Cyber Risk in Shipping

Strategies for Managing Cyber Risk in the Age of Digitalization

Members Training Course

Southampton,
July 7, 2023

HudsonCyber
Managing Cyber Risk

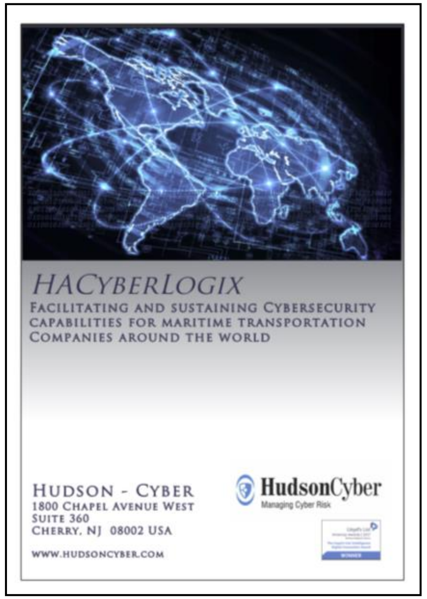
Steamship
Mutual

Agenda

I. Introductions
II. Context and current challenges
III. Cyber threat landscape considerations (and misperceptions)
IV. Case study – what we're seeing with the U.S. Coast Guard
V. Leadership strategies for driving organizational cyber resilience

HudsonCyber – about us

Award Winning Cybersecurity Risk Management Solutions



HACyberLogix

Facilitating and sustaining Cybersecurity capabilities for maritime transportation Companies around the world

Hudson - Cyber
1800 Chapel Avenue West
Suite 360
Cherry, NJ 08002 USA

www.hudsoncyber.com

HudsonCyber
Managing Cyber Risk

HudsonCyber
Managing Cyber Risk

Global
Innovative
Award-winning

PORTLOGIX™

Gain Control of your Maritime Supply Chain

Residing at the nexus of complex global supply chains, ports and marine terminal operators are increasingly reliant on a wide range of suppliers supporting various critical functions. The introduction of AI, Internet-of-Things sensor systems, outsourced cloud services, and mobility-enabled systems accelerate digitalization and outsourcing trends. However, suppliers have their own key vendors, who in turn depend on other third parties, extending supply chain ecosystems outward like ripples in a pond.

Unfortunately, this combination of digitalization and dependence on foreign and domestic suppliers to support essential port functions generates diverse and numerous cybersecurity risks that maritime leaders are only just now recognizing. Supply chains, often the weak underbelly to cyber-mature organizations, are persistently and increasingly targeted and exploited by cyber threat actors. Not only do these attacks damage reputation and security, but they can result in significant operational disruption, liability exposure, and financial loss.

In this environment, it is more important than ever that port and terminal leaders understand, gain visibility into, and proactively manage cyber risks to their supply chains.

PortLogix™ delivers the foundational capability to rapidly establish a cost-efficient and scalable Cyber Supply Chain Risk Management (C-SCRM) program.

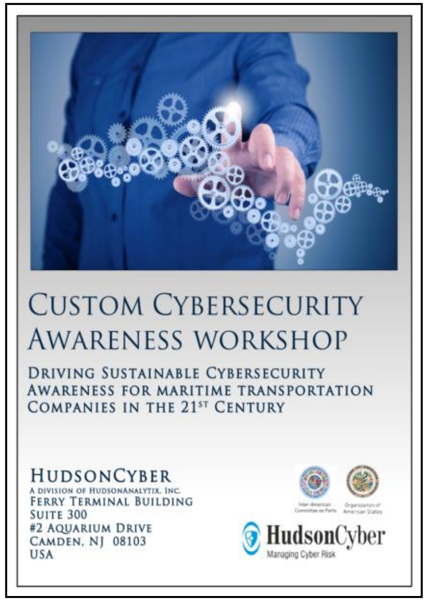
PORTLOGIX™ EMPOWERS PORT-INDUSTRY STAKEHOLDERS TO:

- ✓ ***Establish*** portfolio level oversight of supply chain stakeholders, vendor organizations, and key port community system partners
- ✓ ***Virtually assess, audit, and monitor*** supply chain partners' cybersecurity capabilities for mitigating identified gaps
- ✓ ***Measure and benchmark*** C-SCRM capabilities against pre-defined targets and peers
- ✓ ***Define and implement*** minimum C-SCRM standards and capability targets
- ✓ ***Identify and monitor*** trends in cybersecurity capability gaps and recommendations
- ✓ ***Increase*** visibility of cyber capabilities between organizations within a supply-chain

info@portlogix.com
hudsoncyber.com

+1 856.342.7500

1800 Chapel Avenue West, Suite 360
Cherry Hill, NJ 08002 USA



Custom Cybersecurity Awareness Workshop

Driving Sustainable Cybersecurity Awareness for maritime transportation Companies in the 21st Century

HudsonCyber
A division of HudsonAnalytix, Inc.
Ferry Terminal Building
Suite 300
#2 Aquarium Drive
Camden, NJ 08103
USA

Inter-American Committee on Ports
Organization of American States

HudsonCyber
Managing Cyber Risk

Navigate the Breach!

Hudson Marine Cyber IQ (MCIQ) Service

Unified cyber incident response for vessels in U.S. Jurisdictions

In today's hyper-connected environment maritime transportation companies are under constant cyber attack. Cyber threat actors can not only commit financial fraud and manipulate commercial data for smuggling, but can also compromise shipboard networks and integrated IT/OT systems with the intent to circumvent security to deny, degrade, and/or disrupt vessel operations. The consequences can be severe – environmental damage, property loss, regulatory fines, first and third-party liability exposure, physical injury, or even death.

As cybersecurity regulations, guidelines and reporting requirements rapidly evolve in the United States, the U.S. Coast Guard has mobilized resources to inspect commercial vessels for cybersecurity deficiencies and non-conformities. In a worst-case cybersecurity incident, vessels can even be detained.

To protect shipowner interests, save money and minimize vessel delays, HudsonCyber has responded to this dynamic challenge with CyberIQ. Our CyberIQ service assists vessel owners and operators by coordinating all cyber incident response, reporting, mitigation, management, and oversight actions.

Prepare today with CyberIQ.

HudsonCyber
Managing Cyber Risk

1800 Chapel Avenue West, Suite 360
Cherry Hill, NJ 08002

www.hudsoncyber.com

Lloyd's List
Americas Awards | 2017
Maritime Intelligence | Informa
The Lloyd's List Intelligence Digital Innovation Award
WINNER

Primary cybersecurity services:

- Enterprise cyber risk management
- Tailored threat intelligence
- Custom training solutions

Steamship Mutual
enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY
Maritime Transportation System Information Sharing and Analysis Center
S&P Global Ratings
GMCC
AON Empower Results®
CHAUCER CYBER
AAPA ESSENTIAL. RESILIENT. UNITED. SEAPORTS DELIVER
IAPH International Association of Ports and Harbors
MITRE
SHORELINE
SC CapRock
THE WORLD BANK
OEA OAS
The Nautical Institute

Cybersecurity training

HudsonCyber offers half-day, full-day and customized instructor-led cyber-awareness training to the global maritime industry.

Workshop Objectives are to provide maritime stakeholders with an introduction to cybersecurity, an overview of cyber risk factors in marine terminal facilities, and a deeper understanding of cyber risk factors.

SSM Seatrade Awards Steamship Mutual

THE UNITED STATES NAVAL WAR COLLEGE VIRIBUS MARI VICTORIA

SC CapRock

UNIVERSITY OF PLYMOUTH

CHAUCER CYBER

MARITIME COLLEGE STATE UNIVERSITY OF NEW YORK

AON Empower Results®

CIP Inter-American Committee on Ports

SOCP SHIP OPERATIONS COOPERATIVE PROGRAM
BUSINESS • GOVERNMENT • EDUCATION • WORKFORCE

CMU CARIBBEAN MARITIME UNIVERSITY

The Nautical Institute

caribbean shipping association

MITAGS-PMI
MARITIME INSTITUTE OF TECHNOLOGY & GRADUATE STUDIES
PACIFIC MARITIME INSTITUTE

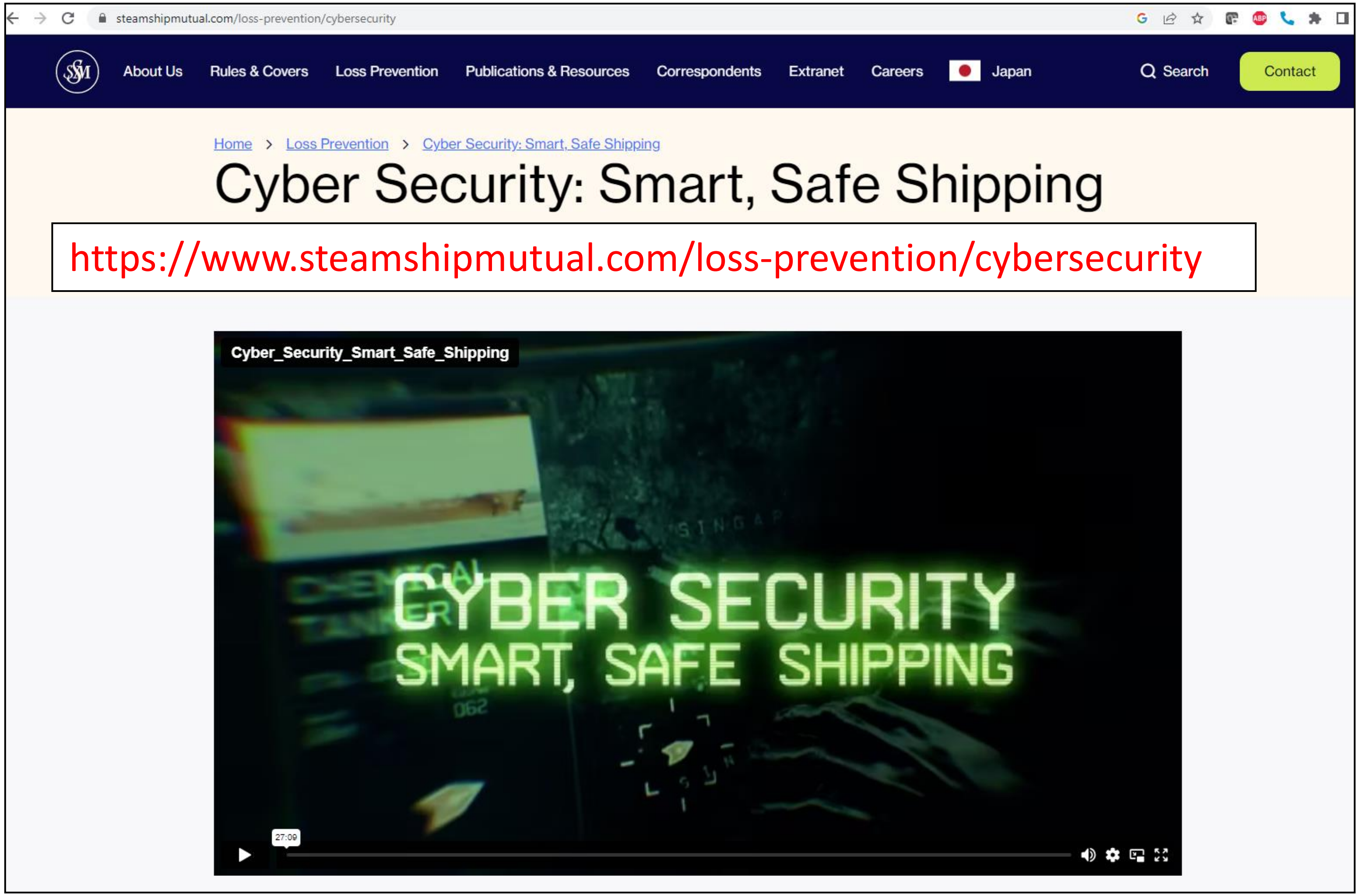
AAPA
ESSENTIAL. RESILIENT. UNITED.
SEAPORTS DELIVER

CHATHAM HOUSE
The Royal Institute of International Affairs

SHORELINE

Still relevant!

Steamship Mutual



steamshipmutual.com/loss-prevention/cybersecurity

Home > Loss Prevention > Cyber Security: Smart, Safe Shipping

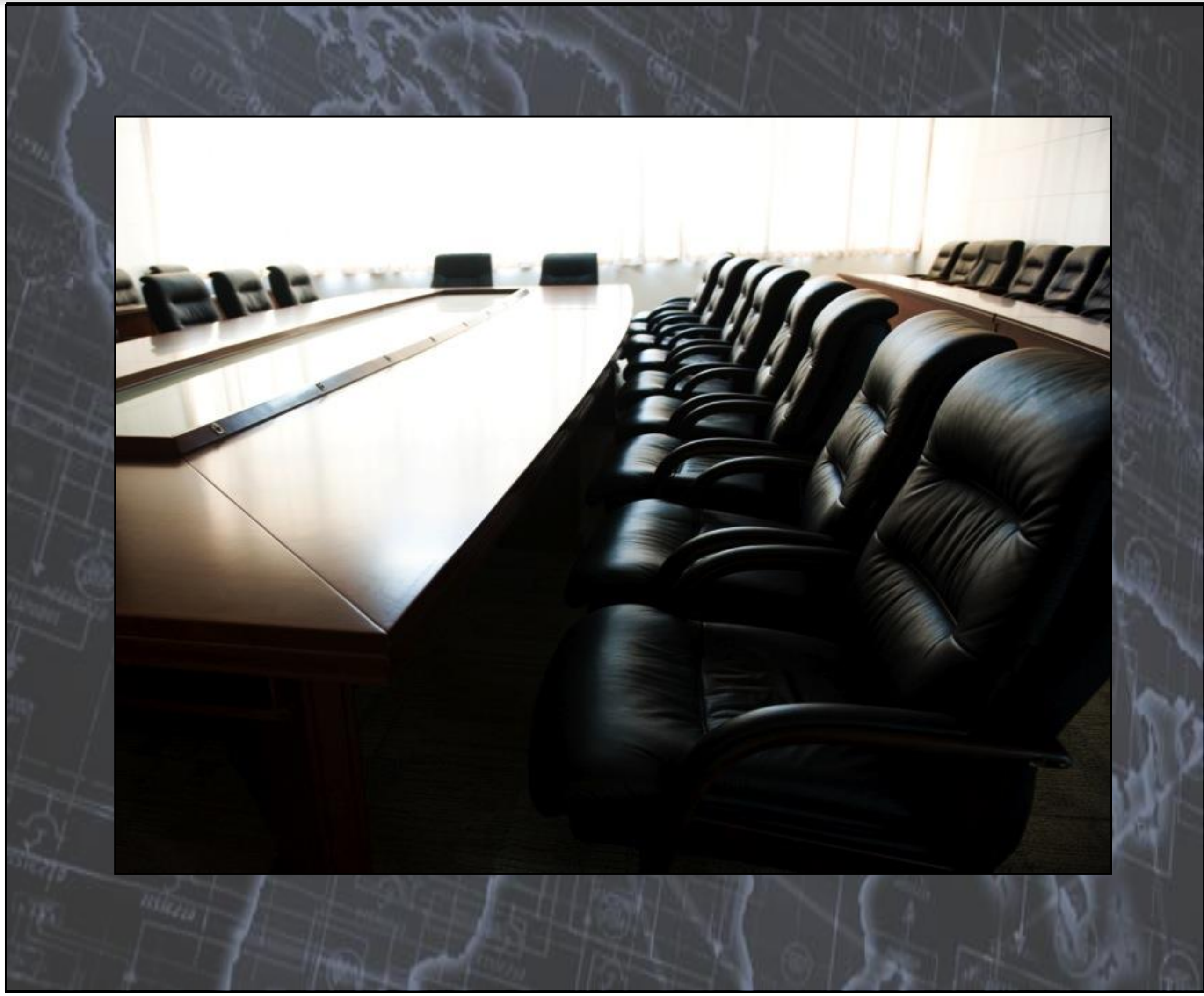
Cyber Security: Smart, Safe Shipping

https://www.steamshipmutual.com/loss-prevention/cybersecurity

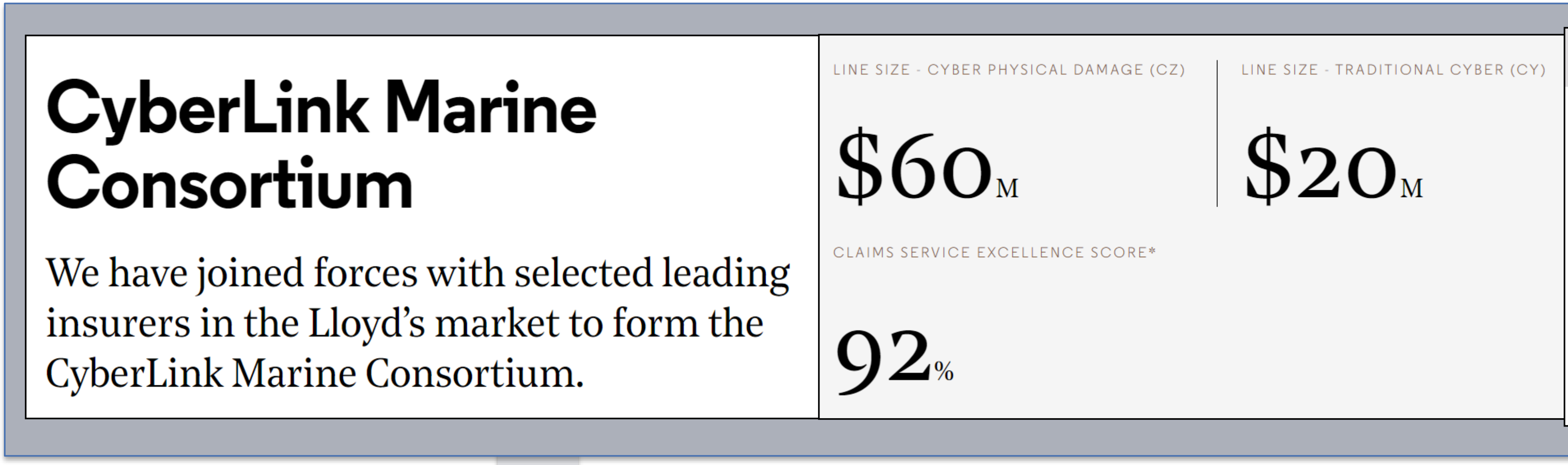
Tailored cyber threat intelligence services

In today's cyber environment CEOs can no longer view cybersecurity as an IT problem. Technologies alone are ineffective at preventing 100% of cyber attacks. There's always a human element.

Our analysts specialize in penetrating and exploiting highly vetted cyber underground forums to protect reputation, brand and shareholder value, as well as to obtain intelligence on compromised assets, emergent threats and/or threat activities specific to our clients.



Context: Cyber insurance
Driving cyber resilience in the global insurance markets / 2020



CyberLink Marine Consortium

We have joined forces with selected leading insurers in the Lloyd's market to form the CyberLink Marine Consortium.

LINE SIZE - CYBER PHYSICAL DAMAGE (CZ)

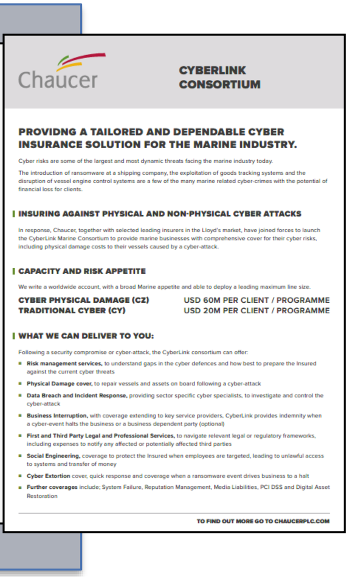
$60M

LINE SIZE - TRADITIONAL CYBER (CY)

$20M

CLAIMS SERVICE EXCELLENCE SCORE*

92%



Chaucer

CYBERLINK CONSORTIUM

PROVIDNG A TAILORED AND DEPENDABLE CYBER INSURANCE SOLUTION FOR THE MARINE INDUSTRY.

Cyber risks are some of the largest and most dynamic threats facing the marine industry today.

The introduction of ransomware at a shipping company, the exploitation of goods tracking systems and the disruption of vessel engine control systems are a few of the many marine related cyber-crimes with the potential of financial loss for clients.

INSURING AGAINST PHYSICAL AND NON-PHYSICAL CYBER ATTACKS

In response, Chaucer, together with selected leading insurers in the Lloyd's market, have joined forces to launch the CyberLink Marine Consortium to provide marine businesses with comprehensive cover for their cyber risks, including physical damage costs to their vessels caused by a cyber-attack.

CAPACITY AND RISK APPETITE

We write a worldwide account, with a broad Marine appetite and able to deploy a leading maximum line size.

CYBER PHYSICAL DAMAGE (CZ)	USD 60M PER CLIENT / PROGRAMME
TRADITIONAL CYBER (CY)	USD 20M PER CLIENT / PROGRAMME

WHAT WE CAN DELIVER TO YOU:

Following a security compromise or cyber-attack, the CyberLink consortium can offer:

- **Risk management services,** to understand gaps in the cyber defences and how best to prepare the Insured against the current cyber threats
- **Physical Damage cover,** to repair vessels and assets on board following a cyber-attack
- **Data Breach and Incident Response,** providing sector specific cyber specialists, to investigate and control the cyber-attack
- **Business Interruption,** with coverage extending to key service providers, CyberLink provides indemnity when a cyber-event halts the business or a business dependent party (optional)
- **First and Third Party Legal and Professional Services,** to navigate relevant legal or regulatory frameworks, including expenses to notify any affected or potentially affected third parties
- **Social Engineering,** coverage to protect the Insured when employees are targeted, leading to unlawful access to systems and transfer of money
- **Cyber Extortion** cover, quick response and coverage when a ransomware event drives business to a halt
- **Further coverages** include; System Failure, Reputation Management, Media Liabilities, PCI DSS and Digital Asset Restoration

TO FIND OUT MORE GO TO CHAUCERPLC.COM

CHAUCER CYBER

- **Private Equity**
- **Shipping**
- **Port Authorities**
- **Terminal Operators**

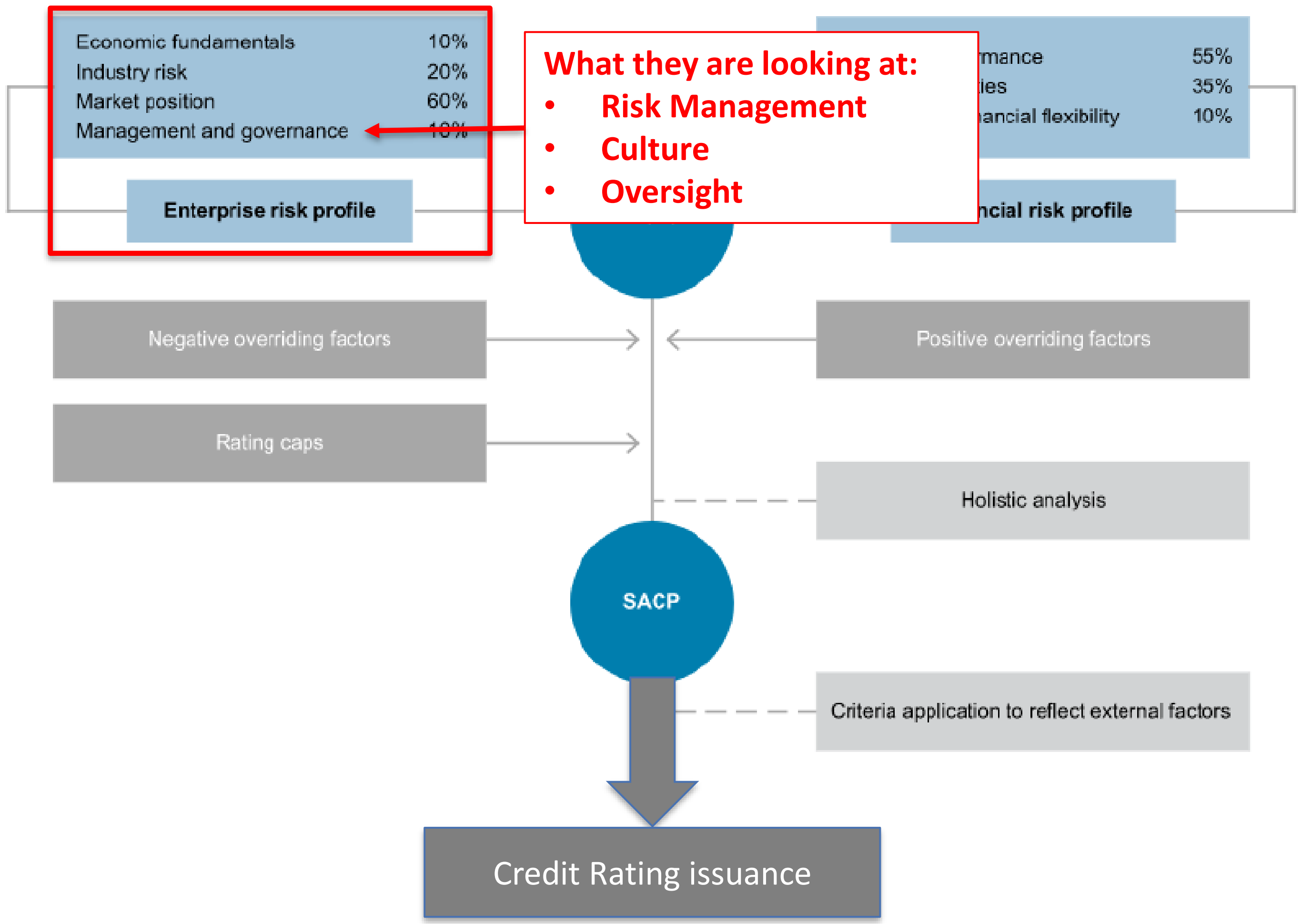
Context: Credit risk and cyber resilience
Driving cyber resilience in the global bond markets / 2023

S&P Global
Ratings

Key concerns for the port sector:

- Economic headwinds with supply chain disruptions
- Shifting trade policies
- Inherent exposures to volatility due to normal economic cycles, shifting supply chains
- Drastic fluctuations in commodity prices
- Rapid adoption of generative Artificial Intelligence by port stakeholders *and* cyber threat actors.
- Geopolitical events can lead to increased cyber risk for ports.

Global Not-For-Profit Transportation Infrastructure Enterprise Criteria Framework



What they are looking at:
- Risk Management
- Culture
- Oversight

Establishing cyber risk context and understanding the challenges

HudsonCyber
Managing Cyber Risk

Personal confessions

Have you been hacked?

Let me count the ways:

BAE SYSTEMS 2009

LinkedIn 2012

Anthem 2015

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT 2015

TARGET 2015

EQUIFAX 2017

NETFLIX 2017, 2019, ?

2016 f

Every Other Year

Cambridge Analytica 2016 ?

Marriott HOTELS & RESORTS 2018

IHG HOTELS & RESORTS 2022

What's old is new

His Primary Theses: War is…

- **"The continuation of policy by other means."**
- **"An act of force to compel our enemy to do our will."**

He Recognized:

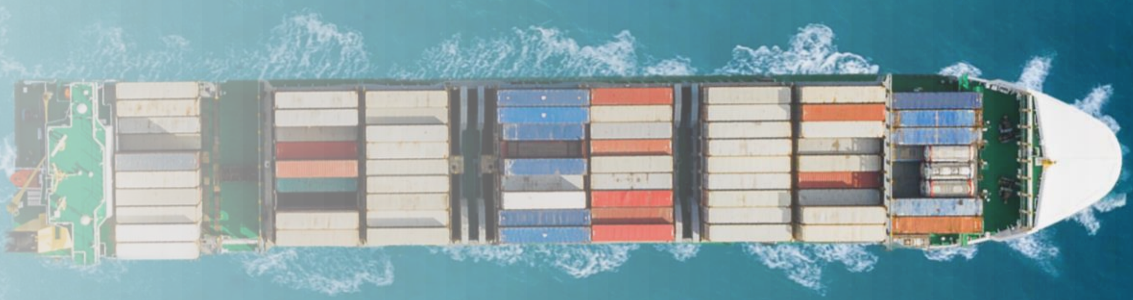
- **War is a political, social and military phenomenon.**
- ***Asymmetries* can defeat the perceived superiority of the defense.**

In today's digitalized world, most asymmetrical cyber risks are Human based.

What is “Cybersecurity”?

Cybersecurity is ***NOT*** just:

- Information Technology (“IT”)
- Compliance (e.g., ISO; ISPS, ISM)
- Solved by a “silver bullet” approach



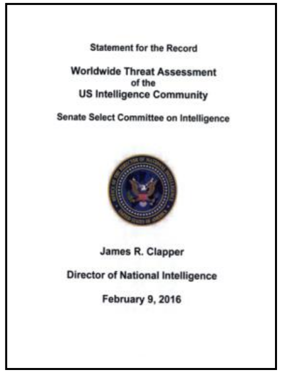
Cybersecurity ***IS:***

- A sustained risk management activity
- Sustained, cross-functional collaboration
- About cultural change and business transformation
- **The mission of protecting the entire business (the *Balance Sheet*)**
- A responsibility that starts at the top (you!)

One of the greatest threat to us all: *data integrity*

> “***ntegrity**. Cyber operations include an increased emphasis on changing or manipulating data to compromise its integrity to affect decision making, reduce trust in systems, or cause adverse physical effects.*”

James Clapper, Director of National Intelligence Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence



Statement for the Record

Worldwide Threat Assessment
of the
US Intelligence Community

Senate Select Committee on Intelligence

James R. Clapper

Director of National Intelligence

February 9, 2016

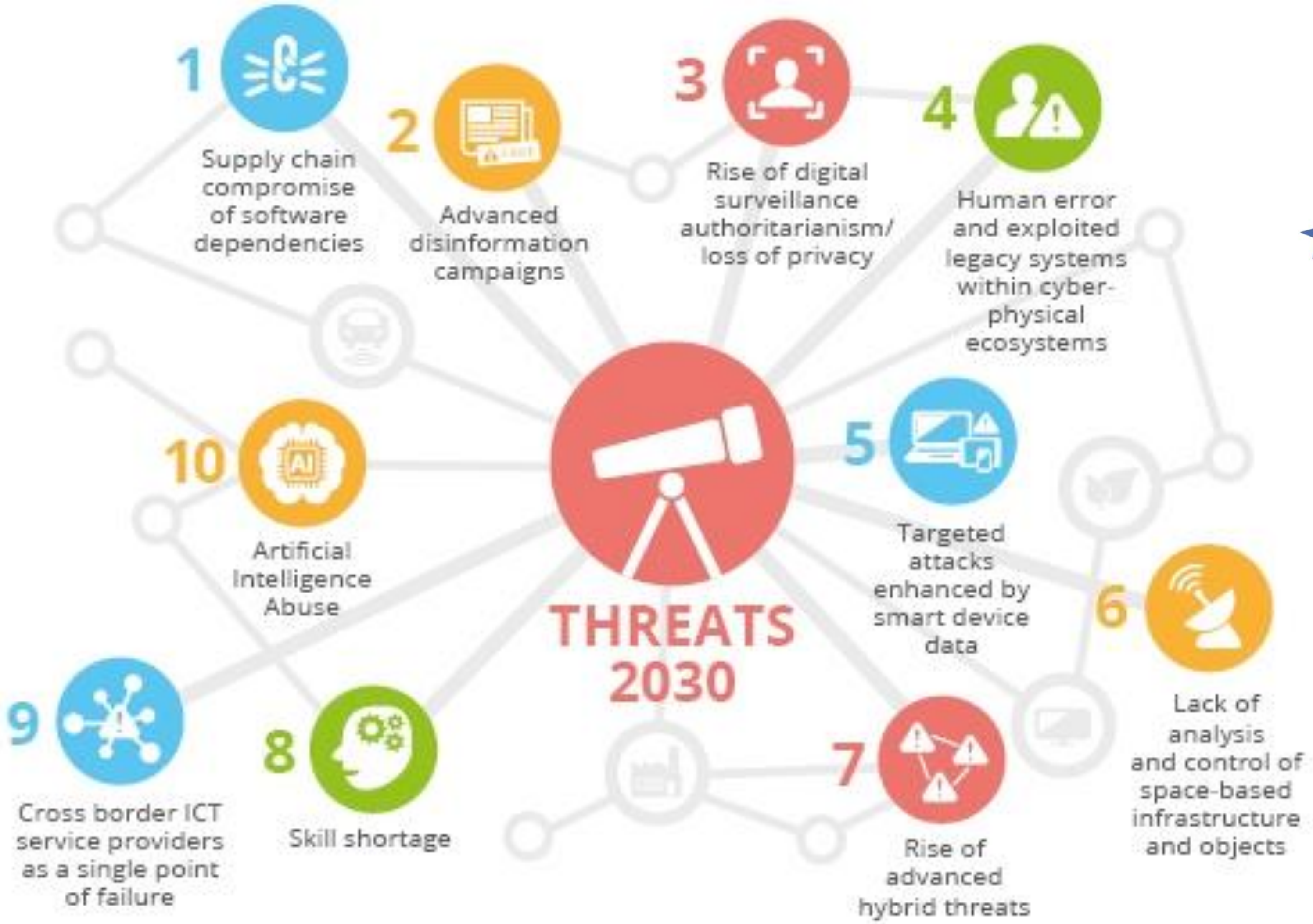
Threats include:

- ***Posting*** disinformation (false data);
- ***Altering*** of online media to influence/confuse public discourse, sentiment
- ***Modifying*** stored data;
- ***Transmitting*** false data; and
- ***Manipulating*** the flow of data

Cyber threat landscape considerations and misperceptions

HudsonCyber
Managing Cyber Risk

Top 10 cybersecurity threats emerging: 2030



THREATS 2030

1 Supply chain compromise of software dependencies

2 Advanced disinformation campaigns

3 Rise of digital surveillance authoritarianism/ loss of privacy

4 Human error and exploited legacy systems within cyber-physical ecosystems

5 Targeted attacks enhanced by smart device data

6 Lack of analysis and control of space-based infrastructure and objects

7 Rise of advanced hybrid threats

8 Skill shortage

9 Cross border ICT service providers as a single point of failure

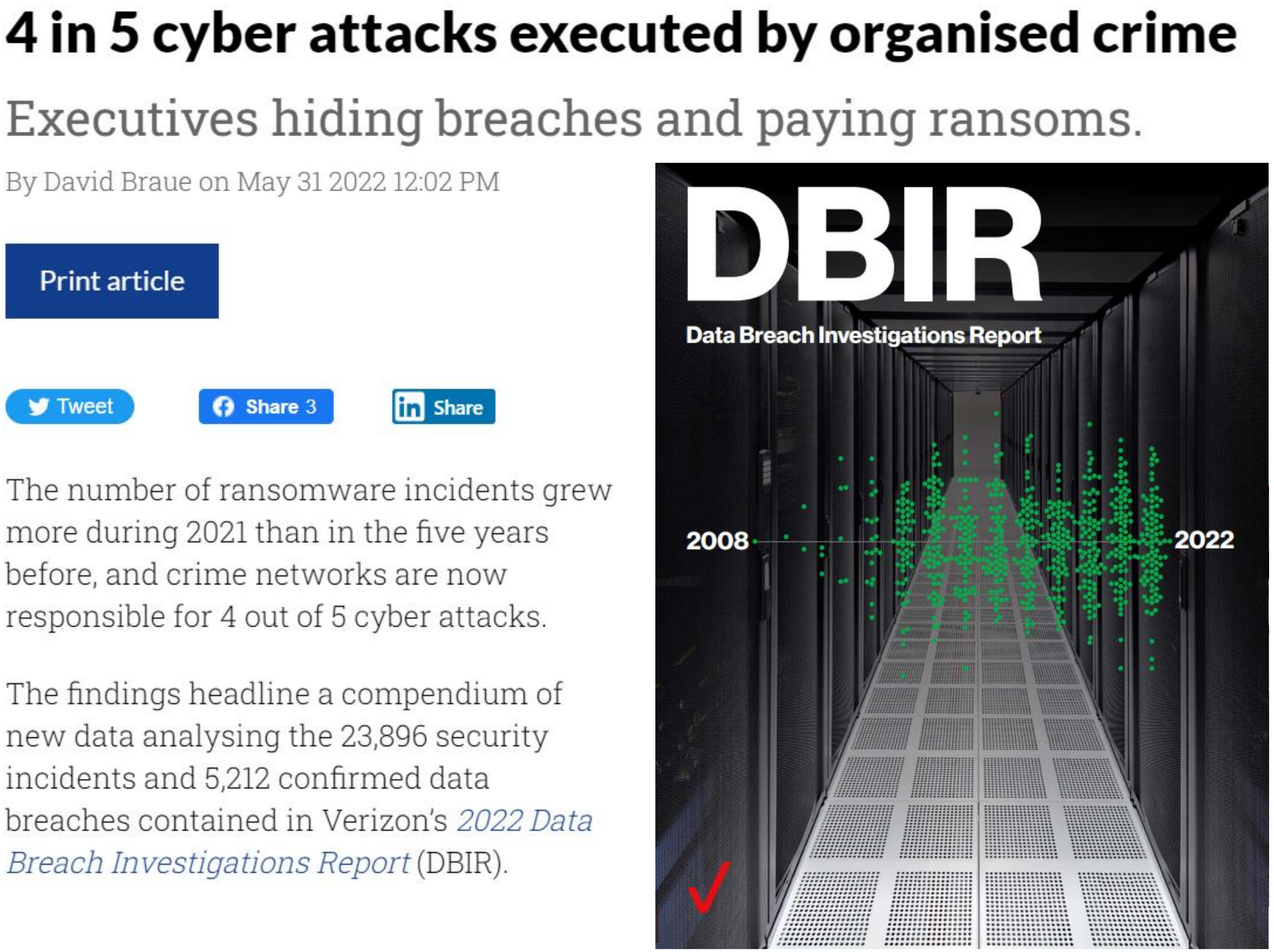
10 Artificial Intelligence Abuse

enisa

THE EU CYBERSECURITY AGENCY

HudsonCyber
Maritime Cyber Security

Key trends for reference



4 in 5 cyber attacks executed by organised crime

Executives hiding breaches and paying ransoms.

By David Braue on May 31 2022 12:02 PM

The number of ransomware incidents grew more during 2021 than in the five years before, and crime networks are now responsible for 4 out of 5 cyber attacks.

The findings headline a compendium of new data analysing the 23,896 security incidents and 5,212 confirmed data breaches contained in Verizon's *2022 Data Breach Investigations Report* (DBIR).

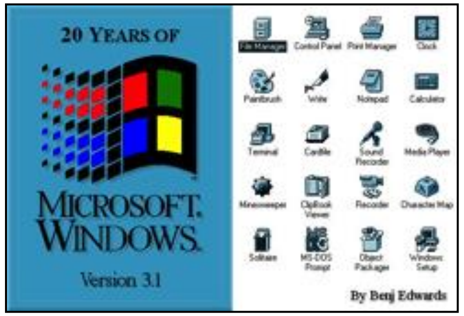
- **Majority of attacked executed by Organized Crime** (over 80%)
- Over 80% caused by **human error**
- Half of the breaches were enabled by **compromised credentials**
- Organizations were **regularly compromised through lateral movement from insecure business partners**, whose access to key company systems may be necessary

The maritime industry is a target because…

1. Volume of information

Lots of Information. Nation states have proven how successful supply chain attacks are. Criminals are likely to launch automated attacks against maritime targets rich in data.

2. Legacy systems



Lots of Legacy Systems. Stakeholders have their own systems. Often, these systems are older and have not been regularly patched or updated, offering easy targets for criminals.

3. Money

Lots of Money. Maritime stakeholders regularly transfer large amounts of money (e.g., between a shipowner and a yard or a shipping company and a bunker operator).

4. Language

Language. Communications are often conducted in a language not native to the participants. Language deficiencies are often forgiven.

HudsonCyber
Maritime Cyber Security

External challenges (threat landscape)

Threats are increasing:

- Hacking tools are readily available and easy to use
- The potential impact of cyber attacks continues to grow

Threat actor motivations are changing:

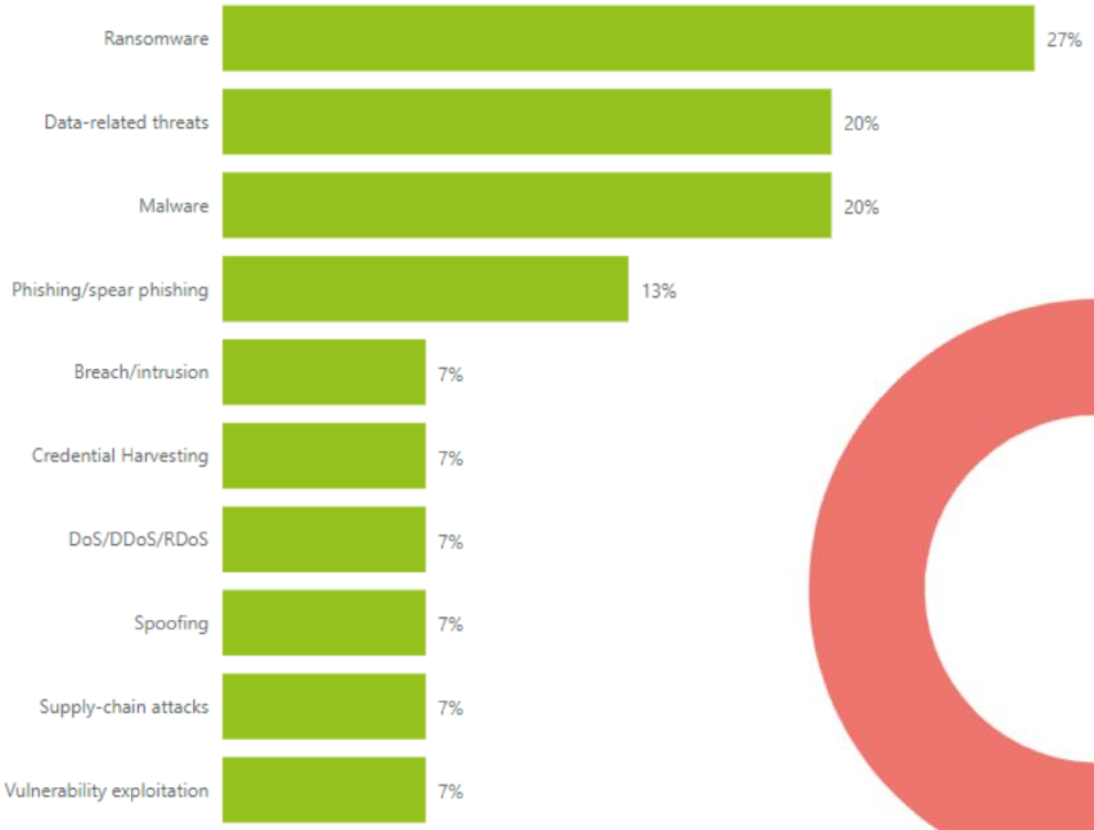
- Hackers seek more than entertainment and status
- Shift to professional cyber criminals motivated by money whose success relies on remaining undetected
- Nation states seeking access

Certain common factors enable threat actor success:

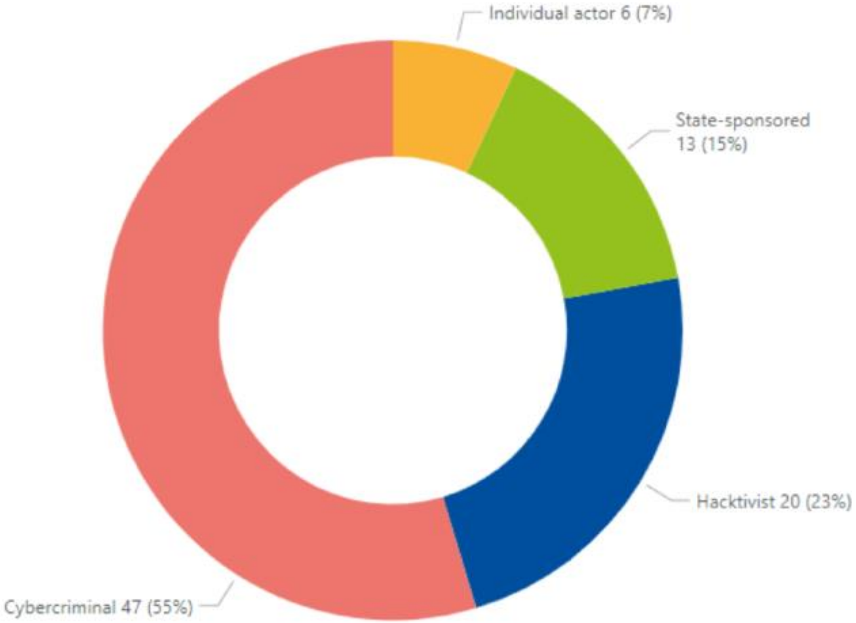
- Economy of organized cybercrime
- Inter-connected systems
- Widespread failure to implement cyber hygiene
- Adoption of generative AI will enable tailored attacks at scale

Threats, threat actors and motivation in the maritime transportation sector*

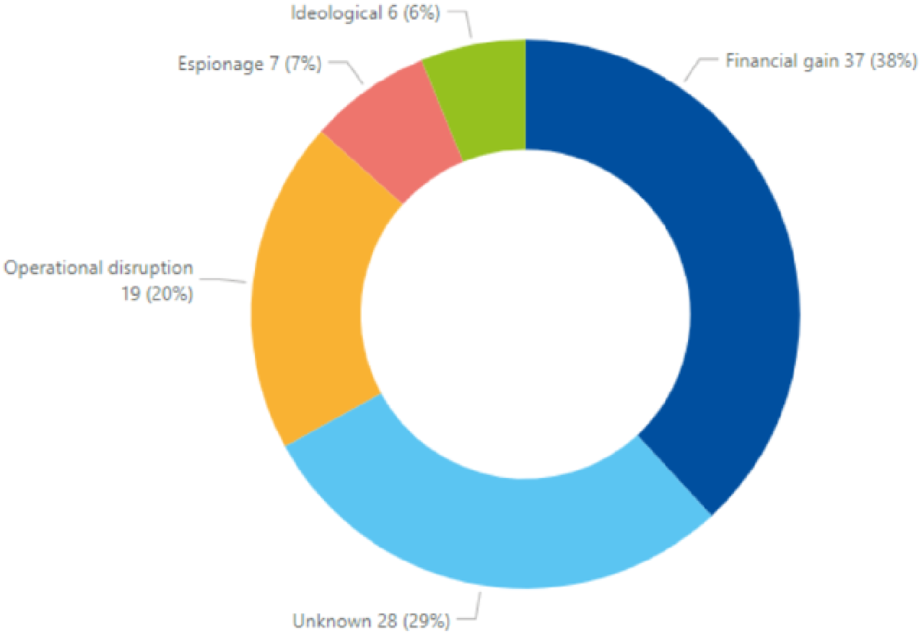
- **Cybercriminals**’ primary motive is financial gain, often stealing data or demanding ransom.
- **Hackers-for-hire** sell their services to people who do not have the skills or capabilities to do so.
- **State-sponsored** actors target organisations to compromise, steal, change, or destroy information. These groups are usually affiliated with a nation state[16].
- **Hacktivists** are politically, socially, or ideologically motivated and target victims for publicity or to effect change.



Threats



Threat Actors



Motivation

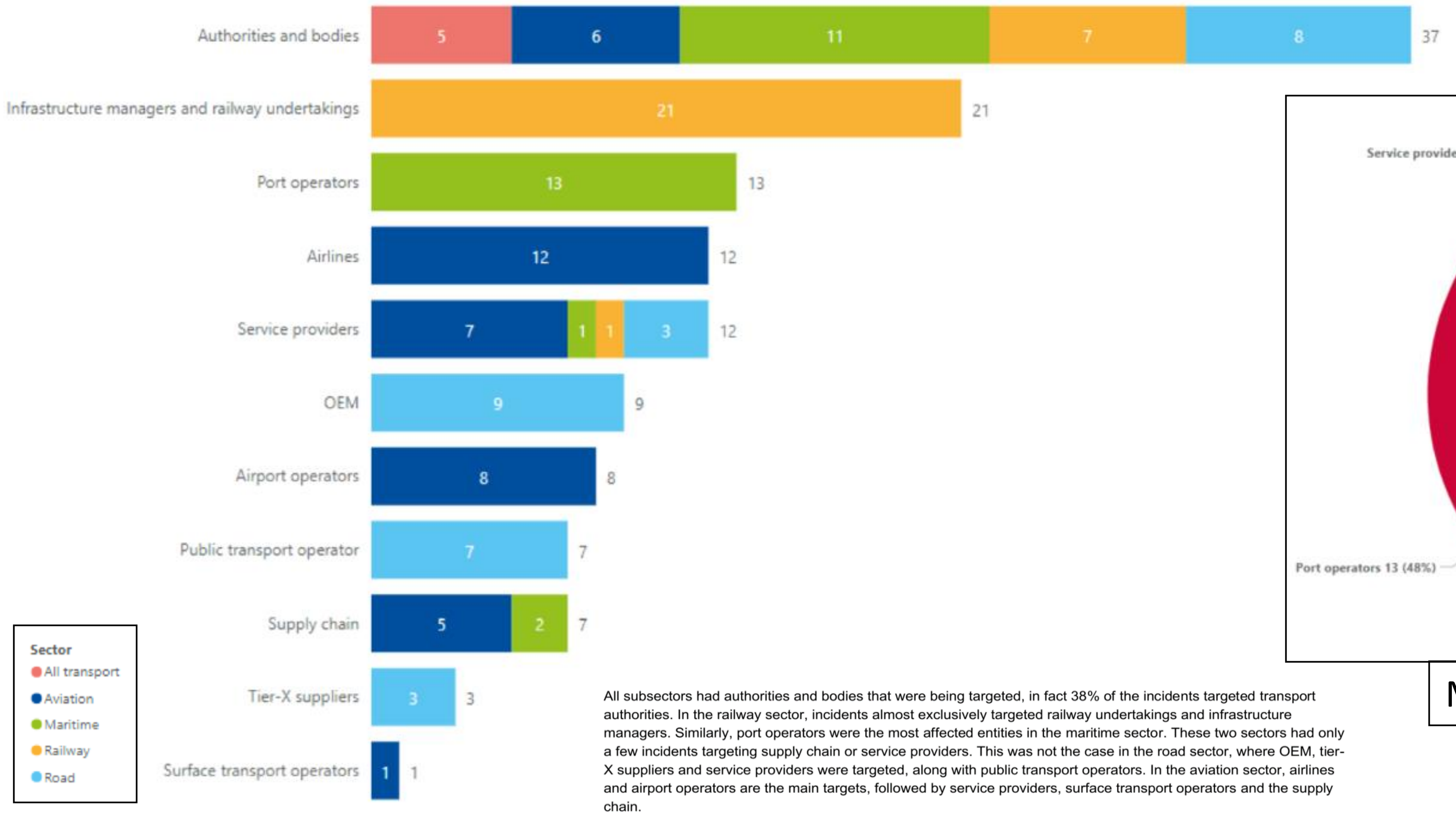
**ENISA Threat Landscape: Transport Sector* (Jan 2021-Oct 2022); Published March 2023

HudsonCyber
Maritime Cyber Security

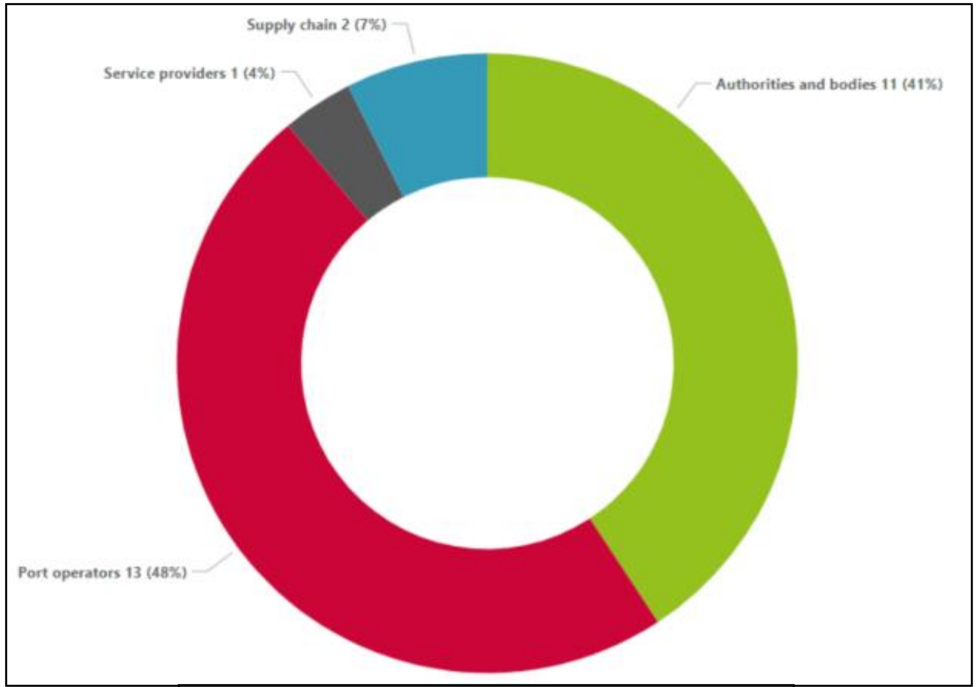
Maritime transportation sector target analysis*
(Port Authorities and Operators most at risk)

***ENISA Threat Landscape: Transport Sector* (Jan 2021-Oct 2022); Published March 2023

Transportation Sector Comparison



All subsectors had authorities and bodies that were being targeted, in fact 38% of the incidents targeted transport authorities. In the railway sector, incidents almost exclusively targeted railway undertakings and infrastructure managers. Similarly, port operators were the most affected entities in the maritime sector. These two sectors had only a few incidents targeting supply chain or service providers. This was not the case in the road sector, where OEM, tier-X suppliers and service providers were targeted, along with public transport operators. In the aviation sector, airlines and airport operators are the main targets, followed by service providers, surface transport operators and the supply chain.

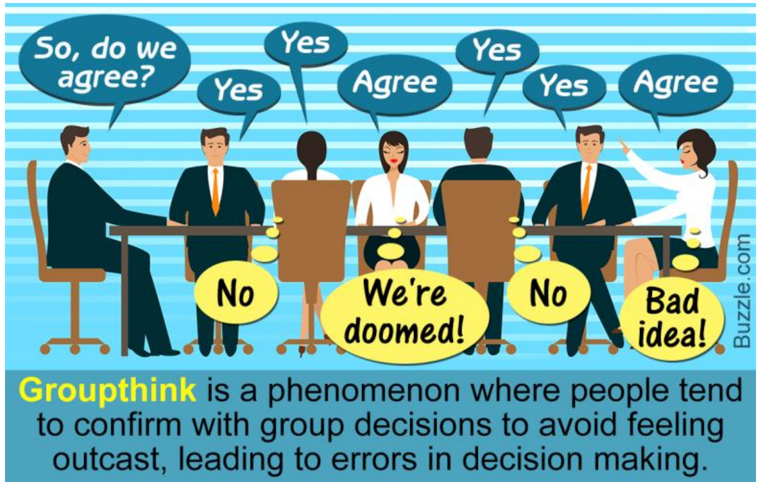


Maritime Target Distribution

Internal challenges: ignorance, indecision and *Groupthink*

Rationale often presented for inaction:

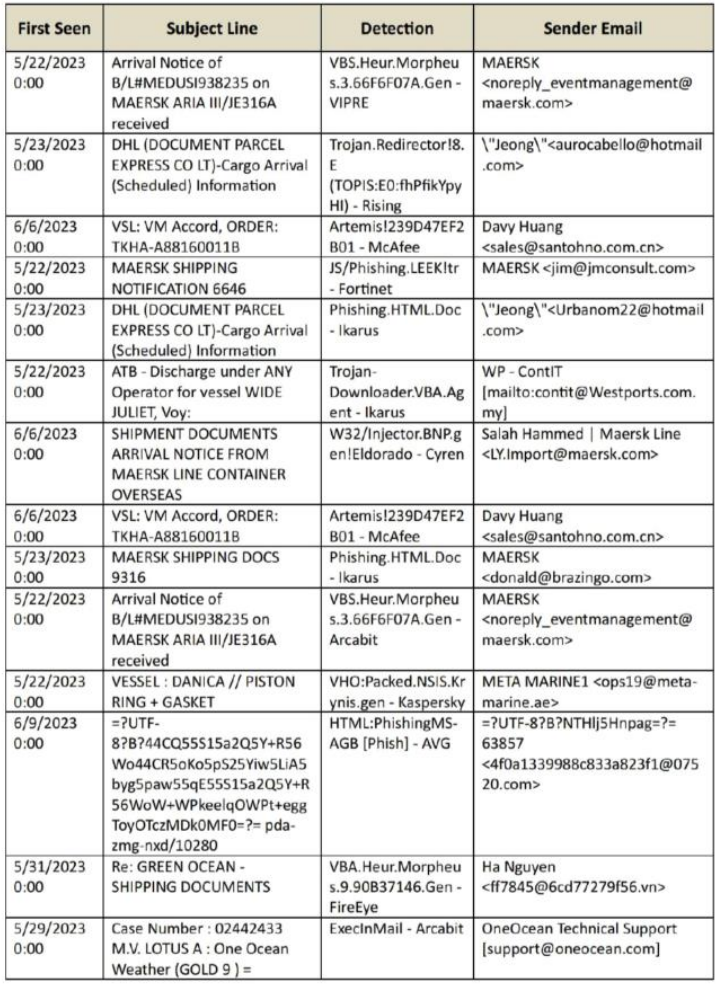
- ***Cybersecurity is too expensive*** **–** There is no budget. Misperception of only technical solutions
- ***The competitive imperative*** – Trade offs are frequently made between security and operations (efficiency!)
- ***Cyber risk is pervasive*** – It is often perceived of as something that is overwhelming
- ***Cyber risk is difficult to quantify*** – No common tools exist to help business leaders understand exposure.
- ***Difficult to change behavior*** – Nothing's happened, so why change?



Groupthink is a phenomenon where people tend to confirm with group decisions to avoid feeling outcast, leading to errors in decision making.

Sample data, common themes, vessel impersonations, etc.

TLP: GREEN



First Seen	Subject Line	Detection	Sender Email
5/22/2023 0:00	Arrival Notice of B/L#MEDUSI938235 on MAERSK ARIA III/JE316A received	VBS.Heur.Morpheus.3.66F6F07A.Gen - VIPRE	MAERSK <noreply_eventmanagement@maersk.com>
5/23/2023 0:00	DHL (DOCUMENT PARCEL EXPRESS CO LT)-Cargo Arrival (Scheduled) Information	Trojan.Redirector!8.E (TOPIS:E0:fhPfikYpyHI) - Rising	\"Jeong\"<aurocabello@hotmail.com>
6/6/2023 0:00	VSL: VM Accord, ORDER: TKHA-A88160011B	Artemis!239D47EF2B01 - McAfee	Davy Huang <sales@santohno.com.cn>
5/22/2023 0:00	MAERSK SHIPPING NOTIFICATION 6646	JS/Phishing.LEEK!tr - Fortinet	MAERSK <jim@jmconsult.com>
5/23/2023 0:00	DHL (DOCUMENT PARCEL EXPRESS CO LT)-Cargo Arrival (Scheduled) Information	Phishing.HTML.Doc - Ikarus	\"Jeong\"<Urbanom22@hotmail.com>
5/22/2023 0:00	ATB - Discharge under ANY Operator for vessel WIDE JULIET, Voy:	Trojan-Downloader.VBA.Agent - Ikarus	WP - ContIT [mailto:contit@Westports.com.my]
6/6/2023 0:00	SHIPMENT DOCUMENTS ARRIVAL NOTICE FROM MAERSK LINE CONTAINER OVERSEAS	W32/Injector.BNP.gen!Eldorado - Cyren	Salah Hammed | Maersk Line <LY.Import@maersk.com>
6/6/2023 0:00	VSL: VM Accord, ORDER: TKHA-A88160011B	Artemis!239D47EF2B01 - McAfee	Davy Huang <sales@santohno.com.cn>
5/23/2023 0:00	MAERSK SHIPPING DOCS 9316	Phishing.HTML.Doc - Ikarus	MAERSK <donald@brazingo.com>
5/22/2023 0:00	Arrival Notice of B/L#MEDUSI938235 on MAERSK ARIA III/JE316A received	VBS.Heur.Morpheus.3.66F6F07A.Gen - Arcabit	MAERSK <noreply_eventmanagement@maersk.com>
5/22/2023 0:00	VESSEL : DANICA // PISTON RING + GASKET	VHO:Packed.NSIS.Krynis.gen - Kaspersky	META MARINE1 <ops19@meta-marine.ae>
6/9/2023 0:00	=?UTF-8?B?44CQ55S15a2Q5Y+R56Wo44CR5oKo5pS25Yiw5LiA5byg5paw55qE55S15a2Q5Y+R56WoW+WPkeelqOWPt+eggToyOTczMDk0MF0=?= pda-zmg-nxd/10280	HTML:PhishingMS-AGB [Phish] - AVG	=?UTF-8?B?NTHlj5Hnpag=?= 63857 <4f0a1339988c833a823f1@07520.com>
5/31/2023 0:00	Re: GREEN OCEAN - SHIPPING DOCUMENTS	VBA.Heur.Morpheus.9.90B37146.Gen - FireEye	Ha Nguyen <ff7845@6cd77279f56.vn>
5/29/2023 0:00	Case Number : 02442433 M.V. LOTUS A : One Ocean Weather (GOLD 9) =	ExecInMail - Arcabit	OneOcean Technical Support [support@oneocean.com]

Table 1.

Table 1. List of dates, subject lines, malware detections, and sender data as identified in malicious email collection since 22 May.

The 5 most common subject lines seen in our recent query are:

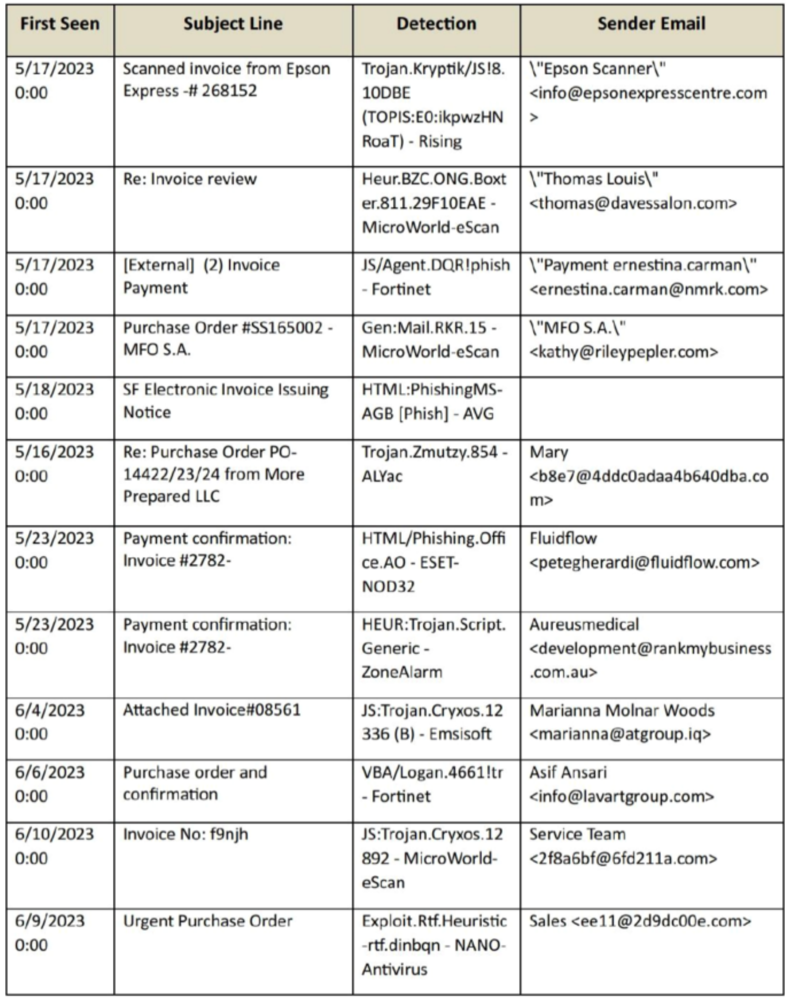
- Cargo Arrival Notice 2/6/2023
- Bill of Lading for 1x40ft Shipping Documents Outstanding Container Release
- CMA CGM Blue Whale – 1QY12N1NL PEB COPY MISSING
- [***SPAM*** Score/Req: 08.0/5.0] FW: M/V MSC QINGDAO – LASHING ITEMS
- Arrival Notice of B/L#MEDUSI938235 on MAERSK ARIA III / JE316A received

The 5 most prevalent malware detections associated with these emails are:

- Hoax.HTML.Phish.aar (ZoneAlarm)
- Other: SNH-gen [Phish] (Avast)
- Phishing.HTML.Doc (Ikarus)
- HTML/FakeLogin.Aiphish (Fortinet)
- Artemis!239D47EF2B01 (McAfee)

Sample data, common themes, shipping supply chains

TLP: GREEN



First Seen	Subject Line	Detection	Sender Email
5/17/2023 0:00	Scanned invoice from Epson Express -# 268152	Trojan.Kryptik/JS!8.10DBE (TOPIS:E0:ikpwzHNRoaT) - Rising	\"Epson Scanner\" <info@epsonexpresscentre.com>
5/17/2023 0:00	Re: Invoice review	Heur.BZC.ONG.Boxter.811.29F10EAE - MicroWorld-eScan	\"Thomas Louis\" <thomas@davessalon.com>
5/17/2023 0:00	[External] (2) Invoice Payment	JS/Agent.DQR!phish - Fortinet	\"Payment ernestina.carman\" <ernestina.carman@nmrk.com>
5/17/2023 0:00	Purchase Order #SS165002 - MFO S.A.	Gen:Mail.RKR.15 - MicroWorld-eScan	\"MFO S.A.\" <kathy@rileypepler.com>
5/18/2023 0:00	SF Electronic Invoice Issuing Notice	HTML:PhishingMS-AGB [Phish] - AVG	
5/16/2023 0:00	Re: Purchase Order PO-14422/23/24 from More Prepared LLC	Trojan.Zmutzy.854 - ALYac	Mary <b8e7@4ddc0adaa4b640dba.com>
5/23/2023 0:00	Payment confirmation: Invoice #2782-	HTML/Phishing.Office.AO - ESET-NOD32	Fluidflow <petegherardi@fluidflow.com>
5/23/2023 0:00	Payment confirmation: Invoice #2782-	HEUR:Trojan.Script.Generic - ZoneAlarm	Aureusmedical <development@rankmybusiness.com.au>
6/4/2023 0:00	Attached Invoice#08561	JS:Trojan.Cryxos.12336 (B) - Emsisoft	Marianna Molnar Woods <marianna@atgroup.iq>
6/6/2023 0:00	Purchase order and confirmation	VBA/Logan.4661!tr - Fortinet	Asif Ansari <info@lavartgroup.com>
6/10/2023 0:00	Invoice No: f9njh	JS:Trojan.Cryxos.12892 - MicroWorld-eScan	Service Team <2f8a6bf@6fd211a.com>
6/9/2023 0:00	Urgent Purchase Order	Exploit.Rtf.Heuristic-rtf.dinbqn - NANO-Antivirus	Sales <ee11@2d9dc00e.com>

Table 2.

Table 2. List of dates, subject lines, malware detections, and sender data as identified in malicious email collection since 17 May.

The 5 most common subject lines seen for supply chain focus are:

- RE: Proforma Invoice
- Payment confirmation: Invoice #2782-
- Arrival Notice / Shipping Documents / Original BL, Invoice & Packing List
- Urgent Purchase Order 29 May 2023
- DHL: AWB Shipment Notification

The 5 most prevalent malware detections associated with these emails are:

- Phishing.HTML.Doc (Ikarus)
- HEUR: Trojan.Script.Generic (ZoneAlarm)
- HTML/Phishing.Office.AO (ESET-NOD 32)
- Trojan[Phishing]/HTML.Agent (Antiy-AVL)
- Script.Trojan.44094 (CAT-QuickHeal)

Impact case study: *NotPetya*

Still Relevant!

Maersk:

- Handles 18% of global container trade with 700+ vessels and 76 ports via APM Terminals
- Books approximately 3,300 TEUs ($2.7 million) *per hour*

The Attack:

- Spread from a single computer in Odessa
- Affected more than 17 APT Terminal sites globally
- Leveraged compromised NSA hacker tools
- Encrypted computer master boot records (destructive)
- “They went back to basics and did everything on paper”
- Affected *hundreds of thousands* of shippers

What Happened:

- “Blank Check” to Deloitte to rebuild the global network
- 4,000 new servers, 45,000+ new PCs, 2,500+ applications
- Reverted to paper, Gmail, WhatsApp and excel used.
- Total *uninsured* losses: USD 300+ million

Impact:

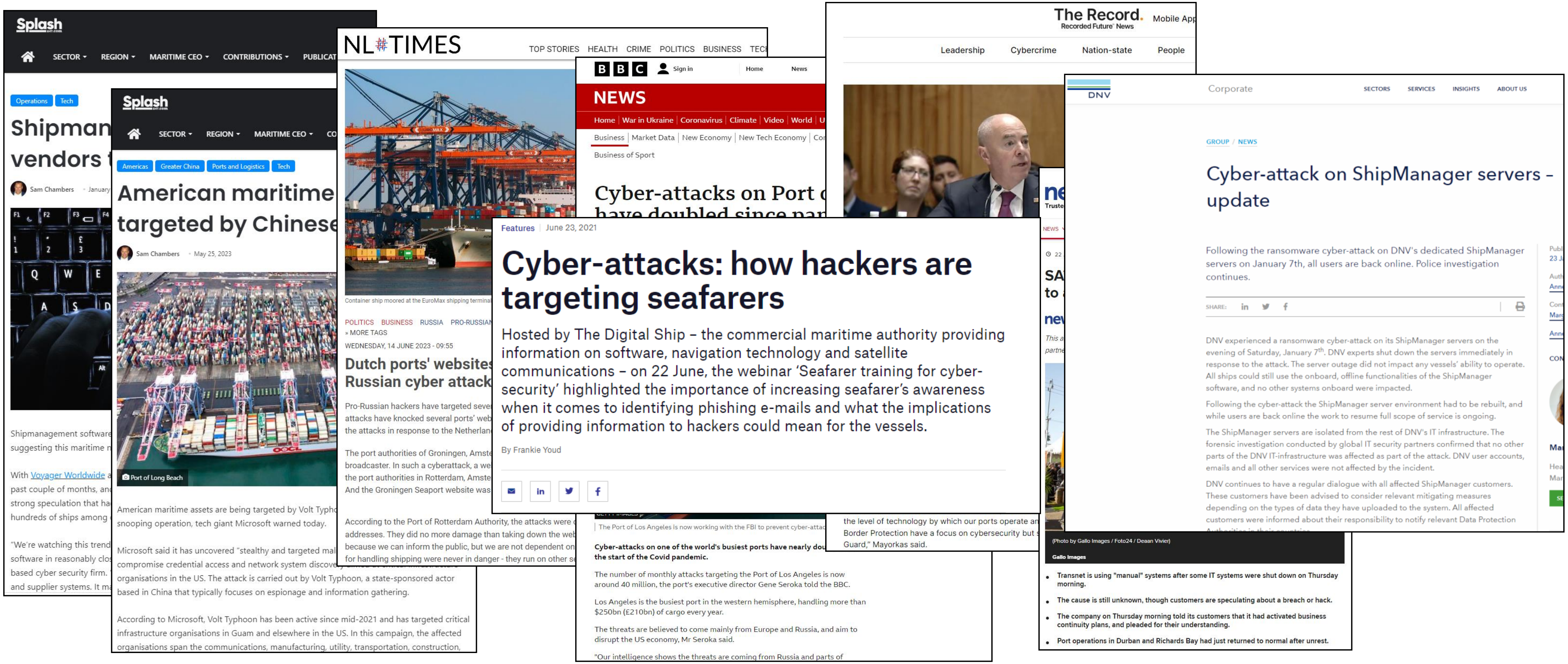
- Global operational delays
- Financial losses
- Liability exposure
- Reputational hit

Impact case study: IRISL (2011)

Still Relevant!

- Servers were compromised
- Logistics systems crashed
- Entire fleet of 172 vessels and shore-based systems were compromised
- False information input into systems:
  - Compromised manifests
  - Falsified Rates
  - Containers ‘cloaked’
  - Delivery dates altered
  - Client / Vendor Data corrupted
- Major Business Interruption!

The attacks never end…



Shipman
vendors

Sam Chambers · January

Shipmanagement software
suggesting this maritime

With Voyager Worldwide
past couple of months, an
strong speculation that ha
hundreds of ships among

"We're watching this trend
software in reasonably clo
based cyber security firm.
and supplier systems. It m

American maritime
targeted by Chinese

Sam Chambers · May 25, 2023

Port of Long Beach

American maritime assets are being targeted by Volt Typho
snooping operation, tech giant Microsoft warned today.

Microsoft said it has uncovered "stealthy and targeted mal
compromise credential access and network system discove
organisations in the US. The attack is carried out by Volt Typhoon, a state-sponsored actor based in China that typically focuses on espionage and information gathering.

According to Microsoft, Volt Typhoon has been active since mid-2021 and has targeted critical infrastructure organisations in Guam and elsewhere in the US. In this campaign, the affected organisations span the communications, manufacturing, utility, transportation, construction,

Container ship moored at the EuroMax shipping terminal

POLITICS BUSINESS RUSSIA PRO-RUSSIAN
» MORE TAGS

WEDNESDAY, 14 JUNE 2023 - 09:55

Dutch ports' websites
Russian cyber attack

Pro-Russian hackers have targeted seve
attacks have knocked several ports' web
the attacks in response to the Netherlan

The port authorities of Groningen, Amste
broadcaster. In such a cyberattack, a we
the port authorities in Rotterdam, Amste
And the Groningen Seaport website was

According to the Port of Rotterdam Authority, the attacks were
addresses. They did no more damage than taking down the web
because we can inform the public, but we are not dependent on
for handling shipping were never in danger - they run on other se

BBC
Sign in
Home
News
NEWS
Home | War in Ukraine | Coronavirus | Climate | Video | World | U
Business | Market Data | New Economy | New Tech Economy | Co
Business of Sport

Cyber-attacks on Port o
have doubled since pa

The Port of Los Angeles is now working with the FBI to prevent cyber-attac

**Cyber-attacks on one of the world's busiest ports have nearly dou
the start of the Covid pandemic.**

The number of monthly attacks targeting the Port of Los Angeles is now around 40 million, the port's executive director Gene Seroka told the BBC.

Los Angeles is the busiest port in the western hemisphere, handling more than $250bn (£210bn) of cargo every year.

The threats are believed to come mainly from Europe and Russia, and aim to disrupt the US economy, Mr Seroka said.

"Our intelligence shows the threats are coming from Russia and parts of

the level of technology by which our ports operate an
Border Protection have a focus on cybersecurity but s
Guard," Mayorkas said.

Features | June 23, 2021

Cyber-attacks: how hackers are targeting seafarers

Hosted by The Digital Ship – the commercial maritime authority providing information on software, navigation technology and satellite communications – on 22 June, the webinar 'Seafarer training for cyber-security' highlighted the importance of increasing seafarer's awareness when it comes to identifying phishing e-mails and what the implications of providing information to hackers could mean for the vessels.

By Frankie Youd

SA
to

ne

This a
partne

(Photo by Gallo Images / Foto24 / Deaan Vivier)

Gallo Images

- Transnet is using "manual" systems after some IT systems were shut down on Thursday morning.
- The cause is still unknown, though customers are speculating about a breach or hack.
- The company on Thursday morning told its customers that it had activated business continuity plans, and pleaded for their understanding.
- Port operations in Durban and Richards Bay had just returned to normal after unrest.

Cyber-attack on ShipManager servers – update

Following the ransomware cyber-attack on DNV's dedicated ShipManager servers on January 7th, all users are back online. Police investigation continues.

DNV experienced a ransomware cyber-attack on its ShipManager servers on the evening of Saturday, January 7th. DNV experts shut down the servers immediately in response to the attack. The server outage did not impact any vessels' ability to operate. All ships could still use the onboard, offline functionalities of the ShipManager software, and no other systems onboard were impacted.

Following the cyber-attack the ShipManager server environment had to be rebuilt, and while users are back online the work to resume full scope of service is ongoing.

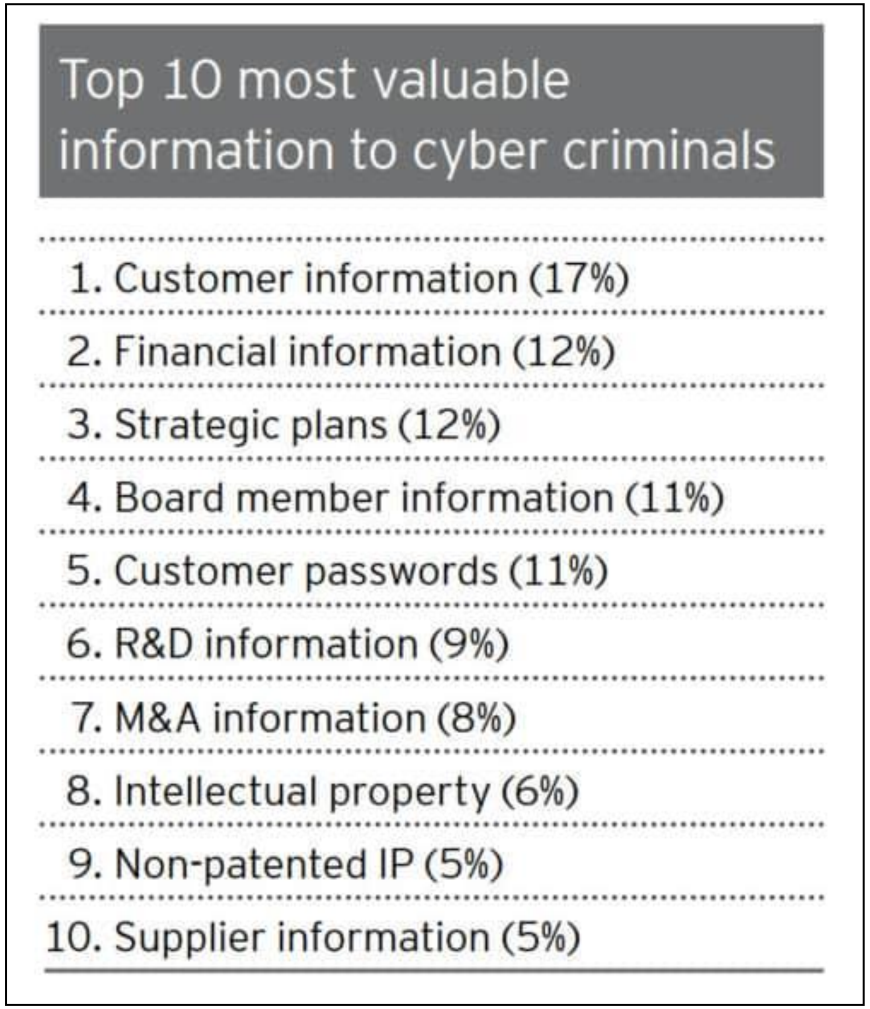
The ShipManager servers are isolated from the rest of DNV's IT infrastructure. The forensic investigation conducted by global IT security partners confirmed that no other parts of the DNV IT-infrastructure was affected as part of the attack. DNV user accounts, emails and all other services were not affected by the incident.

DNV continues to have a regular dialogue with all affected ShipManager customers. These customers have been advised to consider relevant mitigating measures depending on the types of data they have uploaded to the system. All affected customers were informed about their responsibility to notify relevant Data Protection

What's at risk?

Cyber Risk represents more than just data breaches…

- **Personal (employee) information:** credentials; financial data; health information; etc.
- **Intellectual property:** designs; plans; etc.
- **Confidential information:** client data; manifest data
- **Operational Information:** Data Integrity that affects office; operations; Internet of Things enabled platforms; Industrial Control Systems (ICS); security systems (e.g., CCTV, Access Control); etc.
- **Money:** Profit and Loss; Balance Sheet Health
- **Political:** "Hacktivism"
- **Business:** Competition, Competency and Reputation



Top 10 most valuable information to cyber criminals

1. Customer information (17%)
2. Financial information (12%)
3. Strategic plans (12%)
4. Board member information (11%)
5. Customer passwords (11%)
6. R&D information (9%)
7. M&A information (8%)
8. Intellectual property (6%)
9. Non-patented IP (5%)
10. Supplier information (5%)

High-Probably Compromise: ERP Systems
(Note: USCG Compliance does not focus on business-based ERP Systems)

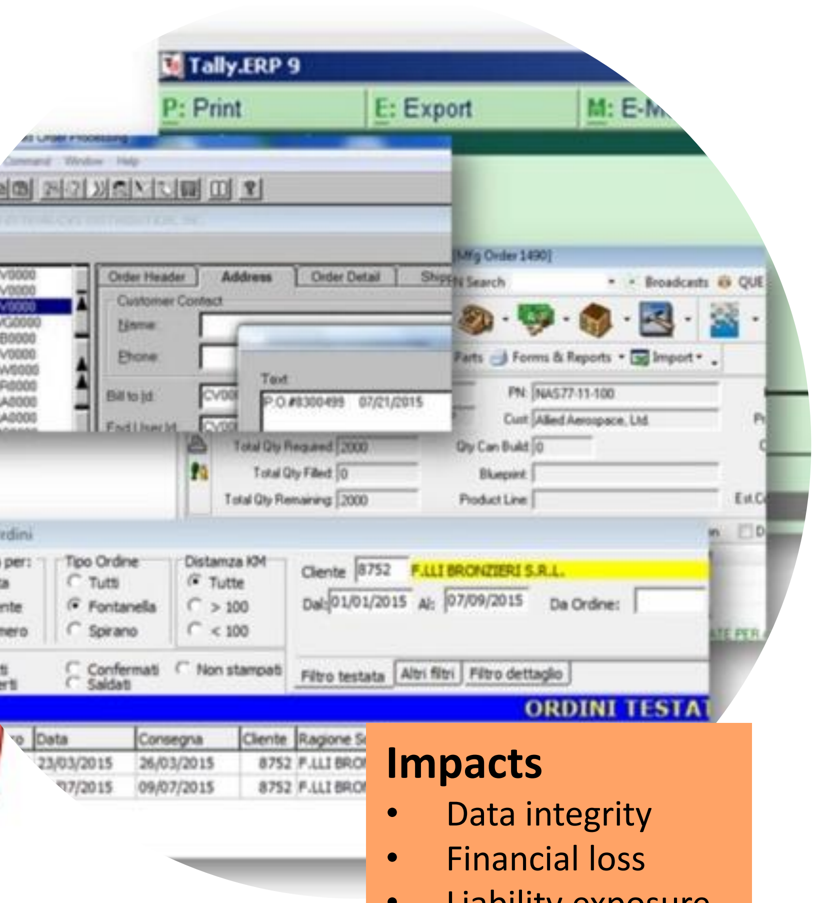
Enterprise Resource Planning (ERP) Systems offer virtual windows into an organization’s activities as it relates to the movement of people, resources, goods, and money.

ERP Systems *integrate core business processes* and leverage shared databases to support multiple functions used by different business units.

Systems affected include:

- Financial (re: Fraud, Payment info)
- Cargo Handling & Management
- Taxes (e.g., VAT)
- Customs
- Banking
- Shipping

FINANCE ACCOUNTING
%
HUMAN RESOURCES
ACCESS CONTROL
ERP
Enterprise Resource Planning
PURCHASING
$
CRM
DATA SERVICES
PROJECT MANAGEMENT



Cliente 8752 F.LLI BRONZIERI S.R.L.

Dal: 01/01/2015 Al: 07/09/2015 Da Ordine:

P.O.#8300499 07/21/2015

PN NAS77-11-100

Cust Allied Aerospace, Ltd

Total Qty Required 2000

Total Qty Filled 0

Total Qty Remaining 2000

Data	Consegna	Cliente	Ragione S
23/03/2015	26/03/2015	8752	F.LLI BRO
07/2015	09/07/2015	8752	F.LLI BRO

Impacts

- Data integrity
- Financial loss
- Liability exposure
- Operational delays

Notable estimates: financial impacts

Annual cost estimates of cyber crime and economic espionage to the world economy ranges from USD 450 billion to 6 trillion – or almost 5% of global income in 2021.

Or…

- *$ 500 billion per month*
- *$ 115.4 million per week*
- *$ 190,000 per second*

This cost estimate does not include intangible damage to brand and reputation.

Cybercrime may cost the world economy approx. $ 10 trillion annually by 2025.

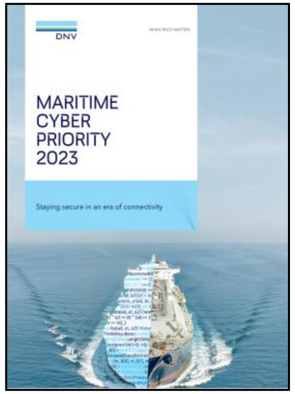
Source: Cybersecurity Ventures

Notable maritime points of reference

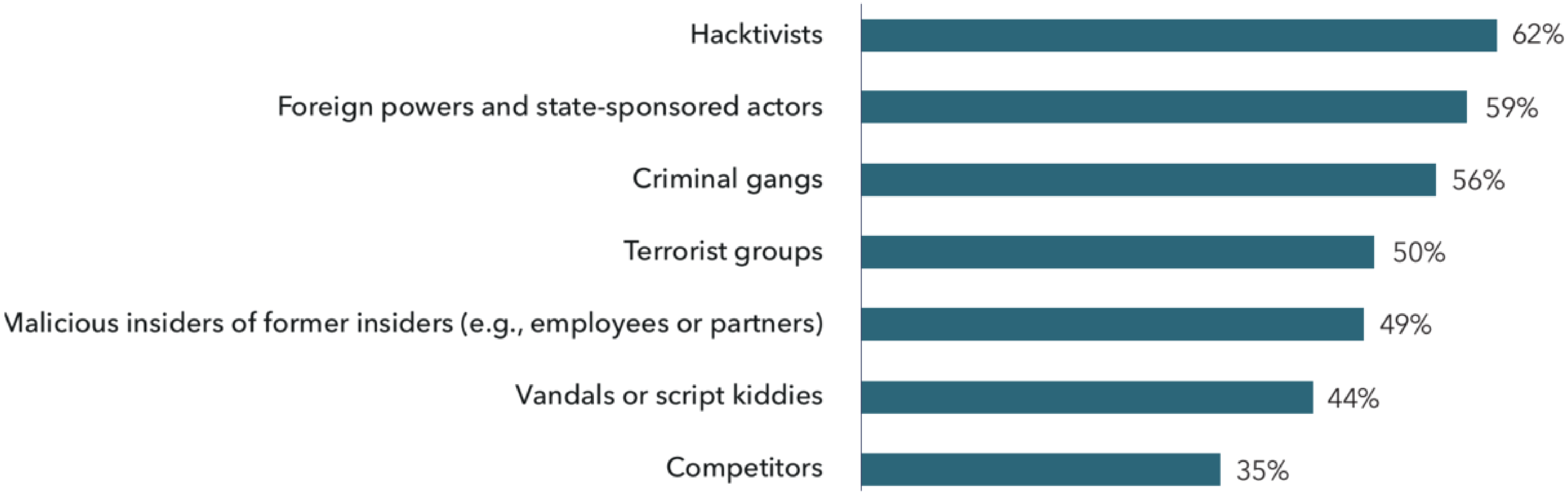
- Inmarsat surveyed 200+ shipping companies in 2021-2022 and **more than 50% reported cyber breaches since 2019.**
- Thetius reported that the average Ransomware payout was more than USD $3.1 million. When not paid, the average **recovery costs averaged $1.8 million**
- The **majority of crews are not given cyber awareness** training.
- **80%+ of cyber breaches are attributed to human error.** For example, more than 50% of vessel system cyber disruptions were caused by USB misuse (e.g., infected USB sticks were inserted in USB ports)
- Across more than 12,000 FleetXpress customer vessels, some ships are **doubling their data usage every six months.**
- **The #1 disconnect identified was ownership disconnectedness.**

HudsonCyber
Maritime Cyber Security

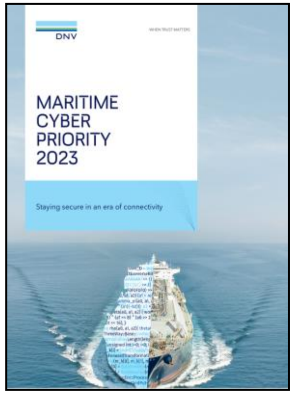
A discussion about the power of perception…


DNV
MARITIME CYBER PRIORITY 2023
Staying secure in an era of connectivity

Hacktivists and foreign powers, which may share the same objectives, are the top threat today



The power of perception (cont.)

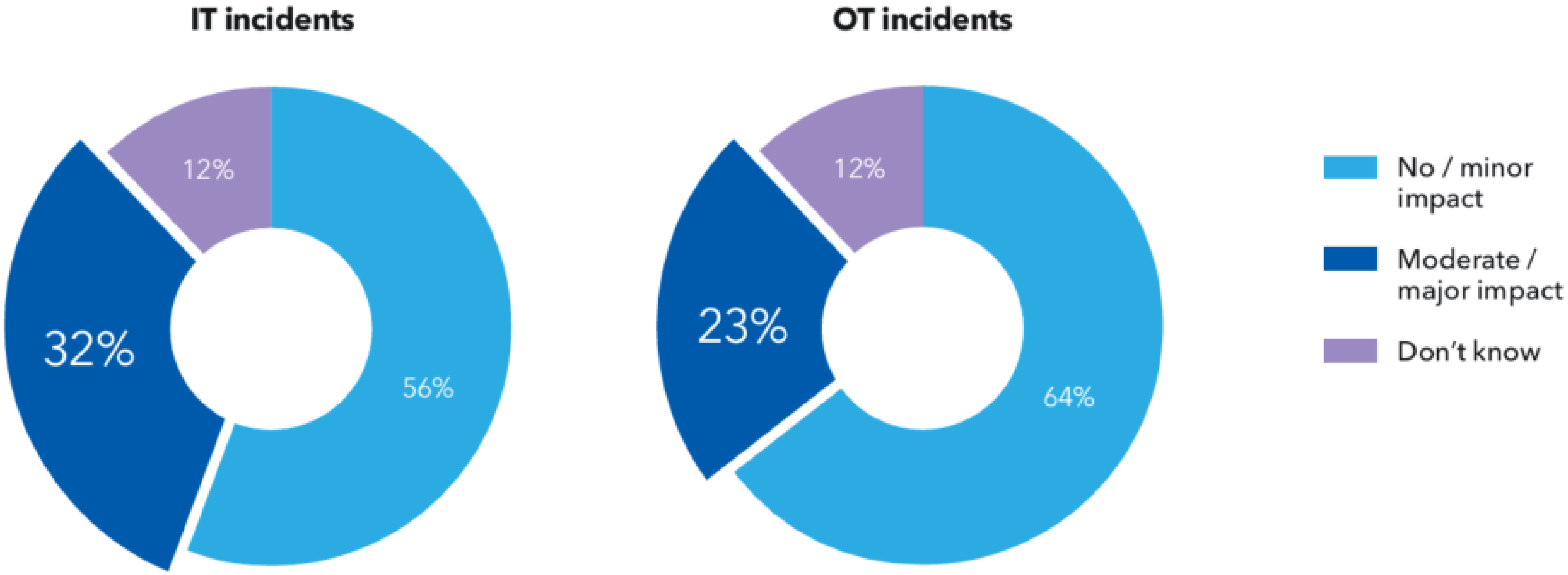


DNV

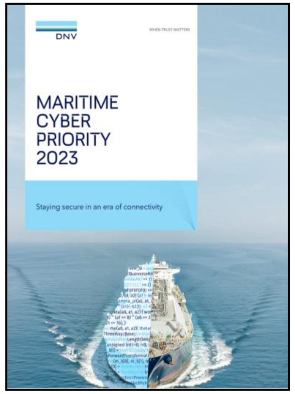
MARITIME
CYBER
PRIORITY
2023

Staying secure in an era of connectivity

Sizable share of maritime professionals say cyber incidents have had a negative impact on their organization



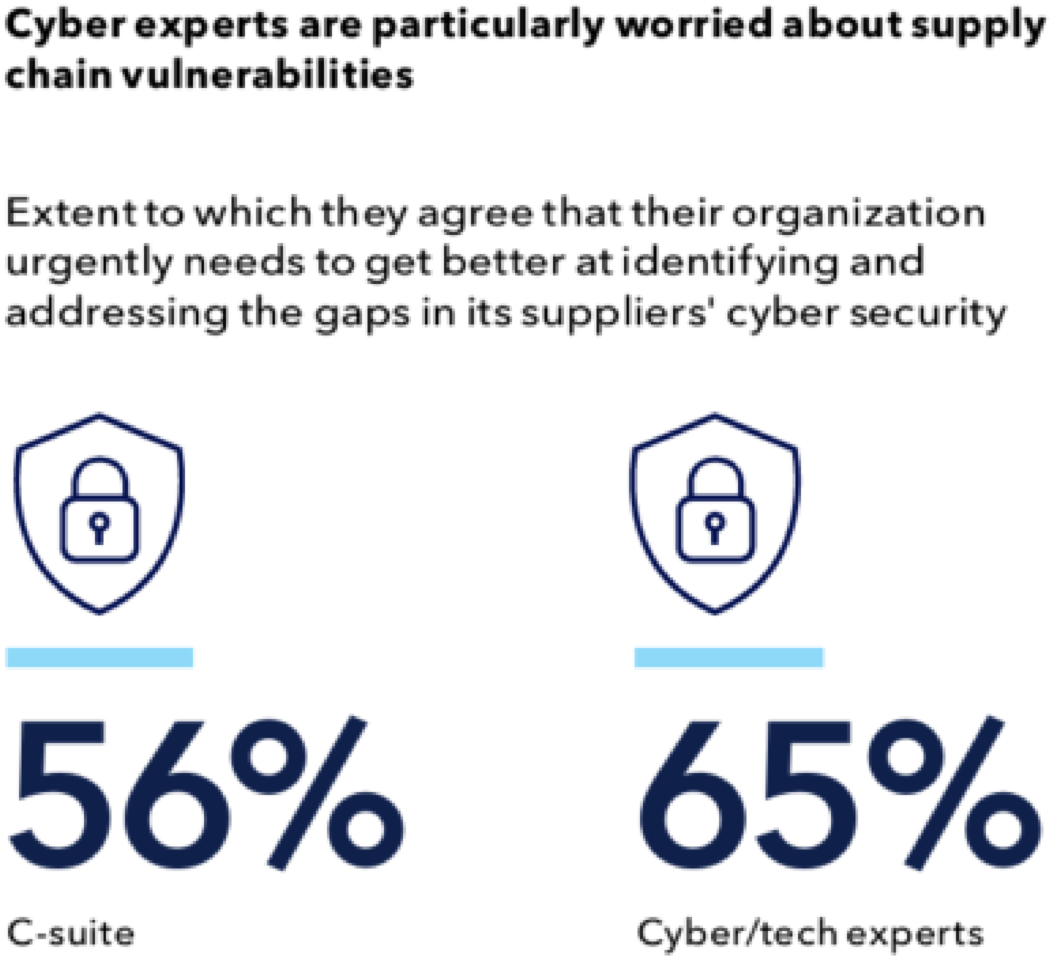
The power of perception (cont.)



DNV

MARITIME CYBER PRIORITY 2023

Staying secure in an era of connectivity



Cyber experts are particularly worried about supply chain vulnerabilities

Extent to which they agree that their organization urgently needs to get better at identifying and addressing the gaps in its suppliers' cyber security

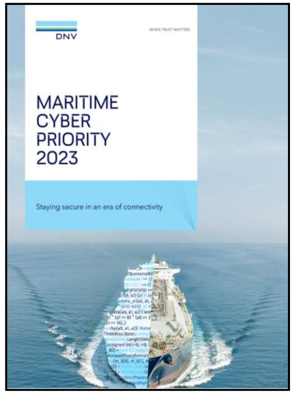
56%

C-suite

65%

Cyber/tech experts

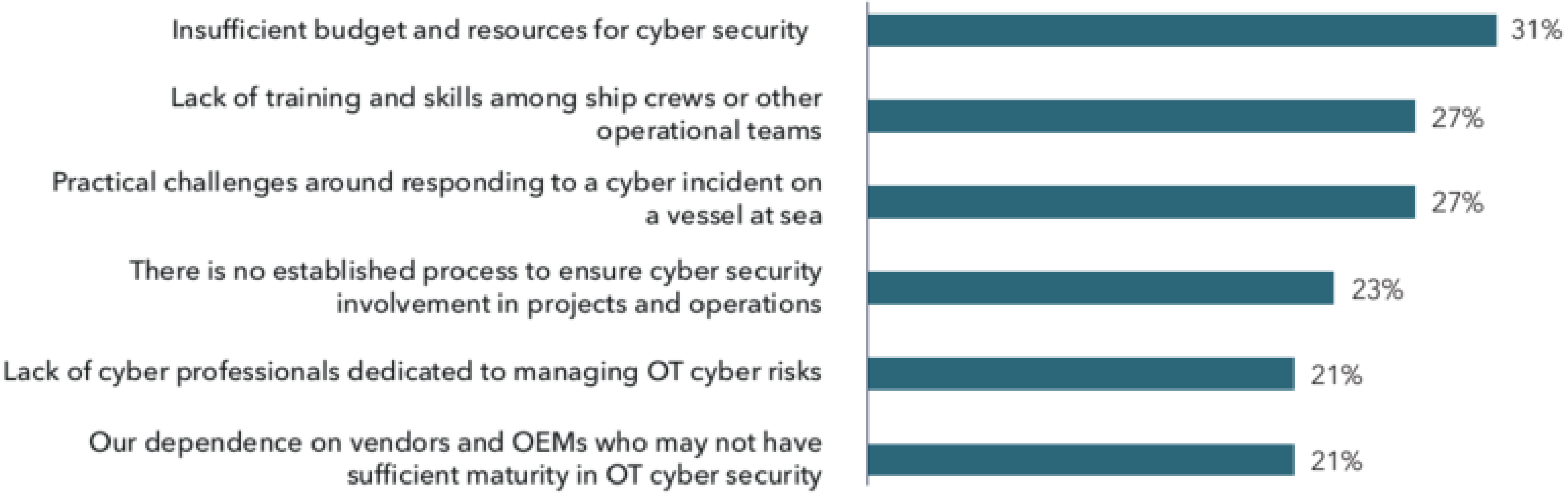
The power of perception (cont.)


DNV

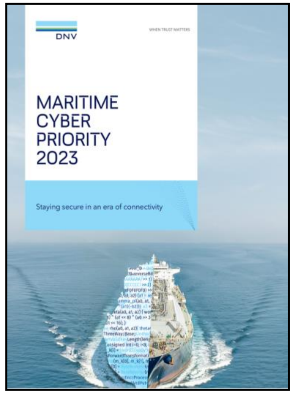
MARITIME CYBER PRIORITY 2023

Staying secure in an era of connectivity

Lack of funding is the biggest cyber-related challenge



The compliance trap

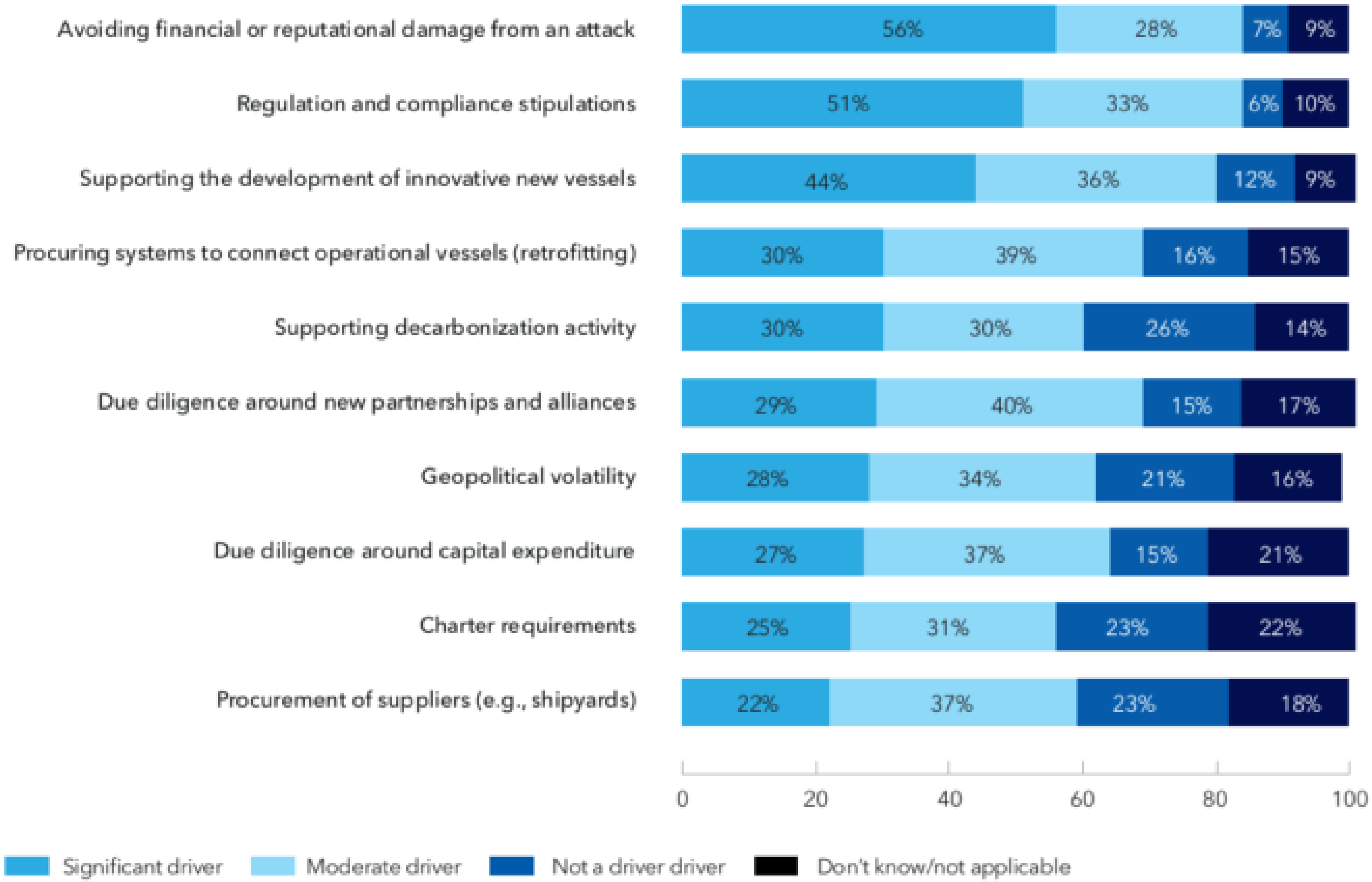


DNV

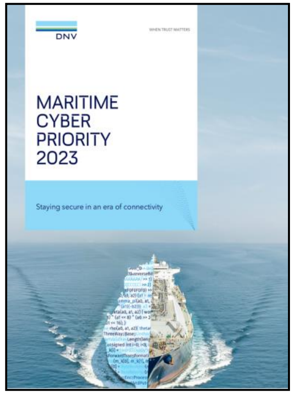
MARITIME CYBER PRIORITY 2023

Staying secure in an era of connectivity

Regulation and reputation are leading drivers of cyber security investment.



The compliance trap



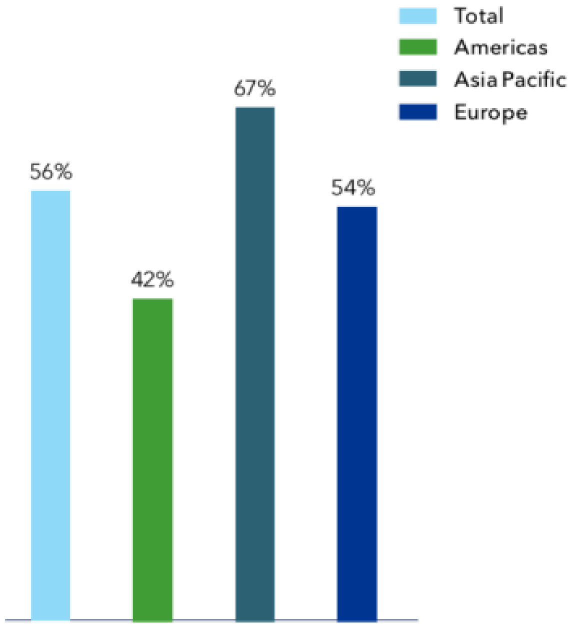
DNV

MARITIME
CYBER
PRIORITY
2023

Staying secure in an era of connectivity

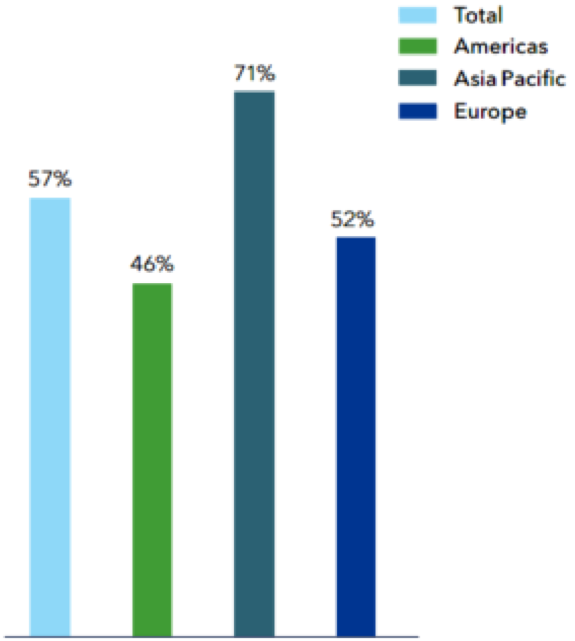
Only half maritime professionals believe compliance will keep the industry secure from cyber threats

Extent to which respondents agree that compliance with cyber security regulation will keep maritime organizations sufficiently secure from cyber threats

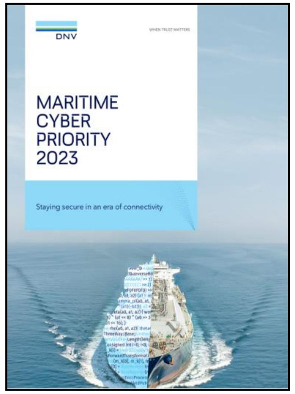


Professionals in Asia Pacific are more confident regulation is driving the right behaviours

Extent to which respondents agree that regulation is effective at encouraging the right cyber security behaviours in maritime organizations



The compliance trap

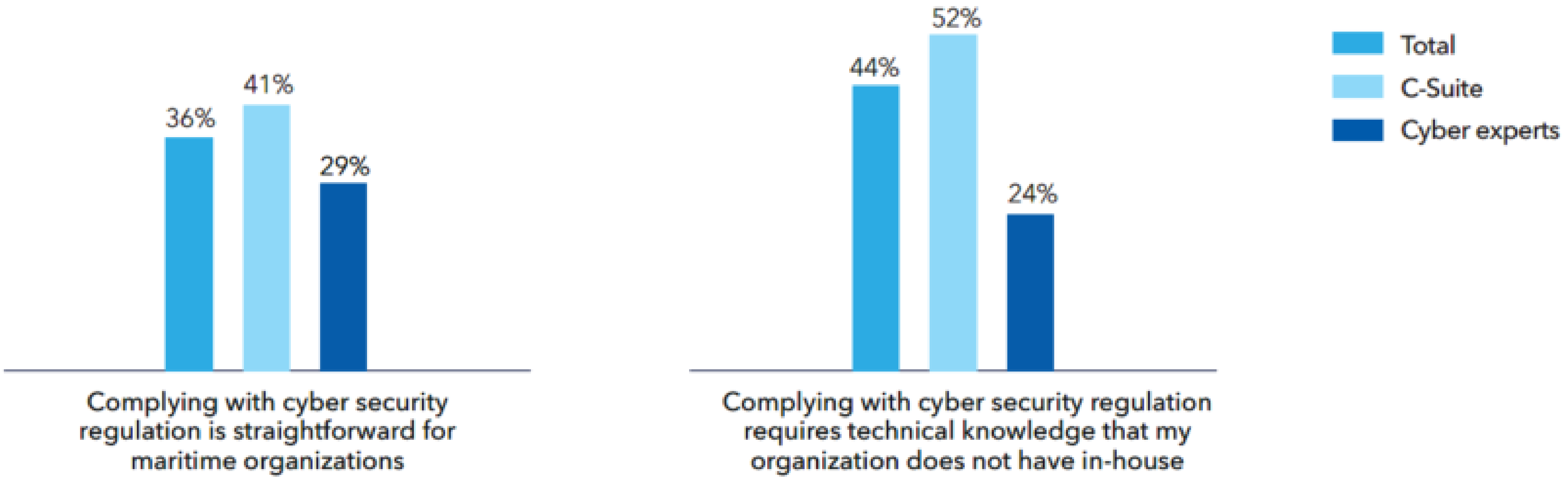


DNV

MARITIME
CYBER
PRIORITY
2023

Staying secure in an era of connectivity

Disconnect between senior management and cyber experts, on whether organizations are ready to comply with regulation



Everyone in the maritime industry is trying to understand cyber risk

Munich RE

DNV

Steamship Mutual

DNK

SHORELINE

NIST

Department for Transport

ISO

speedcast

The Marshall Islands Registry

CHAUCER CYBER

AON

Empowered Results®

Lloyd's Register

LIBERIAN REGISTRY

UNITED STATES COAST GUARD 1790

IMO

INTERNATIONAL MARITIME ORGANIZATION

IACS

International Association of Classification Societies

ClassNK

The Nautical Institute

MARSH

ABS

Autoridad Marítima de Panamá

AIG

enisa

THE EU CYBERSECURITY AGENCY

BUREAU VERITAS 1828

BUREAU VERITAS

THE BALTIC AND INTERNATIONAL MARITIME COUNCIL

BIMCO

The trend we're seeing now: the evolving pressures of money and "changing" regulations

- The global cyber insurance market in 2021: $ 7.1 bn
- By 2025 it's estimated to exceed $ 25 bn

LLOYD'S

beazley

$ € £

AIG

Allianz

AXIS

Munich RE

TOKIO MARINE
T M R

AXA

ZURICH

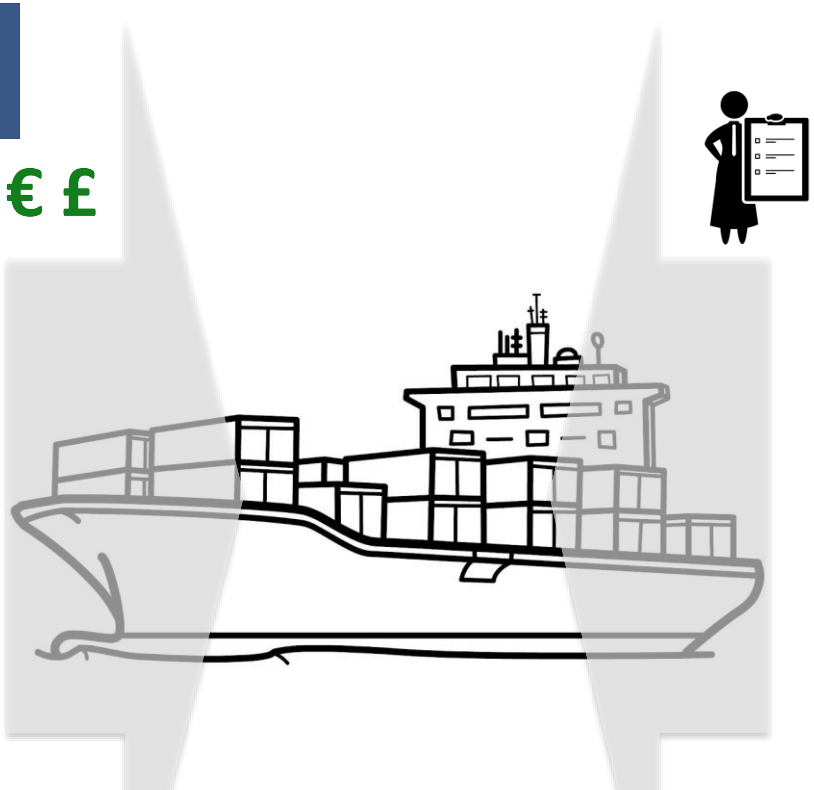
MARSH

TT

AON
Empower Results

CHAUCER
CYBER

SHORELINE



Common Theme:

Incident Response

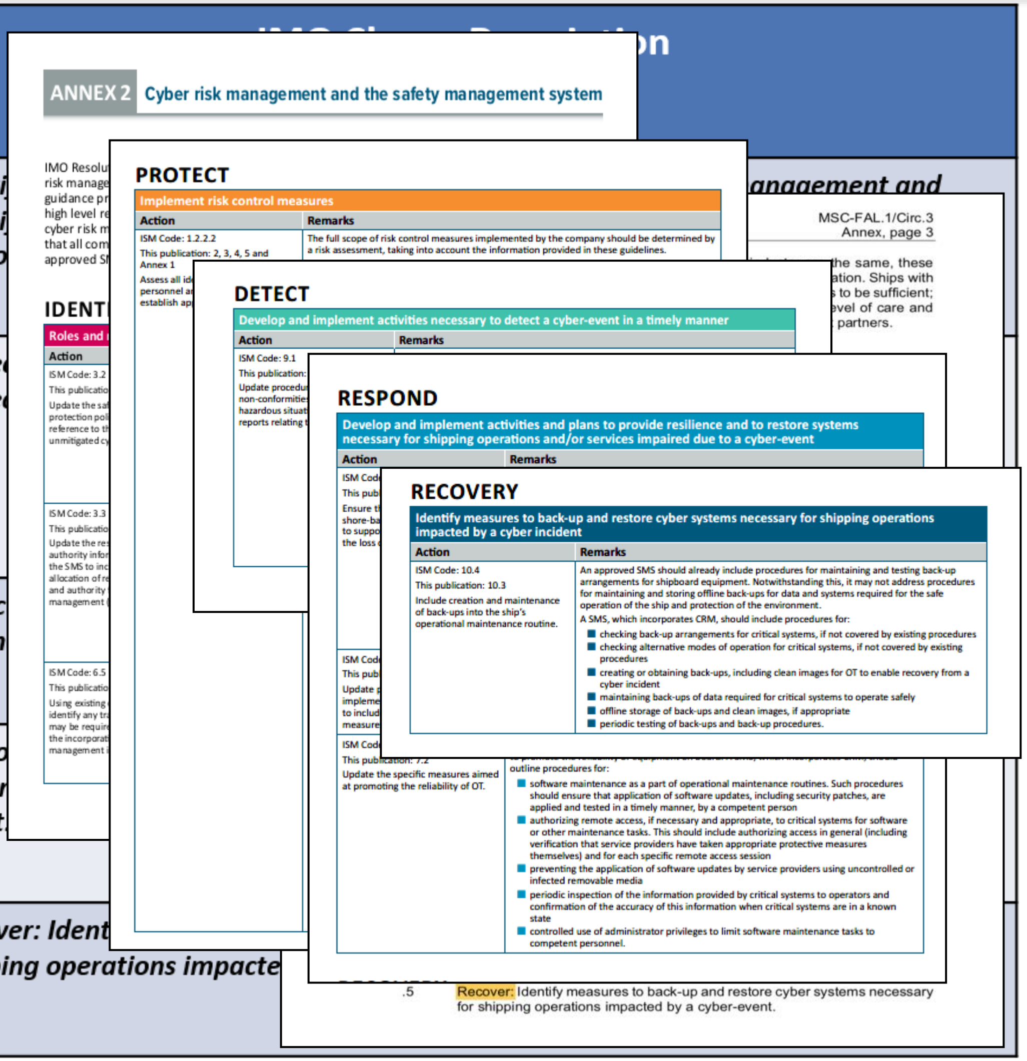
IMO INTERNATIONAL MARITIME ORGANIZATION

UNITED STATES COAST GUARD 1790

- The USCG implemented cyber regulations for all US ports in Oct 2021
- Currently working on updating cyber regulations
- A sign of things to come?

Understanding the referenced standards (IMO & BIMCO)

NIST Cybersecurity Framework Functional Category	NIST CSF Category	IMO Clause (Category)	IMO Clause Description
🟦 **Identify**	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	🟦 **Identify (3.5.1)**	*Identi… identi… ship o… …anagement and*
🟪 **Protect**	• Access Control • Awareness & Training • Data Security • Information Protection Processes & Procedures • Maintenance • Protective Technology	🟪 **Protect (3.5.2)**	*Prote… prote…*
🟨 **Detect**	• Anomalies & Events • Security Continuous Monitoring • Detection Processes	🟨 **Detect (3.5.3)**	*Detec… mann…*
🟥 **Respond**	• Response Planning • Communications • Analysis • Mitigation • Improvements	🟥 **Respond (3.5.4)**	*Resp… restor… event.*
🟩 **Recovery**	• Recovery Planning • Improvements • Communications	🟩 **Recover (3.5.5)**	*Recover: Ident… shipping operations impacte…*



ANNEX 2 Cyber risk management and the safety management system

IMO Resolu… risk manage… guidance pr… high level re… cyber risk m… that all com… approved SM…

IDENT…

Roles and …

Action
ISM Code: 3.2 This publicatio… Update the saf… protection pol… reference to th… unmitigated cy…
ISM Code: 3.3 This publicatio… Update the res… authority infor… the SMS to inc… allocation of re… and authority … management (…
ISM Code: 6.5 This publicatio… Using existing … identify any tra… may be require… the incorporat… management i…

MSC-FAL.1/Circ.3
Annex, page 3

…the same, these …ation. Ships with …s to be sufficient; …evel of care and … partners.

.5 Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

PROTECT

Implement risk control measures

Action	Remarks
ISM Code: 1.2.2.2 This publication: 2, 3, 4, 5 and Annex 1 Assess all ide… personnel ar… establish ap…	The full scope of risk control measures implemented by the company should be determined by a risk assessment, taking into account the information provided in these guidelines.

DETECT

Develop and implement activities necessary to detect a cyber-event in a timely manner

Action	Remarks
ISM Code: 9.1 This publication: … Update procedur… non-conformities… hazardous situat… reports relating t…	

RESPOND

Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations and/or services impaired due to a cyber-event

Action	Remarks
ISM Cod… This pub… Ensure t… shore-ba… to suppo… the loss …	
ISM Cod… This pub… Update p… impleme… to includ… measure…	
ISM Cod… This publication: 7.2 Update the specific measures aimed at promoting the reliability of OT.	outline procedures for: ■ software maintenance as a part of operational maintenance routines. Such procedures should ensure that application of software updates, including security patches, are applied and tested in a timely manner, by a competent person ■ authorizing remote access, if necessary and appropriate, to critical systems for software or other maintenance tasks. This should include authorizing access in general (including verification that service providers have taken appropriate protective measures themselves) and for each specific remote access session ■ preventing the application of software updates by service providers using uncontrolled or infected removable media ■ periodic inspection of the information provided by critical systems to operators and confirmation of the accuracy of this information when critical systems are in a known state ■ controlled use of administrator privileges to limit software maintenance tasks to competent personnel.

RECOVERY

Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident

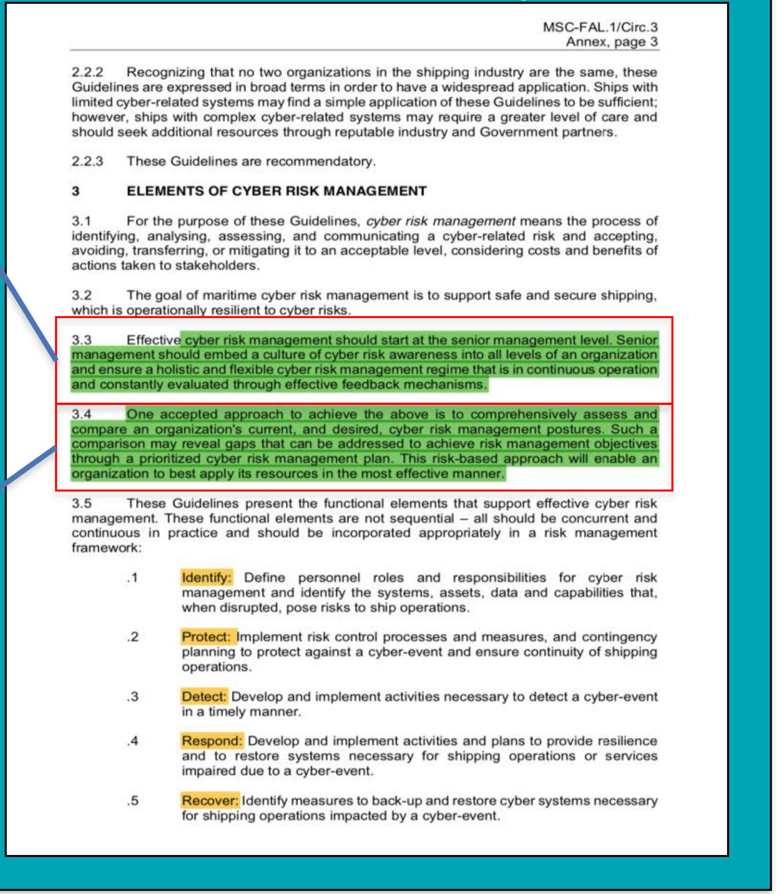
Action	Remarks
ISM Code: 10.4 This publication: 10.3 Include creation and maintenance of back-ups into the ship's operational maintenance routine.	An approved SMS should already include procedures for maintaining and testing back-up arrangements for shipboard equipment. Notwithstanding this, it may not address procedures for maintaining and storing offline back-ups for data and systems required for the safe operation of the ship and protection of the environment. A SMS, which incorporates CRM, should include procedures for: ■ checking back-up arrangements for critical systems, if not covered by existing procedures ■ checking alternative modes of operation for critical systems, if not covered by existing procedures ■ creating or obtaining back-ups, including clean images for OT to enable recovery from a cyber incident ■ maintaining back-ups of data required for critical systems to operate safely ■ offline storage of back-ups and clean images, if appropriate ■ periodic testing of back-ups and back-up procedures.

HudsonCyber
Maritime Cyber Security

Manage cyber risk through cybersecurity capability maturity aligns with the ISM requirements

Clause 3.3	***Effective cyber risk management should start at the senior management level.*** Senior management should embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.
Clause 3.4	One accepted approach to achieve the above is to ***comprehensively assess and compare an organization's current, and desired, cyber risk management postures.*** Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan. ***This risk-based approach will enable an organization to best apply its resources in the most effective manner.***

MSC-FAL.1 / Circ.3
5 July 2017
Guidelines on Maritime Cyber Risk



MSC-FAL.1/Circ.3
Annex, page 3

2.2.2 Recognizing that no two organizations in the shipping industry are the same, these Guidelines are expressed in broad terms in order to have a widespread application. Ships with limited cyber-related systems may find a simple application of these Guidelines to be sufficient; however, ships with complex cyber-related systems may require a greater level of care and should seek additional resources through reputable industry and Government partners.

2.2.3 These Guidelines are recommendatory.

3 ELEMENTS OF CYBER RISK MANAGEMENT

3.1 For the purpose of these Guidelines, *cyber risk management* means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

3.2 The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks.

3.3 Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

3.4 One accepted approach to achieve the above is to comprehensively assess and compare an organization's current, and desired, cyber risk management postures. Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan. This risk-based approach will enable an organization to best apply its resources in the most effective manner.

3.5 These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework:

.1 Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

.2 Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

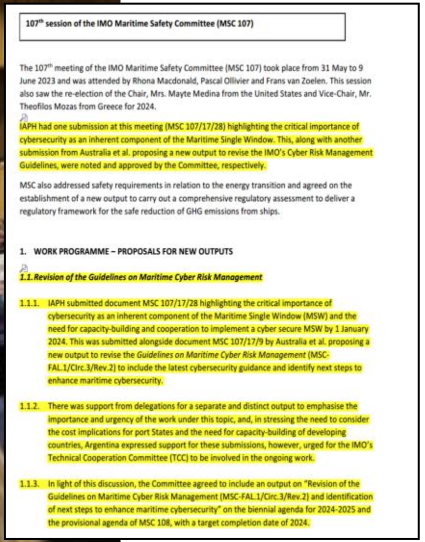
.3 Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.

.4 Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

.5 Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

Developments at the IMO: MSC 107

Maritime Safety Committee (MSC), 107th Session, 31 May – 9 June 2023



107th session of the IMO Maritime Safety Committee (MSC 107)

The 107th meeting of the IMO Maritime Safety Committee (MSC 107) took place from 31 May to 9 June 2023 and was attended by Rhona Macdonald, Pascal Ollivier and Frans van Zoelen. This session also saw the re-election of the Chair, Mrs. Mayte Medina from the United States and Vice-Chair, Mr. Theofilos Mozas from Greece for 2024.

IAPH had one submission at this meeting (MSC 107/17/28) highlighting the critical importance of cybersecurity as an inherent component of the Maritime Single Window. This, along with another submission from Australia et al. proposing a new output to revise the IMO's Cyber Risk Management Guidelines, were noted and approved by the Committee, respectively.

MSC also addressed safety requirements in relation to the energy transition and agreed on the establishment of a new output to carry out a comprehensive regulatory assessment to deliver a regulatory framework for the safe reduction of GHG emissions from ships.

1. WORK PROGRAMME – PROPOSALS FOR NEW OUTPUTS

1.1. Revision of the Guidelines on Maritime Cyber Risk Management

1.1.1. IAPH submitted document MSC 107/17/28 highlighting the critical importance of cybersecurity as an inherent component of the Maritime Single Window (MSW) and the need for capacity-building and cooperation to implement a cyber secure MSW by 1 January 2024. This was submitted alongside document MSC 107/17/9 by Australia et al. proposing a new output to revise the *Guidelines on Maritime Cyber Risk Management* (MSC-FAL.1/Circ.3/Rev.2) to include the latest cybersecurity guidance and identify next steps to enhance maritime cybersecurity.

1.1.2. There was support from delegations for a separate and distinct output to emphasise the importance and urgency of the work under this topic, and, in stressing the need to consider the cost implications for port States and the need for capacity-building of developing countries, Argentina expressed support for these submissions, however, urged for the IMO's Technical Cooperation Committee (TCC) to be involved in the ongoing work.

1.1.3. In light of this discussion, the Committee agreed to include an output on "Revision of the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2) and identification of next steps to enhance maritime cybersecurity" on the biennial agenda for 2024-2025 and the provisional agenda of MSC 108, with a target completion date of 2024.

Proposals for New Outputs – *Committee agreed to include an output on 'revision of the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2) and identification of next steps to enhance maritime cybersecurity" on the biennial agenda for 2024-25 and the provisional agenda of MSC 108, with the target completion date of 2024.*

We’re only focusing on half the story

Cyber risk management describes the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating to an acceptable level, considering costs and benefits of actions to stakeholders.

NIST

- NIST Computer Security Resource Center

Efforts to support vessel cyber resilience
(Shipbuilding / engineering perspectives)

IACS International Association of Classification Societies

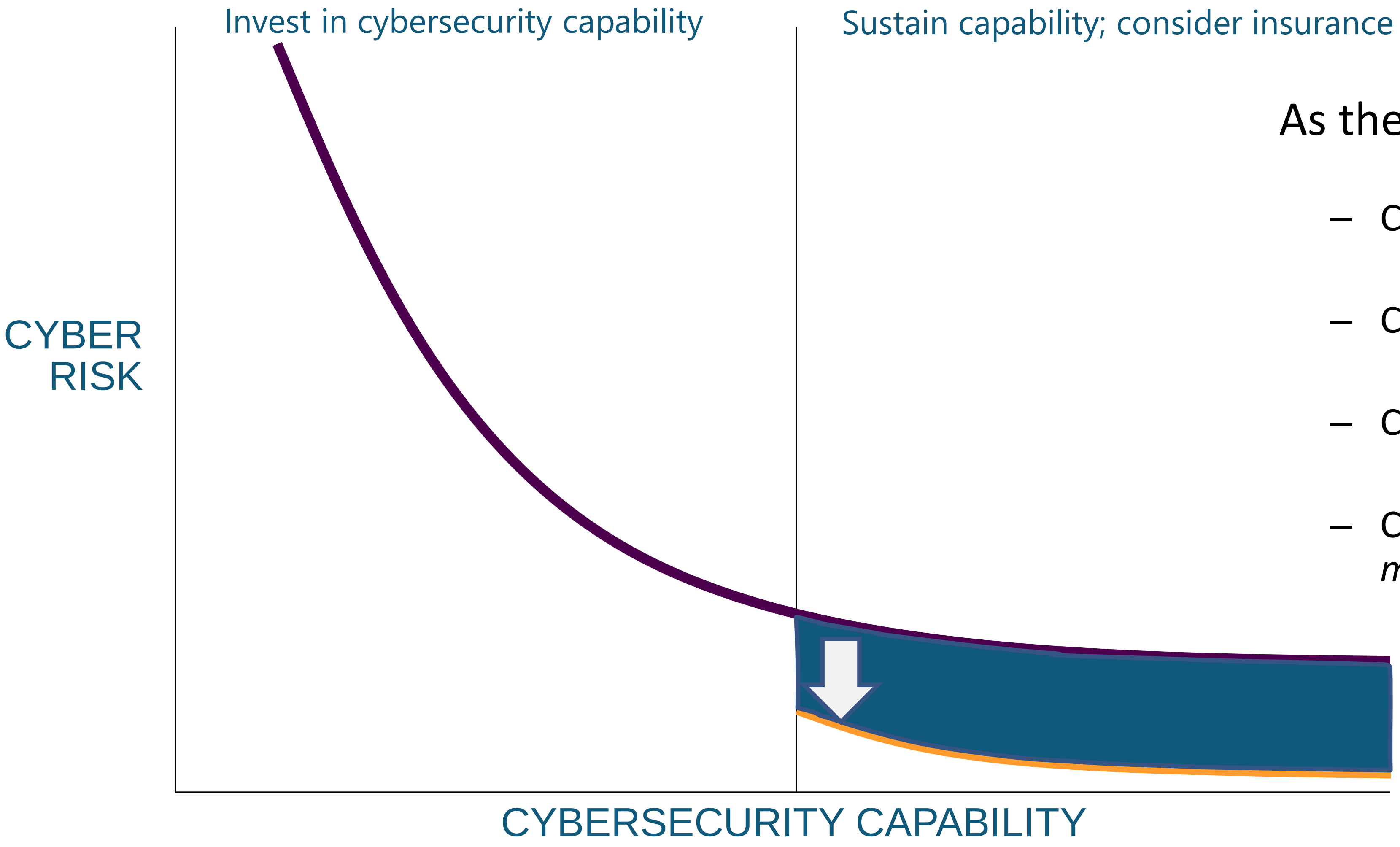
Objective of the Unified Requirements (UR): support cyber resilience onboard vessels

Timeline: These URs will be applied to new ships constructed after 1 January 2024.

- UR E26 aims to ensure the secure integration of both OT and IT equipment into the vessel's network during the design, construction, commissioning, and operational life of the ship. This UR targets the ship as a collective entity for cyber resilience and covers five key aspects: equipment identification, protection, attack detection, response, and recovery.

- UR E27 aims to ensure system integrity is secured and hardened by third-party equipment suppliers. This UR provides requirements for cyber resilience of onboard systems and equipment and provides additional requirements relating to the interface between users and computer-based systems onboard, as well as product design and development requirements for new devices before their implementation onboard ships.

The Cyber Risk Curve in the Age of Digitalization



As the risk curve flattens…

– Compliance is achieved, and

– Cyber resilience is improved

– Cyber insurance is possible

– Cyber risk to the Balance Sheet is *managed*

Image: courtesy of Axio

Cybersecurity capability maturity informs risk transfer

Key insurance sections and sub-limits:

- Cyber physical damage
- Expenses following cyber physical damage
- Incident response
- Legal expenses
- Public relations expenses
- Forensic expenses
- Notification expenses
- Cyber extortion and ransomware
- Bricking event coverage
- Misdirection of funds
- Privacy and confidentiality liability
- Data and software liability
- Electronic media liability
- PCI DSS Assessment costs
- Non-damage business interruption
- Contingent Business interruption

Key questions to consider regarding cyber business risk:

1. Is compliance adequate?
2. How do you assess for all of these cyber risk factors in the absence of actuarial history?
3. How do you demonstrate cybersecurity capability sufficiency and measure progress?

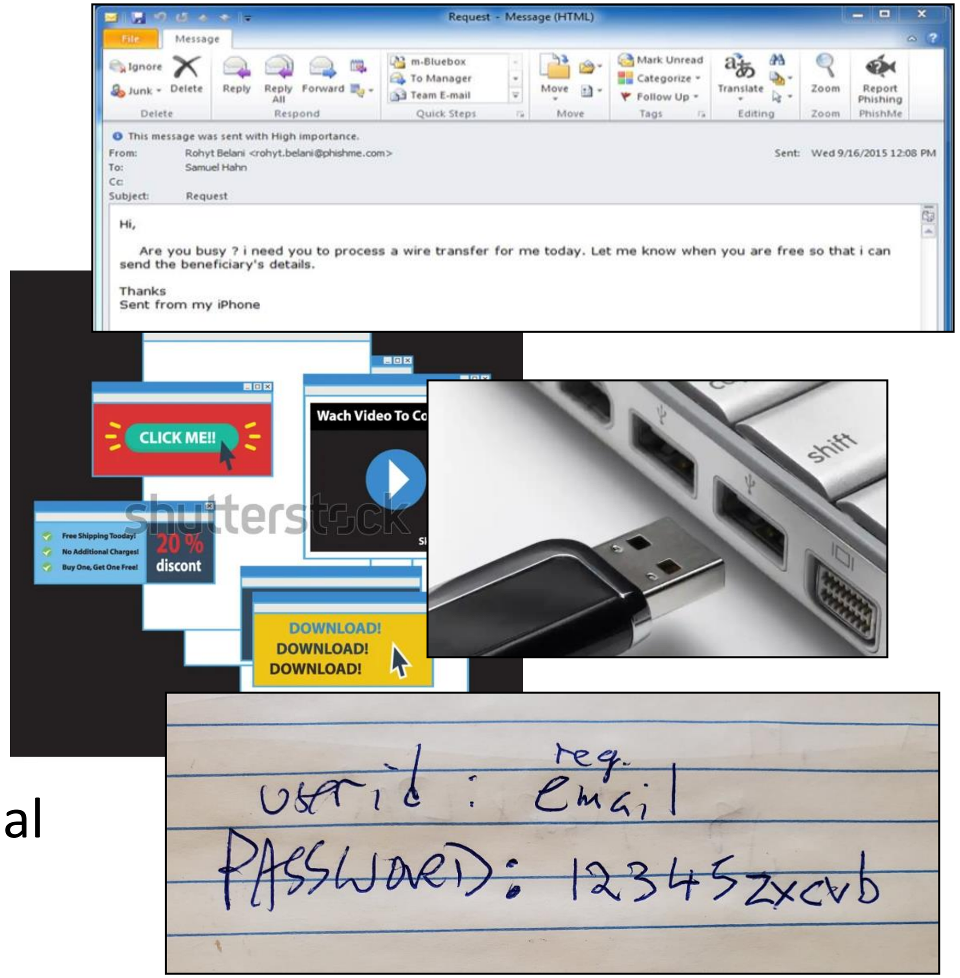
Compliance doesn't always matter – case study: the U.S. Coast Guard and the potential risk of cyber over-reaction

PSCOs are looking at basic cyber behaviors

What are the PSCOs looking for?

Confirming basic cyber best practices are in place. These include:

- **Observations** that appropriate behaviors are (or not) implemented
  - Are passwords written down and taped to computers?
  - Are USB flash drives in use?
- **Evidence** of a cyber attack (e.g., Ransomware, excessive popups on computer screens)
- **Complaints** of unusual network issues and/or reliability impacting shipboard systems
- **Anecdotes** from crew describing how they received potential ‘spoofed’ email from master/crew onboard



This message was sent with High importance.

From: Rohyt Belani <rohyt.belani@phishme.com>

Sent: Wed 9/16/2015 12:08 PM

To: Samuel Hahn

Cc:

Subject: Request

Hi,

Are you busy ? i need you to process a wire transfer for me today. Let me know when you are free so that i can send the beneficiary's details.

Thanks
Sent from my iPhone

userid : reg. email
PASSWORD: 12345zxcvb

Case Study: February 2019

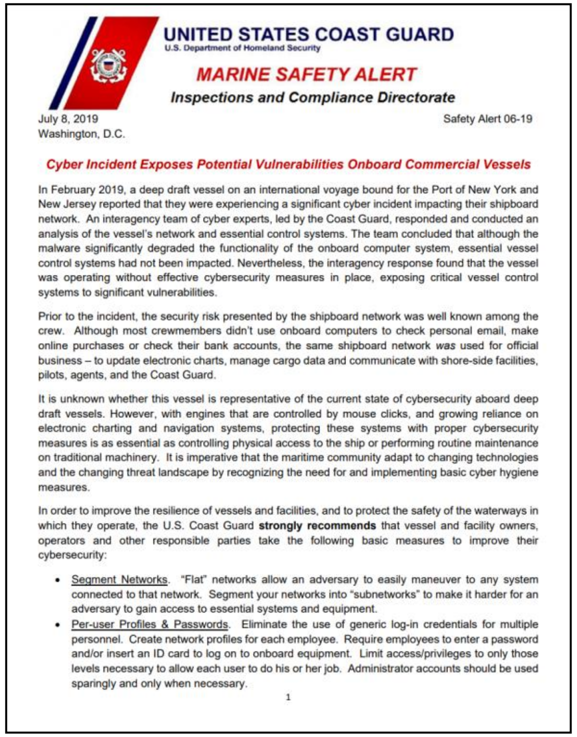
A deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were **experiencing a significant cyber incident** impacting their shipboard network.

An **interagency team** of cyber experts, led by the US Coast Guard, responded and conducted an analysis of the vessel's network and essential control systems.

The team concluded that although the malware significantly degraded the functionality of the onboard computer system, essential vessel control systems had not been impacted.

Nevertheless, the interagency response found that the vessel was operating without effective cybersecurity measures in place, exposing critical vessel control systems to significant vulnerabilities

Now imagine what kind of response the USCG would mobilize for a cyber attack resulting in compromised critical systems?



UNITED STATES COAST GUARD
U.S. Department of Homeland Security

MARINE SAFETY ALERT

Inspections and Compliance Directorate

July 8, 2019
Washington, D.C.

Safety Alert 06-19

Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels

In February 2019, a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were experiencing a significant cyber incident impacting their shipboard network. An interagency team of cyber experts, led by the Coast Guard, responded and conducted an analysis of the vessel's network and essential control systems. The team concluded that although the malware significantly degraded the functionality of the onboard computer system, essential vessel control systems had not been impacted. Nevertheless, the interagency response found that the vessel was operating without effective cybersecurity measures in place, exposing critical vessel control systems to significant vulnerabilities.

Prior to the incident, the security risk presented by the shipboard network was well known among the crew. Although most crewmembers didn't use onboard computers to check personal email, make online purchases or check their bank accounts, the same shipboard network *was* used for official business – to update electronic charts, manage cargo data and communicate with shore-side facilities, pilots, agents, and the Coast Guard.

It is unknown whether this vessel is representative of the current state of cybersecurity aboard deep draft vessels. However, with engines that are controlled by mouse clicks, and growing reliance on electronic charting and navigation systems, protecting these systems with proper cybersecurity measures is as essential as controlling physical access to the ship or performing routine maintenance on traditional machinery. It is imperative that the maritime community adapt to changing technologies and the changing threat landscape by recognizing the need for and implementing basic cyber hygiene measures.

In order to improve the resilience of vessels and facilities, and to protect the safety of the waterways in which they operate, the U.S. Coast Guard **strongly recommends** that vessel and facility owners, operators and other responsible parties take the following basic measures to improve their cybersecurity:

- Segment Networks. "Flat" networks allow an adversary to easily maneuver to any system connected to that network. Segment your networks into "subnetworks" to make it harder for an adversary to gain access to essential systems and equipment.
- Per-user Profiles & Passwords. Eliminate the use of generic log-in credentials for multiple personnel. Create network profiles for each employee. Require employees to enter a password and/or insert an ID card to log on to onboard equipment. Limit access/privileges to only those levels necessary to allow each user to do his or her job. Administrator accounts should be used sparingly and only when necessary.

1

"Inter-Agency" = Delays = Lost $ € £ ¥

A US Coast Guard led "**interagency team"** of can include a wide range of cybersecurity stakeholders drawn from various Federal agencies such as:

- Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Bureau of Investigation (FBI)
- Secret Service
- Customs and Border Protection (CBP)
- Transportation Security Agency (TSA)
- Federal Emergency Management Agency (FEMA)
- Office of Intelligence and Analysis (OI & A)
- Federal Computer Incident Response Center (FCIRC)
- Domestic Nuclear Detection Office (DNDO)
- Department of Defense (including National Guard)

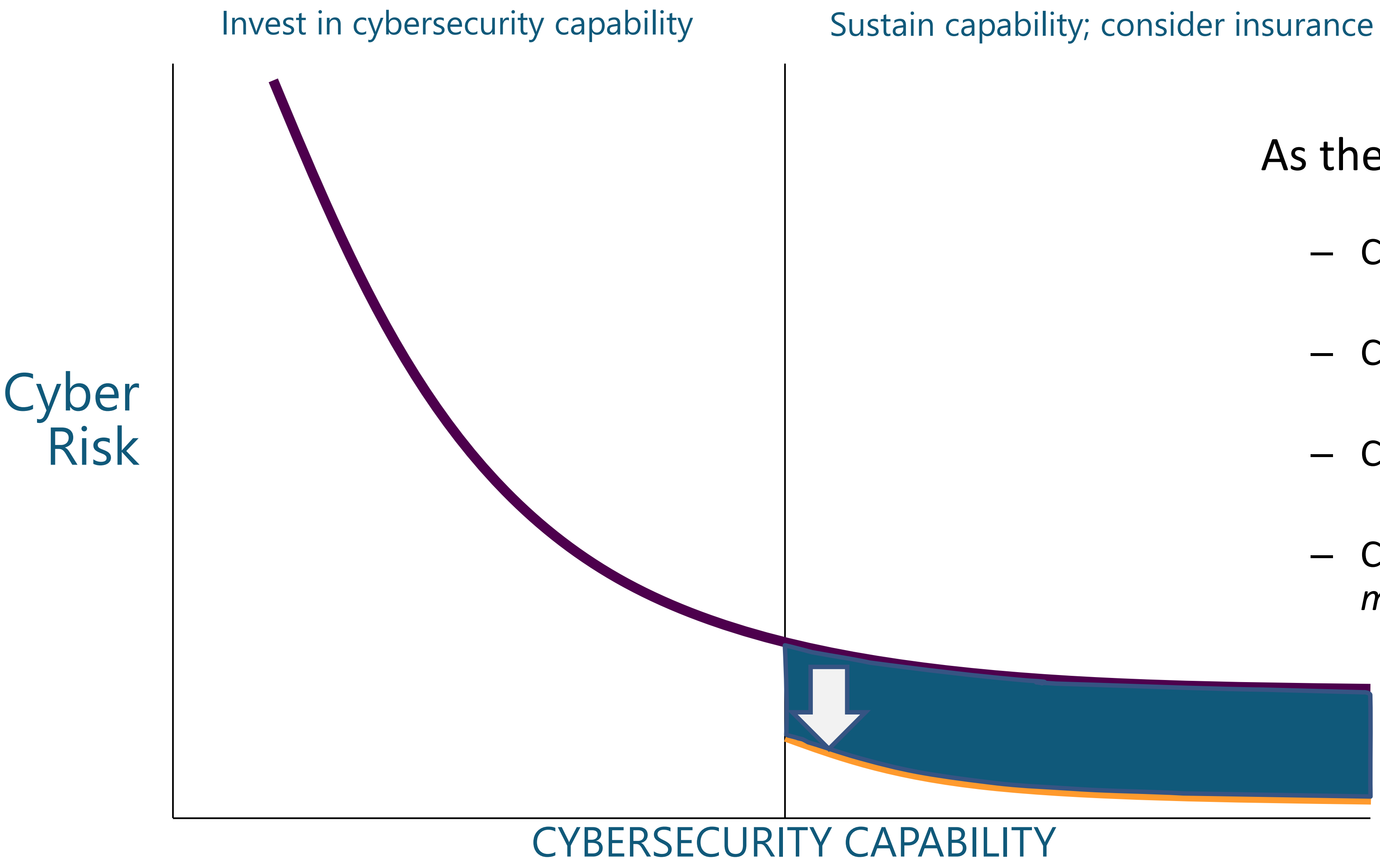
Non-Federal stakeholders can include:

- State and local police departments
- State regulatory agencies

Leadership strategies for driving organizational cyber resilience

HudsonCyber
Managing Cyber Risk

Reducing cyber risk in the age of digitalization

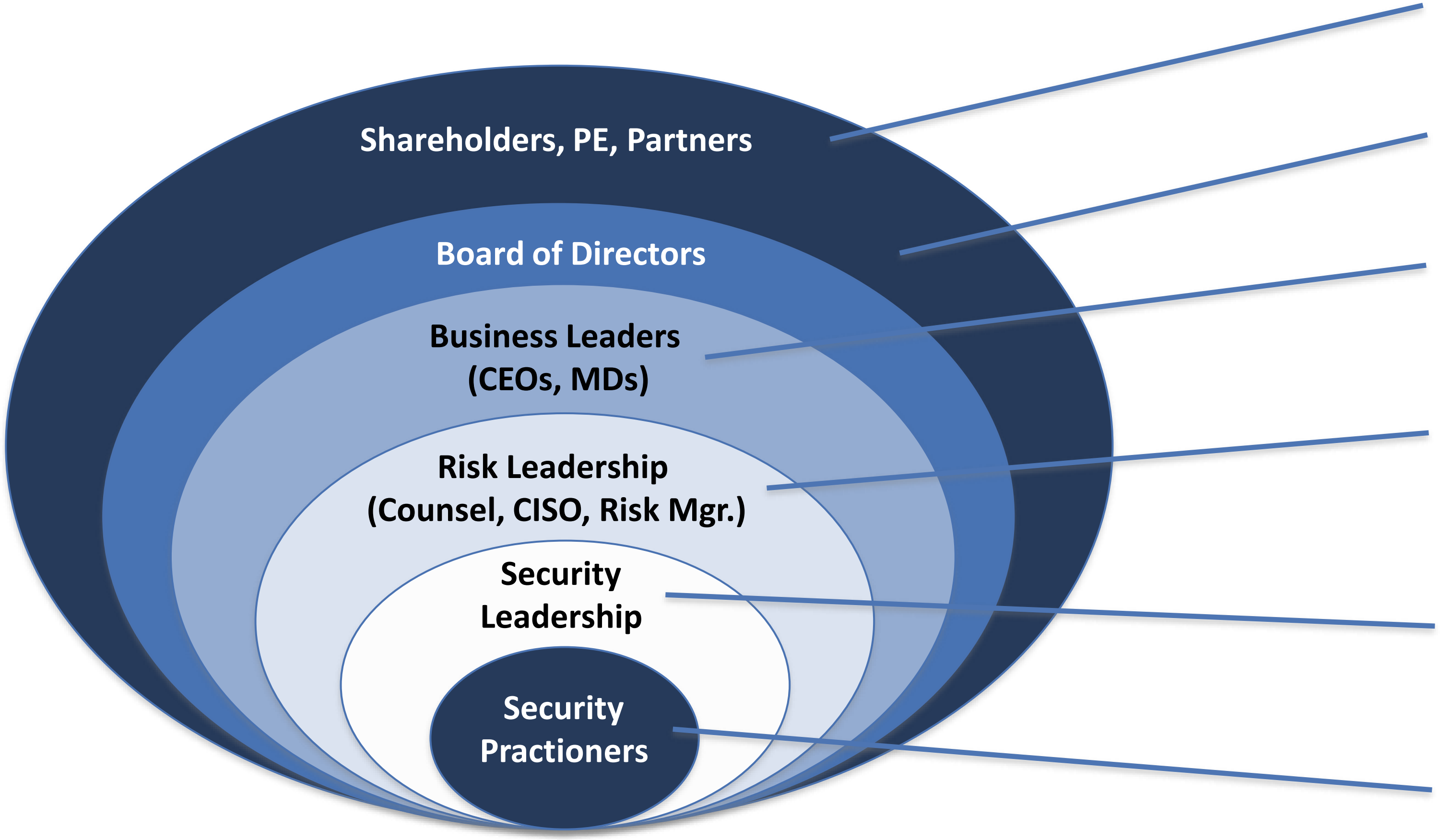


As the risk curve flattens…

- Compliance is achieved, and
- Cyber resilience is achieved
- Cyber insurance is possible
- Cyber risk to the Balance Sheet is *managed*

HudsonCyber
Maritime Cyber Security

First, let’s figure out who actually owns cyber risk


Shareholders, PE, Partners
Board of Directors
Business Leaders (CEOs, MDs)
Risk Leadership (Counsel, CISO, Risk Mgr.)
Security Leadership
Security Practioners

Evaluate and Fund Risk
(In terms of Investment decisions)

Evaluate and Fund Risk
(Minimize losses; support/protect shareholder equity)

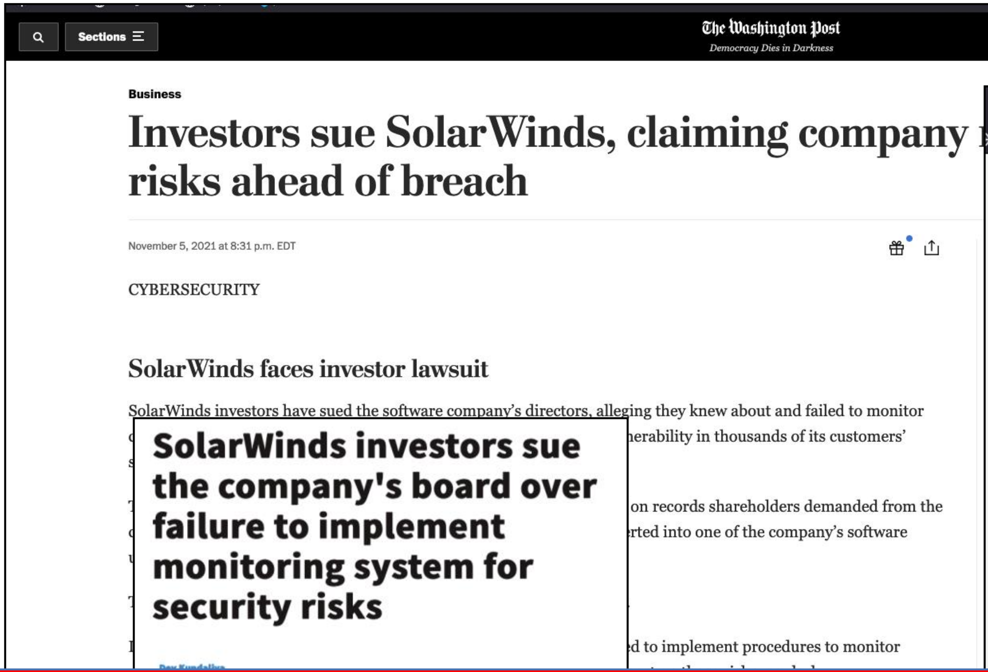
Manage Risk
(Profit and Loss / Balance Sheet)

Identify, Prevent, Accept, and Transfer Risk
(Insurance; Agreements and Contracts *in terms of and risk to* Profit and Loss and the Balance Sheet)

Validate Risk, Allocate Resources
(In terms of cyber risk to operations and Profit and Loss)

Communicate Needs, Solutions
(In terms of cyber *risk to* operations that supports cash flow and profit and loss)

Is settling cyber breach lawsuits against the board the "IT Guy's" job?



Business

Investors sue SolarWinds, claiming company
risks ahead of breach

November 5, 2021 at 8:31 p.m. EDT

CYBERSECURITY

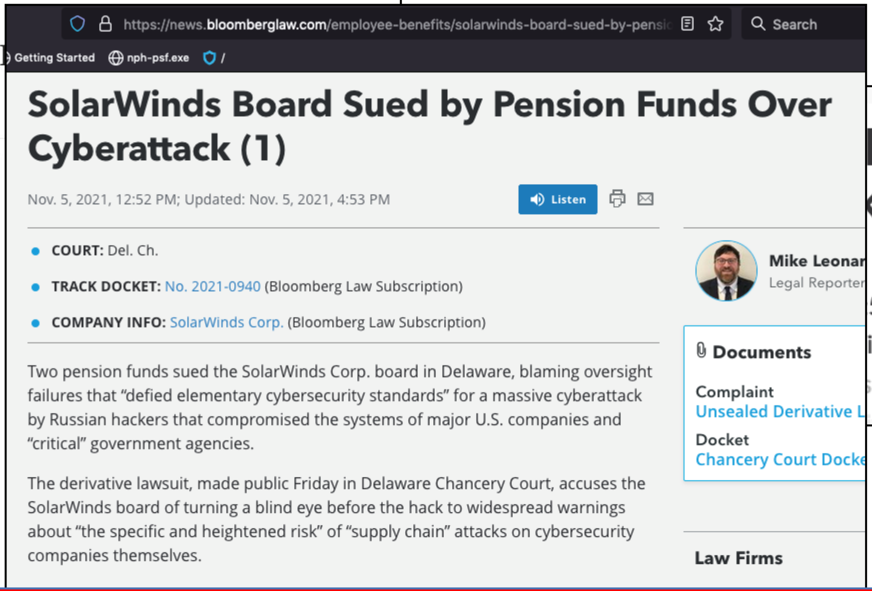
SolarWinds faces investor lawsuit

SolarWinds investors have sued the software company's directors, alleging they knew about and failed to monitor
nerability in thousands of its customers'

on records shareholders demanded from the
rted into one of the company's software

d to implement procedures to monitor

SolarWinds investors sue the company's board over failure to implement monitoring system for security risks



https://news.bloomberglaw.com/employee-benefits/solarwinds-board-sued-by-pensic
Search
Getting Started
nph-psf.exe
Listen

SolarWinds Board Sued by Pension Funds Over Cyberattack (1)

Nov. 5, 2021, 12:52 PM; Updated: Nov. 5, 2021, 4:53 PM

- COURT: Del. Ch.
- TRACK DOCKET: No. 2021-0940 (Bloomberg Law Subscription)
- COMPANY INFO: SolarWinds Corp. (Bloomberg Law Subscription)

Two pension funds sued the SolarWinds Corp. board in Delaware, blaming oversight failures that "defied elementary cybersecurity standards" for a massive cyberattack by Russian hackers that compromised the systems of major U.S. companies and "critical" government agencies.

The derivative lawsuit, made public Friday in Delaware Chancery Court, accuses the SolarWinds board of turning a blind eye before the hack to widespread warnings about "the specific and heightened risk" of "supply chain" attacks on cybersecurity companies themselves.

Mike Leonar
Legal Reporter

Documents

Complaint
Unsealed Derivative L

Docket
Chancery Court Docke

Law Firms

Don't want ads? Subscribe or login now.

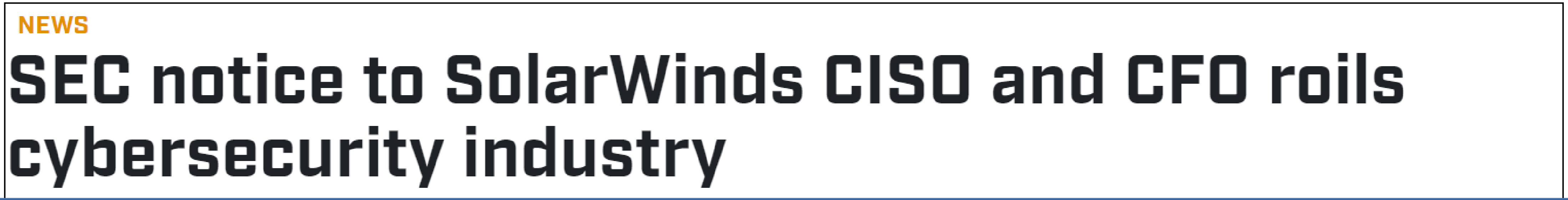
h Del. Derivative Suit
k

55 PM EDT) -- Current and former directors of
inds have been hit with a stockholder derivativ
s they were at fault for the massive hack and da

Oversight failures can have major consequences and breach of fiduciary responsibility allegations are tough (and expensive) to defend against. D & O insurers are starting to look more aggressively at BoD oversight.

HudsonCyber
Maritime Cyber Security

The “gloves” are now starting to come off… (June 27th)



NEWS

SEC notice to SolarWinds CISO and CFO roils cybersecurity industry

The US Securities and Exchange Commission has roiled the cybersecurity industry by putting executives of SolarWind on notice that it may pursue legal action for violations of federal law in connection with their response to the 2020 attack on the company's infrastructure that affected thousands of customers in government agencies and companies globally.

If successful, this move by the SEC will make CFOs, CISOs, and CSOs more individually accountable for cybersecurity

Reconsider cyber risk management as a financial discussion

- ✓ Consider cyber risk in terms of *money*
- ✓ *The cyber-risk-to-money intersection offers measurable value to support resource allocation and prioritization*
- ✓ Financial “grounding” translates cyber risk into a common language
- ✓ Empowers decision-makers with relevant context and inputs so as to make informed decisions on cyber risk

Re-think managing cyber risk as a business discipline

Develop the business case

Determine business impact

- Identify critical assets, systems, equipment, and infrastructure
- Characterize impact– income, health and safety, environment, reputation, etc.
- Define RPO and RTO targets

Develop and apply realistic loss scenarios

- Engage multiple stakeholders
- Develop and agree on scenario scope, probability, realism, context, financial value at risk, primary outcomes, frequency, and bias
- Determine value-at-risk

Enable organizational resilience

Establish a common vocabulary

- Institute a common vocabulary with clear definitions
- Using BIA and loss scenario findings, ground cybersecurity discussions in a financial context

Establish the cyber-risk-to-money intersection

- Frame cybersecurity discussions in financial terms
- Establish a sustainable cybersecurity budget
- Prioritize budget allocations based on BIA and Loss Scenario analysis
- Review and test cyber insurance polices against loss scenarios

Enable organizational change to achieve cyber resilience

First, get organized

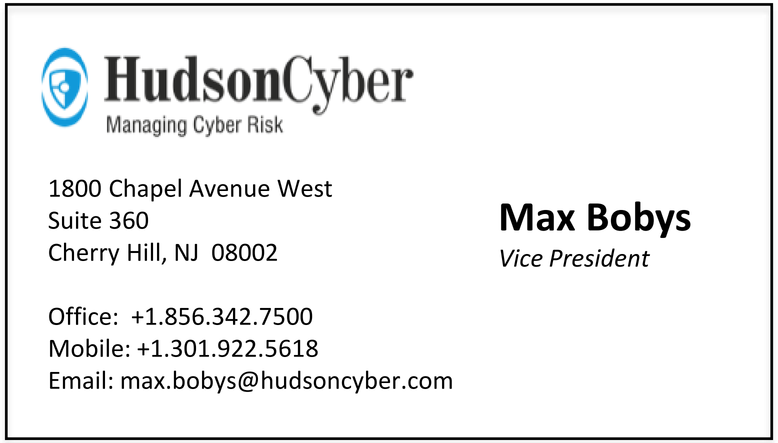
- Identify key stakeholders
- Establish and assign duties and authorities
- Establish oversight
- The role of the Board of Directors
- The cybersecurity steering committee (or working group)

Once organized, take action

Executives can implement the following strategies for facilitating change:

- Facilitate and engage in the decision-making process
- Drive cyber awareness across all functional areas through training
- Implement governance
- Drive organizational accountability

Thank You



HudsonCyber
Managing Cyber Risk

1800 Chapel Avenue West
Suite 360
Cherry Hill, NJ 08002

Office: +1.856.342.7500
Mobile: +1.301.922.5618
Email: max.bobys@hudsoncyber.com

Max Bobys
Vice President