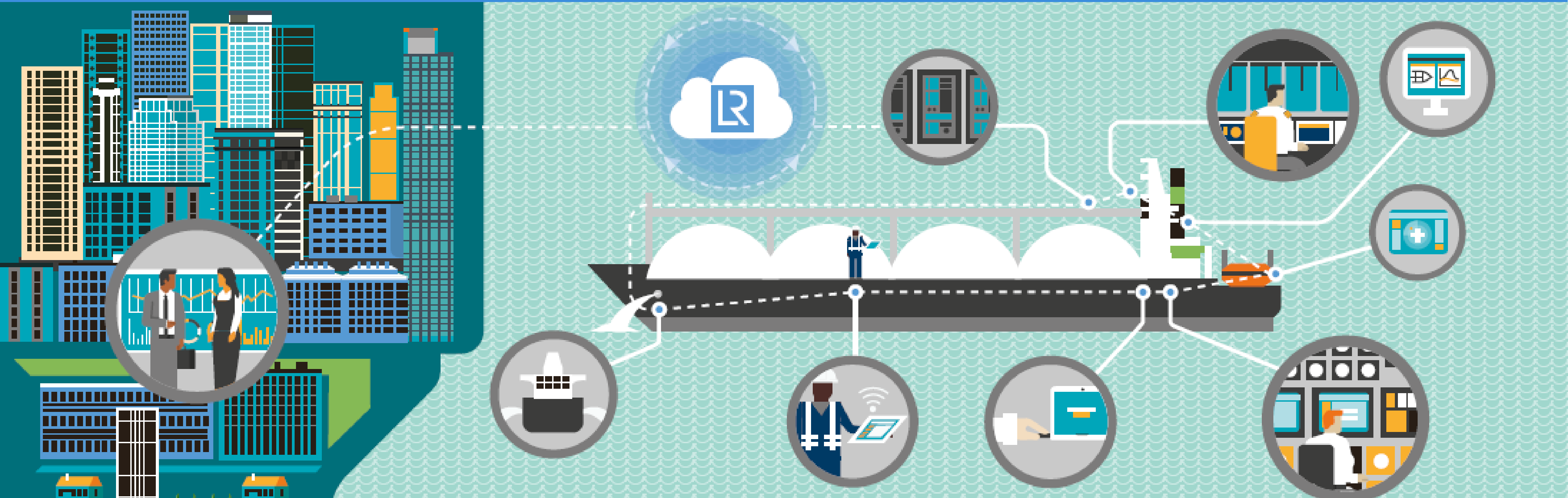
Lloyd's Register

Working
together
for a safer world

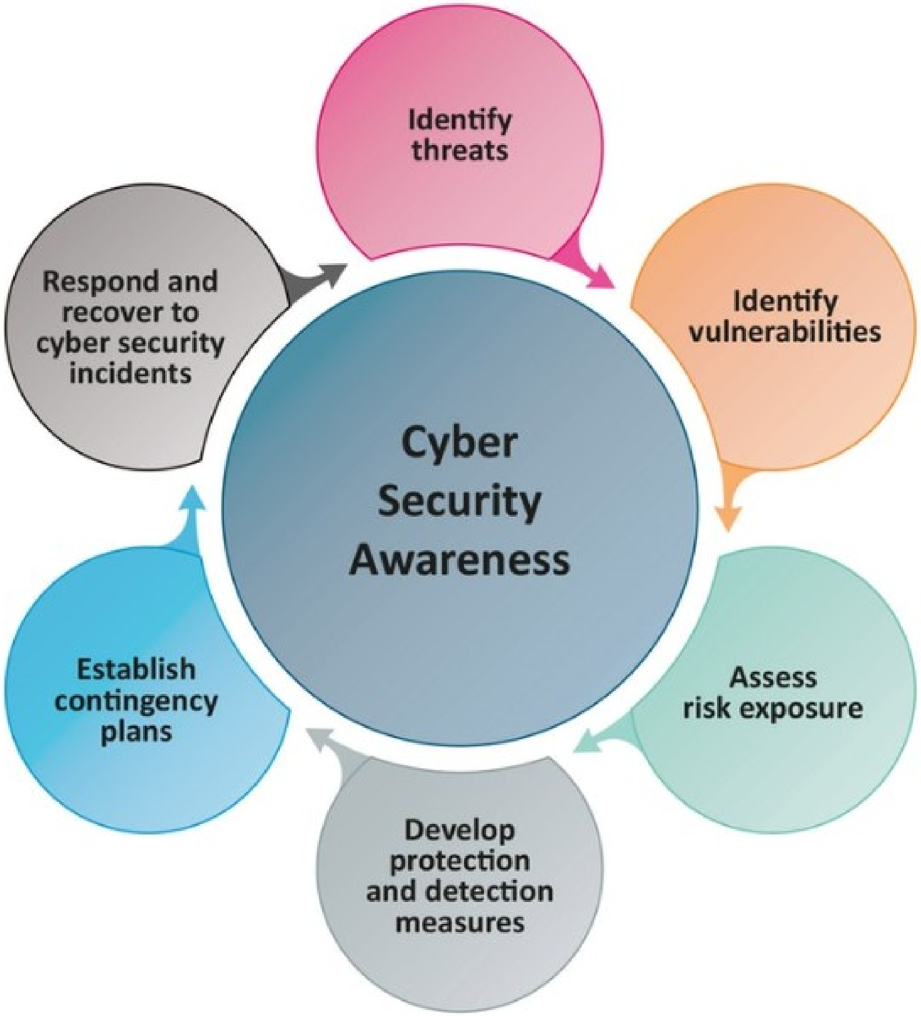
LR approach to cyber security

Marine and Offshore



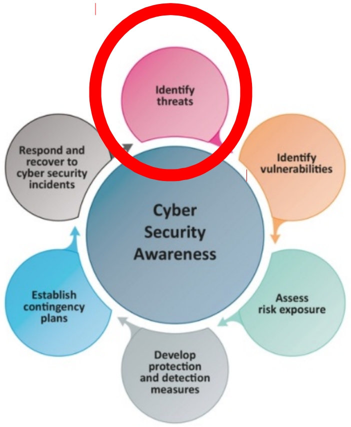
Cyber security approach as set out in the M&O guidelines

***BIMCO,* together with other leading shipping organisations, has launched a set of guidelines to help the global shipping industry prevent major safety, environmental and commercial issues that could result from a cyber incident onboard a ship.**


Cyber Security Awareness
Identify threats
Identify vulnerabilities
Assess risk exposure
Develop protection and detection measures
Establish contingency plans
Respond and recover to cyber security incidents

BIMCO

Baltic and International Maritime Council


Identify threats
Identify vulnerabilities
Assess risk exposure
Develop protection and detection measures
Establish contingency plans
Respond and recover to cyber security incidents
Cyber Security Awareness

The Threats

An increasingly connected world opens the door to vulnerabilities

Automation and use of unmanned systems
Ports and vessels are becoming increasingly automated, with navigation, cargo management, and propulsion control systems increasingly controlled without human input.

Increasingly connected world
Maritime companies are putting more of their navigation and logistics systems online, with the use of AIS and ECDIS navigation systems, and VTMS monitoring systems becoming widely used.

Growth in ship size and technological advancement
The volume of cargo being transported for each ship, and the volume handled at ports has been increasing in recent years.

Increase in vulnerability to breaches

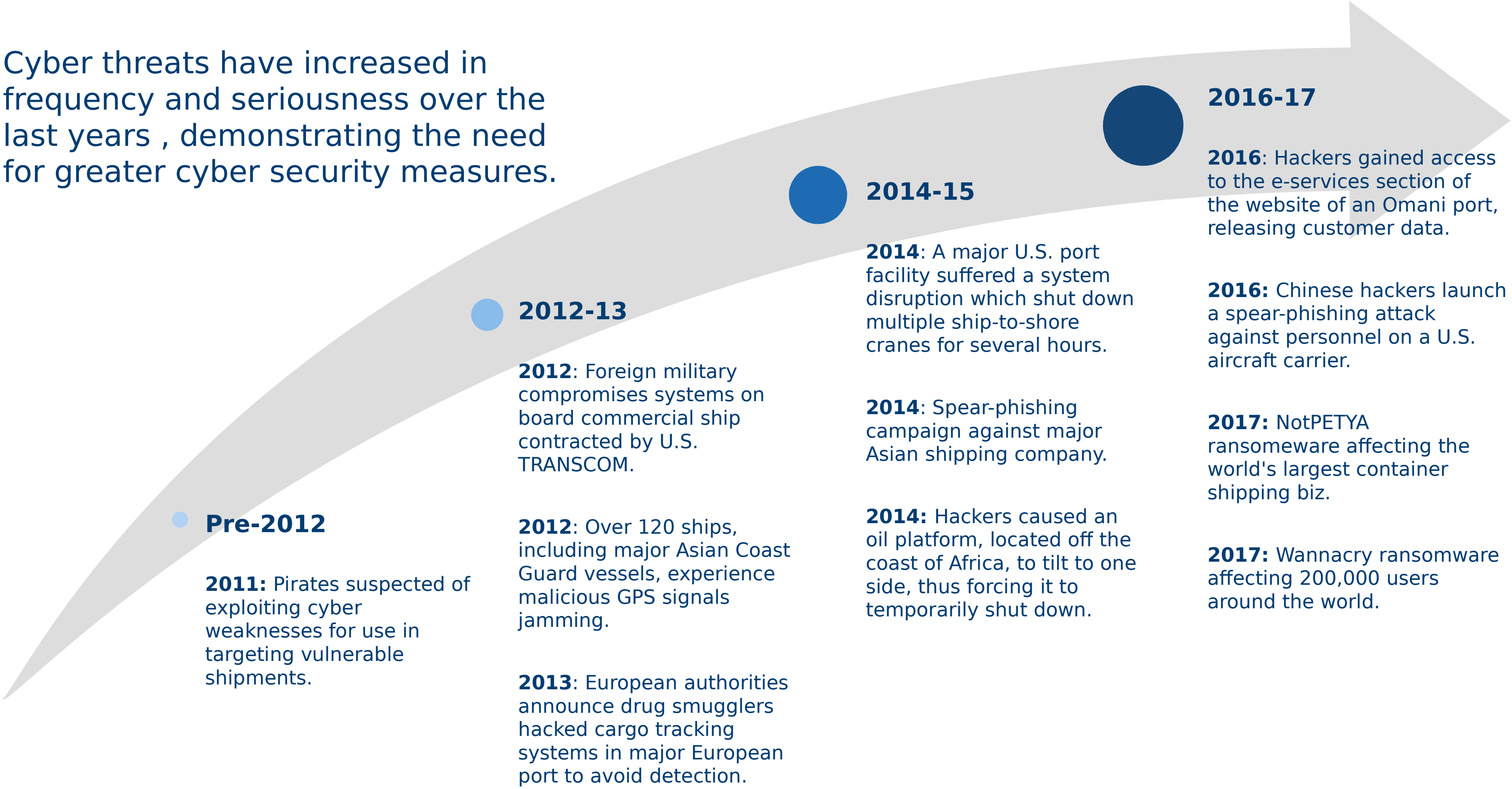
- Greater volumes of cyber entry points that arise from new technology offer greater opportunities for breaches in a company’s cyber perimeter.
- Greater numbers of data [illegible]

Increase in potential loss from a breach

- Data and cyber connectivity are becoming increasingly important in daily operations of businesses, and hence of great commercial importance.
- The increased use and storage of IP and customer data amplifies the risk of a breach in terms of competitive advantages and reputational impact.

Cyber threats have grown significantly and will continue to do so

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



Pre-2012

2011: Pirates suspected of exploiting cyber weaknesses for use in targeting vulnerable shipments.

2012-13

2012: Foreign military compromises systems on board commercial ship contracted by U.S. TRANSCOM.

2012: Over 120 ships, including major Asian Coast Guard vessels, experience malicious GPS signals jamming.

2013: European authorities announce drug smugglers hacked cargo tracking systems in major European port to avoid detection.

2014-15

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

2014: Spear-phishing campaign against major Asian shipping company.

2014: Hackers caused an oil platform, located off the coast of Africa, to tilt to one side, thus forcing it to temporarily shut down.

2016-17

2016: Hackers gained access to the e-services section of the website of an Omani port, releasing customer data.

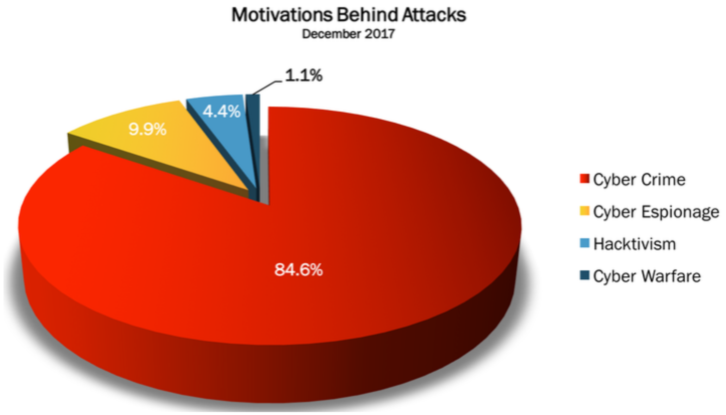
2016: Chinese hackers launch a spear-phishing attack against personnel on a U.S. aircraft carrier.

2017: NotPETYA ransomeware affecting the world's largest container shipping biz.

2017: Wannacry ransomware affecting 200,000 users around the world.

Motivation and objectives of a cyber attack

Motivation	Objectives
Cyber Crime	• Financial gain - Selling stolen data • Ransoming stolen data or system operability • Arranging fraudulent transportation of cargo • Gathering intelligence for more sophisticated crime, exact cargo location, off vessel transportation and handling plans etc
Hacktivism	• Destruction of data • Publication of sensitive data • Media attention • Denial of access to the service or system targeted
Cyber Espionage	• Financial gain – Commercial advantage • Gaining knowledge • “The challenge”
Cyber Warfare	• Disruption to economies and critical national infrastructure • Getting through cyber security defences

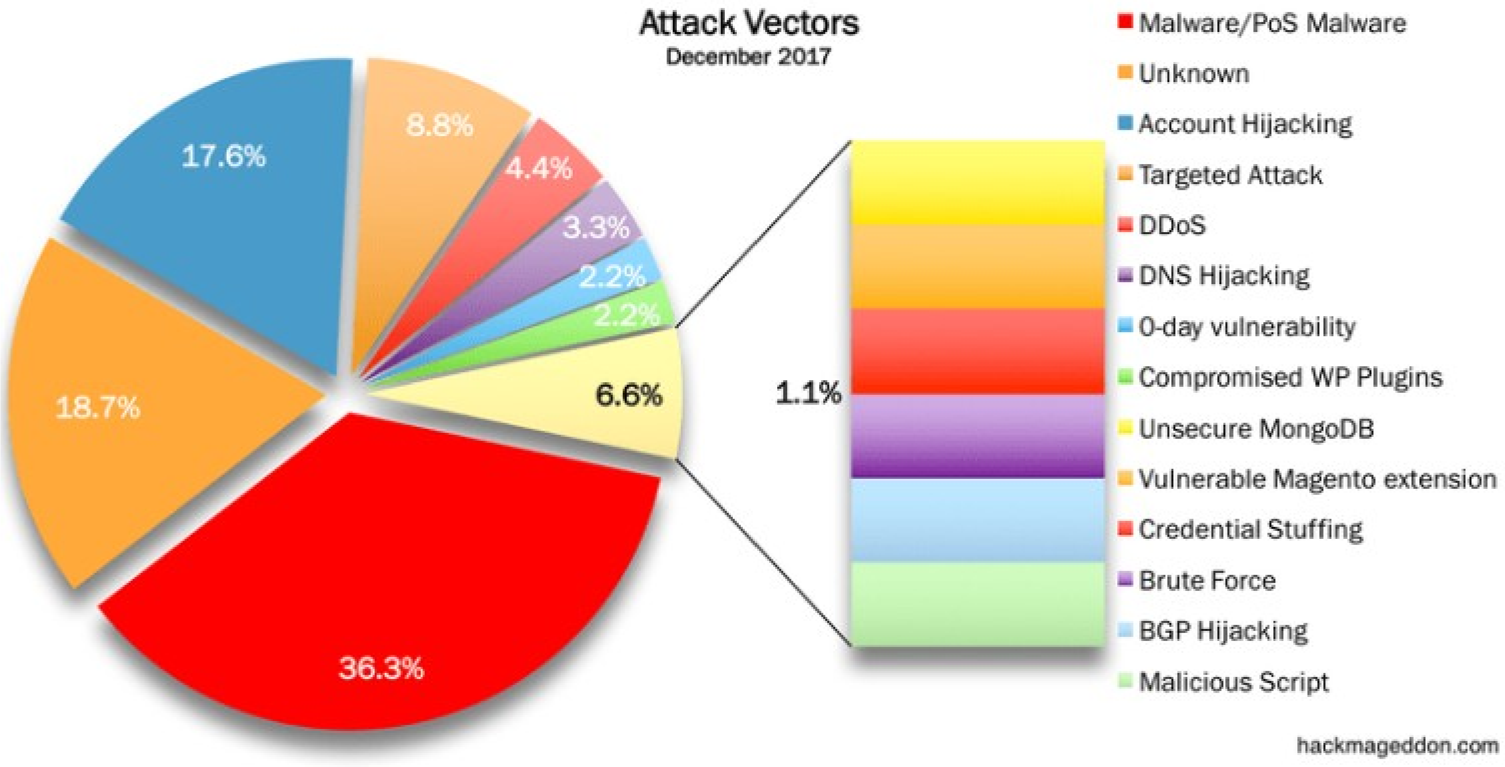


Source: hackmageddon.com

Attack techniques

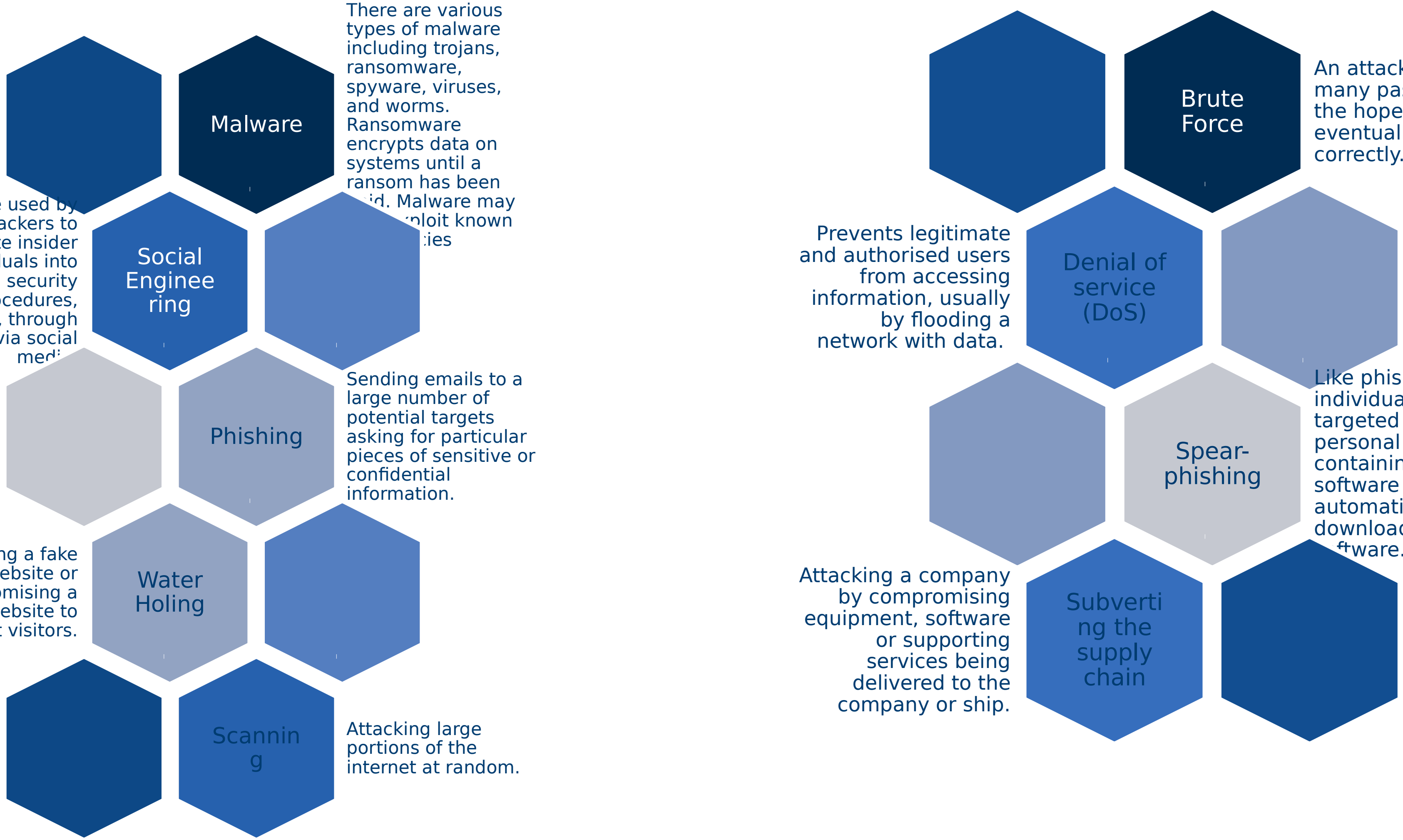
TARGETED ATTACKS *where a company or a ship's systems and data are the intended target.*

… just 8.8%



hackmageddon.com

Attack techniques



UNTARGETED ATTACKS

Malware

There are various types of malware including trojans, ransomware, spyware, viruses, and worms. Ransomware encrypts data on systems until a ransom has been id. Malware may xploit known ties

Social Engineering

Technique used by cyber attackers to manipulate insider individuals into breaking security procedures, normally, through interaction via social medi

Phishing

Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information.

Water Holing

Establishing a fake website or compromising a genuine website to exploit visitors.

Scanning

Attacking large portions of the internet at random.

TARGETED ATTACKS

Brute Force

An attack trying many passwords with the hope of eventually guessing correctly..

Denial of service (DoS)

Prevents legitimate and authorised users from accessing information, usually by flooding a network with data.

Spear-phishing

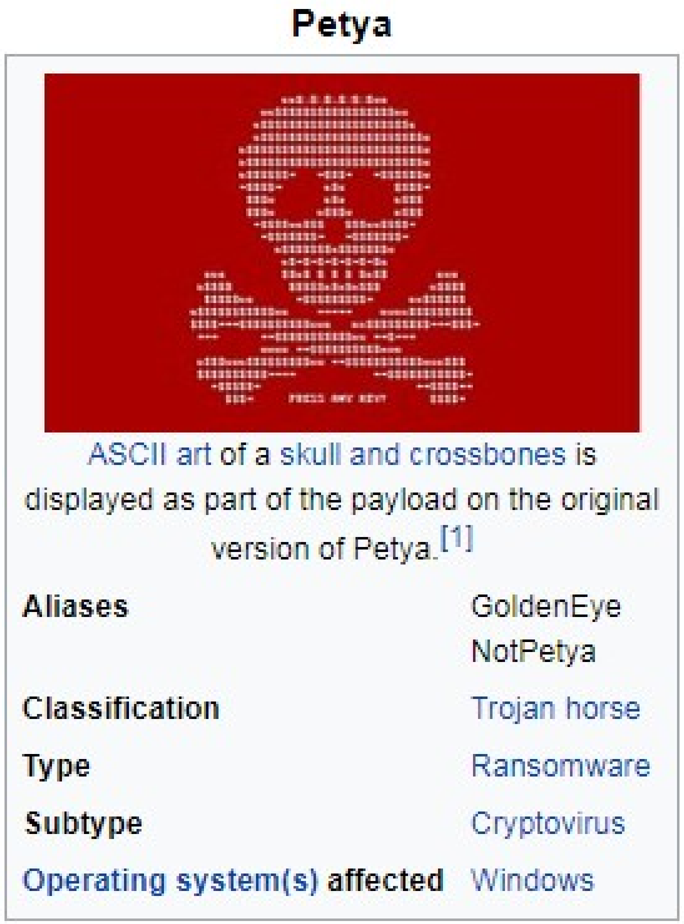
Like phishing but individuals are targeted with personal emails containing malicious software or links that automatically download malicious ftware.

Subverting the supply chain

Attacking a company by compromising equipment, software or supporting services being delivered to the company or ship.

A ransomeware attack: NotPetya on Maersk in 2017

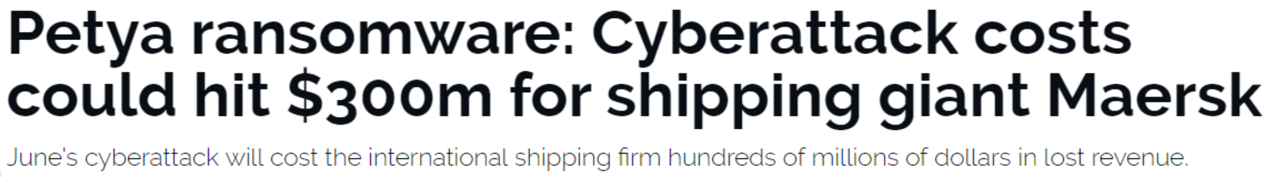
Back



Petya

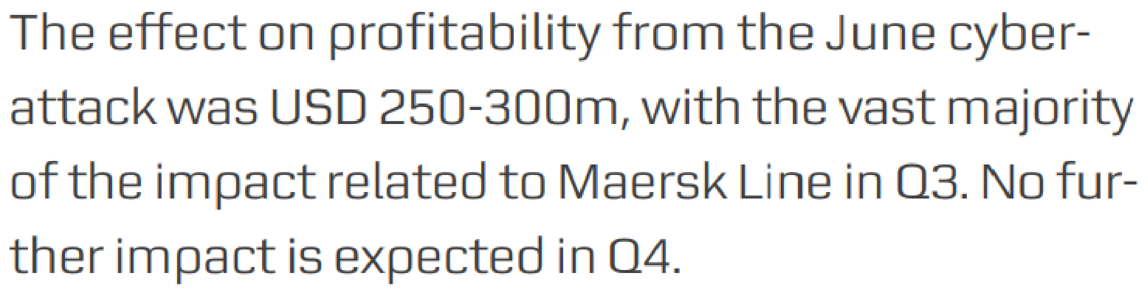
ASCII art of a skull and crossbones is displayed as part of the payload on the original version of Petya.[1]

Aliases	GoldenEye NotPetya
Classification	Trojan horse
Type	Ransomware
Subtype	Cryptovirus
Operating system(s) affected	Windows



Petya ransomware: 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.

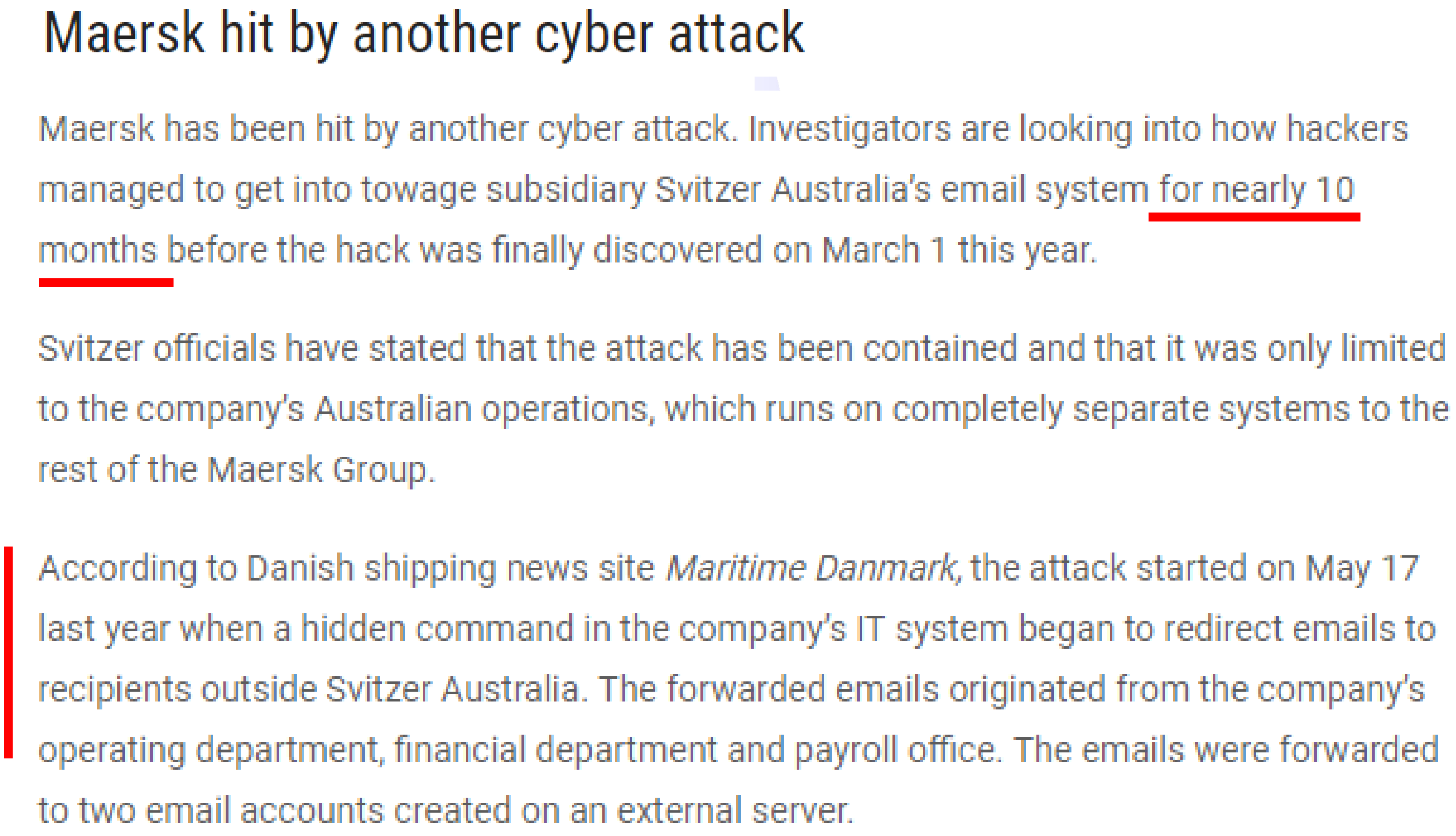


The effect on profitability from the June cyber-attack was USD 250-300m, with the vast majority of the impact related to Maersk Line in Q3. No further impact is expected in Q4.

Ransomware incidents clearly demonstrate the failure in prevention of such events. Poorly patched systems, old or non-existent backups, weak administrator passwords or missing network segmentation are only some examples that contribute to the installation and distribution of ransomware.

… again on Maersk, another attack dicovered in March 2018

Back



Maersk hit by another cyber attack

Maersk has been hit by another cyber attack. Investigators are looking into how hackers managed to get into towage subsidiary Svitzer Australia's email system for nearly 10 months before the hack was finally discovered on March 1 this year.

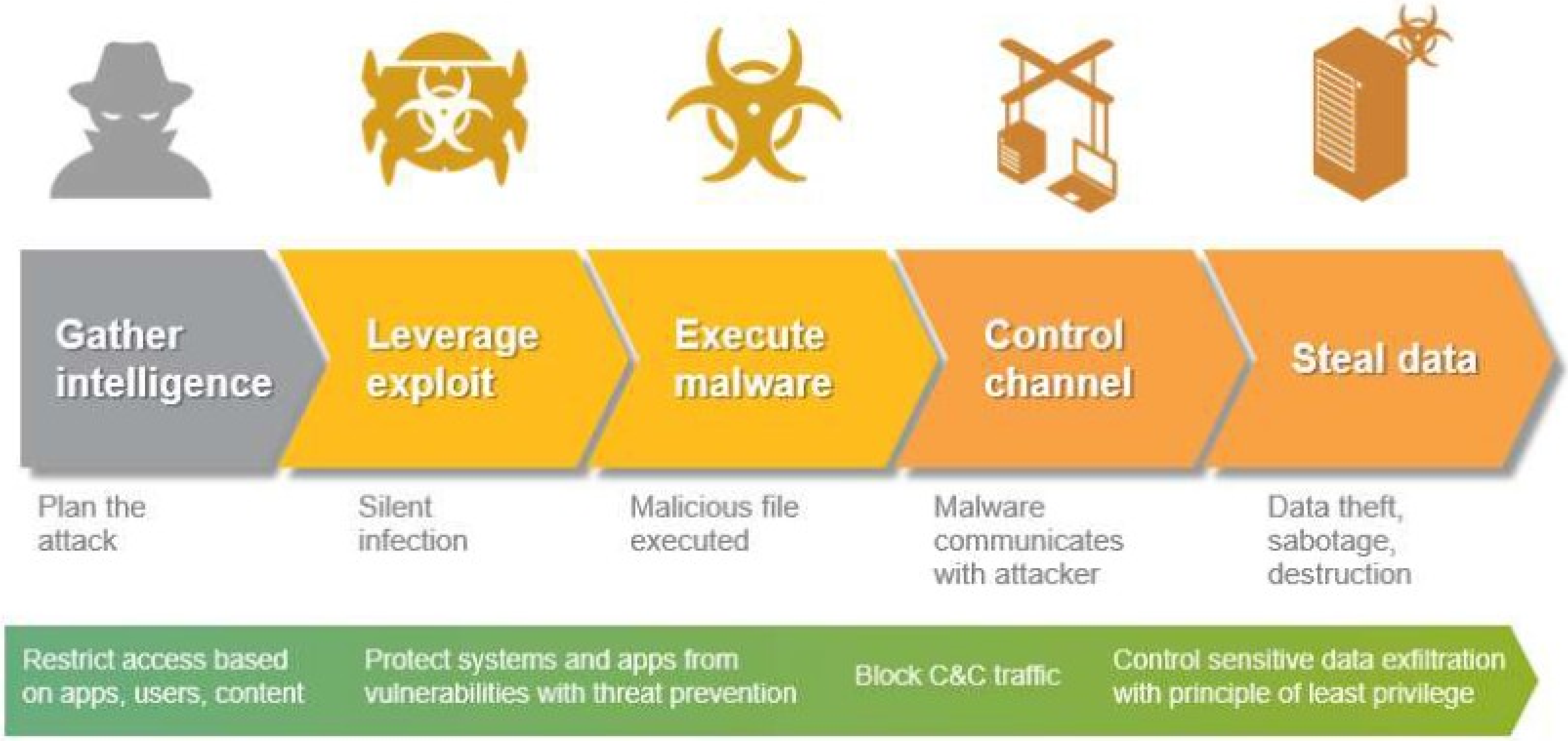
Svitzer officials have stated that the attack has been contained and that it was only limited to the company's Australian operations, which runs on completely separate systems to the rest of the Maersk Group.

According to Danish shipping news site *Maritime Danmark*, the attack started on May 17 last year when a hidden command in the company's IT system began to redirect emails to recipients outside Svitzer Australia. The forwarded emails originated from the company's operating department, financial department and payroll office. The emails were forwarded to two email accounts created on an external server.

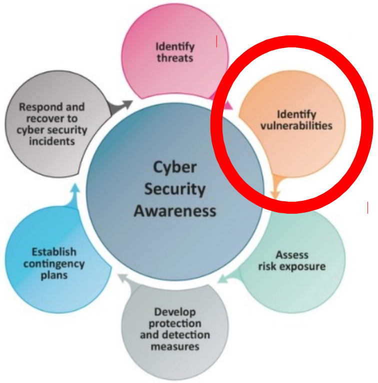
Sensitive personnel data has been stolen from a Maersk-owned shipping company

The Cyber Attack Lifecycle

The Cyber Attack Lifecycle is a sequence of events that an attacker goes through to successfully infiltrate a network and exfiltrate data from it.



Gather intelligence
Leverage exploit
Execute malware
Control channel
Steal data
Plan the attack
Silent infection
Malicious file executed
Malware communicates with attacker
Data theft, sabotage, destruction
Restrict access based on apps, users, content
Protect systems and apps from vulnerabilities with threat prevention
Block C&C traffic
Control sensitive data exfiltration with principle of least privilege


Identify threats
Identify vulnerabilities
Assess risk exposure
Develop protection and detection measures
Establish contingency plans
Respond and recover to cyber security incidents
Cyber Security Awareness

The Vulnerabilities

Common vulnerabilities onboard existing or new build ships

Outdated or missing antivirus software and protection from malware

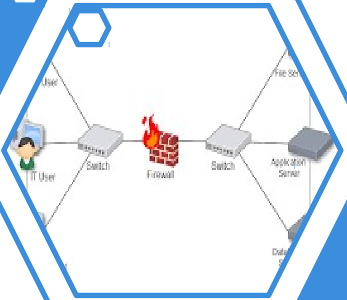
Obsolete and unsupported operating systems

Use of default administrator accounts and passwords

Inadequate access controls for third parties (contractors, service providers..)

Lack of perimeter defences

Inadequate network segmentation



Critical systems connected with the shore side thorough a not secured channel

Examples of vulnerabilities in the navigation systems

1 ***AIS – Automatic identification System***

Because it doesn’t have an inbuilt mechanism to encrypt or authenticate signals, AIS is considered to be a soft target for cyber-attack

- AIS communications do not employ authentication or integrity checks.
- Communication is made over RF. Anyone with a cheap RF receiver can also “listen” to these messages. (Range dependent)

In 2013 Trend Micro (Cyber Security firm) was able to show how AIS could be compromised by preventing a ship from providing movement information, by making “phantom” vessels or structures appear, by staging fake emergencies, and by making it appear to other AIS users that a ship was in a false location. The online services that monitor AIS data to track the position of vessels were also misled by the efforts of Trend Micro.

2 ***ECDIS – Electronic Chart Display and Information System***

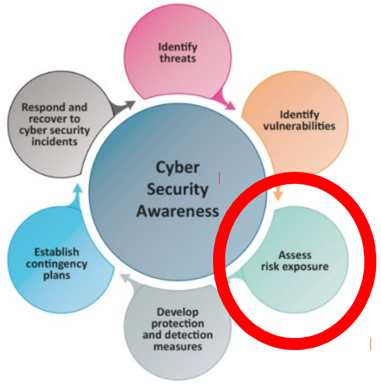
ECDIS systems are in essence desktop PCs

With physical access a malicious person could use the USB slot to load incorrect/outdated maps, access the underlying operating system or spread malware/ransomware. A number of these systems run with administrative rights and no password protection.

3 ***GPS – Global Positioning Systems***

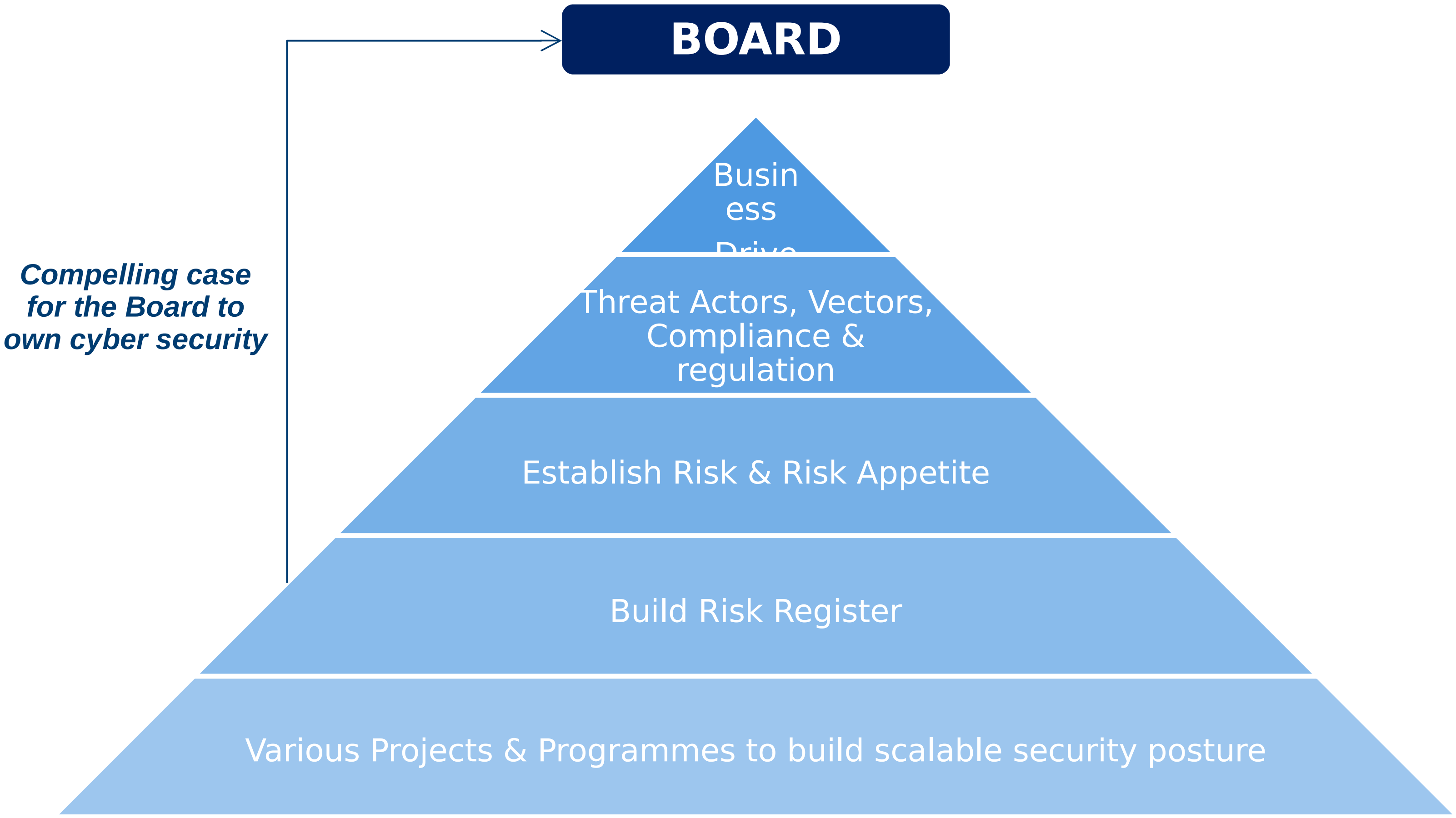
Like AIS, GPS for civilian use is not encrypted or authenticated, and is therefore, a potentially easy target

Earlier in 2013, researchers at the University of Texas were able to demonstrate that they could send a superyacht off course by generating a fake GPS signal that overshadows the genuine signal.
They created false civil GPS signals to gain control of the GPS receivers of a superyacht. This technique, called spoofing, did not trigger alarms on the ship’s navigation equipment and allowed the research team to change the course of the vessel


Identify threats
Identify vulnerabilities
Assess risk exposure
Develop protection and detection measures
Establish contingency plans
Respond and recover to cyber security incidents
Cyber Security Awareness

The Risk Assessment

The top down Risk Assessment approach



BOARD

Compelling case for the Board to own cyber security

Busin
ess
Drive

Threat Actors, Vectors, Compliance & regulation

Establish Risk & Risk Appetite

Build Risk Register

Various Projects & Programmes to build scalable security posture

Risk Assessment on board

Risk Assessment onboard

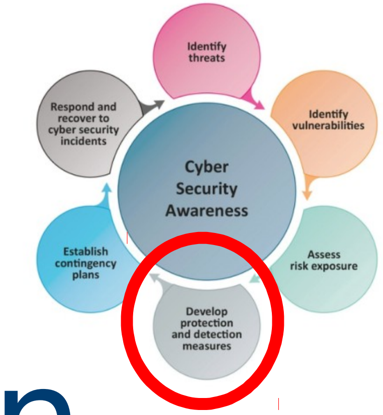
Identification of existing **technical and procedural controls** to protect the onboard IT and OT systems.

Identification of **IT and OT systems** that are vulnerable, the specific vulnerabilities identified, including human factors, and the policies and procedures governing the use of these systems;

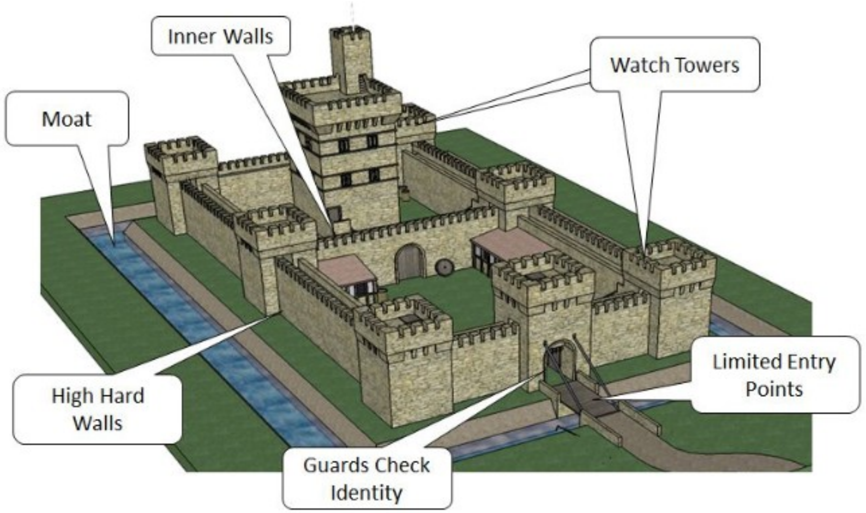
Identification and evaluation of key **ship board operations** that are vulnerable to cyber attacks. These key operations should be protected in order to avoid disruption to commercial operations and ensure the safety of the crew, ship and the marine environment;

Identification of possible **cyber incidents** and their impact on key ship board operations, and the likelihood of their occurrence in order to establish and prioritise mitigating measures

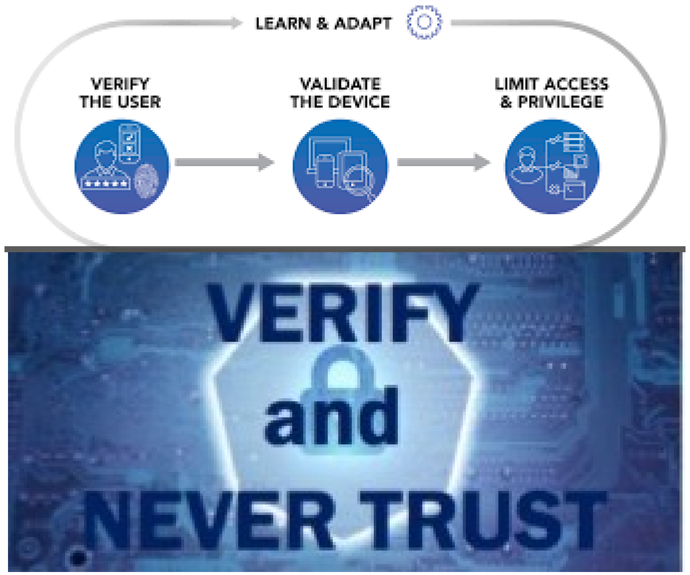
Protection and Detection


Identify threats
Identify vulnerabilities
Assess risk exposure
Develop protection and detection measures
Establish contingency plans
Respond and recover to cyber security incidents
Cyber Security Awareness

From Perimeter Defence to Zero Trust Model

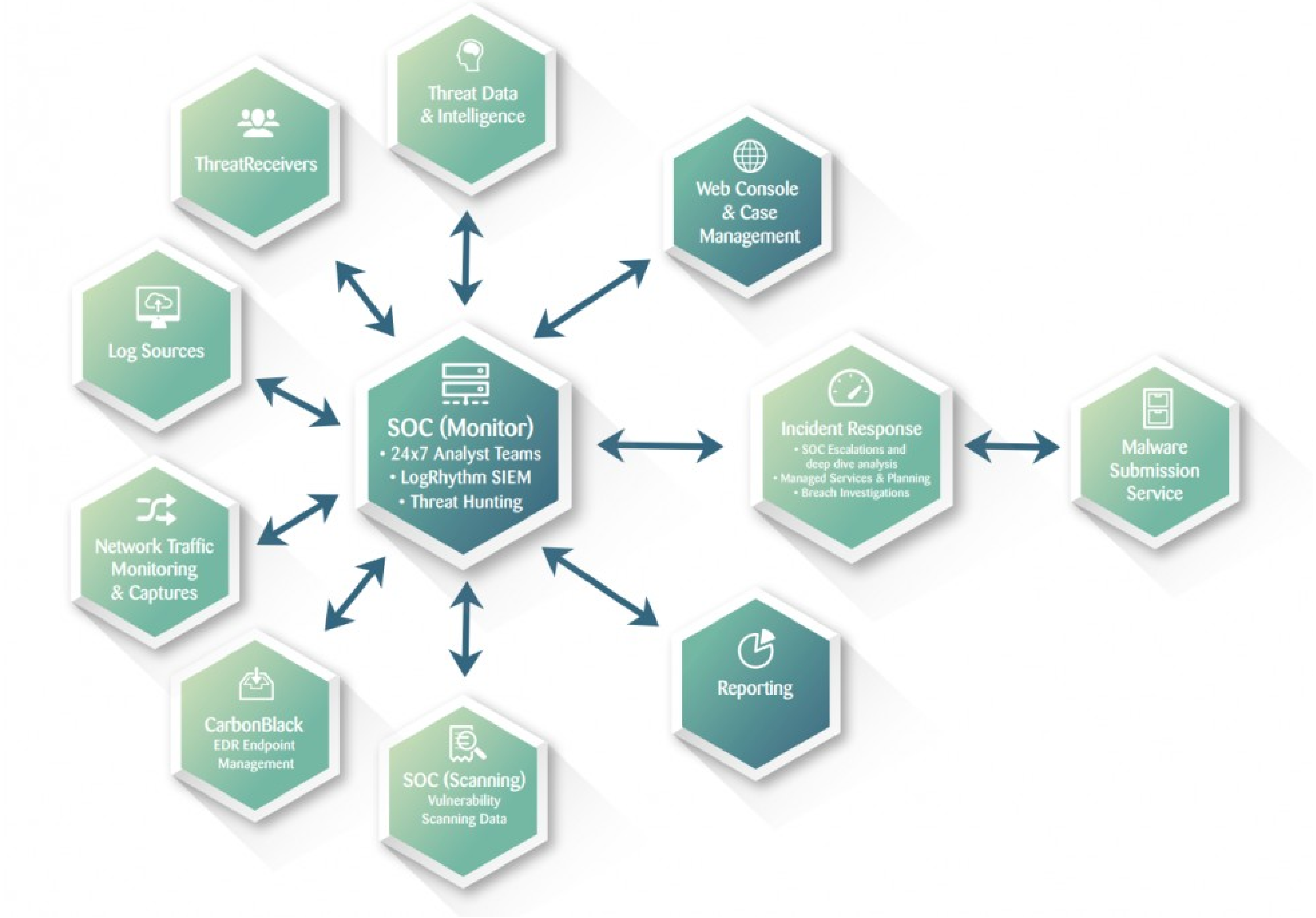


The "Impregnable Fortress"



The "Zero Trust Model"

Protection delivered from a Security Operation Centre (SOC)...



ThreatReceivers

Threat Data & Intelligence

Web Console & Case Management

Log Sources

SOC (Monitor)
- 24x7 Analyst Teams
- LogRhythm SIEM
- Threat Hunting

Incident Response
- SOC Escalations and deep dive analysis
- Managed Services & Planning
- Breach Investigations

Malware Submission Service

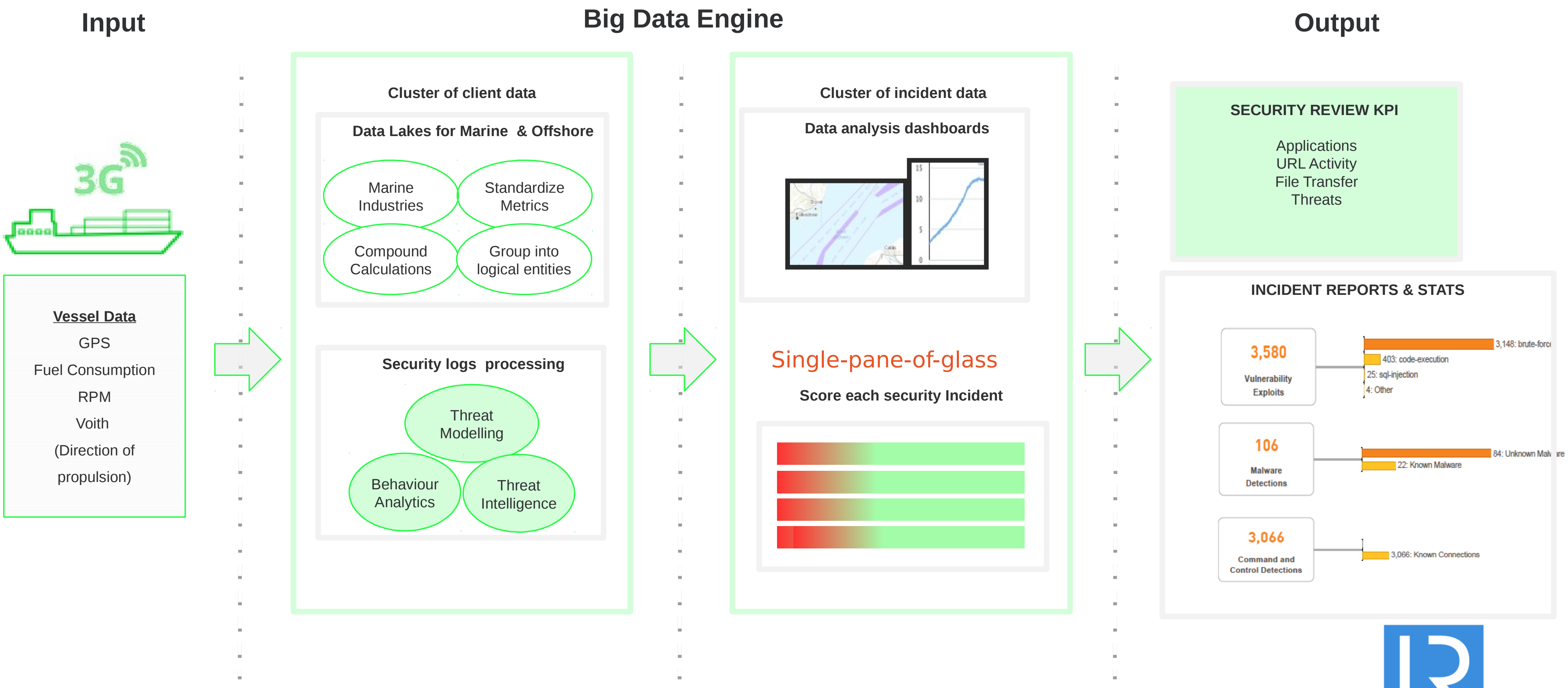
Network Traffic Monitoring & Captures

CarbonBlack EDR Endpoint Management

SOC (Scanning) Vulnerability Scanning Data

Reporting

… trough Analytics and Machine Learning



Input

Big Data Engine

Output

Vessel Data

GPS

Fuel Consumption

RPM

Voith

(Direction of

propulsion)

Cluster of client data

Data Lakes for Marine & Offshore

Marine Industries

Standardize Metrics

Compound Calculations

Group into logical entities

Security logs processing

Threat Modelling

Behaviour Analytics

Threat Intelligence

Cluster of incident data

Data analysis dashboards

Single-pane-of-glass

Score each security Incident

SECURITY REVIEW KPI

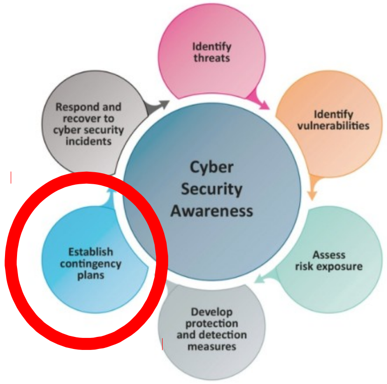
Applications

URL Activity

File Transfer

Threats

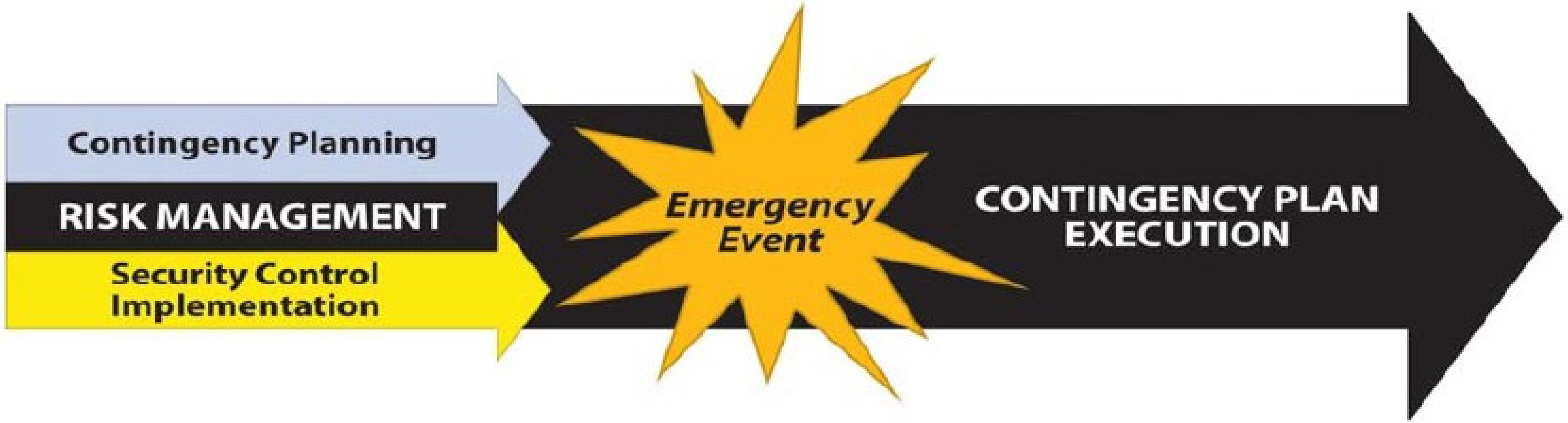
INCIDENT REPORTS & STATS


Identify threats
Identify vulnerabilities
Assess risk exposure
Develop protection and detection measures
Establish contingency plans
Respond and recover to cyber security incidents
Cyber Security Awareness

The Contingency Plan

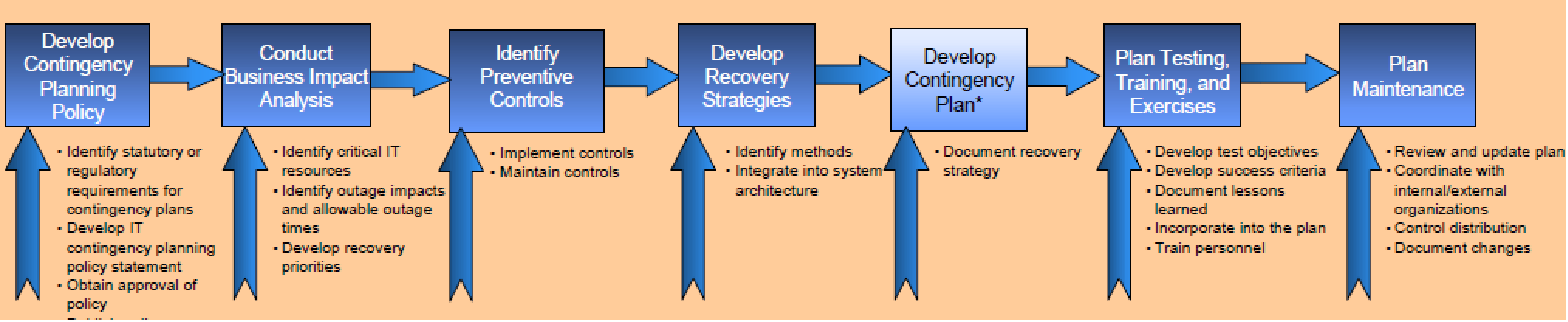
Contingency Plan as an Element of Risk Management Implementation

- Contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency.
- Contingency planning involves identifying, understanding, quantifying and mitigating the risks to the IT systems.



The 7 steps of Contingency Planning

NIST SP800-34 defines the 7 steps of the Contingency Planning as below:



Develop Contingency Planning Policy

- Identify statutory or regulatory requirements for contingency plans
- Develop IT contingency planning policy statement
- Obtain approval of policy

Conduct Business Impact Analysis

- Identify critical IT resources
- Identify outage impacts and allowable outage times
- Develop recovery priorities

Identify Preventive Controls

- Implement controls
- Maintain controls

Develop Recovery Strategies

- Identify methods
- Integrate into system architecture

Develop Contingency Plan*

- Document recovery strategy

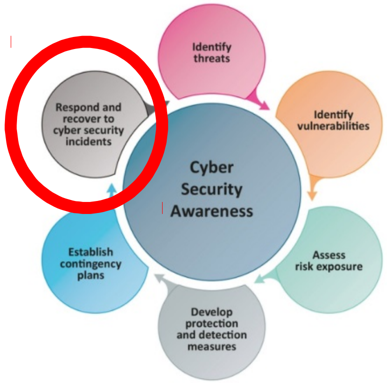
Plan Testing, Training, and Exercises

- Develop test objectives
- Develop success criteria
- Document lessons learned
- Incorporate into the plan
- Train personnel

Plan Maintenance

- Review and update plan
- Coordinate with internal/external organizations
- Control distribution
- Document changes

There are a variety of disaster recovery methods including hot sites, cold sites, managed service provider and cloud-based services. No matter the method, organizations need to ensure the security of the site they're failing over to.


Identify threats
Identify vulnerabilities
Cyber Security Awareness
Assess risk exposure
Develop protection and detection measures
Establish contingency plans
Respond and recover to cyber security incidents

Respond and Recover

The basic steps to respond and recover from a breach

Step 1

Compile an inventory of your assets, then identify the critical assets and data that you hold.

STEP 2

Develop a plan that will outline the steps that your organisation will take during an incident.

STEP 3

Undertake some testing on your Incident Response plan.

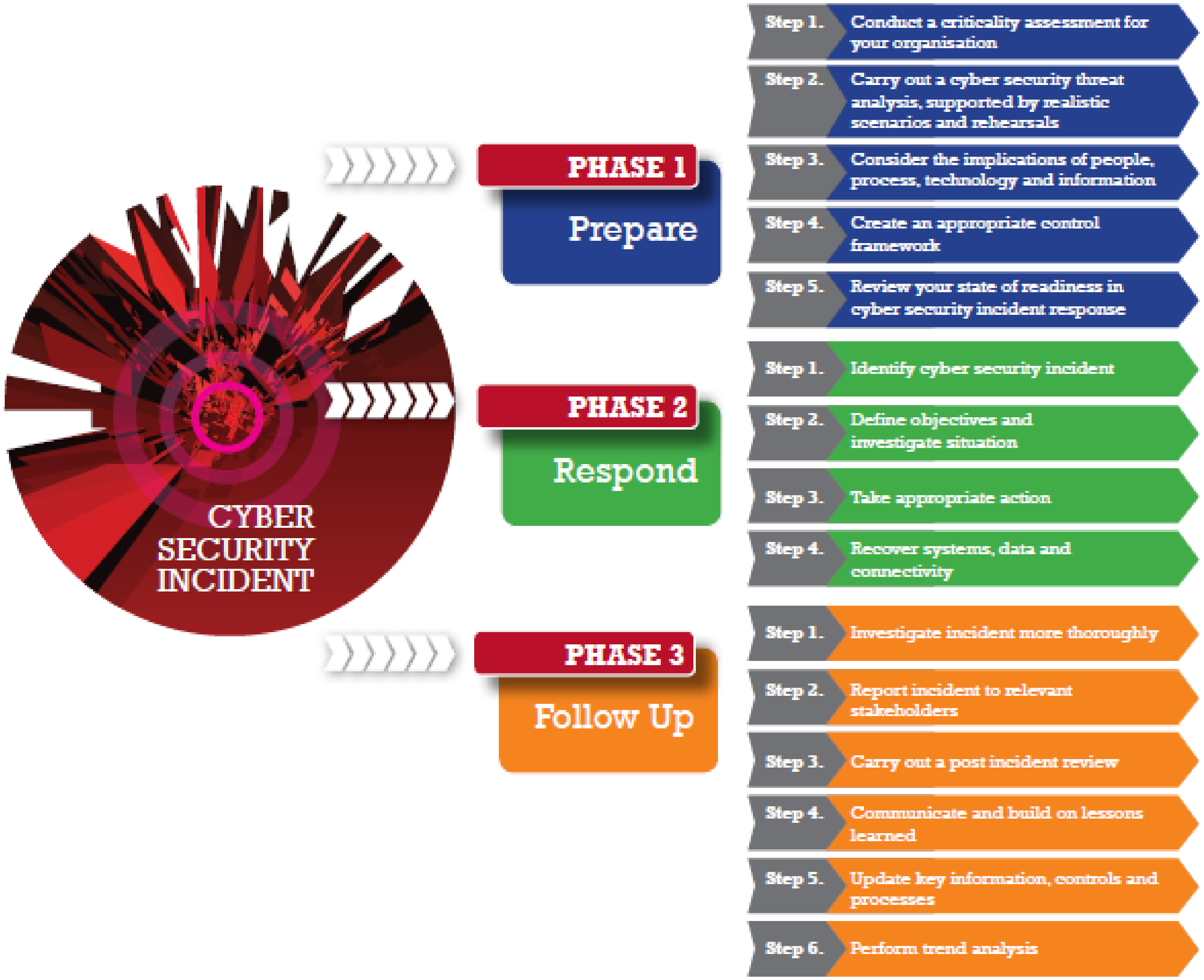
STEP 4

Ensure that you have some staff trained to develop First Responder capability.

STEP 5

Either train technically staff to conduct Incident Response activities or ensure you have swift access to such capability.

The Incident Response framework from CREST



CYBER SECURITY INCIDENT

PHASE 1 Prepare

- Step 1. Conduct a criticality assessment for your organisation
- Step 2. Carry out a cyber security threat analysis, supported by realistic scenarios and rehearsals
- Step 3. Consider the implications of people, process, technology and information
- Step 4. Create an appropriate control framework
- Step 5. Review your state of readiness in cyber security incident response

PHASE 2 Respond

- Step 1. Identify cyber security incident
- Step 2. Define objectives and investigate situation
- Step 3. Take appropriate action
- Step 4. Recover systems, data and connectivity

PHASE 3 Follow Up

- Step 1. Investigate incident more thoroughly
- Step 2. Report incident to relevant stakeholders
- Step 3. Carry out a post incident review
- Step 4. Communicate and build on lessons learned
- Step 5. Update key information, controls and processes
- Step 6. Perform trend analysis

CREST

(Council of Registered Ethical Security Testers)

CREST commissioned a research project into cyber security incident response (CSIR) with the aim of producing a Procurement Guide and a Supplier Selection Guide for CSIR services.

LR’s portfolio of Cyber Security Services

LR’s portfolio of Cyber Security services

Activities typically require a combination of people, technology and processes

LR’s Cyber Security Portfolio

Cyber security functions	Compliance	Training	Advisory	Network Security Monitoring	Advanced Threat Management	Incident Response
Identify	👍	👍	👍	✈	✈	✈
Protect	👍	👍	👍	👍	👍	✈
Detect	✈	👍	👍	👍	👍	✈
Respond	✈	👍	👍	✈	✈	👍
Recover	✈	👍	👍	✈	✈	👍
	Certification is granted based on a companies adherence to standards	Includes training of cyber security specialists, auditors, etc. as well as awareness training for various	Advice on what systems, processes, etc. should be in place to optimise cyber resilience across the organisation	Managed Security Service delivered from a SOC, to scan client’s infrastructure and systems looking for unusual patterns of	Managed Security Service delivered from a SOC, to identify sophisticated and targeted attacks, including malicious	Managed Security Service delivered from a SOC to manage and recover from data breaches using cyber security tools

👍 Relevant

✈ Not typically relevant

Q&A

Lloyd's Register

Contact our experts

www.lr.org/cyber

Elisa Cassi
Product Manager
Cyber Security, Marine and Offshore

T +44 7966 176122
E elisa.cassi@lr.org

JP Cavanna
Head of Business Development
Cyber Security, Lloyd’s Register Group

T +44 207 423 1596
E jp.cavanna@lr.org