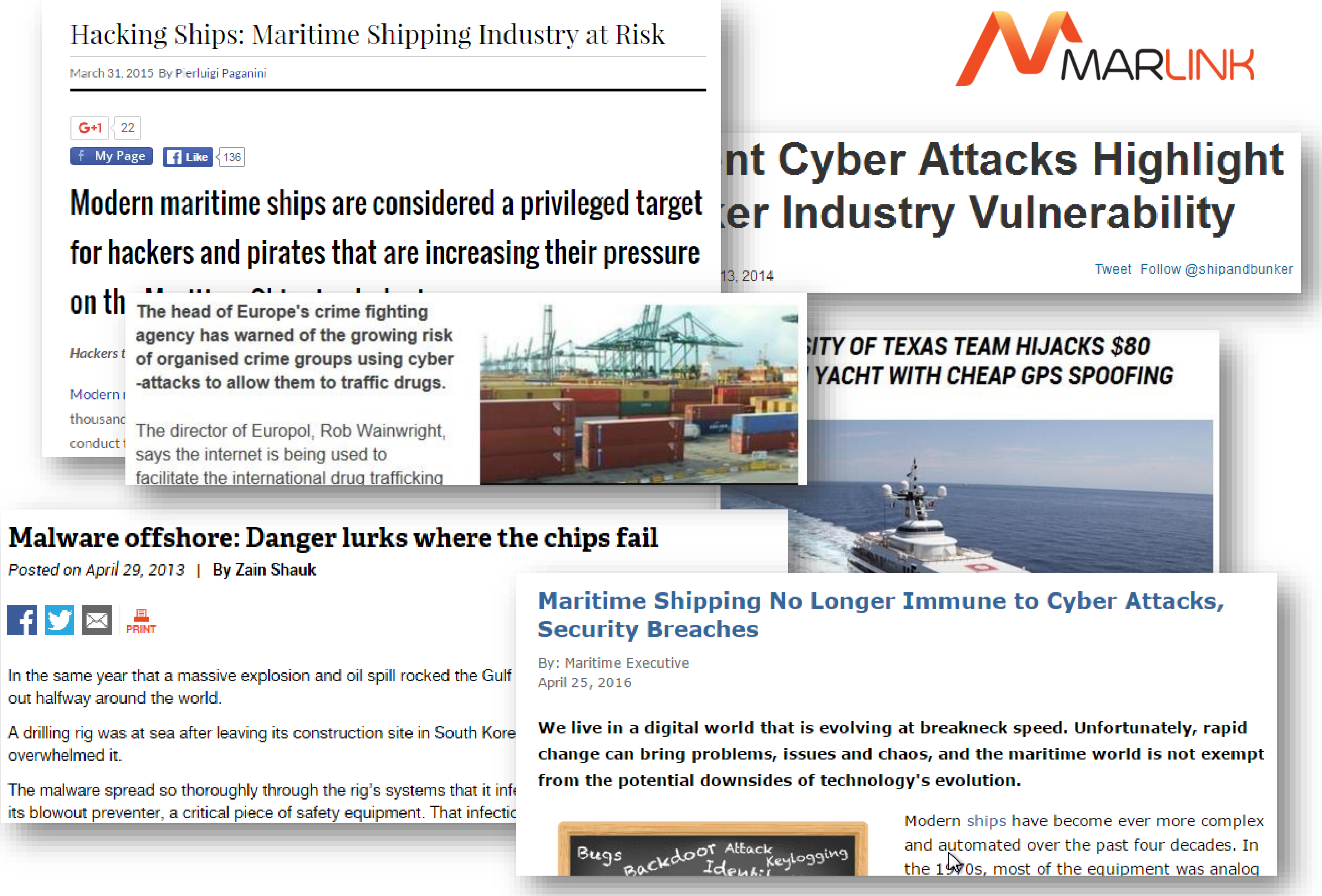
MARLINK

Connect smarter. Anywhere.

The Reality of Shipping's Cyber Challenge

Nov 2016

Usman Tahir – Product Manager



Hacking Ships: Maritime Shipping Industry at Risk

March 31, 2015 By Pierluigi Paganini

G+1 22

My Page Like 136

Modern maritime ships are considered a privileged target for hackers and pirates that are increasing their pressure on th

Hackers t

Modern r

thousand

conduct t

The head of Europe's crime fighting agency has warned of the growing risk of organised crime groups using cyber -attacks to allow them to traffic drugs.

The director of Europol, Rob Wainwright, says the internet is being used to facilitate the international drug trafficking

nt Cyber Attacks Highlight

er Industry Vulnerability

13, 2014

Tweet Follow @shipandbunker

SITY OF TEXAS TEAM HIJACKS $80

YACHT WITH CHEAP GPS SPOOFING

Malware offshore: Danger lurks where the chips fail

Posted on April 29, 2013 | By Zain Shauk

PRINT

In the same year that a massive explosion and oil spill rocked the Gulf out halfway around the world.

A drilling rig was at sea after leaving its construction site in South Kore overwhelmed it.

The malware spread so thoroughly through the rig's systems that it infe its blowout preventer, a critical piece of safety equipment. That infectio

Maritime Shipping No Longer Immune to Cyber Attacks, Security Breaches

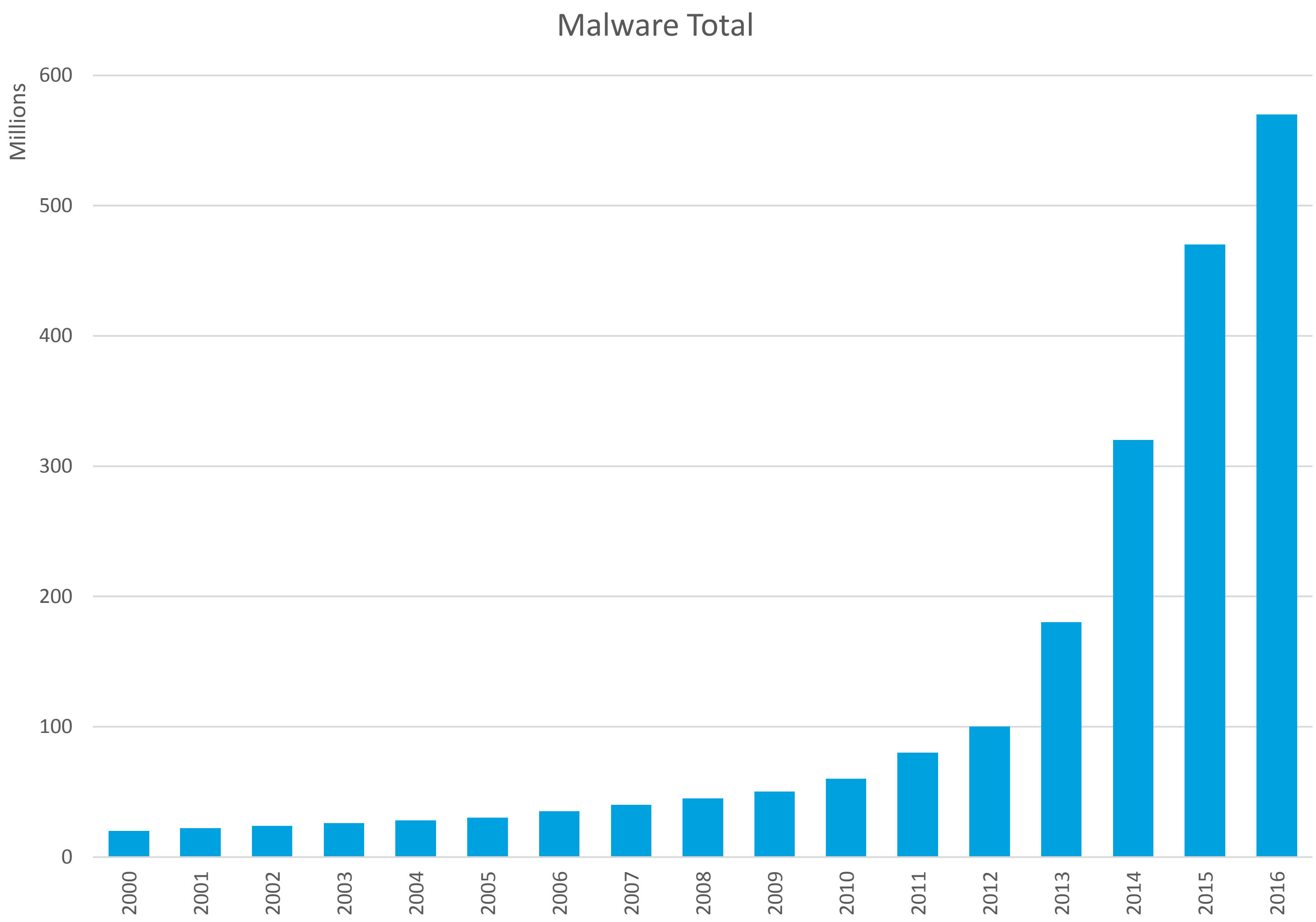
By: Maritime Executive

April 25, 2016

We live in a digital world that is evolving at breakneck speed. Unfortunately, rapid change can bring problems, issues and chaos, and the maritime world is not exempt from the potential downsides of technology's evolution.

Modern ships have become ever more complex and automated over the past four decades. In the 1970s, most of the equipment was analog

Over 390.000 new Malware detected daily…



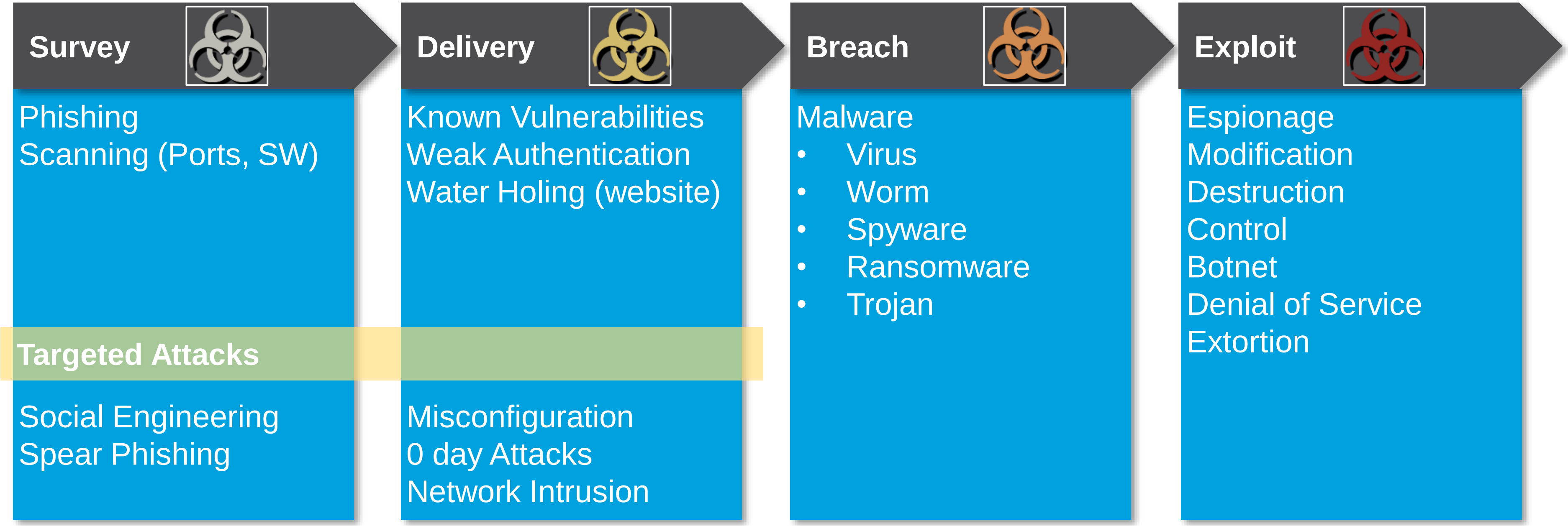
Source: Av-test.org

People will always be the major security weakness…

Legitimate user credentials were used in most data breaches, with some 63% of them using weak, default, or stolen passwords…

Source: 2016 Verizon Data Breach Investigations Report (DBIR)

Cyber Attack Process



Survey

Phishing
Scanning (Ports, SW)

Social Engineering
Spear Phishing

Delivery

Known Vulnerabilities
Weak Authentication
Water Holing (website)

Misconfiguration
0 day Attacks
Network Intrusion

Targeted Attacks

Breach

Malware
- Virus
- Worm
- Spyware
- Ransomware
- Trojan

Exploit

Espionage
Modification
Destruction
Control
Botnet
Denial of Service
Extortion

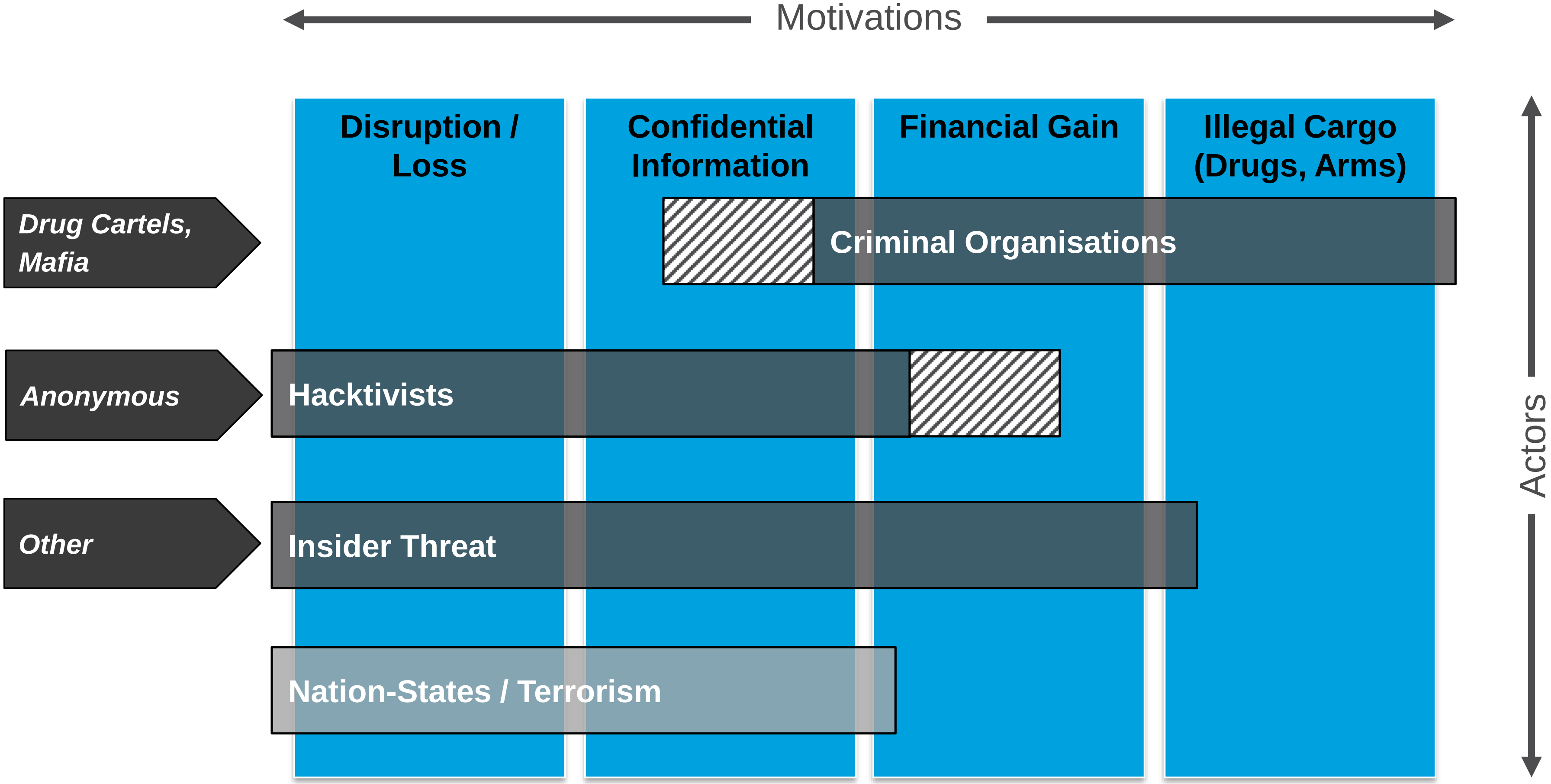
Advanced Persistent Threat (APT)

Sophisticated attack by specialised experts with access to complex IT infrastructure and resources

- **Tailored** to a specific target
- **Low-profile, continuous** (can stay dormant for months)
- **Coordinated human actions** (≠ automated code)
- Typically exploit **multiple vulnerabilities** (0 day, malware, misconfiguration) and **social engineering** (authorised users, secure connections)

➢ **Difficult to detect by conventional means**

Motivations & Actors



Motivations

Disruption / Loss

Confidential Information

Financial Gain

Illegal Cargo (Drugs, Arms)

Drug Cartels, Mafia

Criminal Organisations

Anonymous

Hacktivists

Other

Insider Threat

Nation-States / Terrorism

Actors

Example: Drug Trafficker in Antwerp Port

- An unusually high proportion of containers were reported lost by vessels arriving in Antwerp

- Using malware sent by e-mail, hackers had gained access to the port networks

- The drug traffickers identified and intercepted containers with smuggled drugs

- The cyber attack was professionally organised and executed **stayed undiscovered over two years (2011-2013)**
  - **Advanced Persistent Threat (APT)**

- When the software had been discovered and neutralised, the attackers broke into offices and replaced physical keyboards with keylogging devices
  - **Combination of “old” organised crime and “new” cyber crime**

Source: BBC News (http://www.bbc.com/news/world-europe-24539417)

Maritime Vulnerable to Cyber Attacks

MARLINK

Most shipping operators are lacking the advanced IT capabilities of large corporations

1. **Heterogenic IT network across the fleet**
2. **Running outdated software & hardware on board**
3. **Running 3rd party & unmanaged computers**
4. **Low education on cyber risks & procedures among vessel crew**

The very nature of the Maritime business with remote assets operating around the globe

5. **Significant need for exchanging information across multiple stakeholders**
6. **Most stakeholders scattered across multiple time zones and countries**
7. **Difficult to access the assets in case of emergency**

Maritime Industry Attractive for Cyber Attackers

1 **Illegal Cargo**
Drugs, arms, counterfeit articles can be transported worldwide and hidden among legitimate cargo

2 **Financial Fraud**
Shipping companies are constantly executing large monetary transfers (bunker fuel, freight, port dues, payments to ship yards, vessel owners)

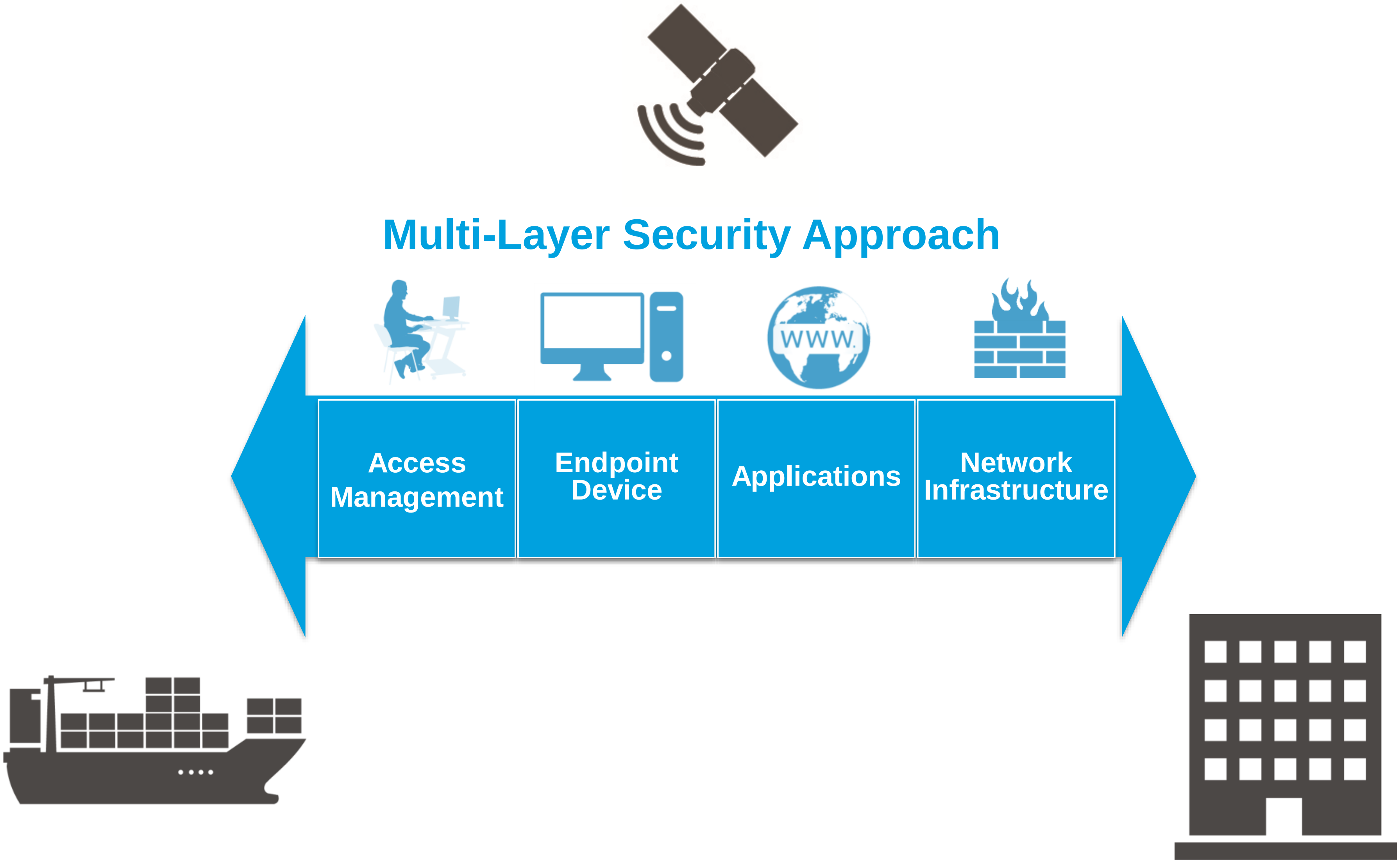
3 **Ransom**
Due to difficulty of physical access to vessels and low crew IT competency, ship'cos might accept paying a ransom for infected PCs to keep the vessel sailing

4 **Political Hacktivism**
High-profile targets for Hacktivists: Oil & Gas industry, Super Yacht VIPs

5 **Piracy**
A cyber attack can support physical piracy (GPS Spoofing, ECDIS manipulation)

6 **Terrorism**
Collisions, blocking major canals or ports can cause huge economic loss

No « Unique » Solution



Multi-Layer Security Approach

Access Management

Endpoint Device

Applications

Network Infrastructure

Available Tools (from Satcom Providers)

- Multi-Satellite Services
- Onboard Network Management
- Web Protection
- Multi-Layer Firewall
- Antivirus Solutions
- Corporate VPN
- Secured BYOD
- User Management

Required for the Ship Digitalisation

Secure remote access solutions to manage all your fleet IT from shore

Managed IT solutions to ensure resiliency of on-board networks & hardware

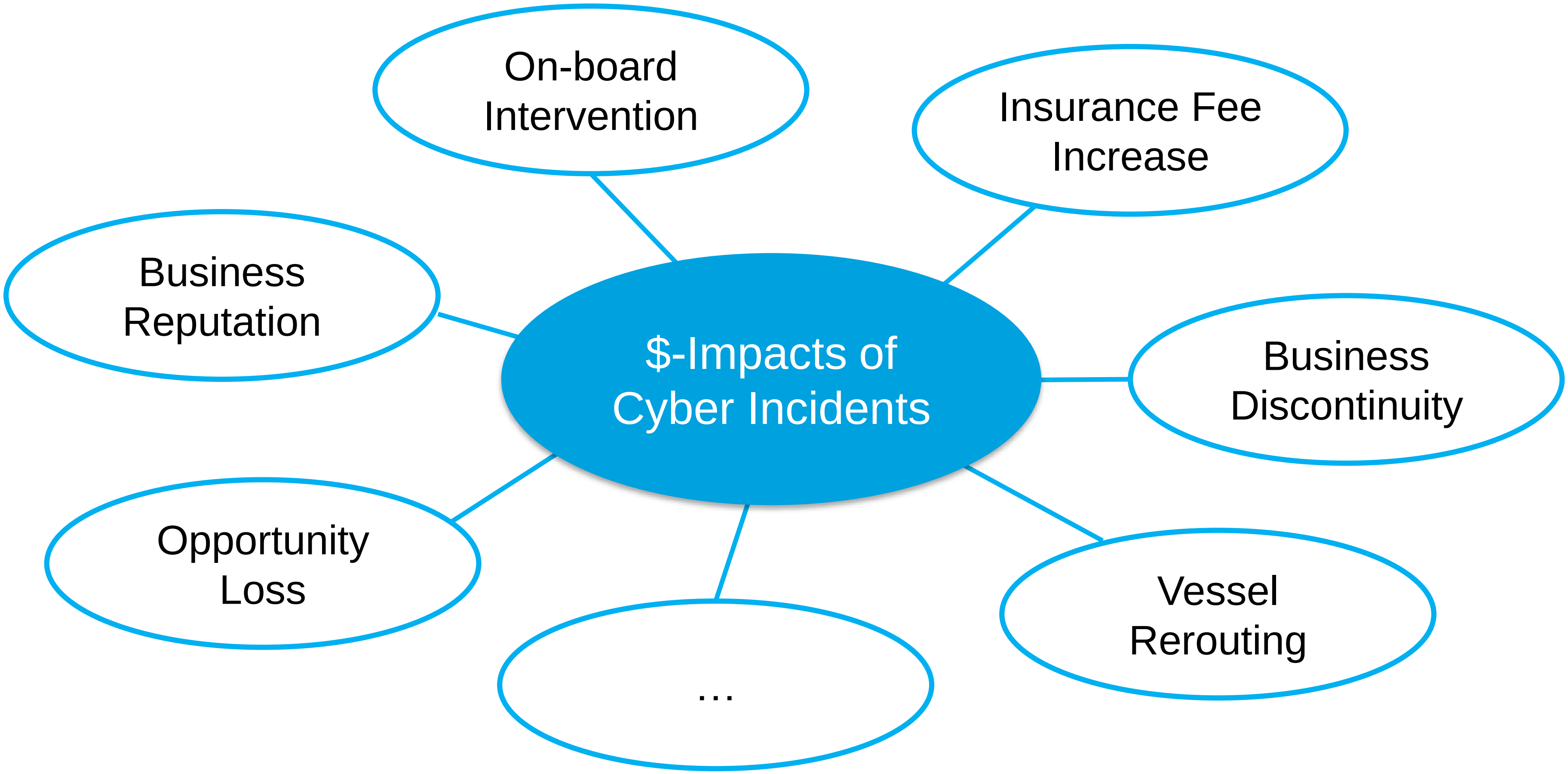
Embarked cloud services to facilitate software deployment & maintenance

Managed content-based services to limit necessity to provide direct Internet access to 3rd party computers or critical navigation systems

Advanced cyber solutions to detect unknown & very sophisticated attacks to limit risk of business damages

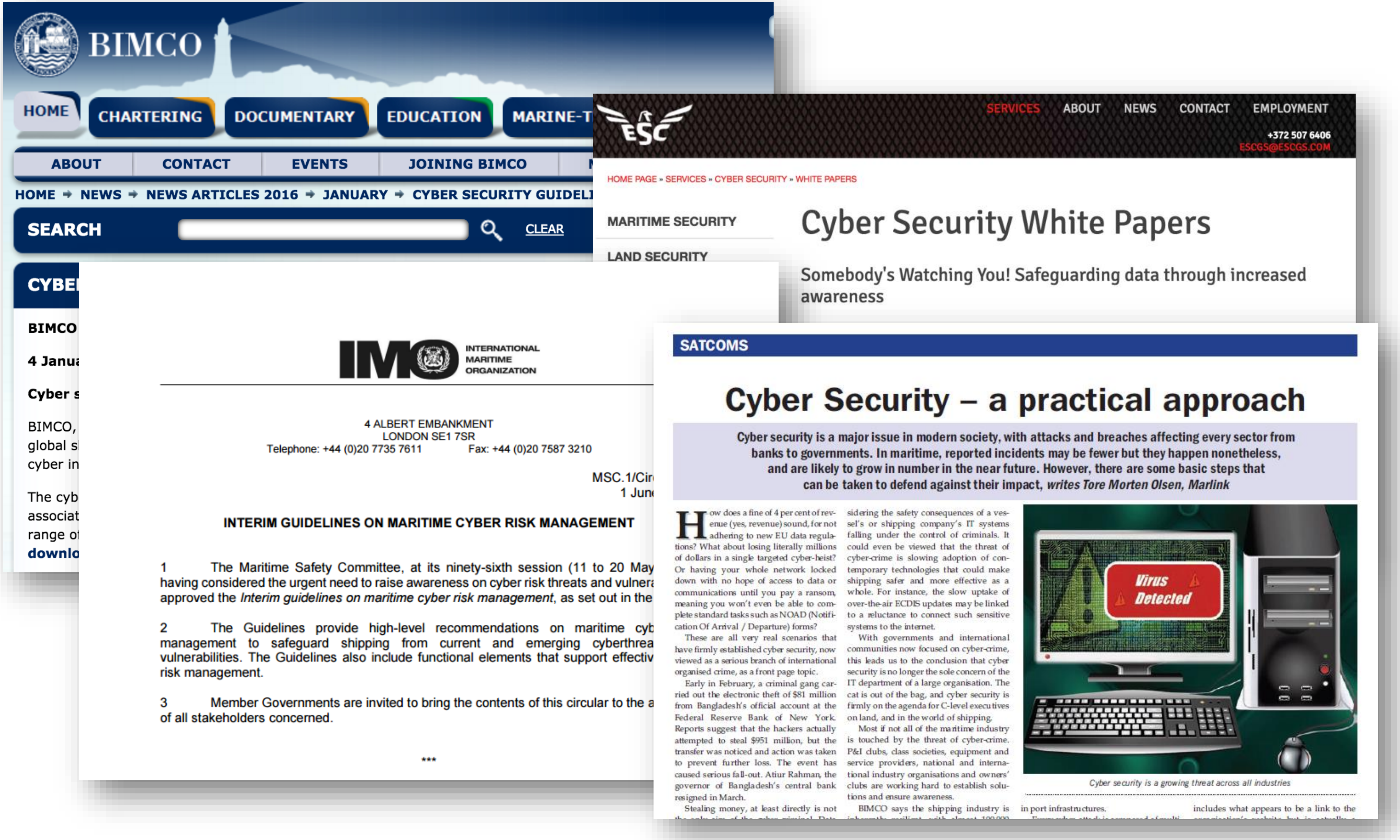
Economics behind Cyber Security (/ TCO)

Cyber Security is not just the matter of ICT…



…would your insurance pay rerouting costs or damages following a cyber attack?

Use Recommendations & Guidelines



CYBE

BIMCO

4 Janu

Cyber s

BIMCO,
global s
cyber in

The cyb
associat
range o
downlo

Cyber Security White Papers

Somebody's Watching You! Safeguarding data through increased awareness

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC.1/Cir
1 Jun

INTERIM GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Maritime Safety Committee, at its ninety-sixth session (11 to 20 May having considered the urgent need to raise awareness on cyber risk threats and vulnera approved the *Interim guidelines on maritime cyber risk management*, as set out in the

2 The Guidelines provide high-level recommendations on maritime cyb management to safeguard shipping from current and emerging cyberthrea vulnerabilities. The Guidelines also include functional elements that support effectiv risk management.

3 Member Governments are invited to bring the contents of this circular to the a of all stakeholders concerned.

***

SATCOMS

Cyber Security – a practical approach

Cyber security is a major issue in modern society, with attacks and breaches affecting every sector from banks to governments. In maritime, reported incidents may be fewer but they happen nonetheless, and are likely to grow in number in the near future. However, there are some basic steps that can be taken to defend against their impact, *writes Tore Morten Olsen, Marlink*

How does a fine of 4 per cent of revenue (yes, revenue) sound, for not adhering to new EU data regulations? What about losing literally millions of dollars in a single targeted cyber-heist? Or having your whole network locked down with no hope of access to data or communications until you pay a ransom, meaning you won't even be able to complete standard tasks such as NOAD (Notification Of Arrival / Departure) forms?

These are all very real scenarios that have firmly established cyber security, now viewed as a serious branch of international organised crime, as a front page topic.

Early in February, a criminal gang carried out the electronic theft of $81 million from Bangladesh's official account at the Federal Reserve Bank of New York. Reports suggest that the hackers actually attempted to steal $951 million, but the transfer was noticed and action was taken to prevent further loss. The event has caused serious fall-out. Atiur Rahman, the governor of Bangladesh's central bank resigned in March.

Stealing money, at least directly is not

sidering the safety consequences of a vessel's or shipping company's IT systems falling under the control of criminals. It could even be viewed that the threat of cyber-crime is slowing adoption of contemporary technologies that could make shipping safer and more effective as a whole. For instance, the slow uptake of over-the-air ECDIS updates may be linked to a reluctance to connect such sensitive systems to the internet.

With governments and international communities now focused on cyber-crime, this leads us to the conclusion that cyber security is no longer the sole concern of the IT department of a large organisation. The cat is out of the bag, and cyber security is firmly on the agenda for C-level executives on land, and in the world of shipping.

Most if not all of the maritime industry is touched by the threat of cyber-crime. P&I clubs, class societies, equipment and service providers, national and international industry organisations and owners' clubs are working hard to establish solutions and ensure awareness.

BIMCO says the shipping industry is

Cyber security is a growing threat across all industries

in port infrastructures.

includes what appears to be a link to the

→ Cyber Security article in DigitalShip August 2016

Thank you!

Any questions?

Usman Tahir
Product Manager

Email: usman.tahir@marlink.com

MARLINK

Connect smarter. Anywhere.