study

CBMU
The Canadian Board of Marine Underwriters

DATA BREACH TRENDS

NOTE this is tip of iceberg…many more undetected or not reported

Breaches

- Human cause 53% of all losses
- Hackers cause 31% of the incidents
- There was insider involvement in 31% of the incidents

Target

- PII was the most frequent exposed data (45% of claims)
- Followed closely by PCI and PHI data

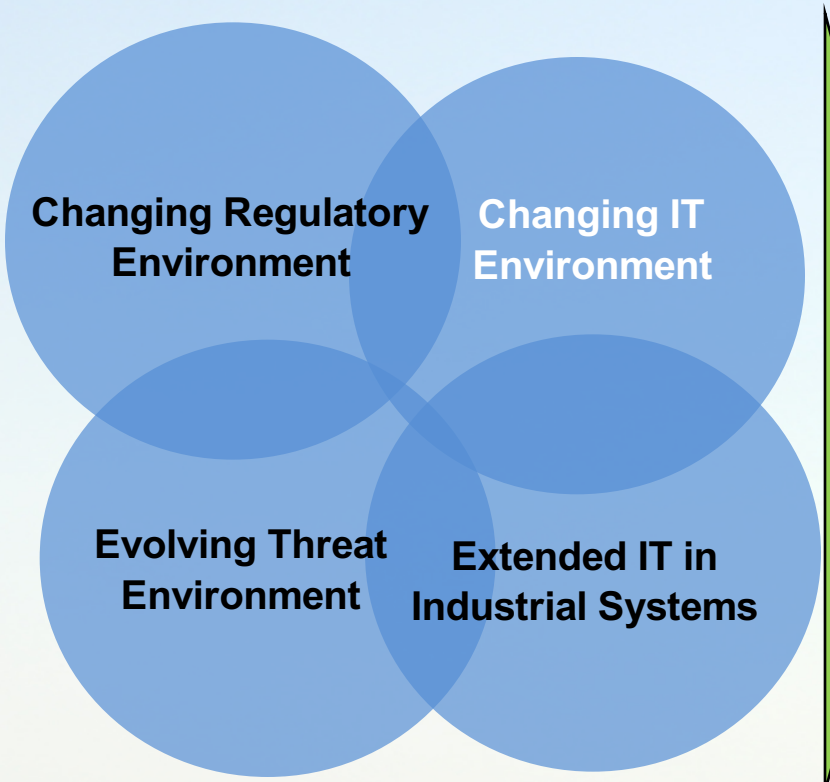
Recovery

- Containment
- Investigate
- Remediation
- Notification
- Defense
- Role of the Breach coach

Costs associated with system downtime
Forensic investigation and repair of IT security weaknesses
Notification of the breach to affected customers
Credit-monitoring service for affected clients
Regulatory fines and associated costs
Possible legal and class action suits
Public relations activities to manage and restore the firm's reputation

CBMU
The Canadian Board of Marine Underwriters

CYBERSECURITY



The business and IT environment is changing…

- New business models – cloud, mobile
- IT Systems find themselves deep in the Industrial Environment
- Regulatory and contractual changes such as OSFI, ITSG, industry regulation, emerging NIST standards, EU, and more

…Leading to new, persistent, evolving risks…

- More frequent, sophisticated & malicious attacks
- Wide range of motives: economic, campaigns, Hactivists
- Hackers already inside the organization
- Data easily available and it's money

…Most are struggling to keep pace:

- Risks are evolving faster than one could react
- Need to **transform** how they think about Cybersecurity
- Organizations large and small do not have the skills in-house
- Greater need for comprehensive risk management enterprise solutions
- Organizations are struggling how to "measure" cyber risk

CBMU
The Canadian Board of Marine Underwriters

THE COLLISION OF CYBER HACKS IS A THREAT TO THE MARINE INDUSTRY

March 2016 a Verizon research study discussed a group of sea pirates which recently hacked into a shipping company's system for managing shipping routes and used the information to target ships with valuable cargo

The risk team was contacted by a global shipping conglomerate that advised they were having problems with piracy. Not software piracy. Actual piracy, as in criminals with boats and guns. It became apparent to the shipping company that the pirates had specific knowledge of the contents of each of the shipping crates being moved. They boarded the vessel, located by bar code specifically sought-after crates containing valuables, stole the contents of that crate—and that crate only—and then departed the vessel without further incident. Further investigation found that the company used a homegrown Web-based content system to manage bills of lading- the hackers breached this system to gain access to the data

CBMU
The Canadian Board of Marine Underwriters

SHIPS ARE VUNERABLE TO HACKERS

Large ships at sea larger than 150 gross tons are required by some governments to be equipped with a voyage data recorder (VDR), which is the maritime equivalent of the “black box” that is required aboard airliners

Cybersecurity analysts have recently discovered that the devices are not hack-proof, finding that the wealth of data they collect can be stolen or wiped out.
In 2014, IOActive a security firm disclosed a series of attacks that affected multiple SATCOM devices, some of which are commonly deployed on vessels. The vulnerabilities included how the software for the devices were developed, weak encryption algorithms, undocumented protocols, and design flaws.

CBMU
The Canadian Board of Marine Underwriters

CYBER IN THE MARINE INDUSTRY IS GROWING

Multiple Systems Hacked In 2012, the Chinese military compromised "multiple systems" on a commercial ship on contract to Transcom

Crew Member Corrupts Data data was corrupted when a crewmember on a Singapore-flagged ship inserted a USB drive into a port on the VDR—causing it to be infected with a virus

Hackers Recently Shut down a floating oil rig by tilting it, while another rig was so riddled with computer malware that it took 19 days to make it seaworthy again

Belgium Port Hacked Hackers infiltrated computers connected to the Belgian port of Antwerp, located specific containers, made off with their smuggled drugs and deleted the records

CBMU
The Canadian Board of Marine Underwriters

POSSIBLE AREAS OF ATTACK ON A SHIP

- Ships and safe navigation
- Satellite communication
- Cargo tracking systems
- Marine radar systems
- Automatic identification systems
- Cranes run on satellite based GPS systems
- VDR systems use Ethernet
- Weak encryption of VDR files




CBMU
The Canadian Board of Marine Underwriters

CYBER RESILIENCE STARTS BY UNDERSTANDING THE ORGANIZATION RISKS

Who might attack?

- Cyber criminals
- Hactivists (agenda driven)
- Nation states
- Malicious insiders
- Rogue suppliers
- Competitors
- Skilled individual hacker

What are they after and what key business risks must be mitigated ?

- Sensitive data
- Financial fraud (e.g. wire transfer, payments)
- Business disruption (ship systems, etc.)

What tactics might they use?

- Spear phishing, drive by download, etc.
- Software or hardware vulnerabilities
- Third party compromise
- Stolen credentials
- Control systems compromise

CBMU
The Canadian Board of Marine Underwriters

CONTROLS TO MITIGATE CYBER

Communications Security Establishment

CSE Top 10

- Use SSC Internet Gateways
- Patch OS & applications
- Enforce Administrative privileges
- Harden OS
- Segment and separate information
- Awareness training
- Manage devices at enterprise level
- Apply protection at host level
- Isolate web-facing applications
- Implement Application Whitelisting

2015 Study

- Cybersecurity vulnerabilities can be addresses through a risk based approach
- Companies need to identify Cyber threats and vulnerabilities and operations
- Plan barrier to mitigate incidents and consequences of a Cyber breach
- Companies need to put procedures in place

BIMCO

2015 Study

- Industry stakeholders should develop, manage and update computer-based systems on-board ships in a secure way
- Minimize the risk of a cyber attack through user access management
- Protect on board systems
- Develop contingency plans
- Ship networks should be configured to have controlled and uncontrolled networks

CBMU
The Canadian Board of Marine Underwriters

CLOSINGS THOUGHTS

- Organizations need to know critical data and assets – not just what to protect but what they need to protect
- Fortify and monitor- build, maintain and proactively monitor
- Prepare for the inventible
- Understand what threats impact the organization and invest in the right controls
- Ships carry data there needs to be a risk based approach on how to protect the data
- Cyber security considerations should start at the software development stage
- Know where the data is going
- A national database