AAPA
Recovery and Lessons Learned from Cyber Attacks

APRIL 17, 2018

Stephen Viña
Senior Vice President
Marsh

New York, NY

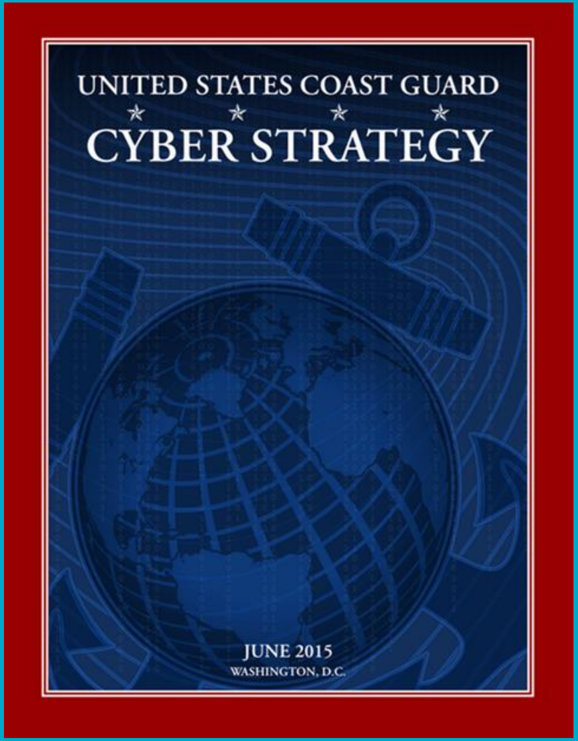
Daniel J. Healy, Esq.

Partner
Anderson Kill

Washington D.C.

“Threats in cyberspace, particularly to the maritime community and transportation sector, are real and growing”

– U.S. Coast Guard Cyber Strategy (June 2015)

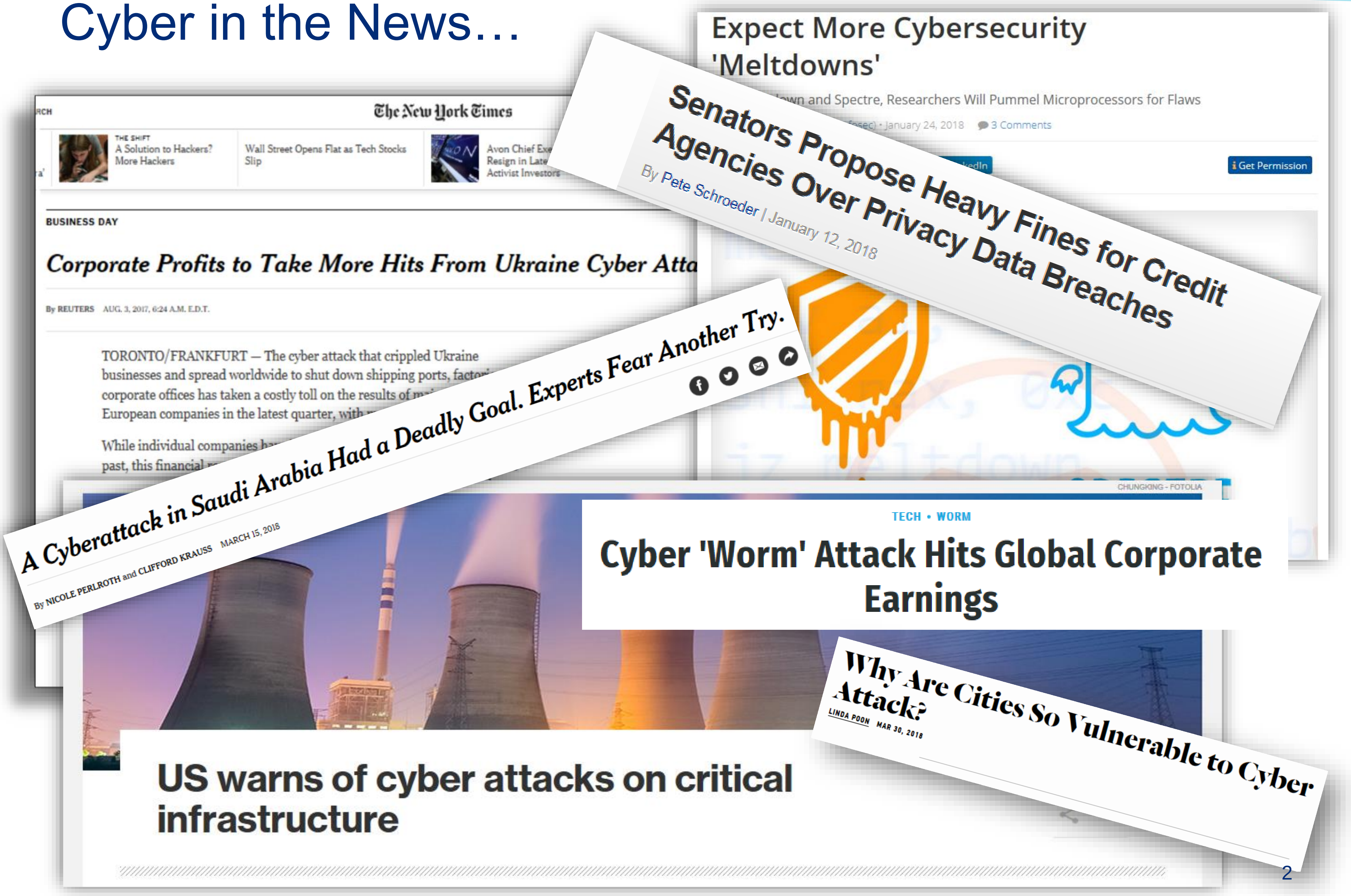

UNITED STATES COAST GUARD

CYBER STRATEGY

JUNE 2015

WASHINGTON, D.C.

Cyber in the News…



Expect More Cybersecurity 'Meltdowns'

…own and Spectre, Researchers Will Pummel Microprocessors for Flaws

…fosec) • January 24, 2018 3 Comments

…kedIn

Get Permission

Senators Propose Heavy Fines for Credit Agencies Over Privacy Data Breaches

By Pete Schroeder | January 12, 2018

RCH

The New York Times

ra'

THE SHIFT
A Solution to Hackers? More Hackers

Wall Street Opens Flat as Tech Stocks Slip

Avon Chief Exe… Resign in Late… Activist Investors

BUSINESS DAY

Corporate Profits to Take More Hits From Ukraine Cyber Atta…

By REUTERS AUG. 3, 2017, 6:24 A.M. E.D.T.

TORONTO/FRANKFURT — The cyber attack that crippled Ukraine businesses and spread worldwide to shut down shipping ports, factor… corporate offices has taken a costly toll on the results of m… European companies in the latest quarter, with…

While individual companies h… past, this financial…

A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.

By NICOLE PERLROTH and CLIFFORD KRAUSS MARCH 15, 2018

CHUNGKING - FOTOLIA

TECH • WORM

Cyber 'Worm' Attack Hits Global Corporate Earnings

US warns of cyber attacks on critical infrastructure

Why Are Cities So Vulnerable to Cyber Attack?

LINDA POON MAR 30, 2018

Understanding Your Cyber Risk Profile

Threat

How likely am I to experience a cyber event?

How does my threat profile compare to my peers?

Vulnerability

How mature is my cybersecurity program?

How significant are the vulnerabilities in my controls?

Impact

How much financial exposure do I face from a cyber event?

Is my company buying an appropriate level of limits?

CYBER RISK

Who Are The Threat Actors?

MORE THAN HOODED SILHOUETTES

- The modern cyber risk landscape is populated by threat actors with myriad motivations.
- Some attack targets, but many are opportunists who attack vulnerabilities wherever they find them.
- Attack methods can very from highly-targeted and deliberate attacks that develop over months, to mass-scale, self-spreading malware.

Hacktivists

Hacktivists use computer network exploitation to further their political and social cause.

Criminals

Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.

Insiders

Trusted insiders steal proprietary information for personal, financial, and ideological reasons.

Espionage

Nation-state actors conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.

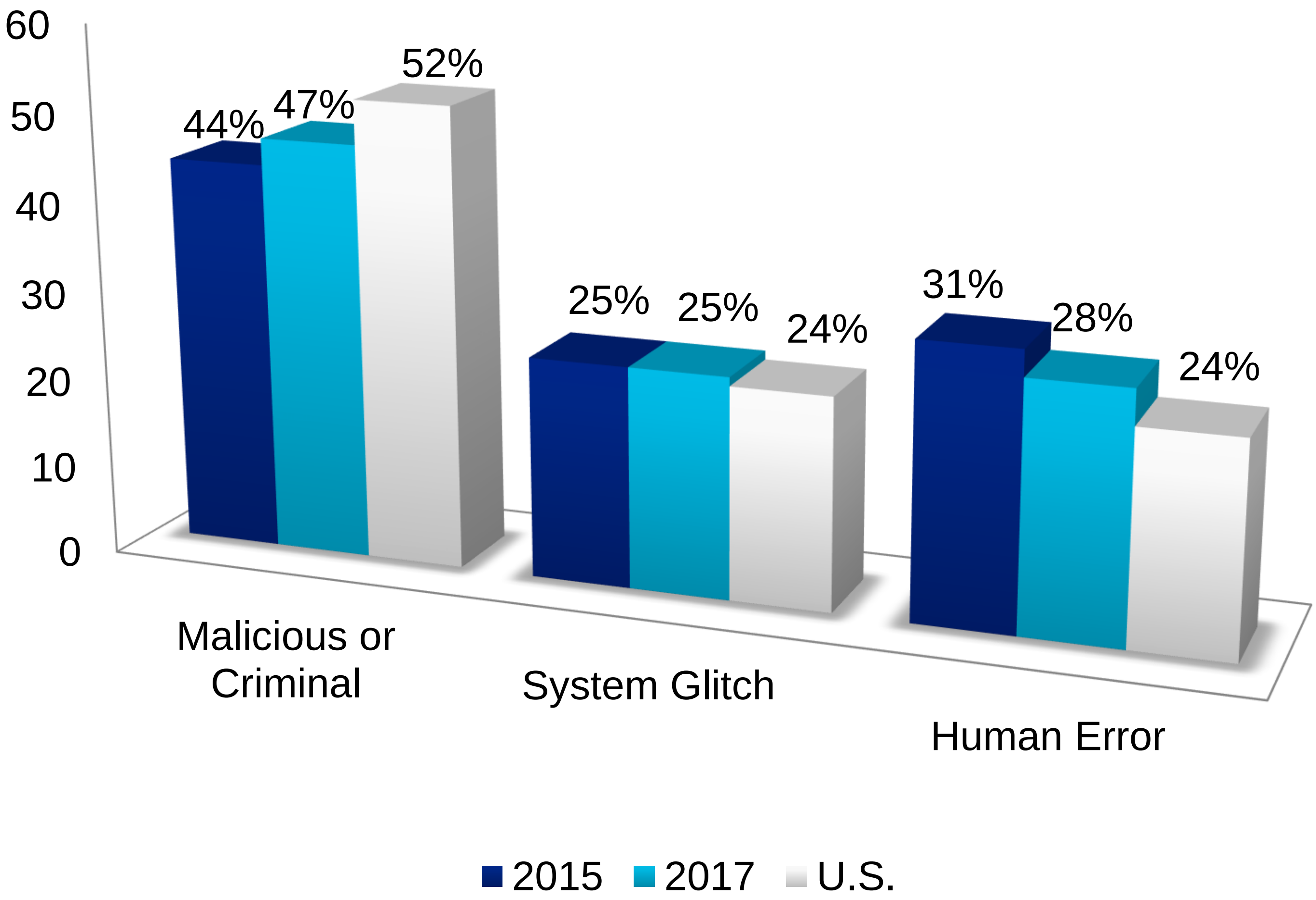
Sabotage

Nation-states, terrorist groups, etc sabotage computer systems that operate our critical infrastructure, such as electric grids and water systems.

System Failure

Unintentional and unplanned outage of a computer system.

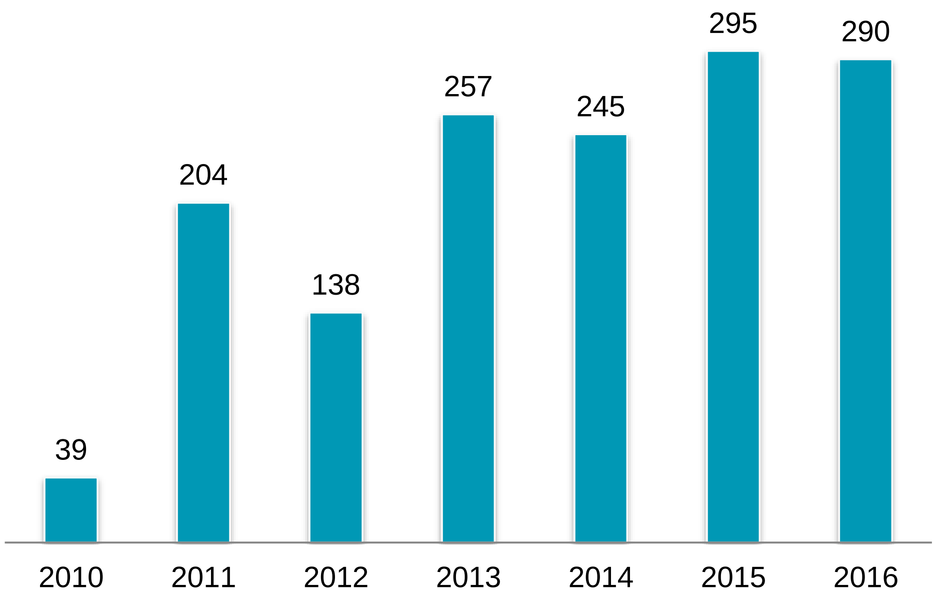
2015-2017 – Root Cause - Ponemon



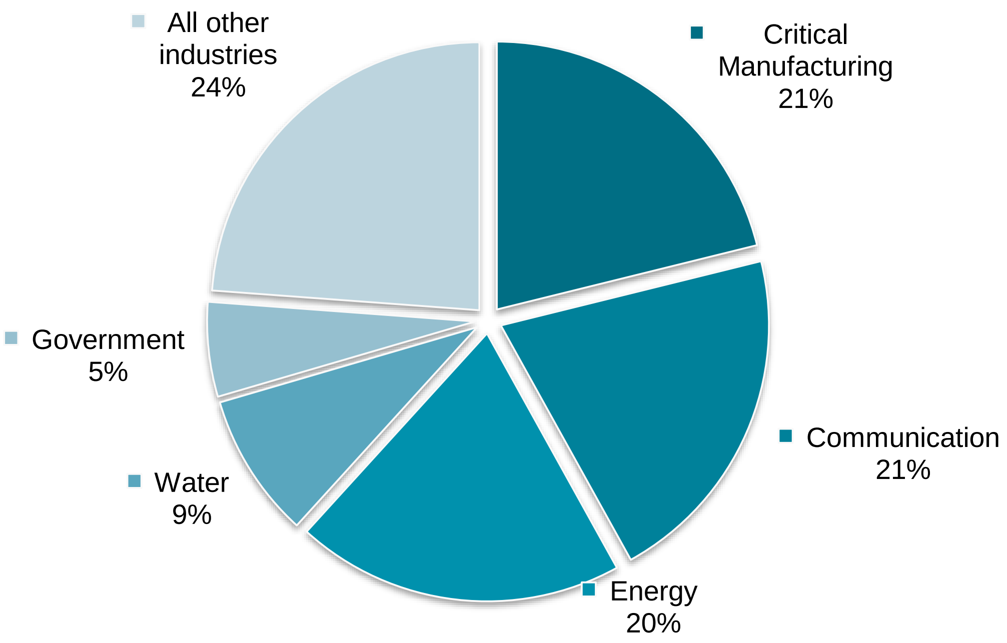
Industrial Control System Threats

- In 2016, the U.S. Department of Homeland Security’s Industrial Control Systems Cybersecurity Emergency Response Team, responded to 290 cyber attacks against industrial control systems (ICS).

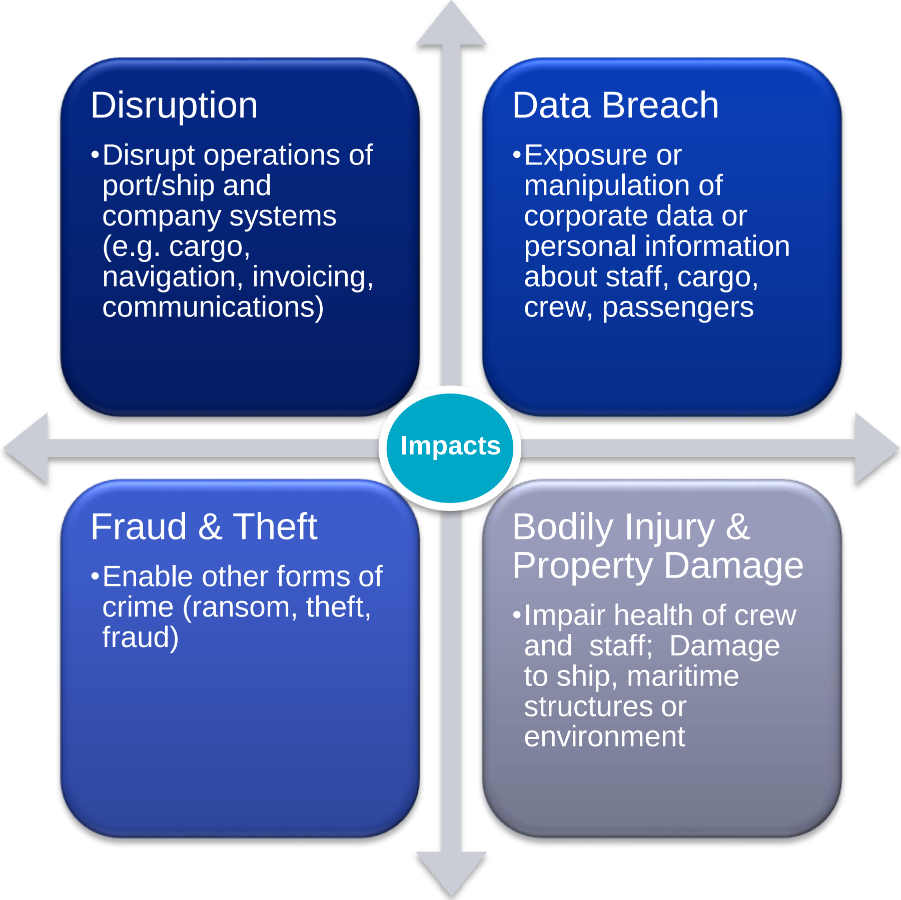
ICS-CERT INCIDENT RESPONSES BY YEAR
Source: ICS-CERT annual reports



ICS-CERT RESPONSES BY SECTOR
Source: ICS-CERT 2016 annual report



Cyber Attacks in the Maritime Sector



Impacts

Disruption

- Disrupt operations of port/ship and company systems (e.g. cargo, navigation, invoicing, communications)

Data Breach

- Exposure or manipulation of corporate data or personal information about staff, cargo, crew, passengers

Fraud & Theft

- Enable other forms of crime (ransom, theft, fraud)

Bodily Injury & Property Damage

- Impair health of crew and staff; Damage to ship, maritime structures or environment

2010 - Malware overwhelms off-shore drilling rig in Asia, forcing a prolonged shut-down.

2011- Pirates suspected of exploiting cyber weaknesses for use in targeting shipments near Somalia

2012 - Over 120 vessels in Asia experience malicious jamming of GPS signals

2013 - Drug smugglers hacked cargo tracking systems in European port to hide drug shipments.

2014 - A domestic port facility suffered a system disruption which shut down multiple ship-to-shore cranes for several hours.

2017 – Pseudo ransomware attack impacts multiple global corporations, including shipping industry, disrupting operations across the world.

NotPetya Cyber Attack

Encrypts computer files and demands **$300 Bitcoin ransom** – but ransom feature not functional, effectively destroying data.

Similar to ransomware "WannaCry" – but allowed easier movement across networks, such as **capturing passwords and administrator rights**.

Serious disruptions to government systems, critical infrastructure, and global businesses resulting in **more than $1 billion aggregate losses**.

*"The NotPetya cyber attack in June hit many different organizations across the globe **including some in the shipping sector**. It showed that the **industry is vulnerable** to these type of attacks. And we **may encounter more** in the years to come."*

Lord Callanan
UK Transport Minister

Evolving Cyber Risk – Destructive Attacks

“More hacks targeting electrical grids, transportation systems, and other parts of countries’ critical infrastructure are going to take place in 2018. Some will be designed to cause immediate disruption (see “A Hack Used to Plunge Ukraine into Darkness Could Still Do Far More Damage”) …”

-MIT Technology Review, 1/2/2018

Destructive Attacks – Power Grid, Nuclear Facility

- Industroyer –
  - ➢ left 20% of Ukraine’s capital, Kiev, dark
  - ➢ 2nd time – had suffered a prior 2015 attack

- Stuxnet
  - ➢ Iran’s Natanz uranium enrichment facility targeted
  - ➢ Caused damage to 1000 industrial centrifuges
  - ➢ Overtook controls and changed motor speeds – from a USB drive

Iran confirms Stuxnet worm halted centrifuges

Iran's president, Mahmoud Ahmadinejad, confirmed on Monday night that a computer worm affected centrifuges in the country's uranium enrichment programme.

The Telegraph, 30 Nov 2010

Technicians work at the Bushehr nuclear power plant Photo: AP

Destructive Attack — Steel Mill

- 2014: Germany
- Cyber attack on steel mill via spear phishing
  - Disrupted industrial control system for blast furnace
  - Furnace could not be shut down
  - Resulted in “massive” unspecified damage
- Revealed by German Federal Office for Information Security (BSI) in December 2014. Few details are known about the event; Germans remain quiet.

Source – bbc.co.uk - © 2014 BBC

Image from BBC: http://www.bbc.co.uk/schools/gcsebitesize/science/aqa_pre_2011/rocks/metalsrev2.shtml

Destructive Attack — BTC Pipeline

Source – Bloomberg.com, 12/10/2014 © 2015 Bloomberg

Image from Bloomberg: http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

- 2008: Turkey, deemed cyber attack in 2014
- Attackers entered through wireless network for surveillance cameras
  - Shut down alarms,
  - Severed communications, and
  - Super-pressurized oil in pipeline
- Impact
  - Spilled 30,000 barrels of crude
  - 3-week pipeline disruption
  - Azerbaijan lost $1B in revenue
  - BP lost $10 million in tariffs
  - Replaces Stuxnet as first cyber attack resulting in major physical damage

Data Destruction Attacks

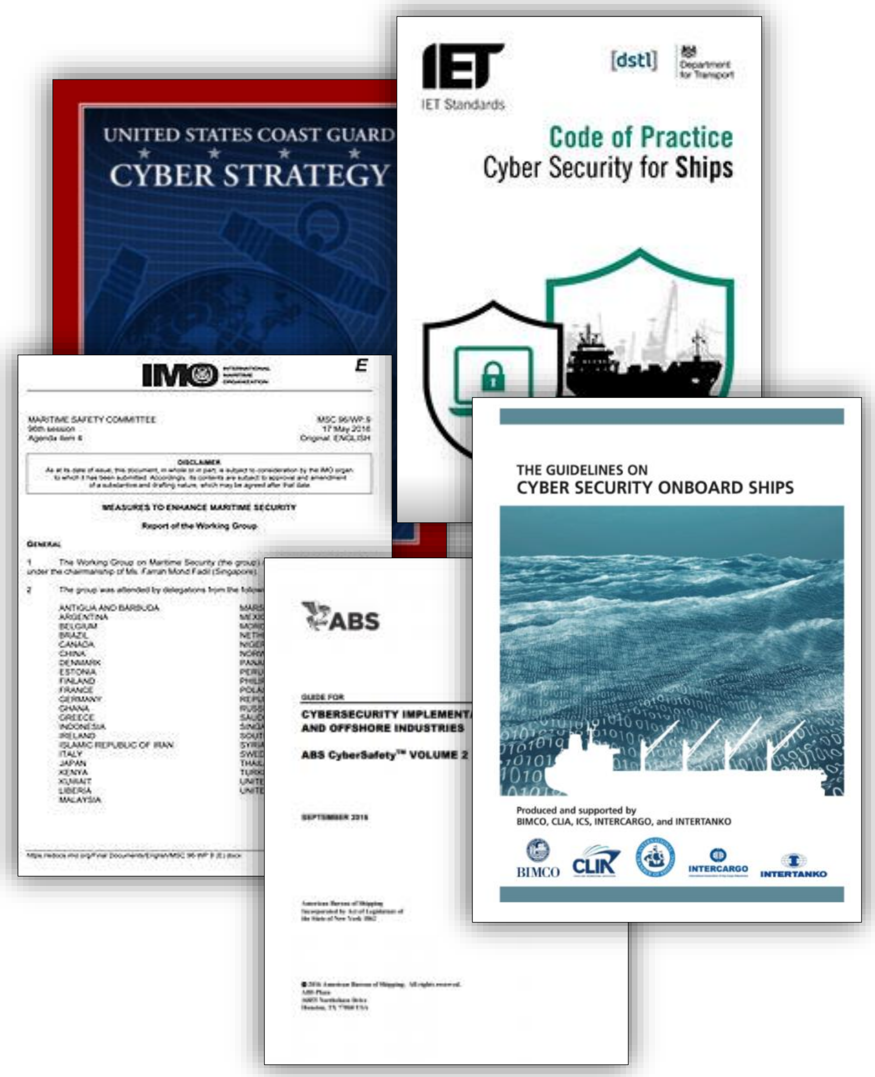
- Saudi Aramco attack:
  August 15, 2012 — Islamic holy day
  - Insider deployed Shamoon wiper malware at Saudi Aramco
  - Destroyed data on 30,000 computers, rendering them inoperable
  - 10-day recovery; oil production not impacted
- Similar attack on RasGas, Qatari natural gas company, 2 weeks later

Cyber Rules and Guidance for the Maritime Sector

Growing and Evolving Cyber Regulatory Environment

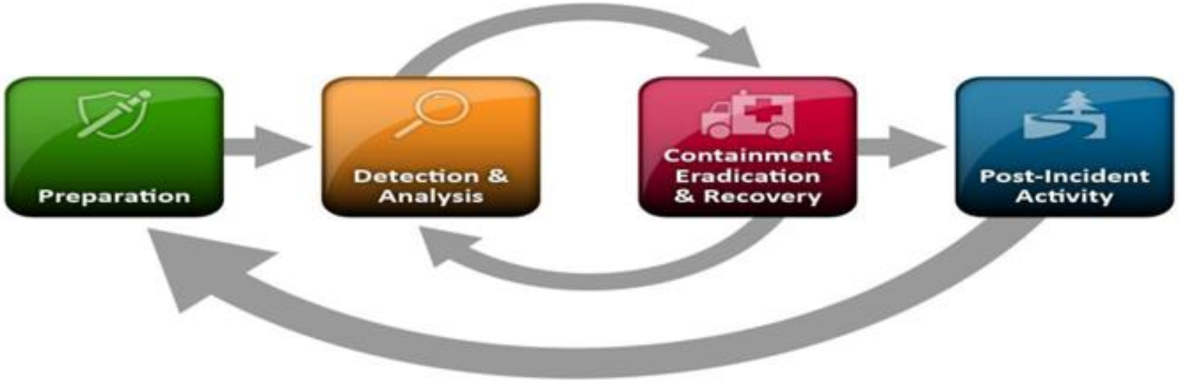
> *"A major disruption in the maritime transportation system could have a significant impact on global shipping, international trade, and the global economy, as well as posing risks to public safety."*

Gregory C. Wilshusen, GAO, Testimony before the Committee on Homeland Security, U.S. House of Representatives (Oct. 8, 2015)


UNITED STATES COAST GUARD
CYBER STRATEGY
IET
IET Standards
[dstl]
Department for Transport
Code of Practice
Cyber Security for Ships
IMO
MARITIME SAFETY COMMITTEE
MEASURES TO ENHANCE MARITIME SECURITY
Report of the Working Group
ABS
GUIDE FOR
CYBERSECURITY IMPLEMENTA
AND OFFSHORE INDUSTRIES
ABS CyberSafety™ VOLUME 2
THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS
Produced and supported by
BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO
BIMCO
CLIA
INTERCARGO
INTERTANKO

NIST Standards

- Industry standards and norms for evaluating reasonableness
- Handbooks, guidance and other literature
- NIST Computer Security Incident Handling Guide (SP 800-61 Rev 2)
- Use NIST Terminology and ensure consistent terminology between the IRP and internal policies

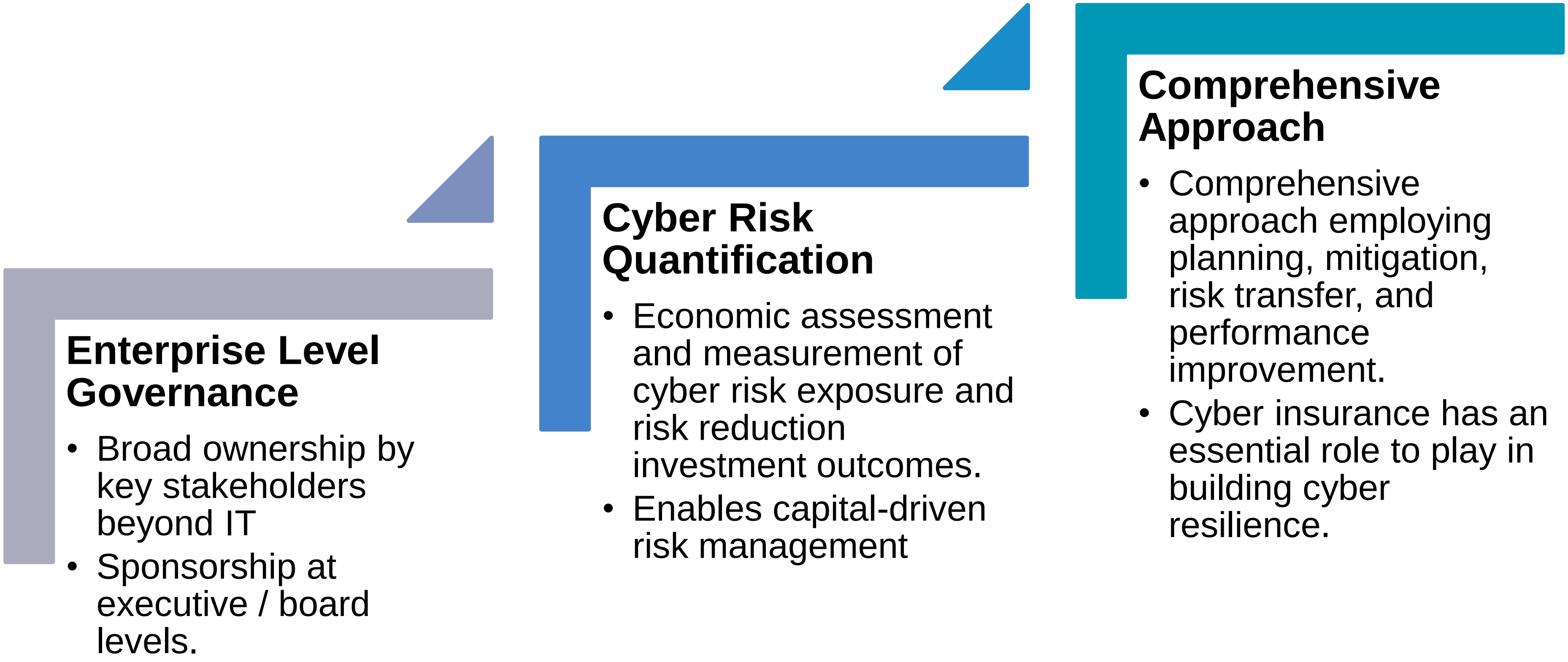


“[T]his was a wake-up call to become not just good —we actually have a plan to come in a situation where our ability to manage cyber-security becomes a competitive advantage."

Jim Hagemann Snabe, Maersk Chairman
World Economic Forum , Davos, 2018

Best Practices for Cyber Risk Management

Cyber Risk Requires a Mature Risk Management Strategy



Enterprise Level Governance

- Broad ownership by key stakeholders beyond IT
- Sponsorship at executive / board levels.

Cyber Risk Quantification

- Economic assessment and measurement of cyber risk exposure and risk reduction investment outcomes.
- Enables capital-driven risk management

Comprehensive Approach

- Comprehensive approach employing planning, mitigation, risk transfer, and performance improvement.
- Cyber insurance has an essential role to play in building cyber resilience.

Cyber Risk Management Best Practices

- Cyber Risk is a permanent entry on the enterprise risk register.
- Cyber risk can be managed, but it cannot be eliminated.
- Cyber is technical in nature, but should be managed economically.
- Managing cyber risk engages the entire enterprise, not just IT.

Four Basic Components of Risk Management

Avoidance

Mitigation

Transfer

Acceptance

Reality-Driven Cyber Risk Management

- Acceptance: not allowed, costly, career ender
- Mitigation: costly, diminishing returns, resource intensive
- Avoidance: bury what's left, not always practical, can kill innovation
- Transfer: often skipped, viewed as defeat, limited budget

~~Four~~ Three Basic Components of Risk Management

Acceptance is
Not Acceptable

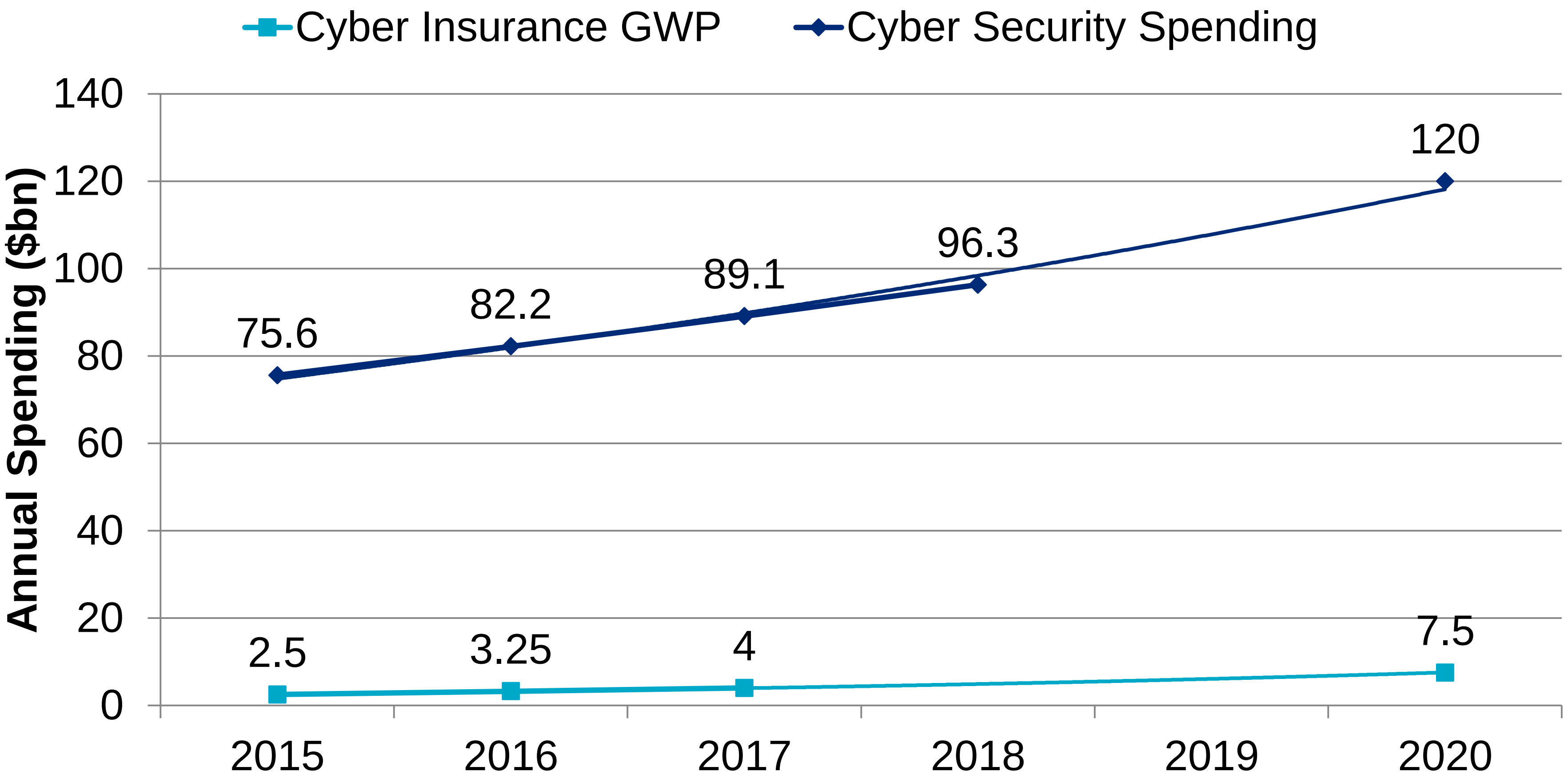
Mitigation = Spend
What it Takes

Avoidance =
Duck Whatever's Left

Transfer = Defeat

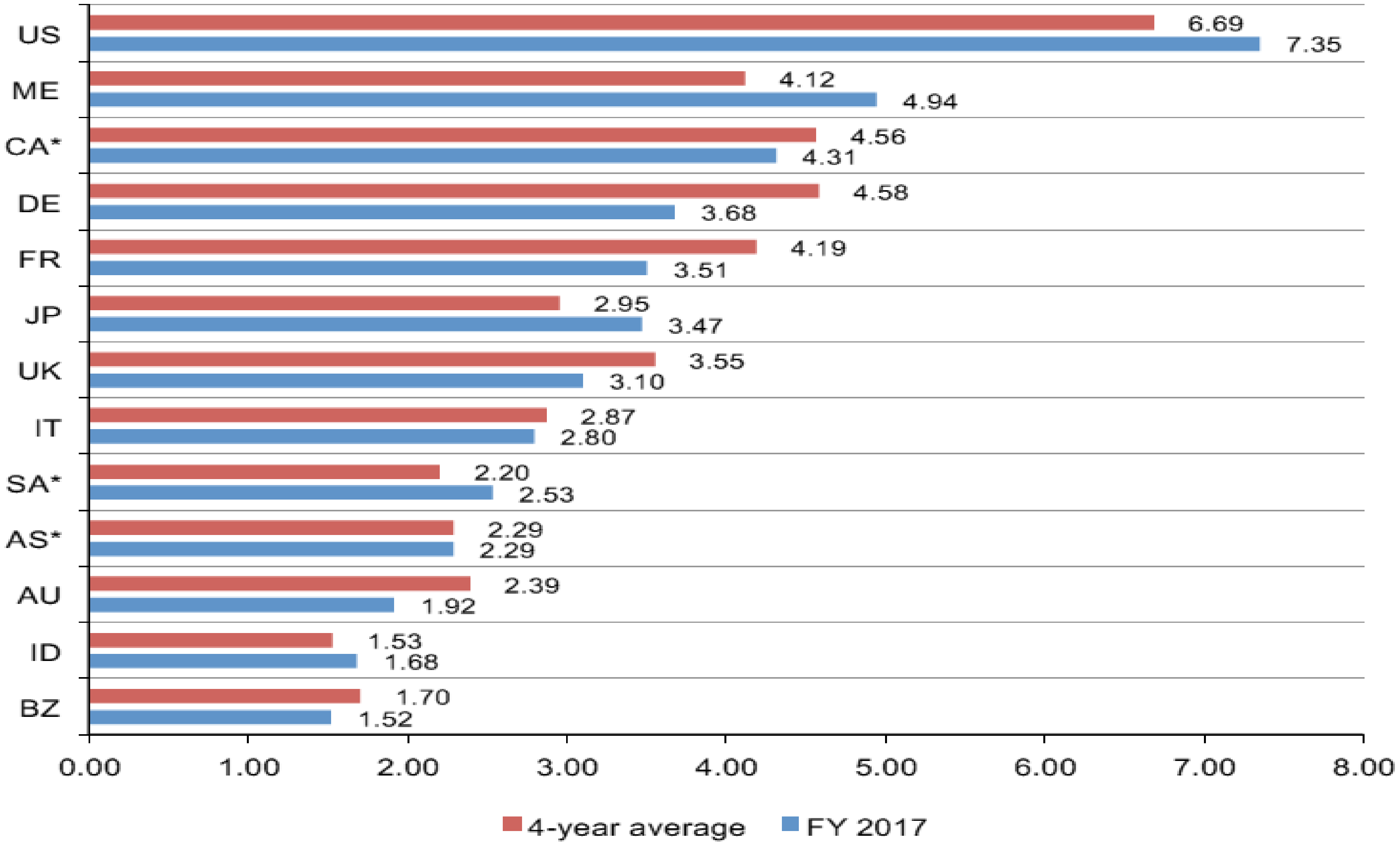
Cybersecurity Spending vs. Cyber Insurance GWP

Risk Management Out of Balance



Annual Cybersecurity Spending vs. Cyber Insurance GWP, 2015 - 2020

Ponemon 2017 Organizational Cost



Post-Breach Costs

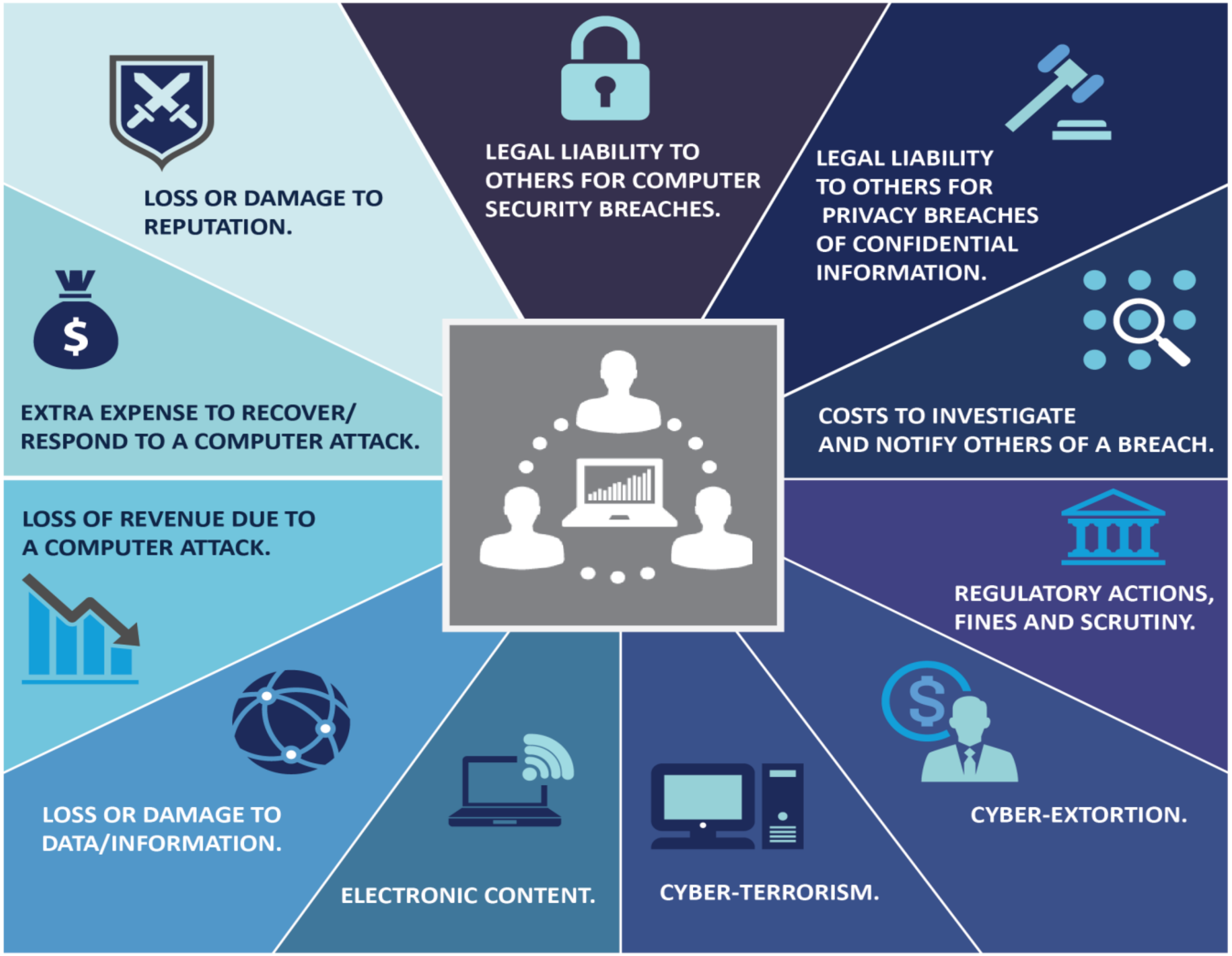
- U.S. and Middle East Post Breach costs are the highest:
  - Response team
  - Forensic experts
  - Regulatory investigations
  - Lawsuits an third-party claims

- US notification costs are the highest
  - create contact databases,
  - determine regulatory requirements,
  - hire outside experts,
  - postal expenditures, email bounce-backs and inbound communication setup

Policies Potentially Covering Loss

- Take Inventory of Policies
- GL, D&O, E&O, Crime, All Risk Property, Cyber Policies
- 1st Party, 3rd Party, Hybrid Coverage Issues

Insurable Cyber Risks



LOSS OR DAMAGE TO REPUTATION.

LEGAL LIABILITY TO OTHERS FOR COMPUTER SECURITY BREACHES.

LEGAL LIABILITY TO OTHERS FOR PRIVACY BREACHES OF CONFIDENTIAL INFORMATION.

EXTRA EXPENSE TO RECOVER/ RESPOND TO A COMPUTER ATTACK.

COSTS TO INVESTIGATE AND NOTIFY OTHERS OF A BREACH.

LOSS OF REVENUE DUE TO A COMPUTER ATTACK.

REGULATORY ACTIONS, FINES AND SCRUTINY.

LOSS OR DAMAGE TO DATA/INFORMATION.

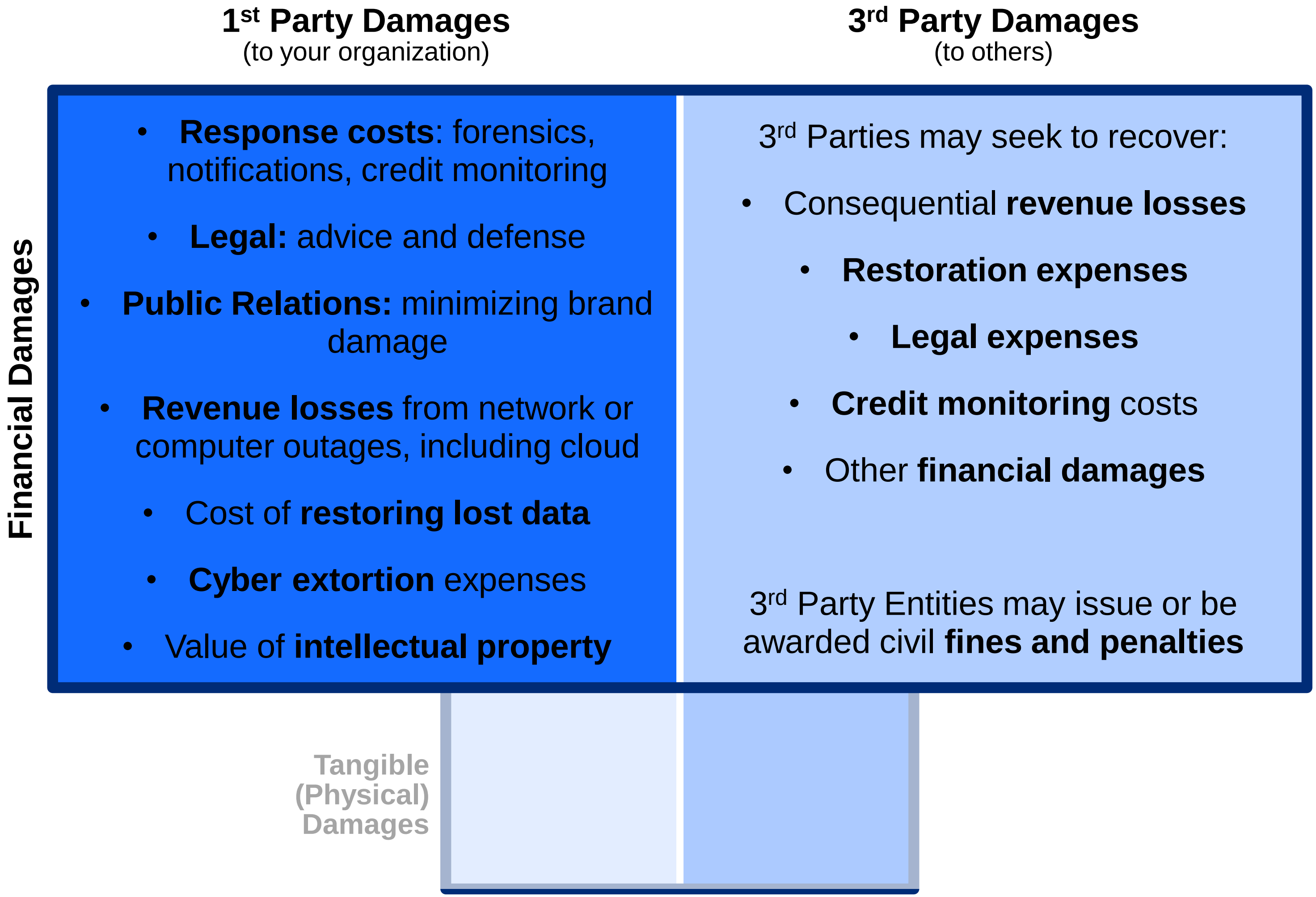
CYBER-EXTORTION.

ELECTRONIC CONTENT.

CYBER-TERRORISM.

Pure Financial Damage from a Cyber Event

Some of these impacts are data-breach centric; many could apply to any event



1st Party Damages
(to your organization)

3rd Party Damages
(to others)

Financial Damages

- **Response costs**: forensics, notifications, credit monitoring
- **Legal:** advice and defense
- **Public Relations:** minimizing brand damage
- **Revenue losses** from network or computer outages, including cloud
- Cost of **restoring lost data**
- **Cyber extortion** expenses
- Value of **intellectual property**

3rd Parties may seek to recover:

- Consequential **revenue losses**
- **Restoration expenses**
- **Legal expenses**
- **Credit monitoring** costs
- Other **financial damages**

3rd Party Entities may issue or be awarded civil **fines and penalties**

Tangible (Physical) Damages

Standard Cyber Coverages & Exclusions

First Party

- Data Breach Response
- Data Restoration
- Network Business Interruption
- Cyber Extortion

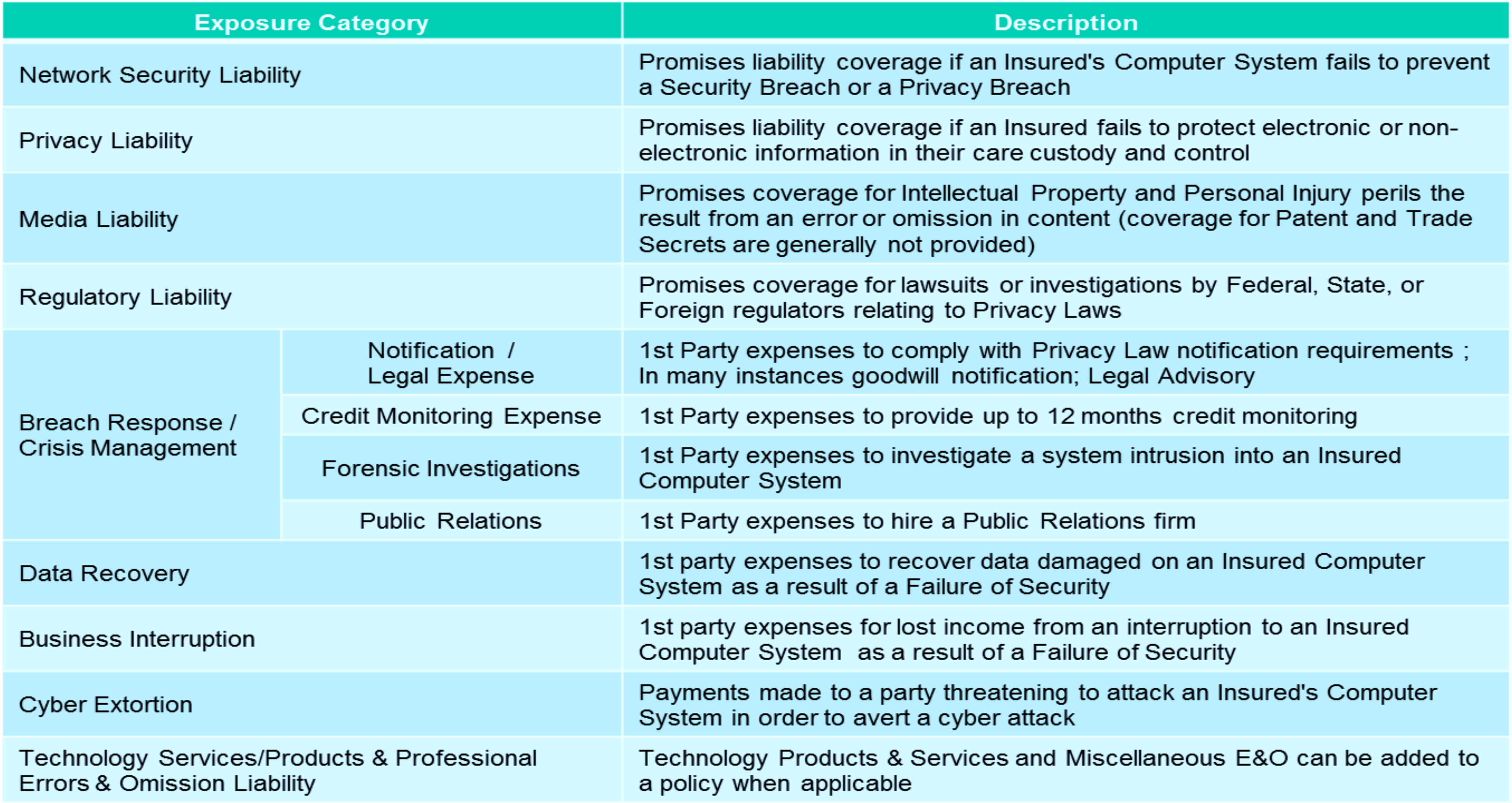
Third Party

- Privacy Liability
- Network Security Liability
- Privacy Regulatory Defense Costs
- Media Liability

General Exclusions

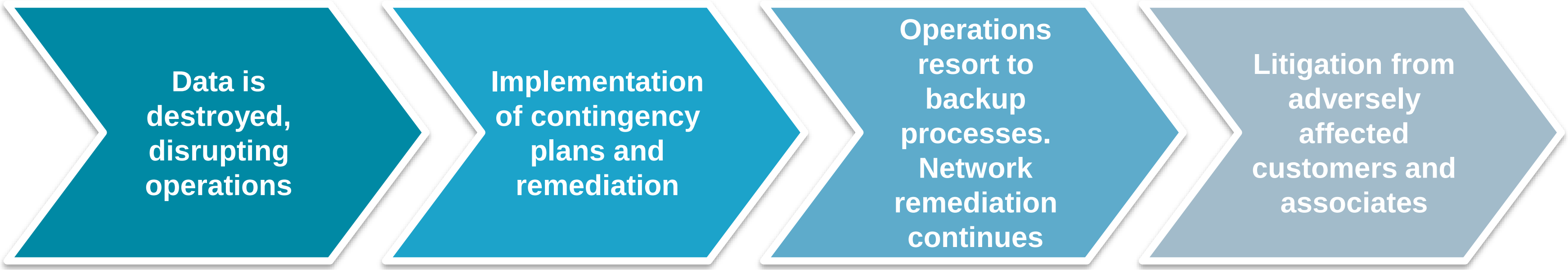
- Intellectual property
- Loss of personal device
- Bodily injury and property damage
- War (possible cyber terrorism carveback)
- Third party provider
- D&O criminal activity

The Insurance Policy



Exposure Category		Description
Network Security Liability		Promises liability coverage if an Insured's Computer System fails to prevent a Security Breach or a Privacy Breach
Privacy Liability		Promises liability coverage if an Insured fails to protect electronic or non-electronic information in their care custody and control
Media Liability		Promises coverage for Intellectual Property and Personal Injury perils the result from an error or omission in content (coverage for Patent and Trade Secrets are generally not provided)
Regulatory Liability		Promises coverage for lawsuits or investigations by Federal, State, or Foreign regulators relating to Privacy Laws
Breach Response / Crisis Management	Notification / Legal Expense	1st Party expenses to comply with Privacy Law notification requirements ; In many instances goodwill notification; Legal Advisory
	Credit Monitoring Expense	1st Party expenses to provide up to 12 months credit monitoring
	Forensic Investigations	1st Party expenses to investigate a system intrusion into an Insured Computer System
	Public Relations	1st Party expenses to hire a Public Relations firm
Data Recovery		1st party expenses to recover data damaged on an Insured Computer System as a result of a Failure of Security
Business Interruption		1st party expenses for lost income from an interruption to an Insured Computer System as a result of a Failure of Security
Cyber Extortion		Payments made to a party threatening to attack an Insured's Computer System in order to avert a cyber attack
Technology Services/Products & Professional Errors & Omission Liability		Technology Products & Services and Miscellaneous E&O can be added to a policy when applicable

How Would Cyber Insurance Respond to NotPetya?



Data is destroyed, disrupting operations

- Coverage triggers as a result of the security failures, including any voluntary shutdown to mitigate harm.
- Policy reimburses costs for retained counsel and computer forensic experts.

Implementation of contingency plans and remediation

- Policy reimburses cost of executing cyber incident response plan, including extra expense for redundant facilities.
- Mitigation costs include reasonable cost to replace data.

Operations resort to backup processes. Network remediation continues

- Reimburses revenue lost from reduced efficiency, including expense of retaining additional personal.
- Extra expense also includes cost of forensic accounting to documentation to document the loss

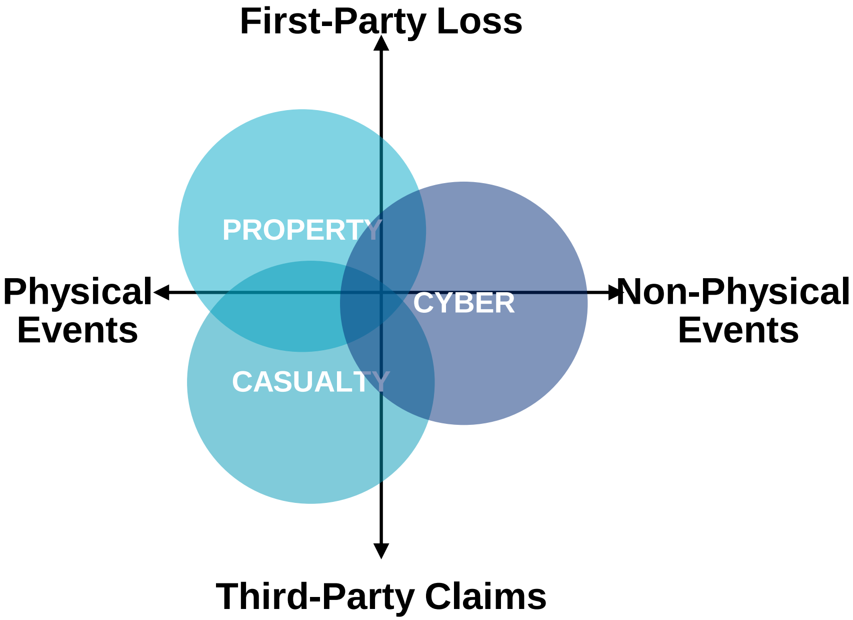
Litigation from adversely affected customers and associates

- Reimburses defense costs and damages.
- Reimburses legal costs from any regulatory investigation.

Risk Transfer Options

Keys to Program Alignment

- P&C tower generally focuses on physical events, while the cyber tower focuses on non-physical events.
- As cyber events become more complex, the potential for conflict between in P&C, crime, and other towers with the cyber tower increases.
- Sometimes overlap is inevitable, and may even be desirable.
- Important to recognize and mitigate coverage gaps
- Other Insurance clauses for all programs should always be aligned.



Cyber - Physical Event

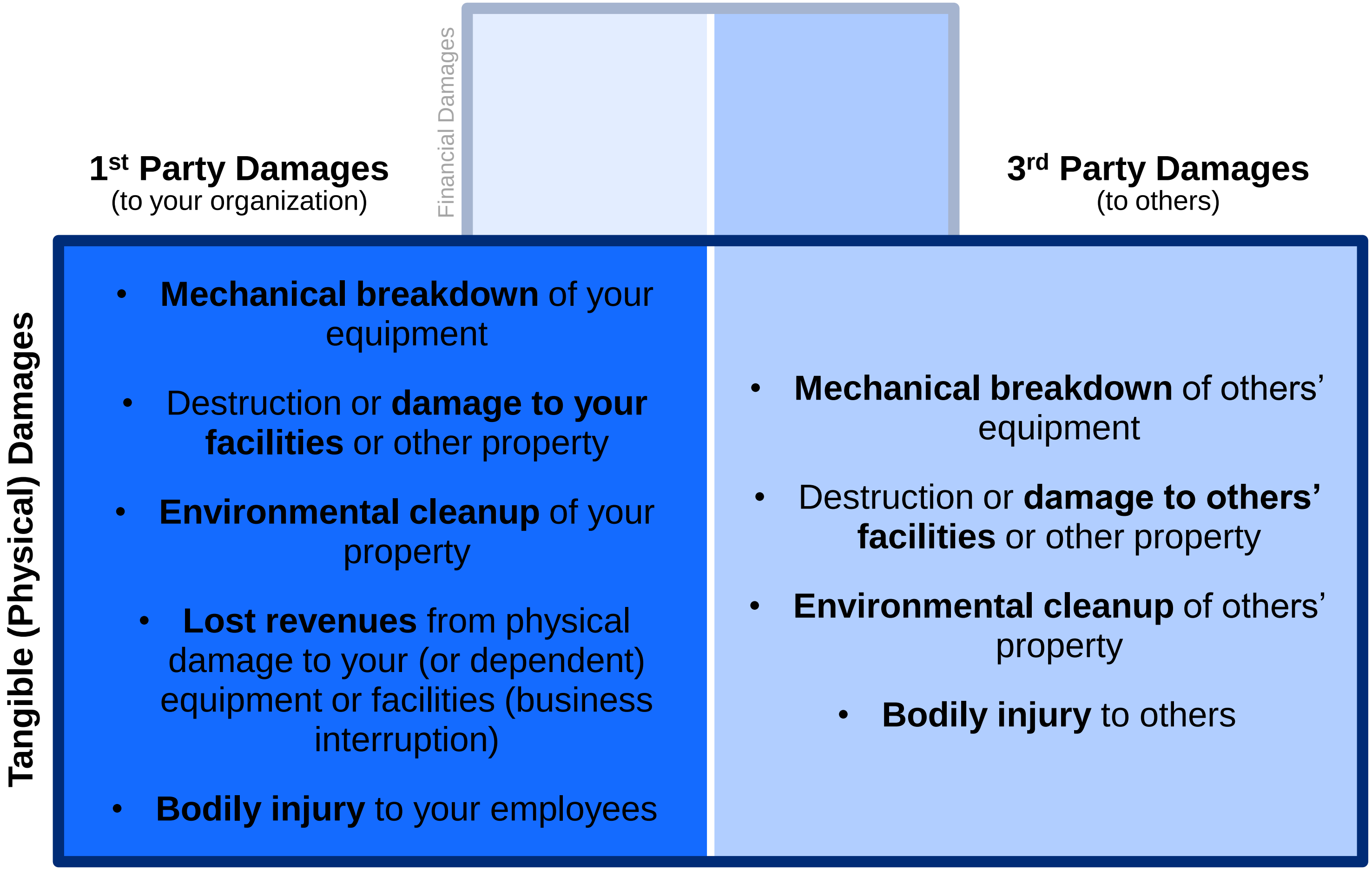
Bodily Injury and Property Damage Typically Not Covered by Cyber Policy

Cyber event causing property damage and bodily injury typically excluded by maritime policies

- CL380 – AIMU Cyber Attack Exclusion Clause

Physical Damage from a Cyber Event

These are concerning cyber risks for industrial companies or maritime activities



1st Party Damages
(to your organization)

3rd Party Damages
(to others)

Financial Damages

Tangible (Physical) Damages

- **Mechanical breakdown** of your equipment
- Destruction or **damage to your facilities** or other property
- **Environmental cleanup** of your property
- **Lost revenues** from physical damage to your (or dependent) equipment or facilities (business interruption)
- **Bodily injury** to your employees

- **Mechanical breakdown** of others' equipment
- Destruction or **damage to others' facilities** or other property
- **Environmental cleanup** of others' property
- **Bodily injury** to others

Cyber Coverage Gaps in the Marine Sector

Institute Cyber Attack Exclusion Clause CL 380

1.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss, damage, liability, or expense directly or indirectly caused by, or contributed to by, or arising from, the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

Possible Solutions

- ✓ Marine Policy with Affirmative Cyber Cover
- ✓ CL 380 Carvebacks
- ✓ Wraps / Difference in Condition
- ✓ Standalone Cyber Policy with BI/PD Cover
- ✓ Indemnity Provisions

Indemnity Provisions

Service Provider Provision

Service Provider shall defend, indemnify and hold harmless Client … from and against any and all claims, demands, suits, judgments, losses, liabilities, damages, costs or expenses of any nature whatsoever … caused solely by any: (i) negligent act or omission of Service Provider, its officers, directors, agents or employees; (ii) failure of Service Provider to perform the Services in accordance with generally accepted professional standards; or (iii) breach of Service Provider's representations and warranties, agreements, duties or obligations as set forth in this Agreement.

Coverage Complexity

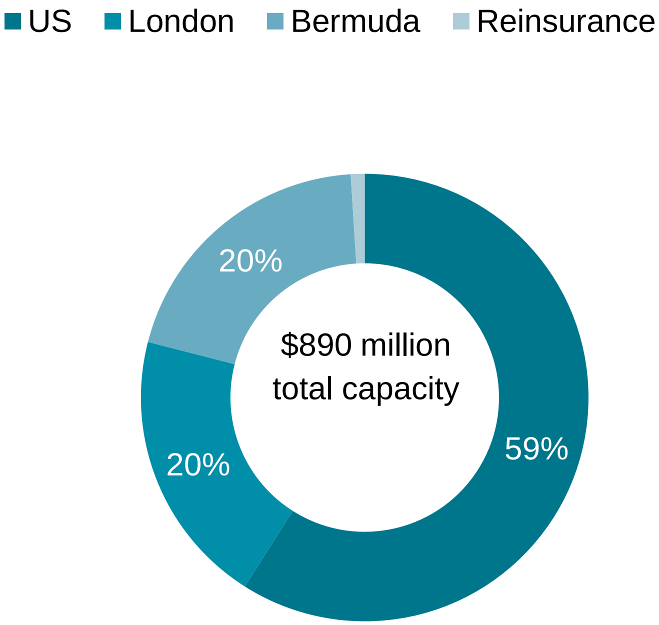
INCREASING SOPHISTICATION

COVERAGE SPECTRUM	RISKS
BASIC CYBER POLICY	▪ Event management ▪ Data privacy breaches ▪ Network security liability ▪ Privacy regulatory investigations ▪ Cyber extortion ▪ IT network business interruption ▪ Restoration of data and cyber assets
TAILORED CYBER POLICY	▪ System failure business interruption ▪ OT system business interruption and security ▪ IoT & product security risk ▪ Network security regulatory investigations ▪ Dependent network interruption
P&C, CYBER EXCESS DIC, OR CYBER GAP EXCLUSION BUYBACK	▪ 1st party property damage ▪ Bodily injury / 3rd party property damage ▪ Intellectual property risks

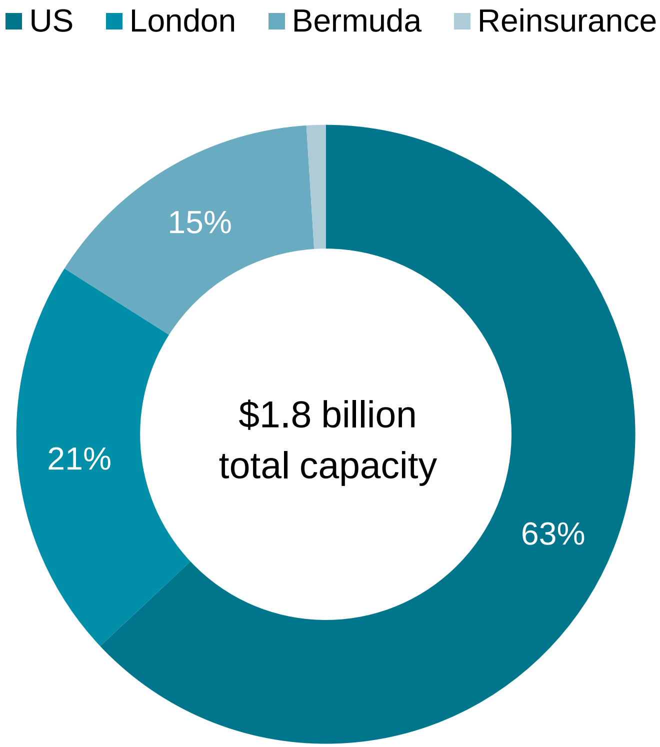
Market Capacity

Marsh’s recent survey of capacity for large purchasers indicates notional cyber capacity – stated but not necessarily deployed – is approximately $1.8 billion. Through 2017, there were many large towers placed between $200 million and $700 million in limits. Insurers are increasingly willing to deploy large lines either in single layers or with ventilation.

2014 MARKET CAPACITY



2018 MARKET CAPACITY



Ten Tips for Managing Your Cyber Risks

1. Examine Cyber Hygiene, including 3rd Party relationships
2. Check your response and recovery plan activities
3. Quantify potential exposures and response costs
4. Be careful in applications for coverage
5. Look for symmetry with other insurance (*e.g*., CGL, Crime, D&O, All Risk)
6. Look for endorsements for special coverage needs (e.g., cloud providers)
7. Identify gaps, including sub-limits and carve outs
8. Beware conditions on "reasonable“ cyber security measures
9. Pay attention to Business Interruption, including how it is measured
10. Give Notice!

QUESTIONS

Daniel J. Healy, Esq.
Partner
Anderson Kill
(202) 416-6547
dhealy@andersonkill.com

Stephen R. Viña
Senior Vice President
Marsh
(212) 345-0399
stephen.vina@marsh.com

MARSH

ANDERSON KILL
ATTORNEYS AND COUNSELORS AT LAW

The views expressed by the participants in this program are not those of the participants' employers, their clients, or any other organization. The opinions expressed do not constitute legal advice, or risk management advice. The views discussed are for educational purposes only, and provided only for use during this session.