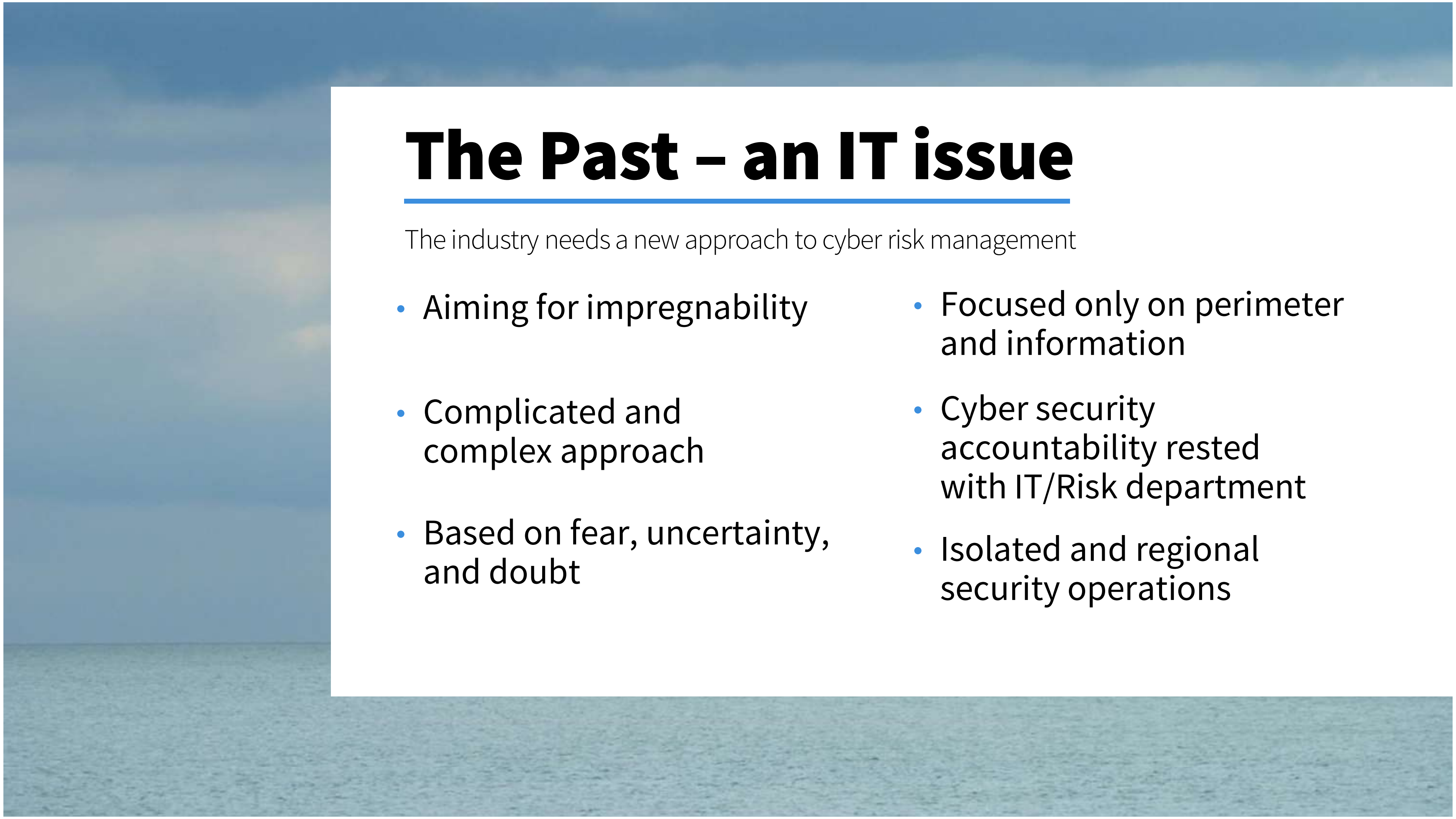
Cyber Security in the Shipping Industry

JP Cavanna Lloyd's Register

23 October 2018

Agenda

- An overview of the evolution of cyber security and its management today
- Vulnerabilities in the shipping sector
- What do cyber attacks typically look like?
- How can we as businesses make ourselves more resilient to attacks?



The Past – an IT issue

The industry needs a new approach to cyber risk management

- Aiming for impregnability
- Complicated and complex approach
- Based on fear, uncertainty, and doubt
- Focused only on perimeter and information
- Cyber security accountability rested with IT/Risk department
- Isolated and regional security operations

Vulnerabilities in the shipping industry

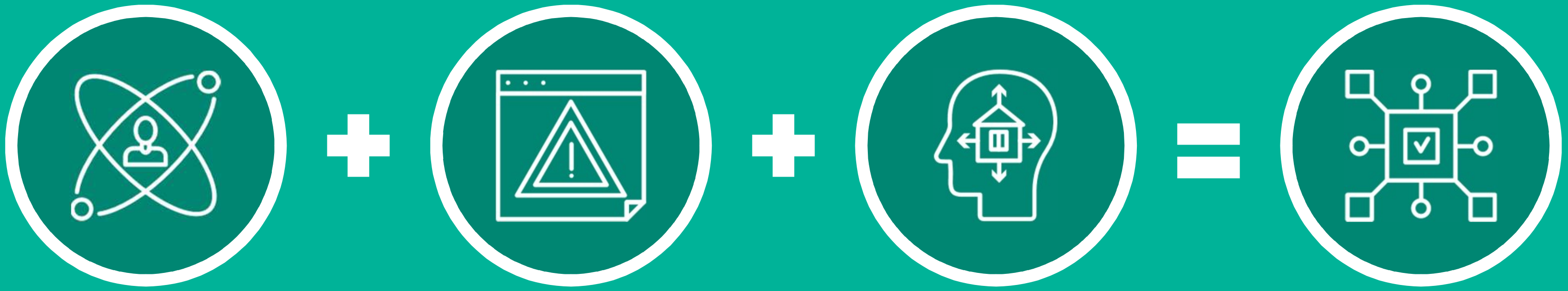
Technology is transforming the marine world

Advanced manufacturing
Advanced materials
Autonomous systems
Big data analytics
Carbon capture and storage
C
Carbon
Communications
Cyber and electronic warfare
Deep ocean mining
Energy management
Human augmentation
Human computer interaction
Marine biotechnology
Propulsion
Robotics
Sensors
Shipbuilding techniques
Smart ship
Sustainable energy

=

- ✓ Reduce costs
- ✓ Increase operational efficiencies
- ✓ Enhance safety
- ✓ Become more sustainable
- ✓ Reduce environmental impacts

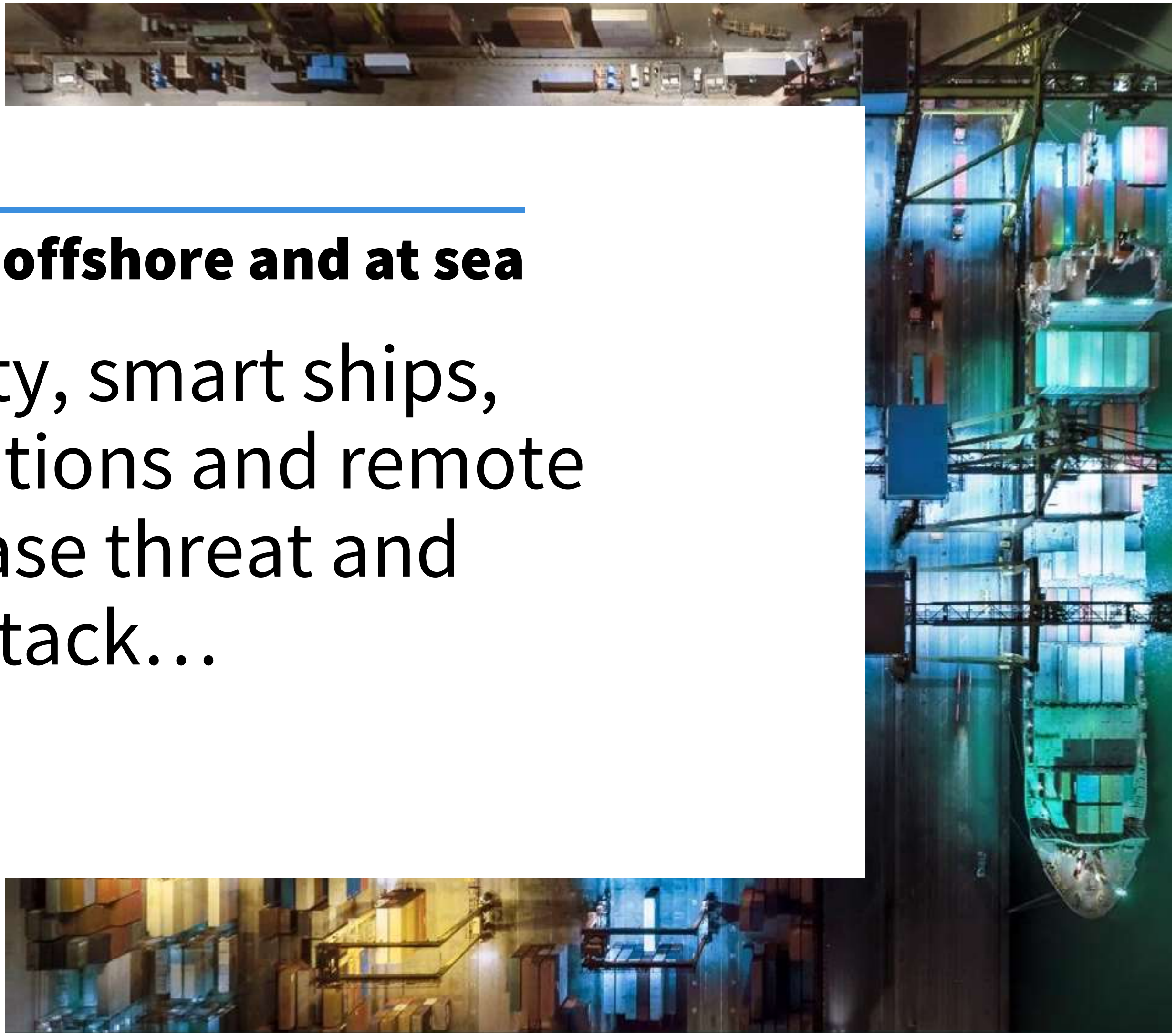
With more opportunity, comes more risk



New technology + Autonomy + Connected environments = More risk

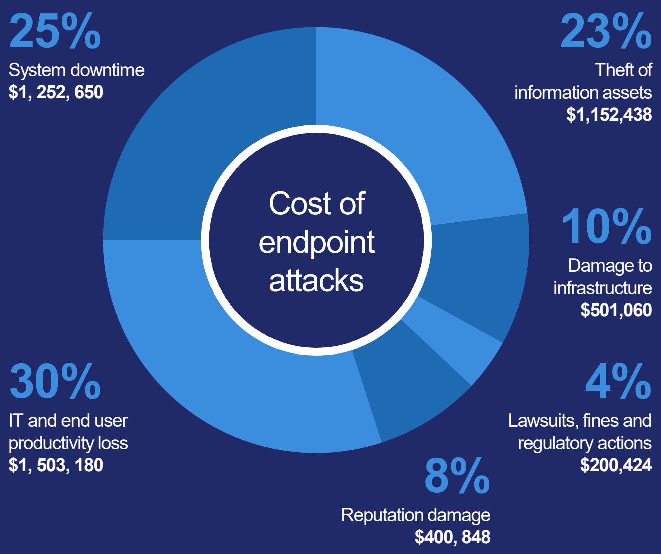
Risks exist onshore, offshore and at sea

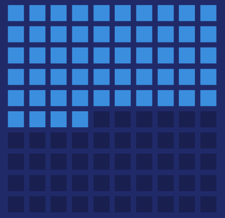
VSAT connectivity, smart ships, intelligent operations and remote control all increase threat and risk of a cyber attack…



Cyber-attacks are on the rise

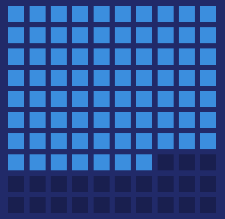
70% of organisations say their security risk increased significantly in 2017, with **more attacks** than the previous four years





54%

of companies experienced one or more successful attacks that compromised data and/or IT infrastructure

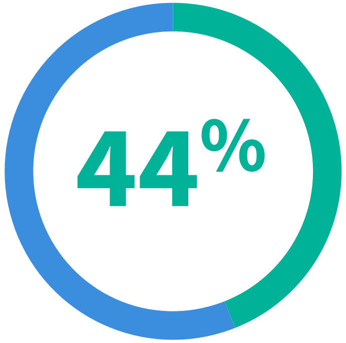


77%

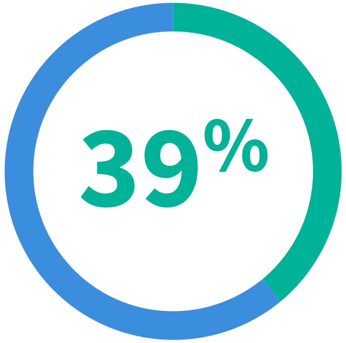
of those attacks utilised exploits or fireless techniques

Source: AIG EMEA (2013-2017)
Source: https://blog.barkly.com/2018-cybersecurity-statistics

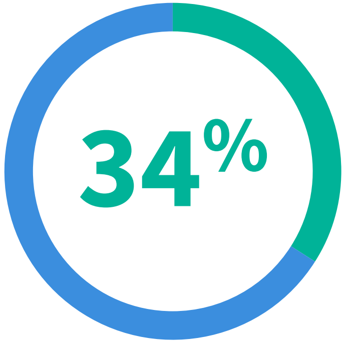
The marine industry knows it needs to act...



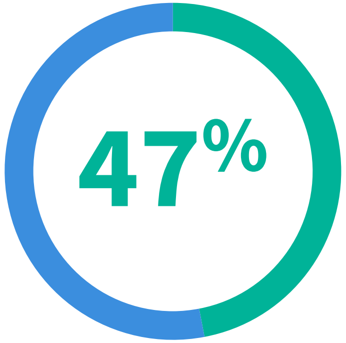
of ship operators believe current IT defences are not effective*



experienced a cyber-attack in the last 12 months*



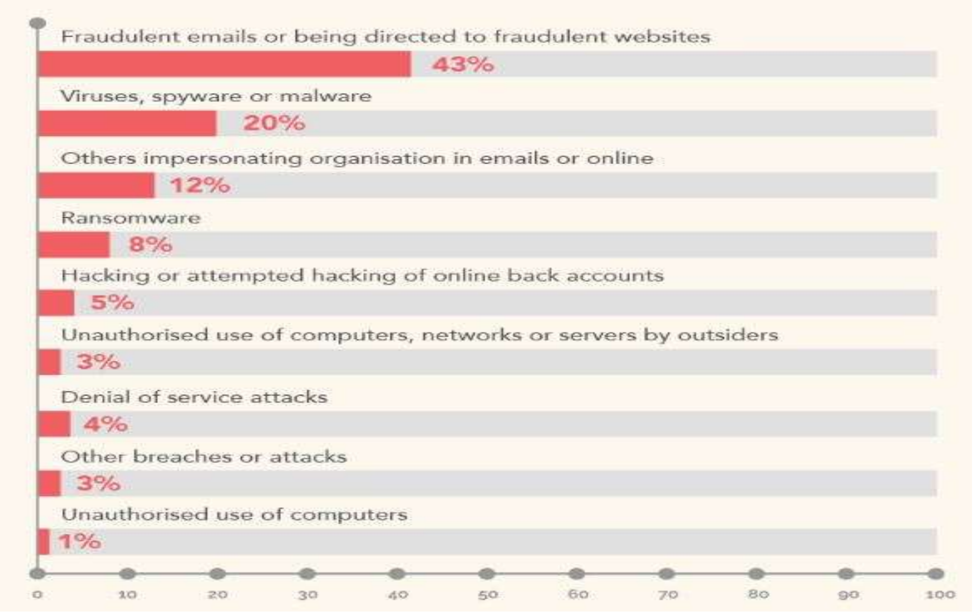
didn’t have an IT security policy**

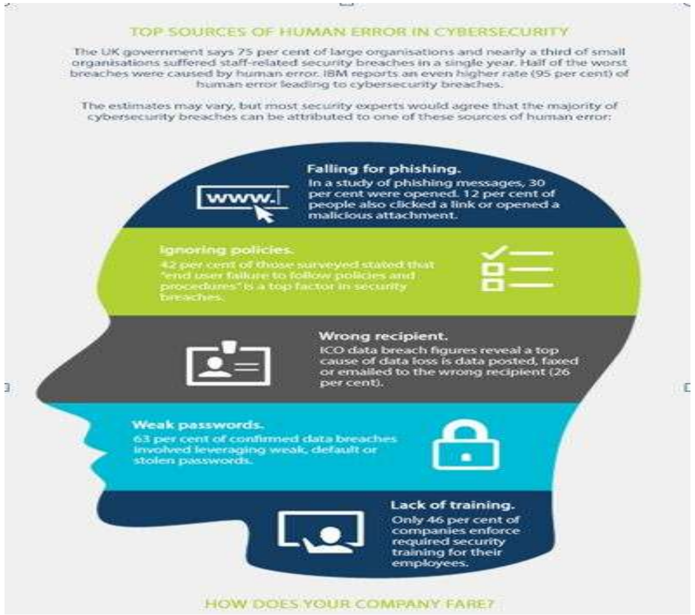


believed the biggest cyber vulnerability was their staff**

*Source: Futurenautics
**Source: www.maritime-executive.com cyber-security-at-sea-the-real-threats

The more immediate threat…?





TOP SOURCES OF HUMAN ERROR IN CYBERSECURITY

The UK government says 75 per cent of large organisations and nearly a third of small organisations suffered staff-related security breaches in a single year. Half of the worst breaches were caused by human error. IBM reports an even higher rate (95 per cent) of human error leading to cybersecurity breaches.

The estimates may vary, but most security experts would agree that the majority of cybersecurity breaches can be attributed to one of these sources of human error:

Falling for phishing. In a study of phishing messages, 30 per cent were opened. 12 per cent of people also clicked a link or opened a malicious attachment.

Ignoring policies. 42 per cent of those surveyed stated that "end user failure to follow policies and procedures" is a top factor in security breaches.

Wrong recipient. ICO data breach figures reveal a top cause of data loss is data posted, faxed or emailed to the wrong recipient (26 per cent).

Weak passwords. 63 per cent of confirmed data breaches involved leveraging weak, default or stolen passwords.

Lack of training. Only 46 per cent of companies enforce required security training for their employees.

HOW DOES YOUR COMPANY FARE?

…and perception

Cyber Security Maturity Scale Based on CMMI

Level 0 Nothing in place	Level 1 Initial	Level 2 Managed	Level 3 Defined	Level 4 Quantitatively Managed	Level 5 Optimising
Industry Self-Perception		**Maturity Level 2.5 – 3.0**	The Reality		**Maturity Level 0.9 – 1.2**

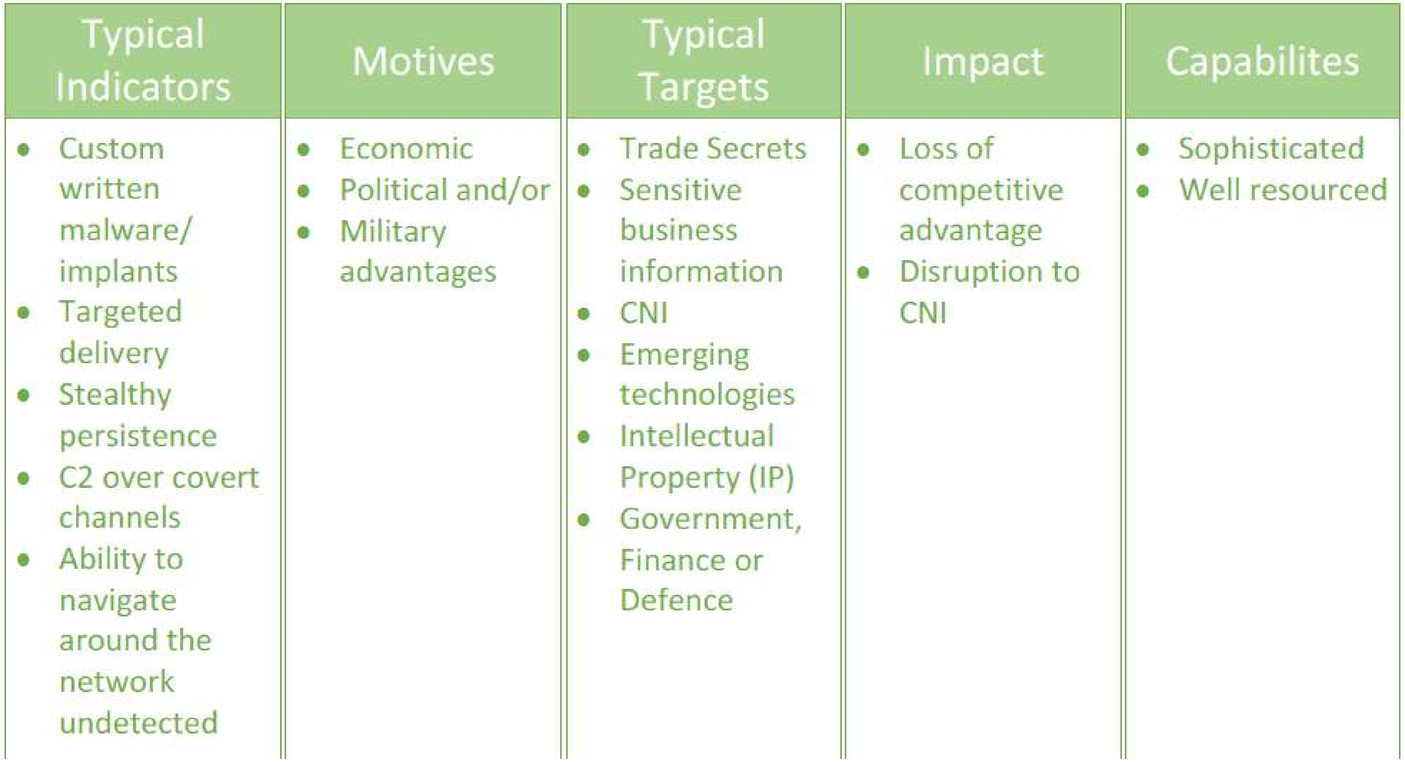
The above is based on aggregation of data from industry verticals including FSI, Pharma, Energy, Oil & Gas and Telecomms,

The Threat Landscape

Motivation and capability

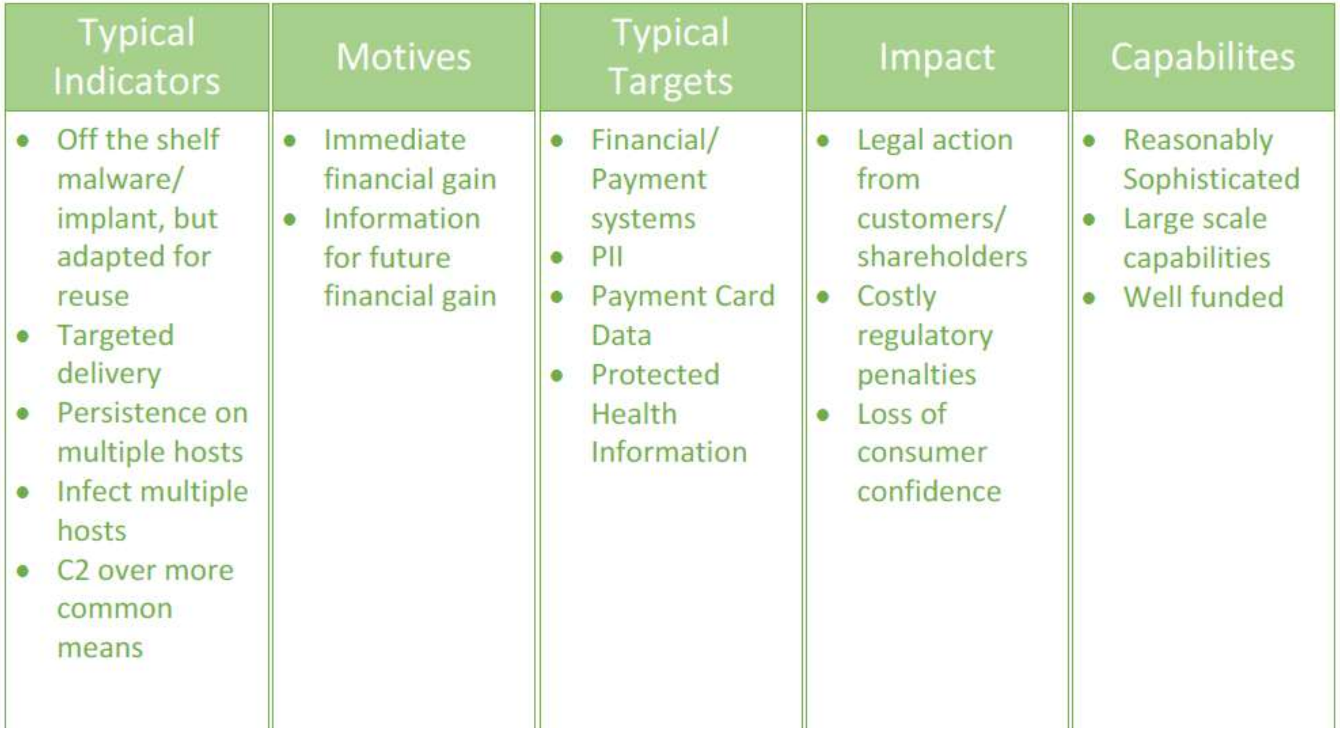
- State Sponsored Threat Actors
- Organised Cyber Crime
- Disorganised Cyber Crime
- Hactivists
- Lone wolf/Insiders

State Sponsored Threat Actors

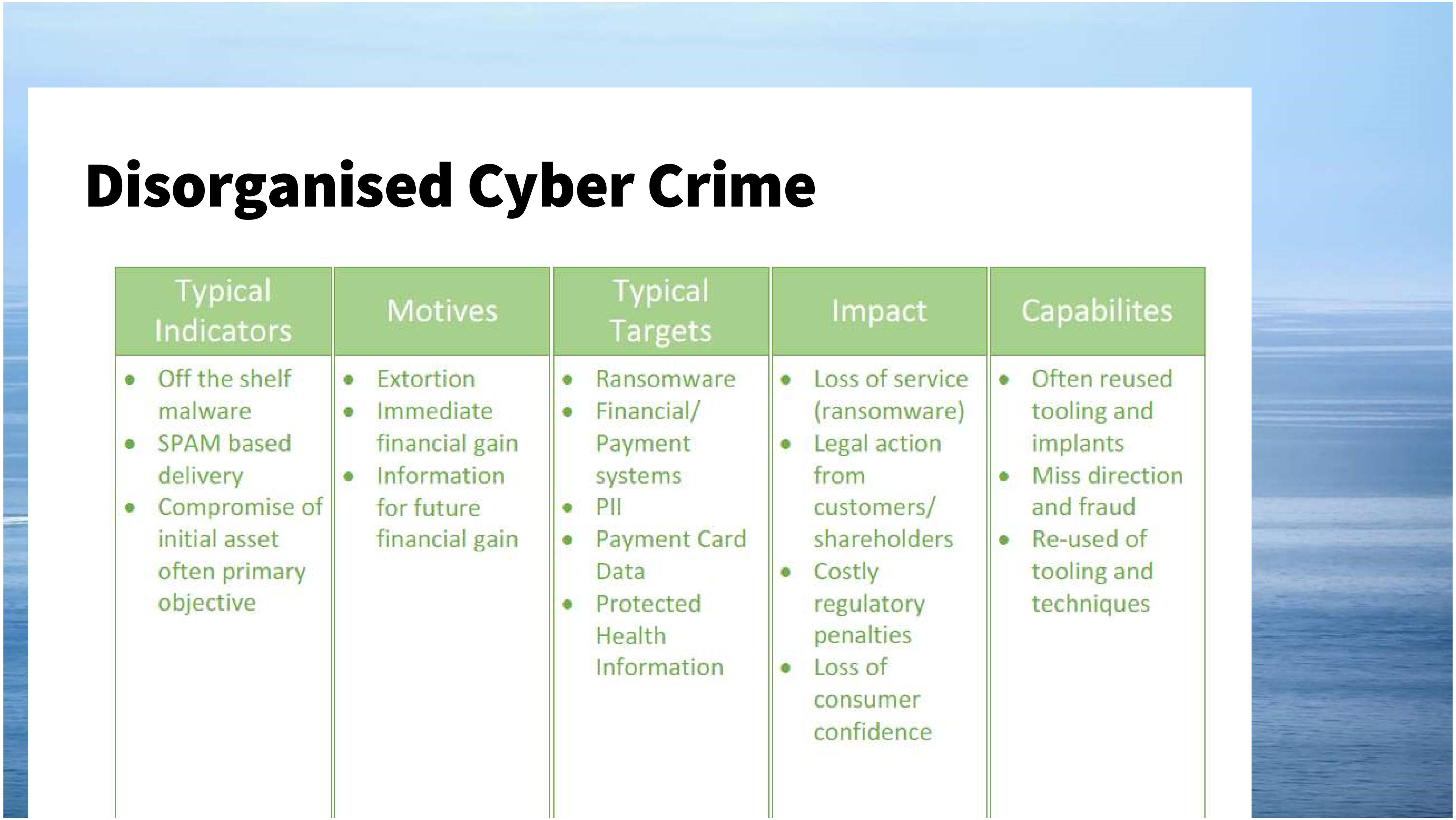


Typical Indicators	Motives	Typical Targets	Impact	Capabilites
• Custom written malware/ implants • Targeted delivery • Stealthy persistence • C2 over covert channels • Ability to navigate around the network undetected	• Economic • Political and/or • Military advantages	• Trade Secrets • Sensitive business information • CNI • Emerging technologies • Intellectual Property (IP) • Government, Finance or Defence	• Loss of competitive advantage • Disruption to CNI	• Sophisticated • Well resourced

Organised Cyber Crime

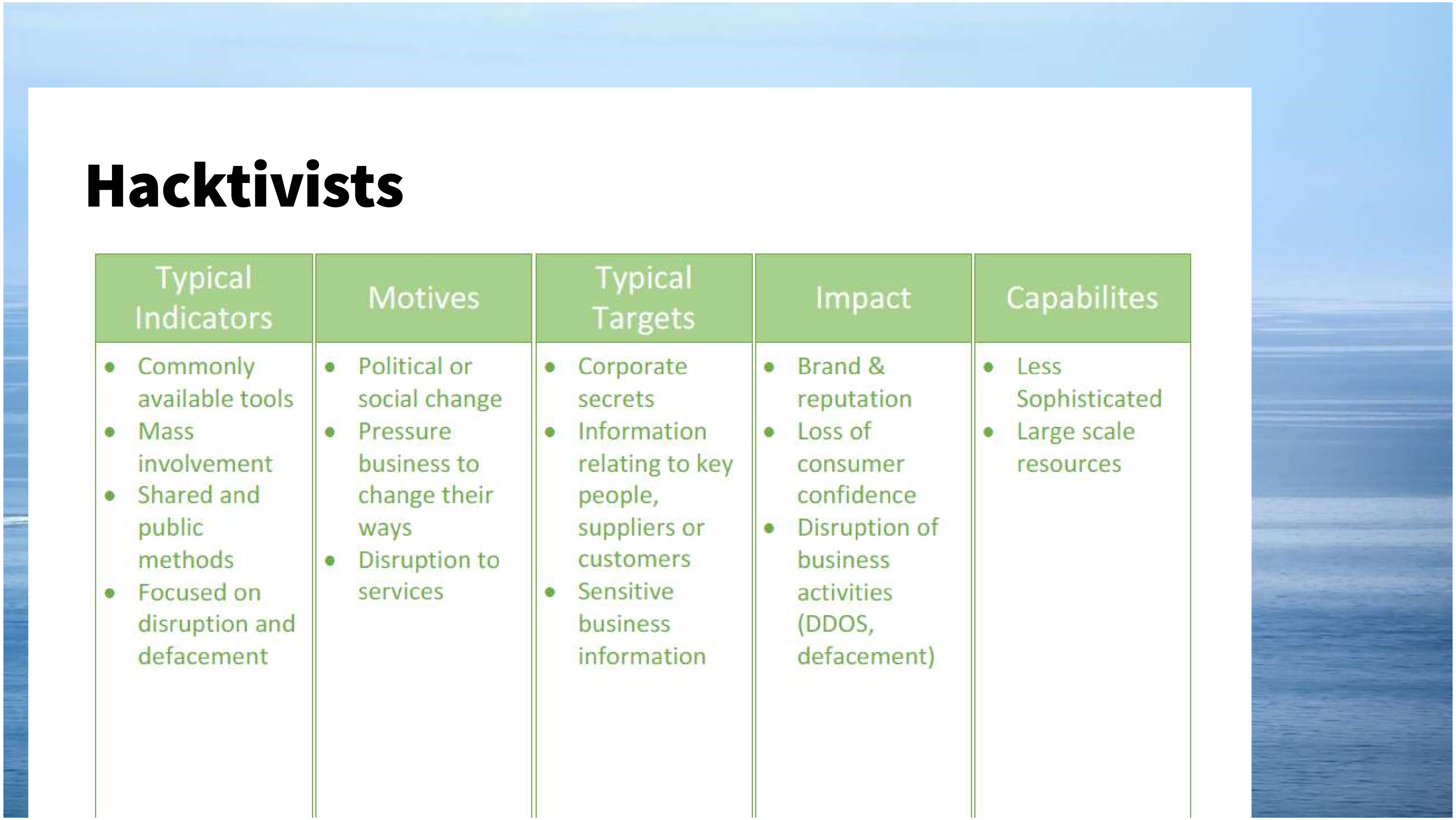


Typical Indicators	Motives	Typical Targets	Impact	Capabilites
• Off the shelf malware/ implant, but adapted for reuse • Targeted delivery • Persistence on multiple hosts • Infect multiple hosts • C2 over more common means	• Immediate financial gain • Information for future financial gain	• Financial/ Payment systems • PII • Payment Card Data • Protected Health Information	• Legal action from customers/ shareholders • Costly regulatory penalties • Loss of consumer confidence	• Reasonably Sophisticated • Large scale capabilities • Well funded



Disorganised Cyber Crime

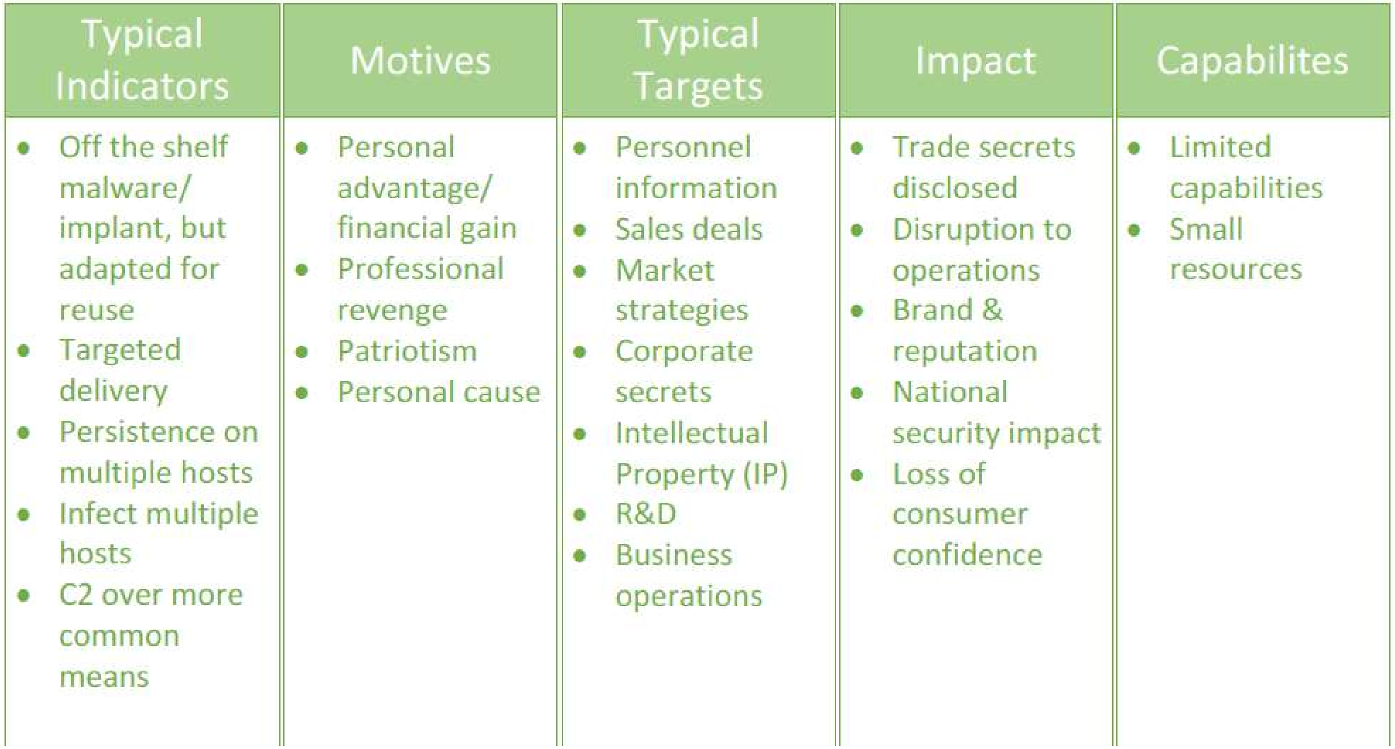
Typical Indicators	Motives	Typical Targets	Impact	Capabilites
• Off the shelf malware • SPAM based delivery • Compromise of initial asset often primary objective	• Extortion • Immediate financial gain • Information for future financial gain	• Ransomware • Financial/ Payment systems • PII • Payment Card Data • Protected Health Information	• Loss of service (ransomware) • Legal action from customers/ shareholders • Costly regulatory penalties • Loss of consumer confidence	• Often reused tooling and implants • Miss direction and fraud • Re-used of tooling and techniques



Hacktivists

Typical Indicators	Motives	Typical Targets	Impact	Capabilites
• Commonly available tools • Mass involvement • Shared and public methods • Focused on disruption and defacement	• Political or social change • Pressure business to change their ways • Disruption to services	• Corporate secrets • Information relating to key people, suppliers or customers • Sensitive business information	• Brand & reputation • Loss of consumer confidence • Disruption of business activities (DDOS, defacement)	• Less Sophisticated • Large scale resources

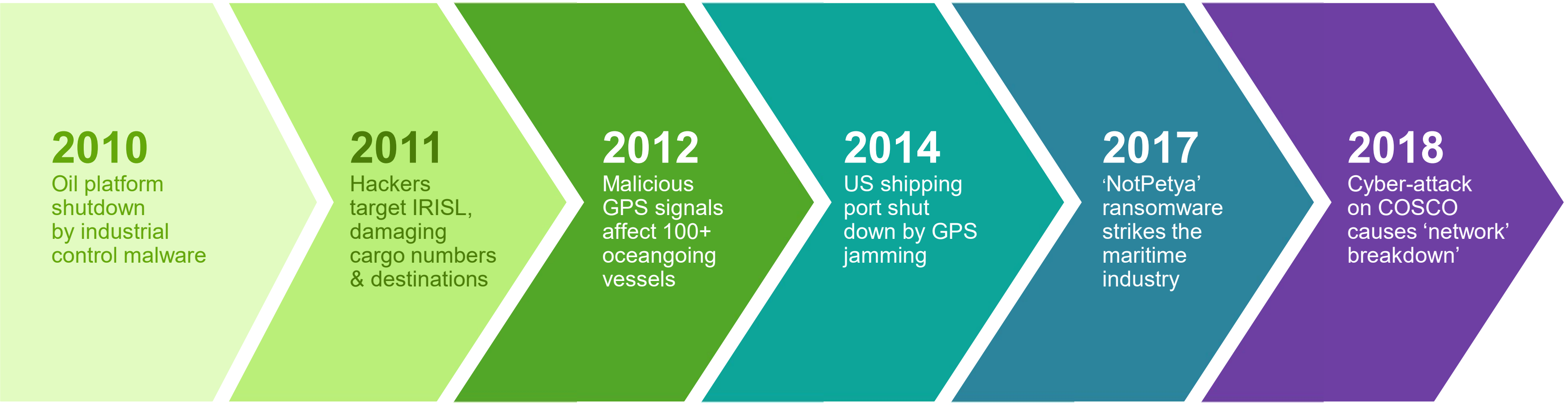
Lone wolf/Insiders



Typical Indicators	Motives	Typical Targets	Impact	Capabilites
• Off the shelf malware/ implant, but adapted for reuse • Targeted delivery • Persistence on multiple hosts • Infect multiple hosts • C2 over more common means	• Personal advantage/ financial gain • Professional revenge • Patriotism • Personal cause	• Personnel information • Sales deals • Market strategies • Corporate secrets • Intellectual Property (IP) • R&D • Business operations	• Trade secrets disclosed • Disruption to operations • Brand & reputation • National security impact • Loss of consumer confidence	• Limited capabilities • Small resources

Shipping is not immune

Cyber threats have increased in frequency and seriousness in recent years, demonstrating the need for greater cyber security measures.



2010
Oil platform shutdown by industrial control malware

2011
Hackers target IRISL, damaging cargo numbers & destinations

2012
Malicious GPS signals affect 100+ oceangoing vessels

2014
US shipping port shut down by GPS jamming

2017
'NotPetya' ransomware strikes the maritime industry

2018
Cyber-attack on COSCO causes 'network' breakdown'

Cosco Shipping Faces Ransomware Attack

Cosco July 2018

On July 24, 2018, a cyber-attack on the American region of China's state-run shipping company, Cosco Shipping Holdings, Co.

The cyber-incident has been chalked up to a "local network breakdown" in the Americas region, which impacted email and telephone. In a remedial step, the company cut communications with other regions, although operations were maintained.

The potential cost of inaction is high

$2.5 - $3bn

NotPetya Malware
total global losses

July 2017

"The impact of [NotPetya] is that we basically found that we had to reinstall an entire infrastructure… we had to install 4,000 new servers, 45,000 new PCs, 2,500 applications."

Maersk Chairman - Jim Hagemann Snabe

NOTPETYA MALWARE:

Cyberattack costs could hit $300m for shipping giant Maersk.

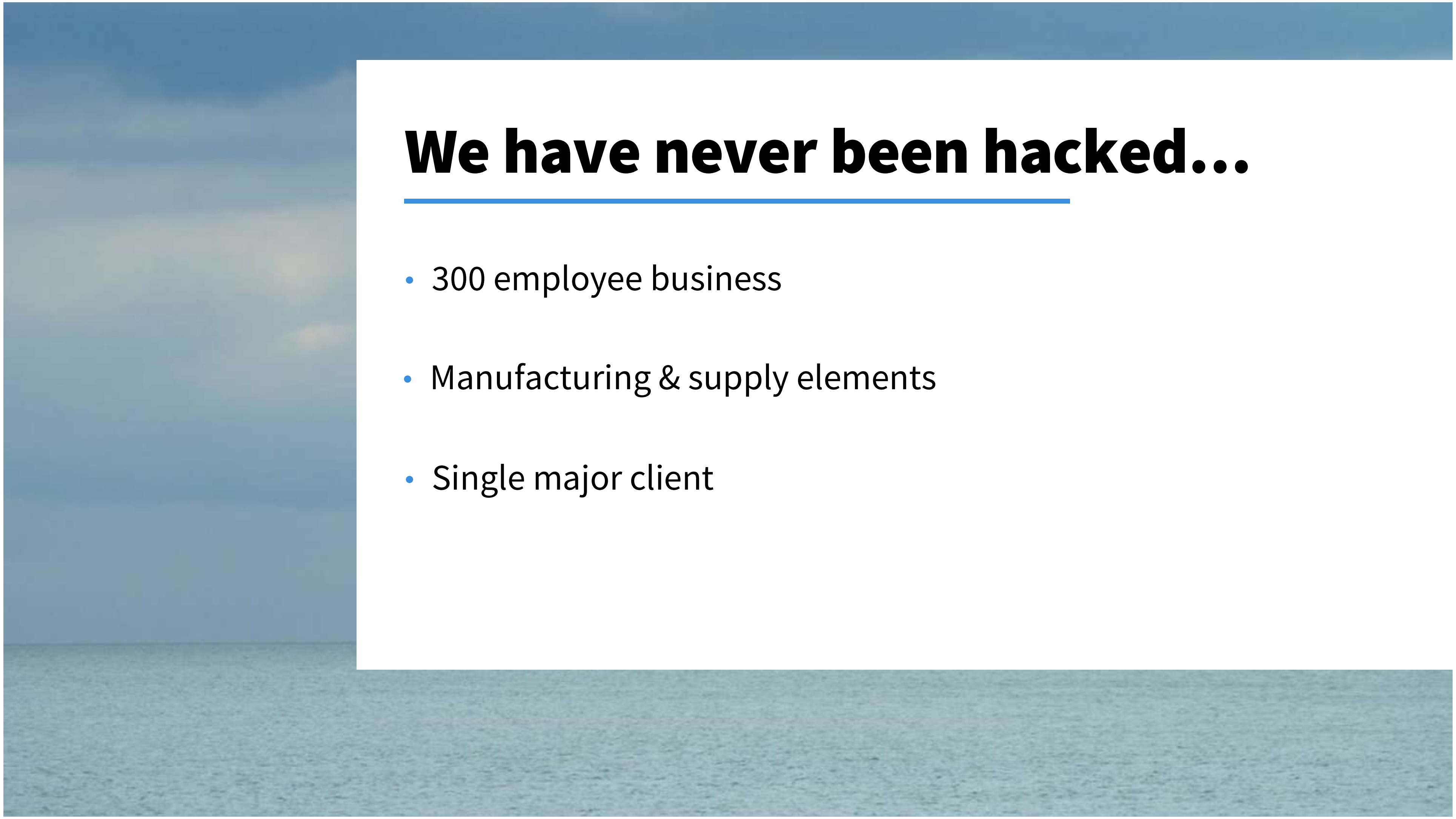
June's cyberattack will cost the international shipping firm hundreds of millions of dollars in lost revenue.

What do cyber attacks typically look like?

What is a cyber attack?

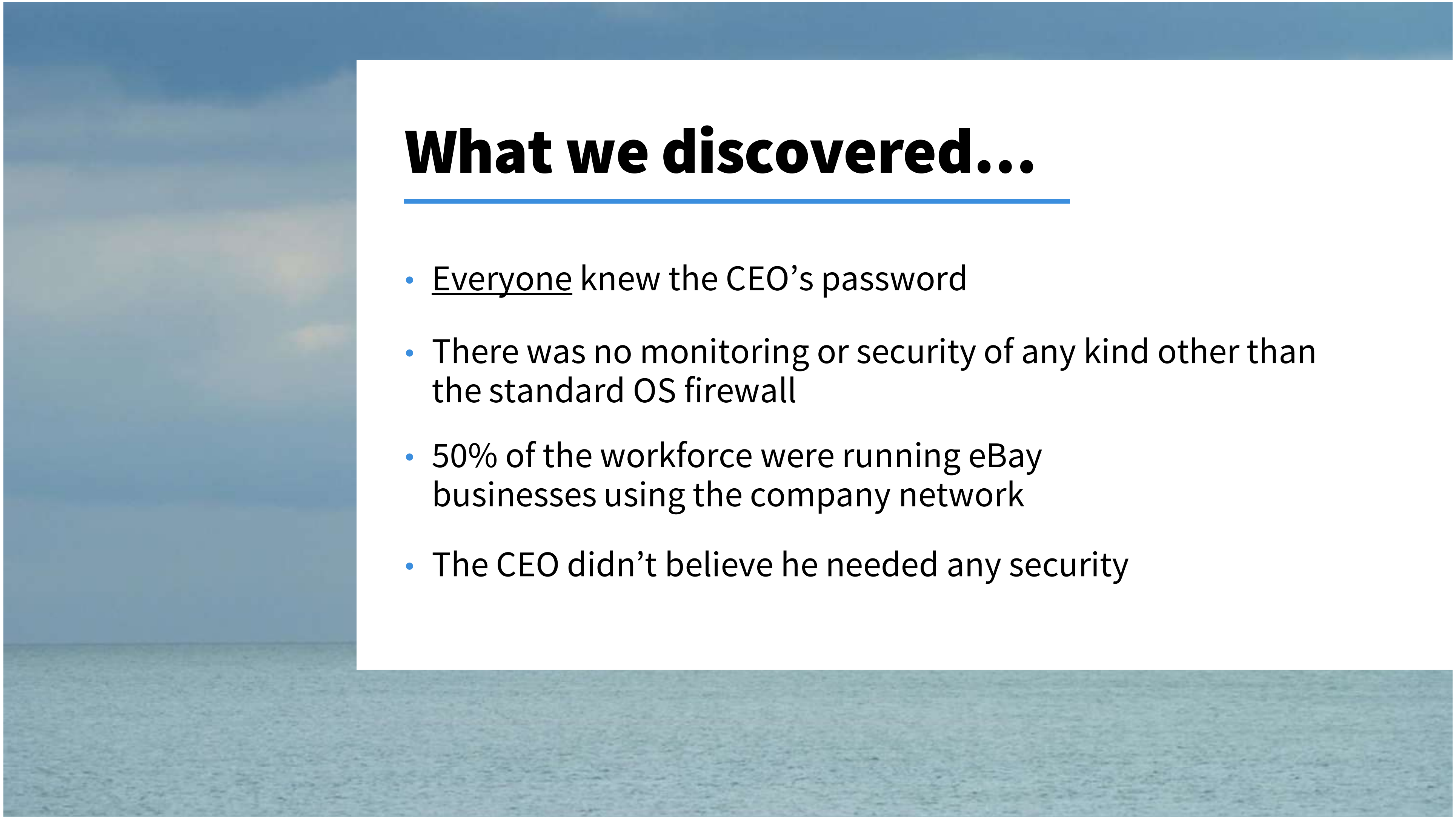
A cyberattack is a **malicious and deliberate attempt** by an individual or organisation **to breach** the information system of another individual or organisation.

Former Cisco CEO John Chambers once said, “There are two types of companies: those that have been hacked, and those who don’t yet know they have been hacked.”



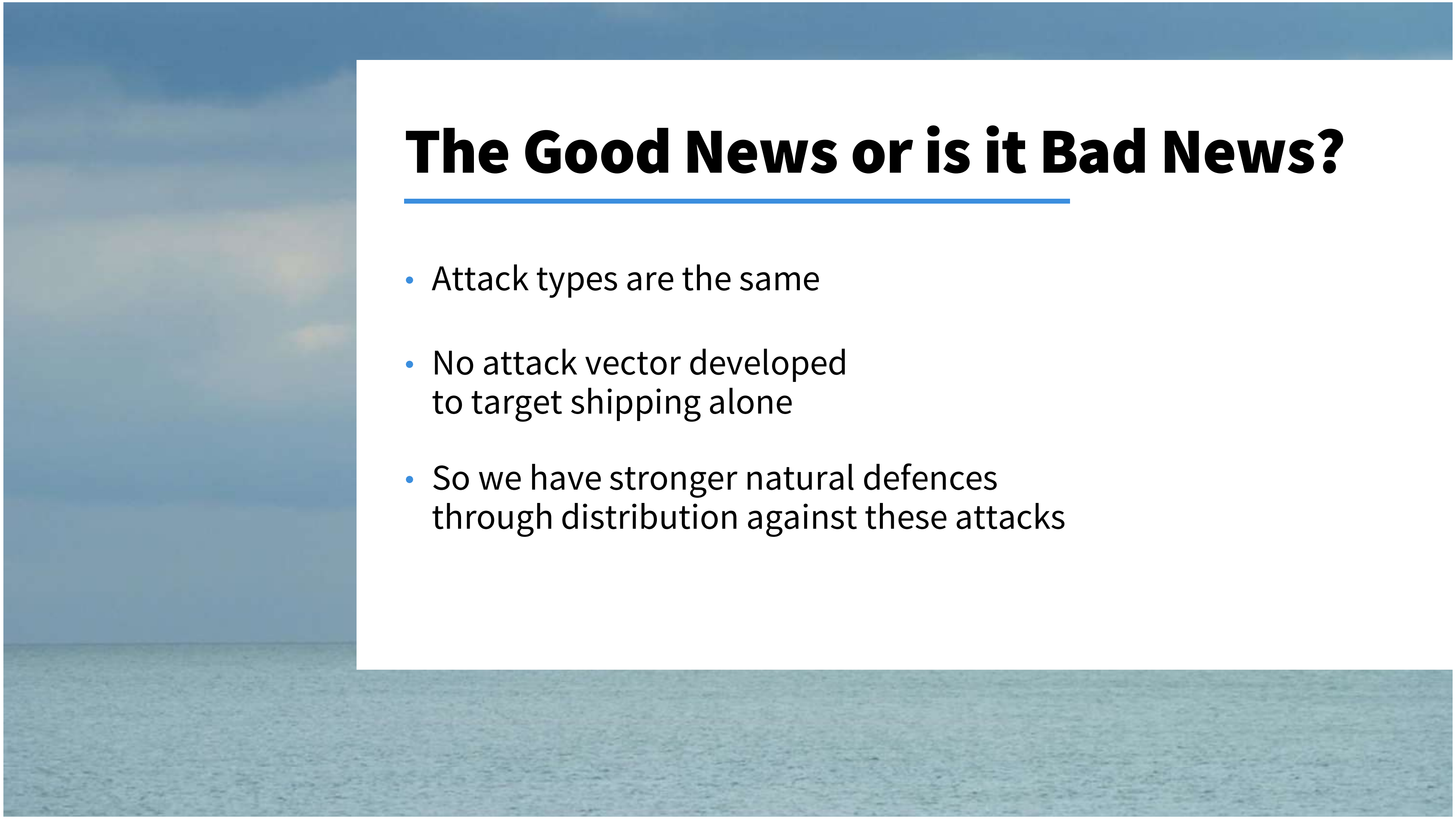
We have never been hacked…

- 300 employee business
- Manufacturing & supply elements
- Single major client



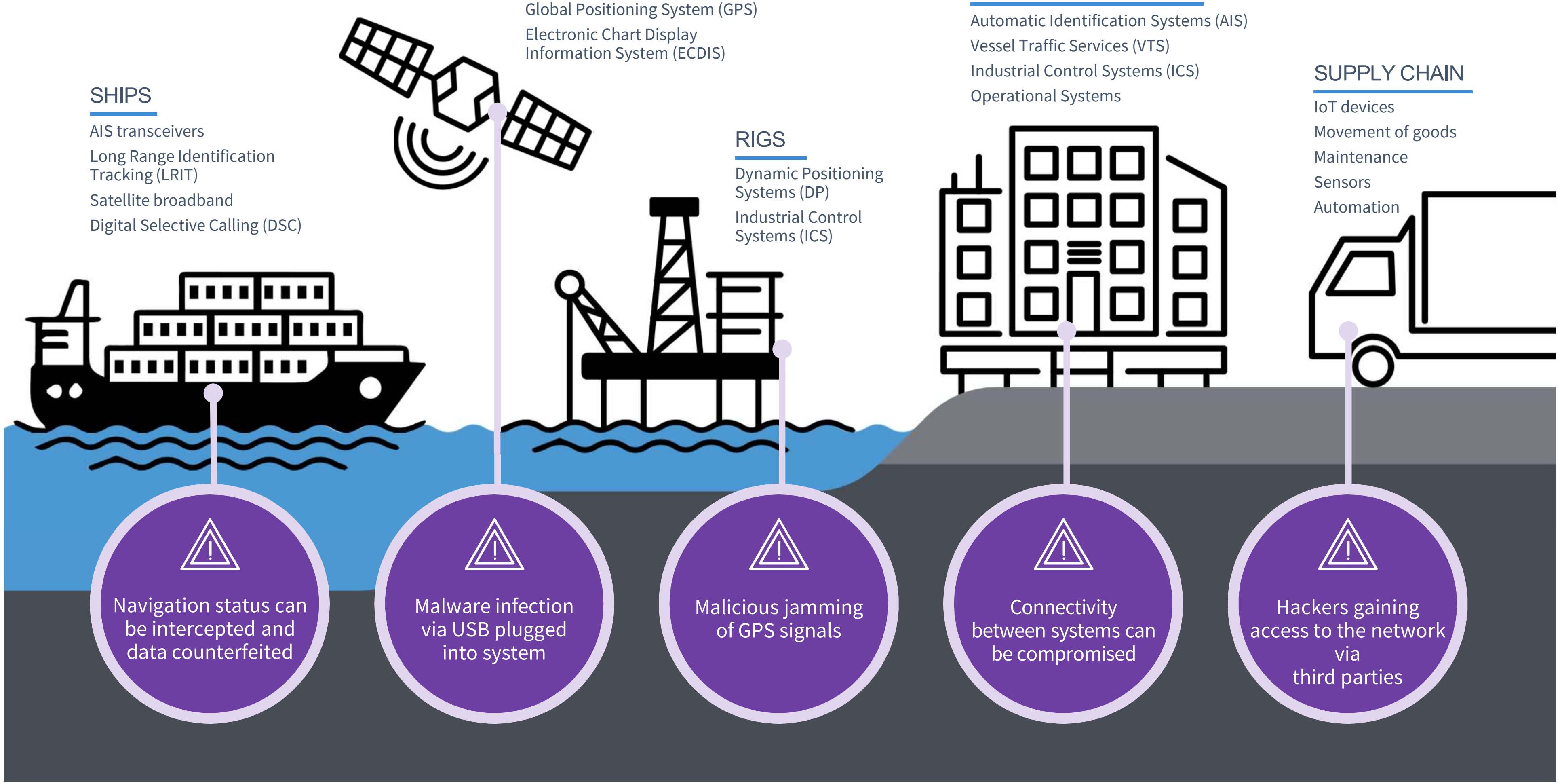
What we discovered…

- Everyone knew the CEO’s password
- There was no monitoring or security of any kind other than the standard OS firewall
- 50% of the workforce were running eBay businesses using the company network
- The CEO didn’t believe he needed any security



The Good News or is it Bad News?

- Attack types are the same
- No attack vector developed to target shipping alone
- So we have stronger natural defences through distribution against these attacks



SHIPS

AIS transceivers

Long Range Identification Tracking (LRIT)

Satellite broadband

Digital Selective Calling (DSC)

NAVIGATION

Global Navigation Satellite System (GNSS)

Global Positioning System (GPS)

Electronic Chart Display Information System (ECDIS)

RIGS

Dynamic Positioning Systems (DP)

Industrial Control Systems (ICS)

HARBOR/OPERATIONS

Automatic Identification Systems (AIS)

Vessel Traffic Services (VTS)

Industrial Control Systems (ICS)

Operational Systems

SUPPLY CHAIN

IoT devices

Movement of goods

Maintenance

Sensors

Automation

Navigation status can be intercepted and data counterfeited

Malware infection via USB plugged into system

Malicious jamming of GPS signals

Connectivity between systems can be compromised

Hackers gaining access to the network via third parties

Attack techniques

Some examples:

- **Malware**
- **Social Engineering**
- **Phishing**
- **Man in the middle**
- **Denial of Service**
- **Zero day exploit**
- **…**

Malware:

Malware is a term used to describe **malicious software**, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.

Once inside the system, malware can do the following:

- Block access to key components of the network (ransomware)
- Install malware or additional harmful software
- Covertly obtain information by transmitting data from the hard drive (spyware)
- Disrupt certain components and renders the system inoperable

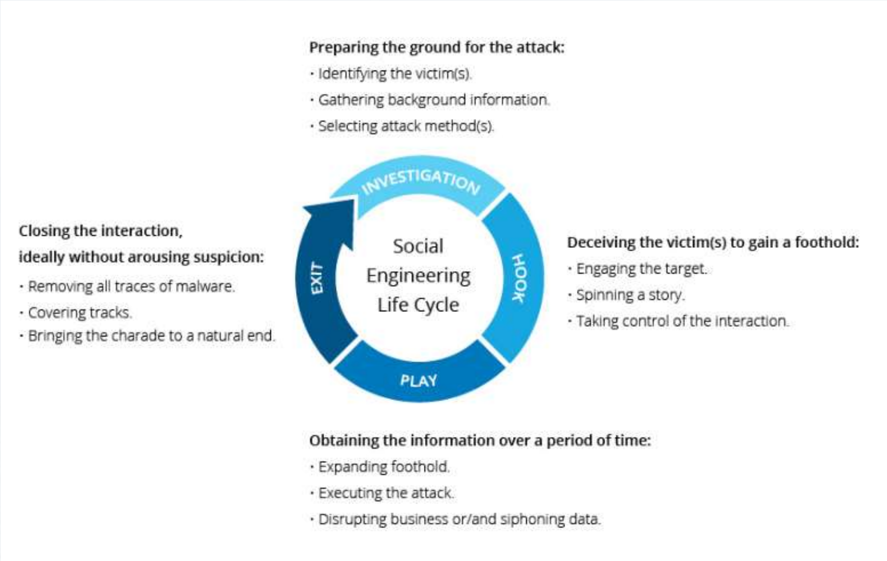
Attack techniques

Some examples:

- **Malware**
- **Social Engineering**
- **Phishing**
- **Man in the middle**
- **Denial of Service**
- **Zero day exploit**
- **…**

Social Engineering:

Social Engineering is the psychological manipulation of people into performing actions or divulging confidential information.



Preparing the ground for the attack:
- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:
- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:
- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction, ideally without arousing suspicion:
- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

Social engineering attack lifecycle

Attack techniques

Some examples:

- **Malware**
- **Social Engineering**
- **Phishing**
- **Man in the middle**
- **Denial of Service**
- **Zero day exploit**
- **…**

Phishing:

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email.

The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine.

Phishing is an increasingly common cyberthreat.

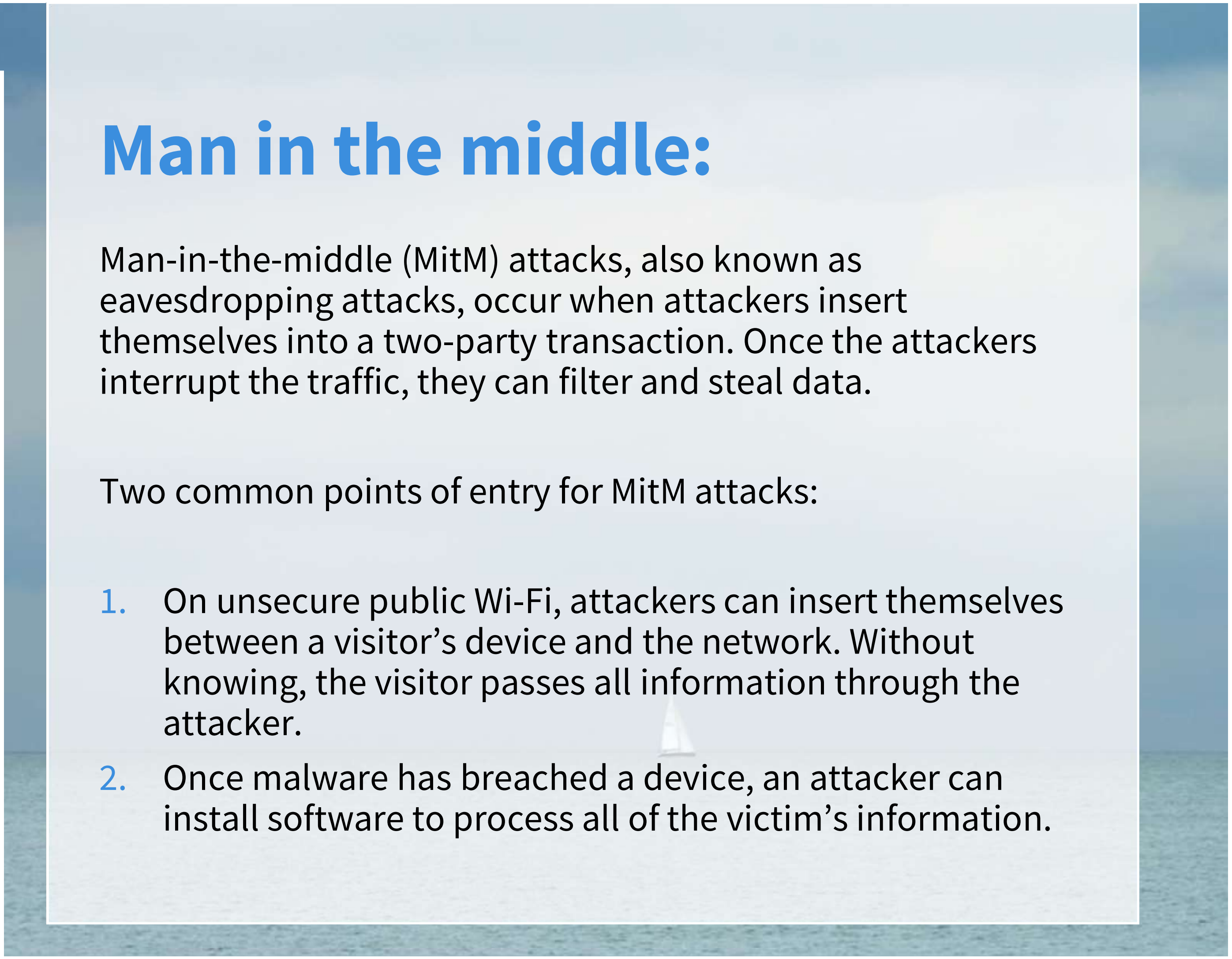
Various types:

- Deceptive phishing (confidential information)
- Spear phishing (targeted)
- Whaling (the “big fish”)
- Pharming (fraudulent website)

Attack techniques

Some examples:

- **Malware**
- **Social Engineering**
- **Phishing**
- **Man in the middle**
- **Denial of Service**
- **Zero day exploit**
- **…**



Man in the middle:

Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

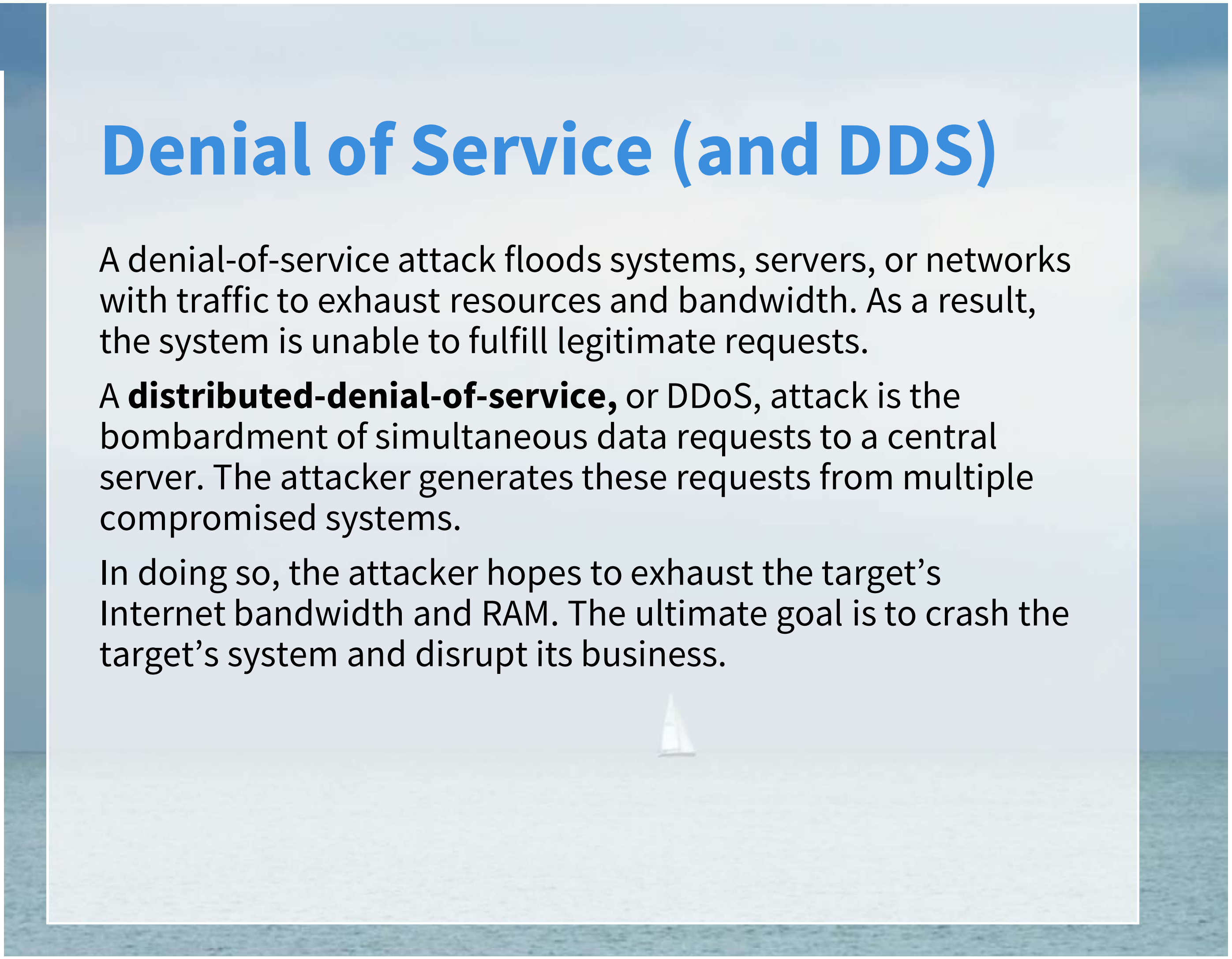
Two common points of entry for MitM attacks:

1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker.
2. Once malware has breached a device, an attacker can install software to process all of the victim's information.

Attack techniques

Some examples:

- **Malware**
- **Social Engineering**
- **Phishing**
- **Man in the middle**
- **Denial of Service**
- **Zero day exploit**
- **…**



Denial of Service (and DDS)

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests.

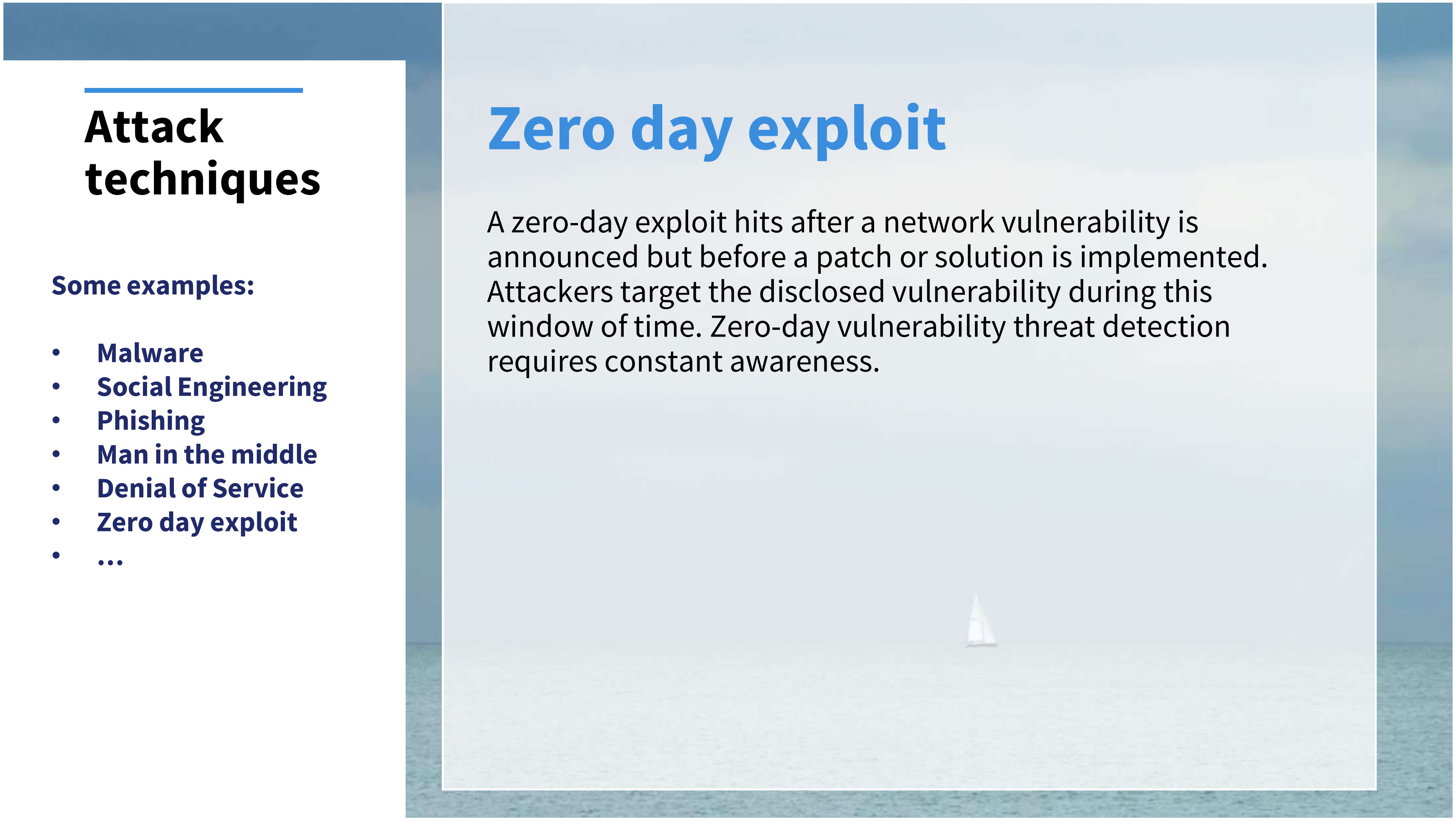
A **distributed-denial-of-service,** or DDoS, attack is the bombardment of simultaneous data requests to a central server. The attacker generates these requests from multiple compromised systems.

In doing so, the attacker hopes to exhaust the target’s Internet bandwidth and RAM. The ultimate goal is to crash the target’s system and disrupt its business.

Attack techniques

Some examples:

- **Malware**
- **Social Engineering**
- **Phishing**
- **Man in the middle**
- **Denial of Service**
- **Zero day exploit**
- **…**



Zero day exploit

A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zero-day vulnerability threat detection requires constant awareness.

How can we as businesses make ourselves more resilient to attacks?

The Future – a Board Responsibility

Cyber security is not an IT issue – it is a Business issue

- Identify & protect critical assets using a threat intelligence and risk based approach
- Accountability aligned to Board, CEO, and business

- Confident. Assured. Visible. Prepared to respond.
- Full cyber awareness, global sharing across all devices
- Detect early, respond effectively and prevent business disruption,

Building a solid security strategy is not easy

People

Lack of awareness of the risks and prevention

Outdated

Old technology is costly to maintain and upgrade

Compliance

Political and maritime organisations starting to take note

Knowledge

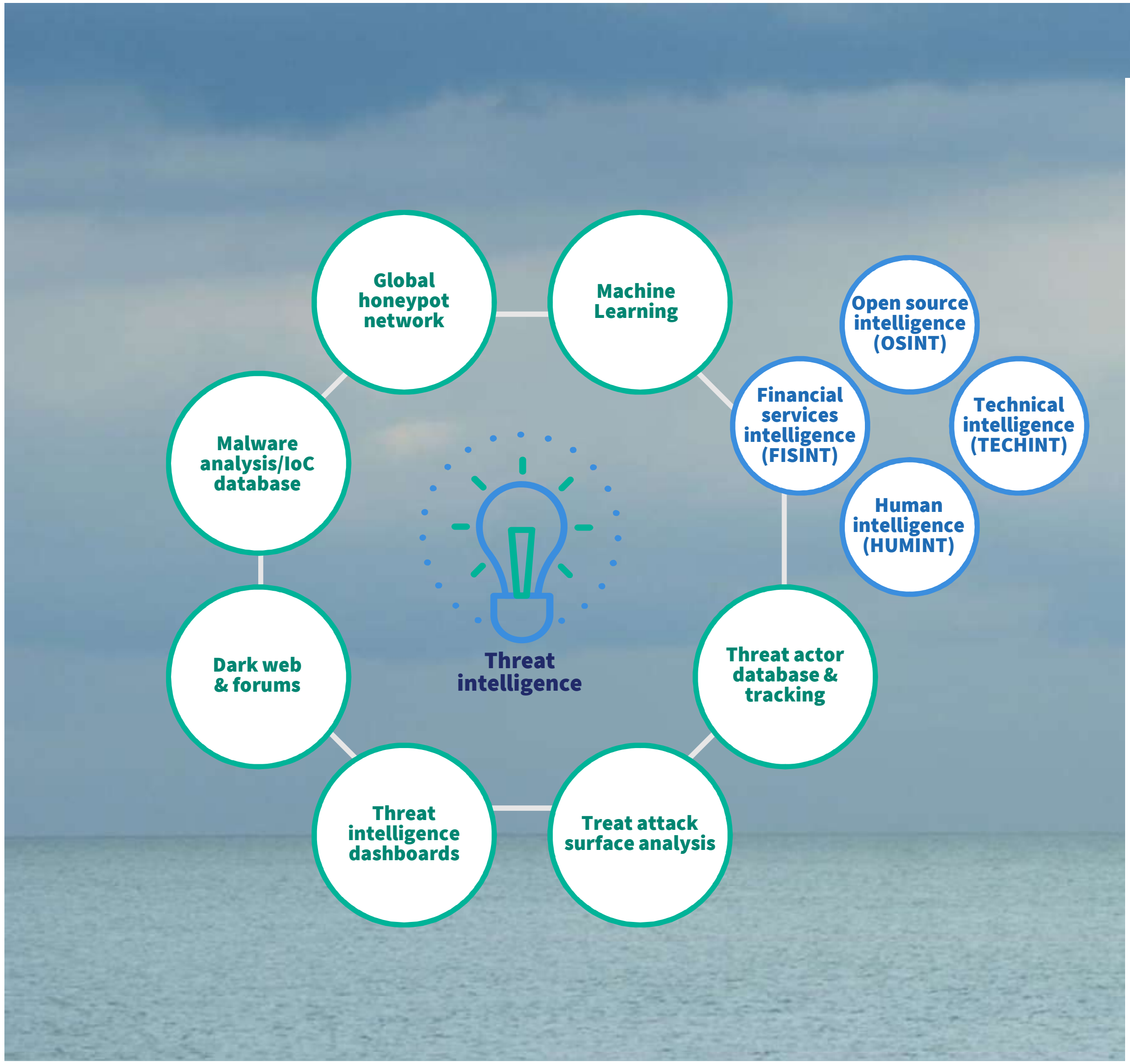
Lack of security training and expertise

Reputation

Negative brand impact affecting share price and customer

A selection of services that will help protect your business

Threat intelligence	Security testing	Training and strategy	Governance, risk and compliance	Managed security services	Incident response
Gain the knowledge to take action	*Understand real and present threats*	*Prepare your people*	*Create a framework for ongoing control*	*Delegate the day to day*	*Take immediate action*
Proactive threat hunting service enabled by a dedicated R&D team	Risk based, real world, human led testing services	Bespoke training tailored to your people, processes and technology	Assess effectiveness, prepare for the future and manage risks	24/7 security; detecting and responding to a spectrum of cyber threats	All levels and specialisations of cyber offensive and defence activities
Seeks out dormant and active threats	**Identify vulnerabilities & weaknesses**	**Improve security from within**	**Adapt to meet client needs**	**Proactive and reactive services**	**Prevent further losses with early resolution**
The foundations of your security strategy			Additional security support		


Global honeypot network
Machine Learning
Open source intelligence (OSINT)
Financial services intelligence (FISINT)
Technical intelligence (TECHINT)
Human intelligence (HUMINT)
Malware analysis/IoC database
Threat intelligence
Dark web & forums
Threat actor database & tracking
Threat intelligence dashboards
Treat attack surface analysis

Threat Intelligence

Threat Intelligence, advanced machine learning and artificial intelligence algorithms can identify novel and emerging threats.

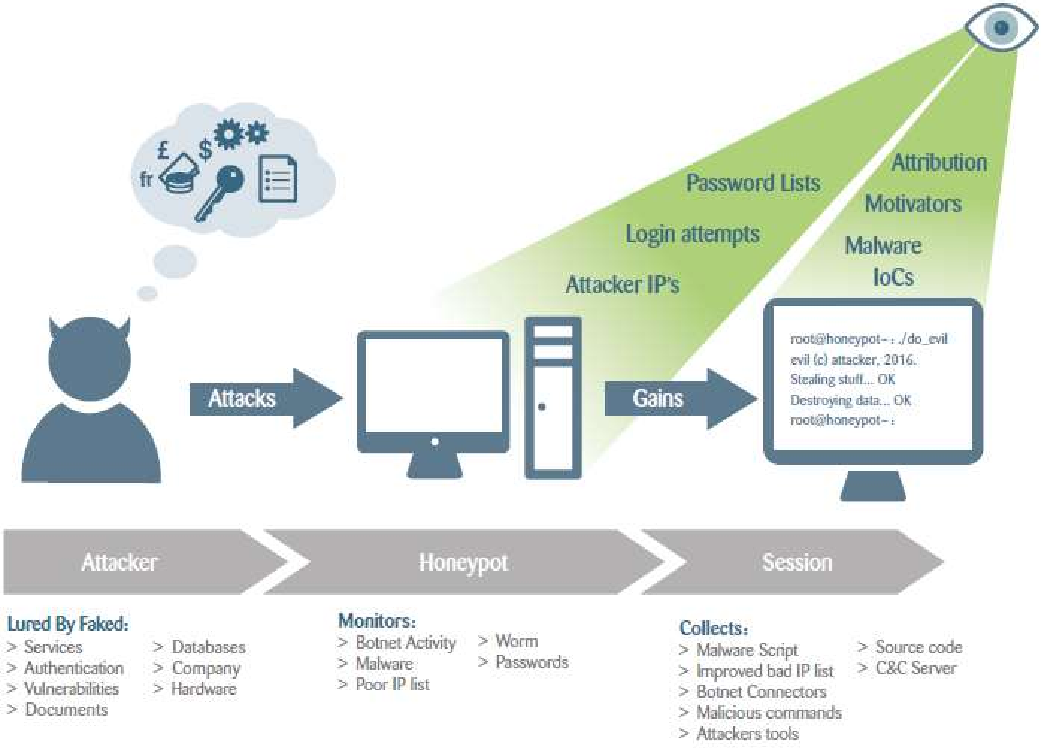
Machine learning's biggest strength in security is training to understand what is "baseline" or "normal" for a system, and then flagging anything unusual for human review.

Intelligence gathered through Honeypots

No matter how sophisticated attackers are, they do not have unlimited resources.

They will inevitably reuse part, or all, of their infrastructure in more than one attack.

Honeypot data can be of great value if utilized correctly



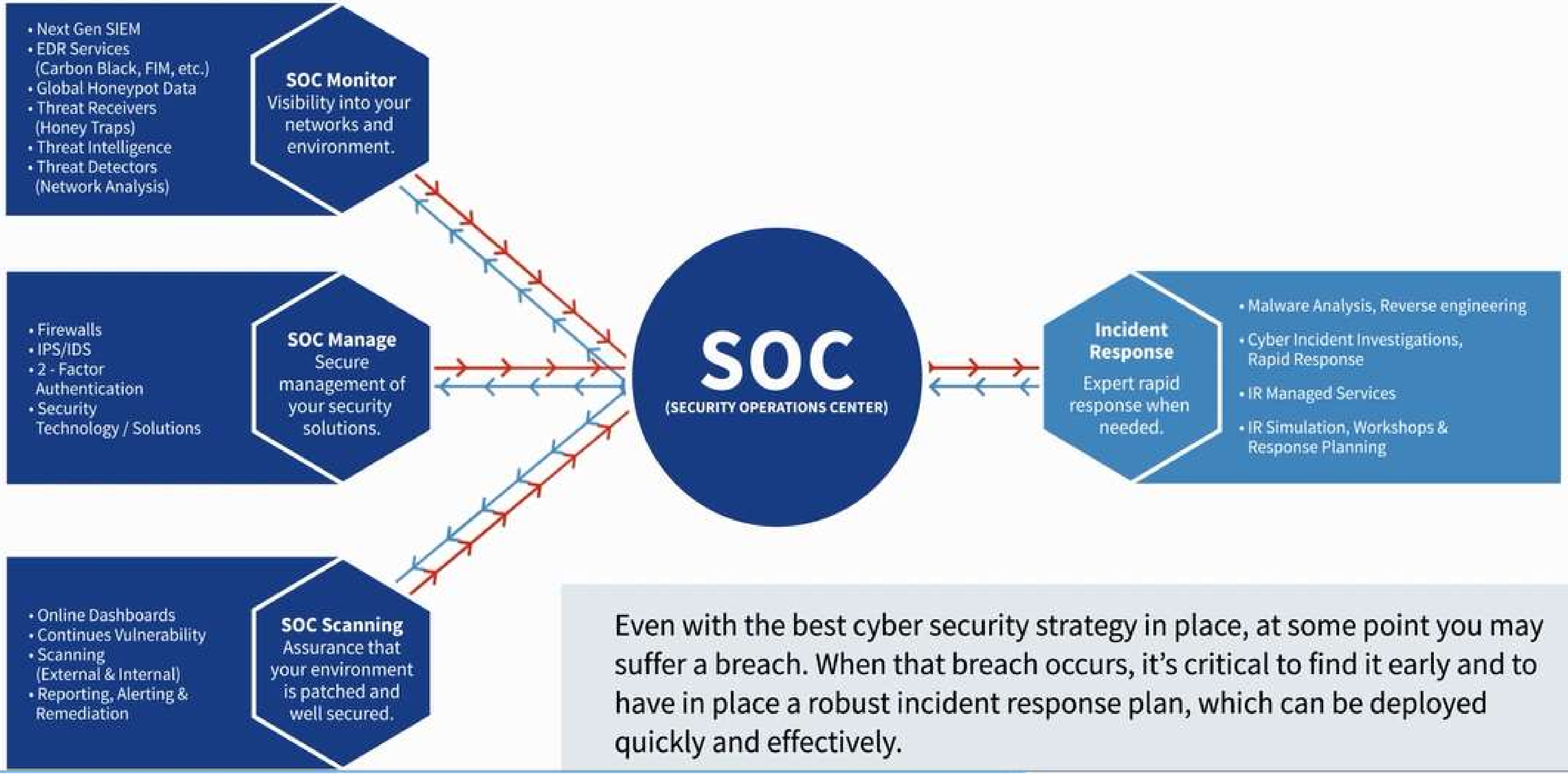
```
root@honeypot~ : ./do_evil
evil (c) attacker, 2016.
Stealing stuff... OK
Destroying data... OK
root@honeypot~ :
```

Lured By Faked:
- > Services
- > Authentication
- > Vulnerabilities
- > Documents
- > Databases
- > Company
- > Hardware

Monitors:
- > Botnet Activity
- > Malware
- > Poor IP list
- > Worm
- > Passwords

Collects:
- > Malware Script
- > Improved bad IP list
- > Botnet Connectors
- > Malicious commands
- > Attackers tools
- > Source code
- > C&C Server

Taking actions early.



- Next Gen SIEM
- EDR Services (Carbon Black, FIM, etc.)
- Global Honeypot Data
- Threat Receivers (Honey Traps)
- Threat Intelligence
- Threat Detectors (Network Analysis)

SOC Monitor
Visibility into your networks and environment.

- Firewalls
- IPS/IDS
- 2 - Factor Authentication
- Security Technology / Solutions

SOC Manage
Secure management of your security solutions.

- Online Dashboards
- Continues Vulnerability
- Scanning (External & Internal)
- Reporting, Alerting & Remediation

SOC Scanning
Assurance that your environment is patched and well secured.

SOC
(SECURITY OPERATIONS CENTER)

Incident Response
Expert rapid response when needed.

- Malware Analysis, Reverse engineering
- Cyber Incident Investigations, Rapid Response
- IR Managed Services
- IR Simulation, Workshops & Response Planning

Even with the best cyber security strategy in place, at some point you may suffer a breach. When that breach occurs, it's critical to find it early and to have in place a robust incident response plan, which can be deployed quickly and effectively.

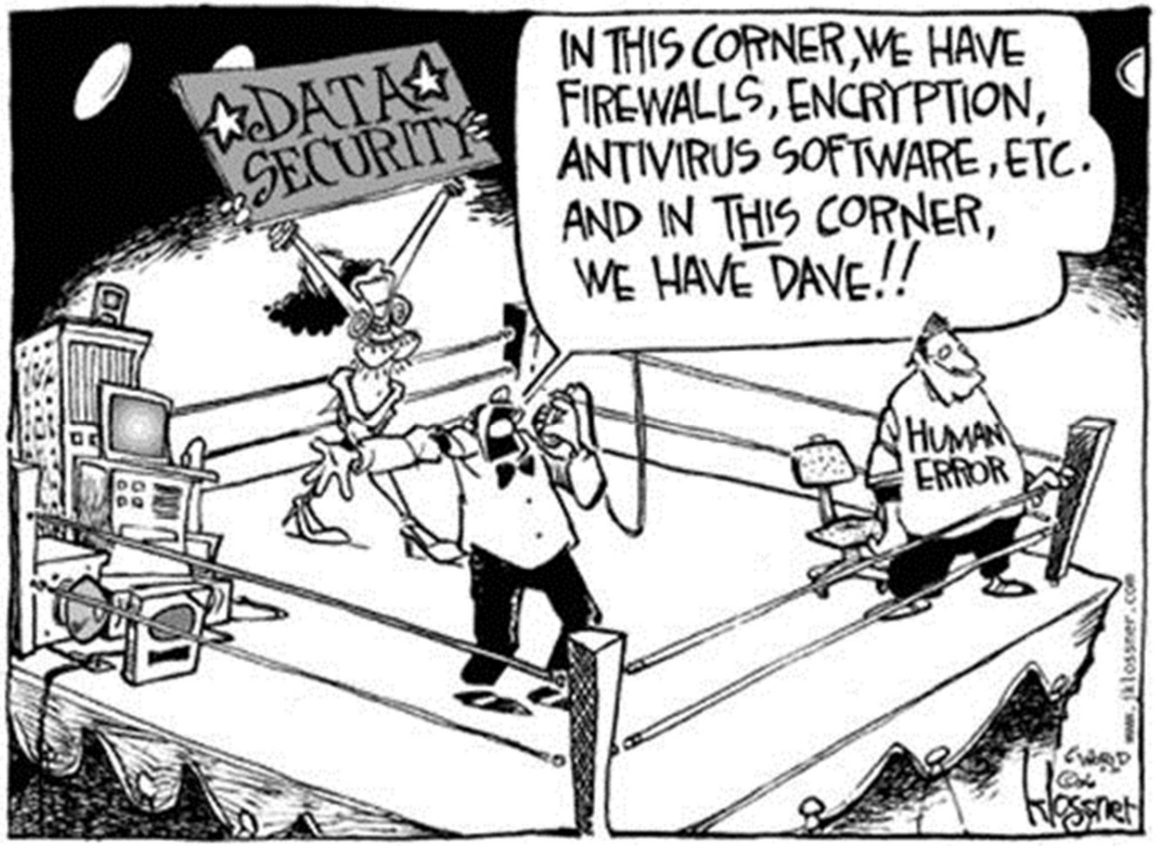
Cyber Awareness

People……..

…a constant factor

YOUR STAFF ARE YOUR BEST DEFENCE AND GREATEST POTENTIAL WEAKNESS

Cyber Awareness & Training


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©WRLD ©06 Klossner

Cyber Awareness & Training

Effective learning principles

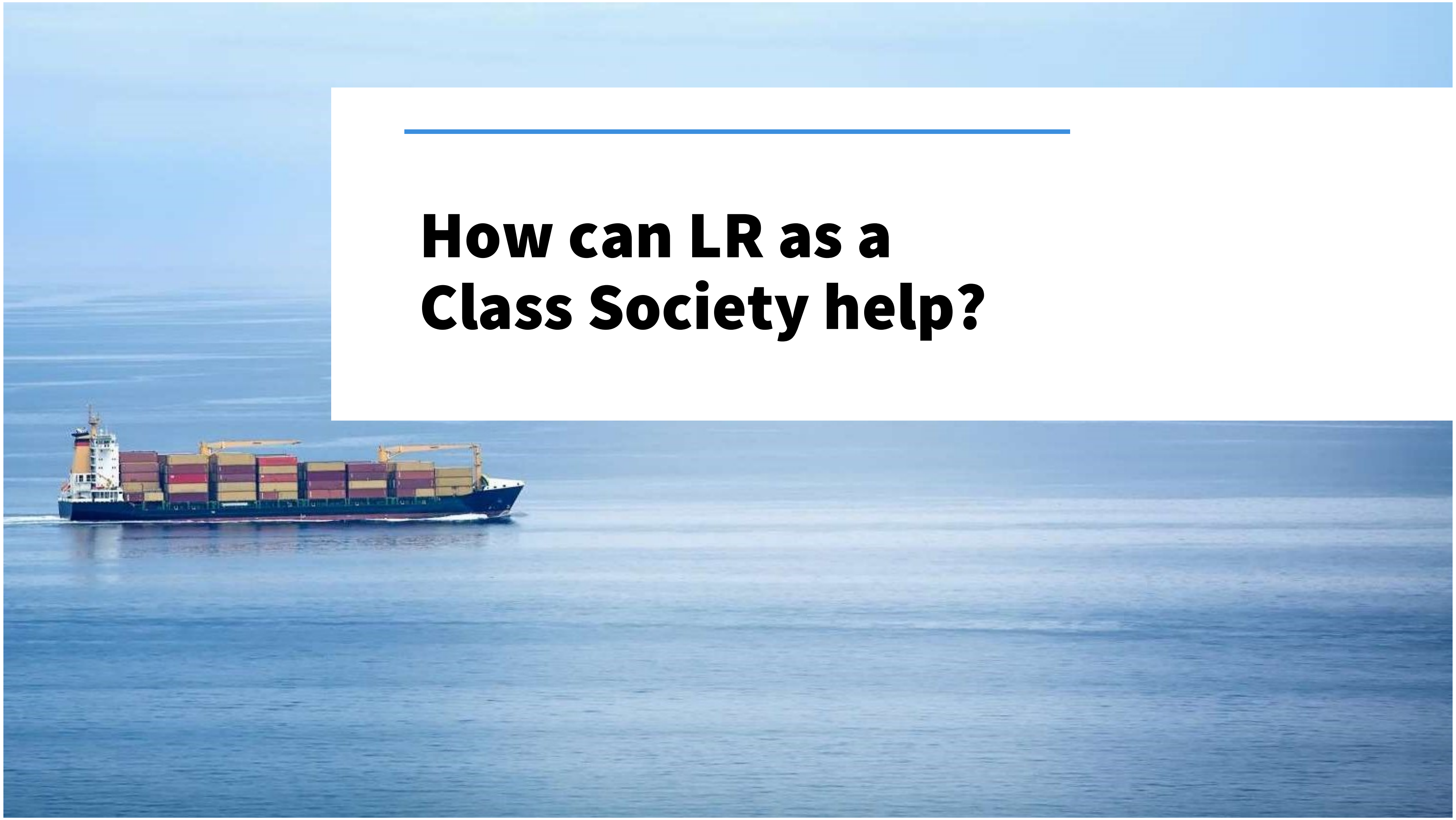
PRINCIPLES

- Engaging, relevant and valuable
- On-going, regular learning
- Adaptive & personalised
- Measurable benefit

AXELOS
GLOBAL BEST PRACTICE

Protecting your corporate reputation: cyber resilience starts at the top and involves everyone

AXELOS.com



How can LR as a Class Society help?

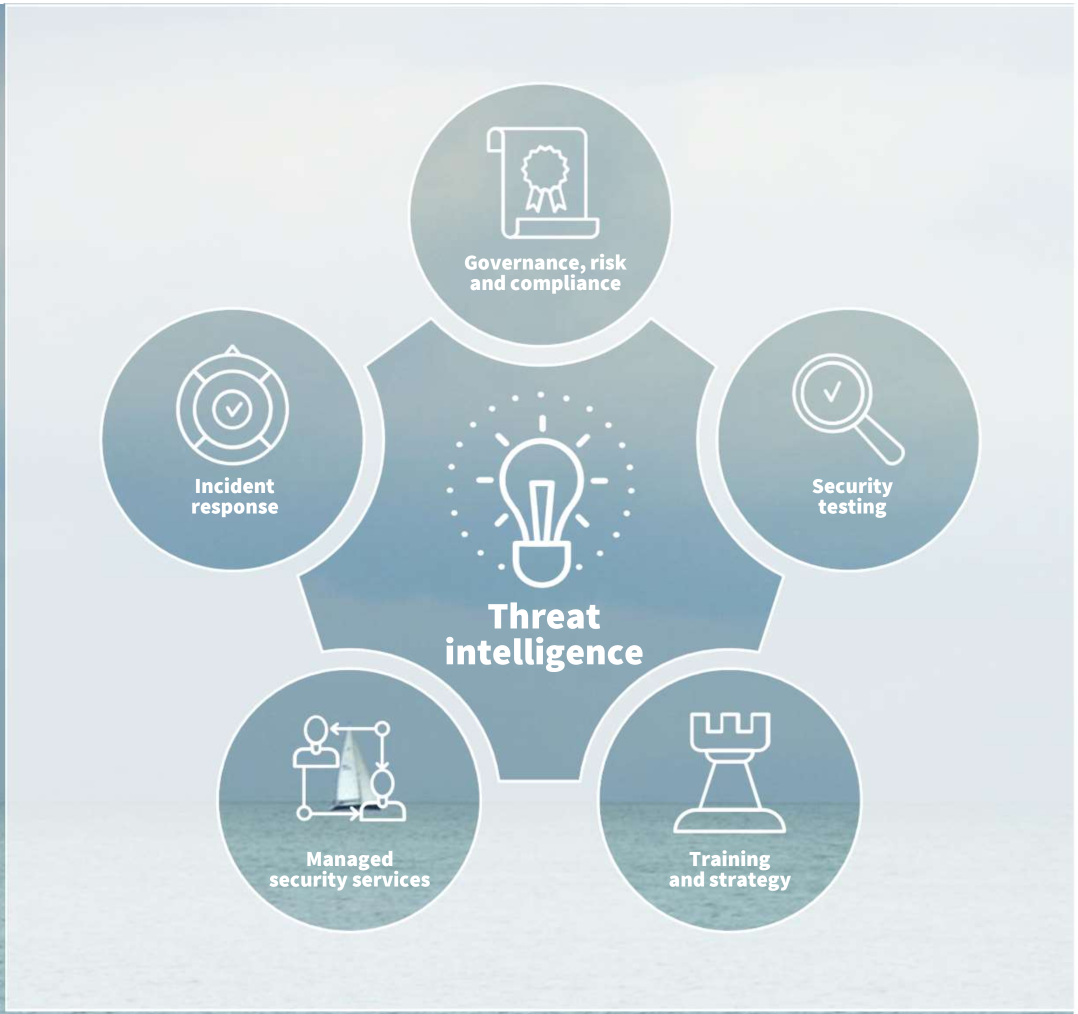
Our heritage is managing risk

Cyber threats are simply the newest evolution of risk type. The marine industry needs to approach cyber security in the same way it treats health & safety.

This makes Lloyd’s Register the natural partner for cyber security – our heritage and credentials in keeping people and ships safe at sea has now extended into the digital space.

An holistic approach to cyber security

Working with you to build and implement an end to end security strategy – with threat intelligence at the core.



Lloyd's Register

- Deep technical and industry knowledge
- Dedication to assurance
- Independence
- Understanding and empathy
- Social business

We have undergone significant change and growth over recent years

- Building a portfolio of data, digital and software solutions, including Acoura, RTAMO and Seasafe
- Acquired Senergy and Nettitude

£887m	£100m	32%
Turnover in 2016/17 achieved	Invested in our Southampton and Singapore global technology centres	year on year improvements in lost time incidents

NETTITUDE

- 15 years' experience
- 100 security professionals
- Global presence
- In-house research team
- Delivering security services to finance & banking, IT, technology and engineering firms
- A trusted cyber security provider
- Supports thousands of businesses around the world
- CREST and CHECK approved

2015 Penetration Tester of the Year

2016 Cyber Security Services Provider of the Year

2017 Cyber Security Services Provider of the Year

LogRhythm MSSP Partner of the Year 2015

2014 Computing Security Awards

SC Awards 2017 Europe Highly Commended

Portfolio overview

1: Threat intelligence
Dedicated research and innovation team to inform clients with up to date threat intelligence and proprietary tooling

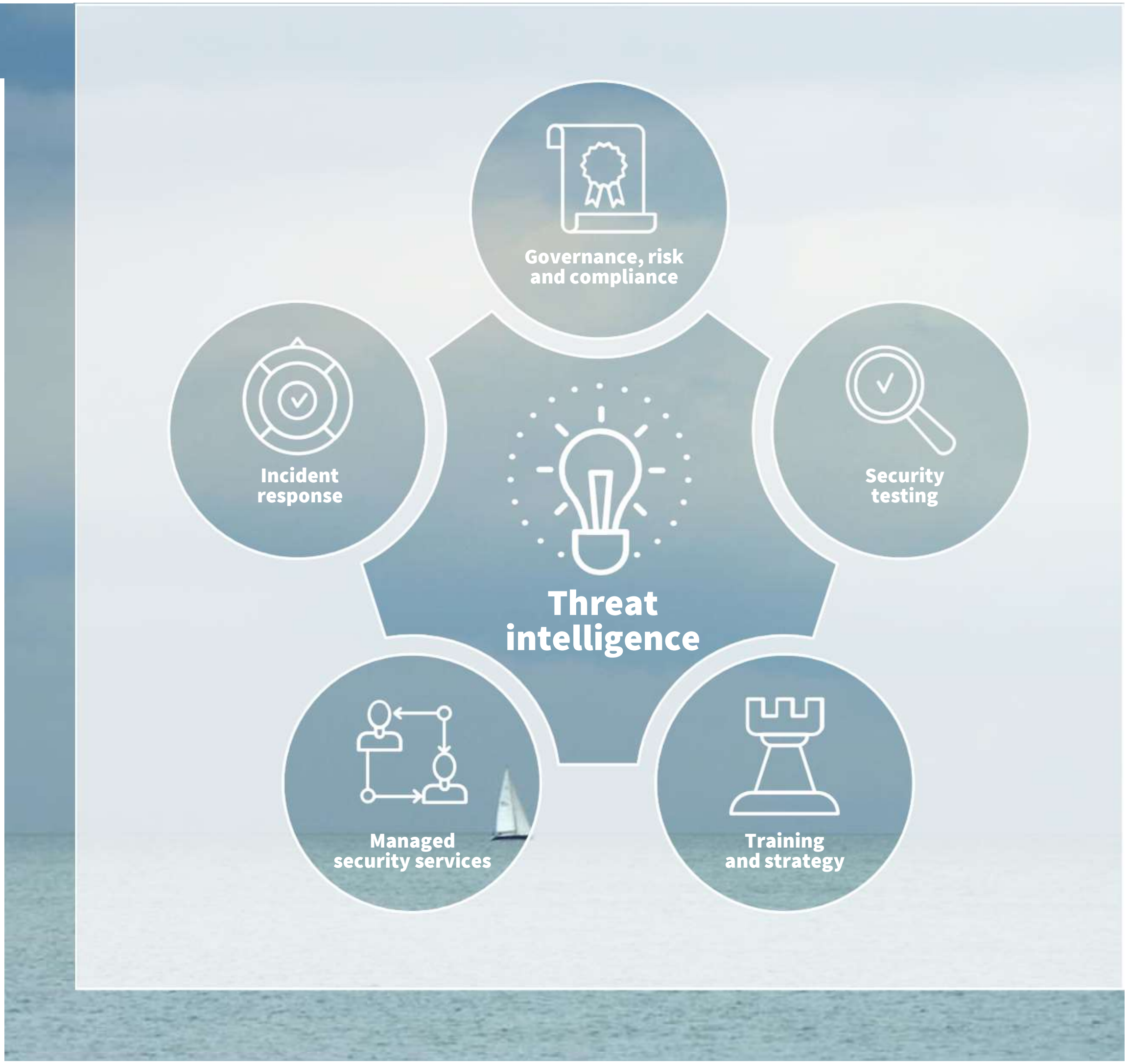
2: Governance, risk and compliance
Security services for managing corporate governance, risk management and compliance with regulatory requirements

3: Security testing
Threat intelligence led testing, red teaming, penetration testing and continuous scanning

4: Training and strategy
Customised cyber strategy that aligns people, processes, and technology with enterprise business priorities and risks

5: Managed security services
An extension of our clients' security operations team

6: Incident response
Immediate response in the event of a cyber breach



Intelligence led assurance

An effective cyber security strategy and a realistic awareness of cyber threats will enable organisations to embrace automation, connectivity, and ‘Industry 4.0’ technology area.

Additional security support

Governance, risk and compliance

Security services for managing corporate governance, risk management and compliance with regulatory requirements

Features:

- *ISO 27001/ ISO/IEC 20001*
- *Risk assessments*
- *Policies & Procedures*
- *PCI/PA QSA/ PCI approved scanning vendor*
- *P2PE QSA*
- *Tanker management self assessment*
- *Cyber security BIMCO guidelines*
- *ISM code*
- *Cyber Security FAQ and Threat Briefing - Guidance for Shipowners*

Managed security services

An extension of our clients' security operations team

Features:

- *SOC monitor*
- *SOC manage*
- *SOC scanning*

Incident response

Immediate response in the event of a cyber breach

Features:

- *Crisis management simulations*
- *Emergency breach response*
- *First responder training*

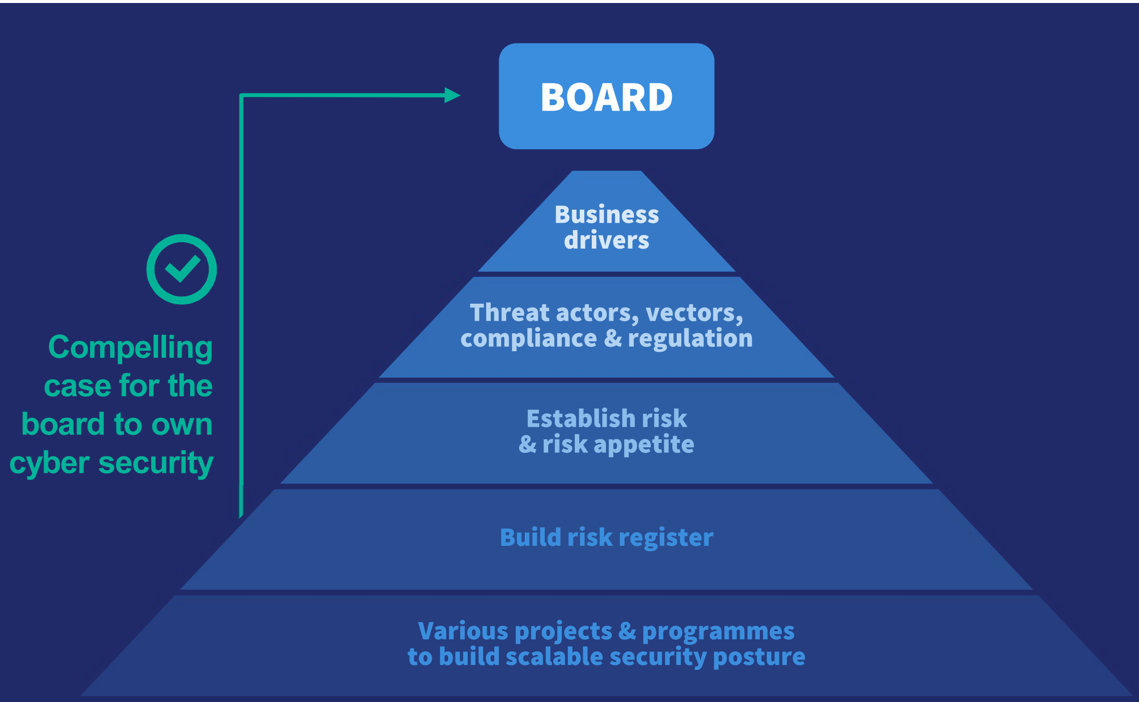
Define a cyber security strategy

Scope:

- Create a customised cyber strategy that aligns people, processes, and technology with enterprise business priorities and risks
- Identify and protect the key items that matter most
- Develop a roadmap, bringing a greater level of security maturity
- Create operational efficiencies and maximum return on technology investments

We help you take a ‘top-down’ approach

Attend to the need but drive the conversation back to the top of the pyramid to identify and address the problem



Compelling case for the board to own cyber security

BOARD

Business drivers

Threat actors, vectors, compliance & regulation

Establish risk & risk appetite

Build risk register

Various projects & programmes to build scalable security posture

Q&A

Lloyd's Register