MARLINK

Connect smarter. Anywhere.

The Reality of Shipping's Cyber Challenge

Michael Owen
VP Business Capture & Development

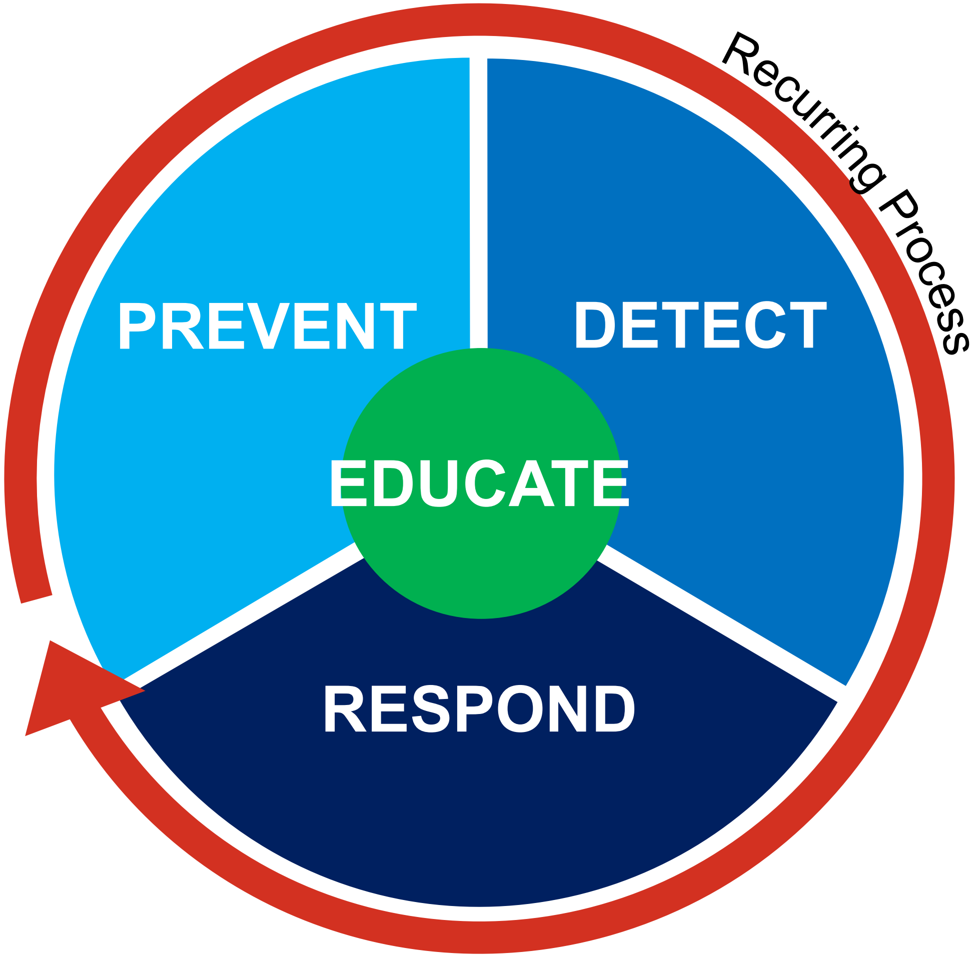
Michael Owen

VP Business Capture & Development

Oslo, Norway

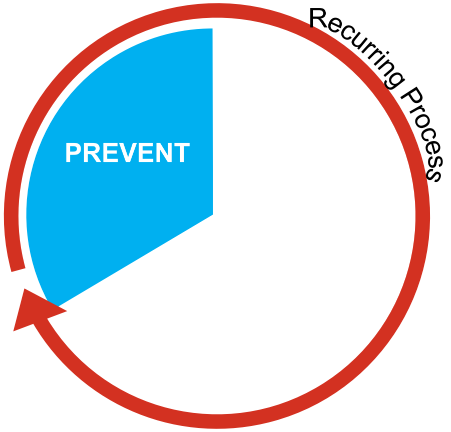
Email: Michael.Owen@marlink.com
Phone: +47 994 404 91

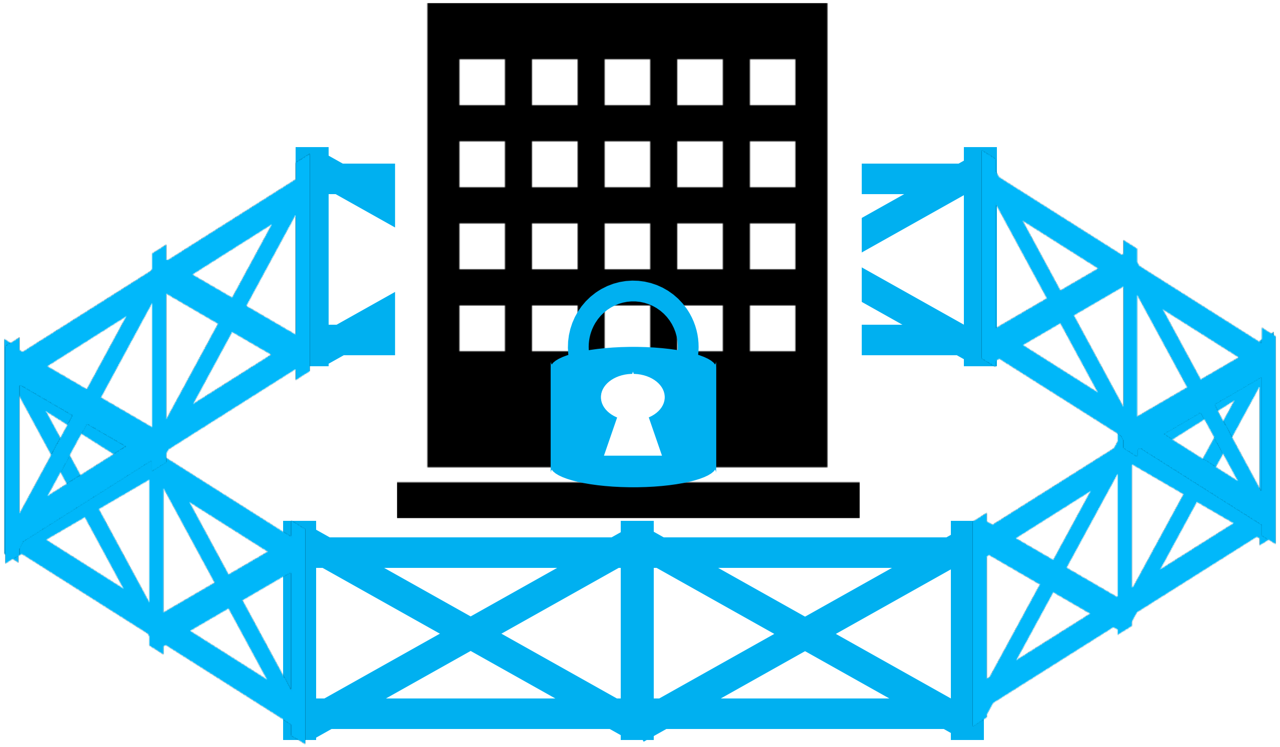
The Reality of Cyber Security



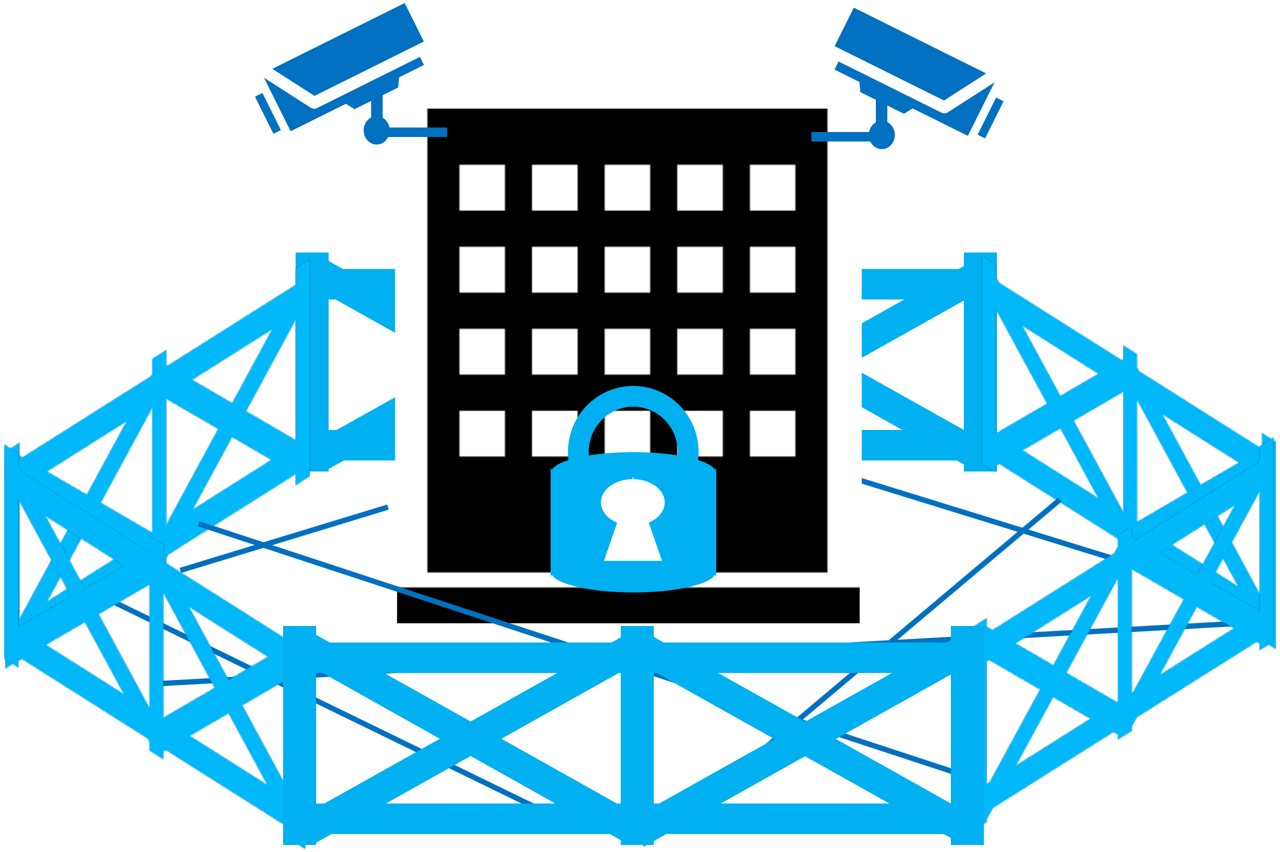
Analogy

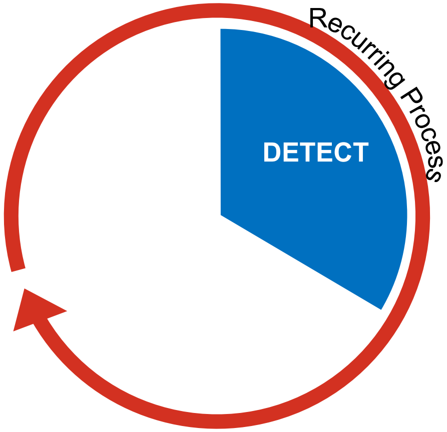
It’s like protecting a property…



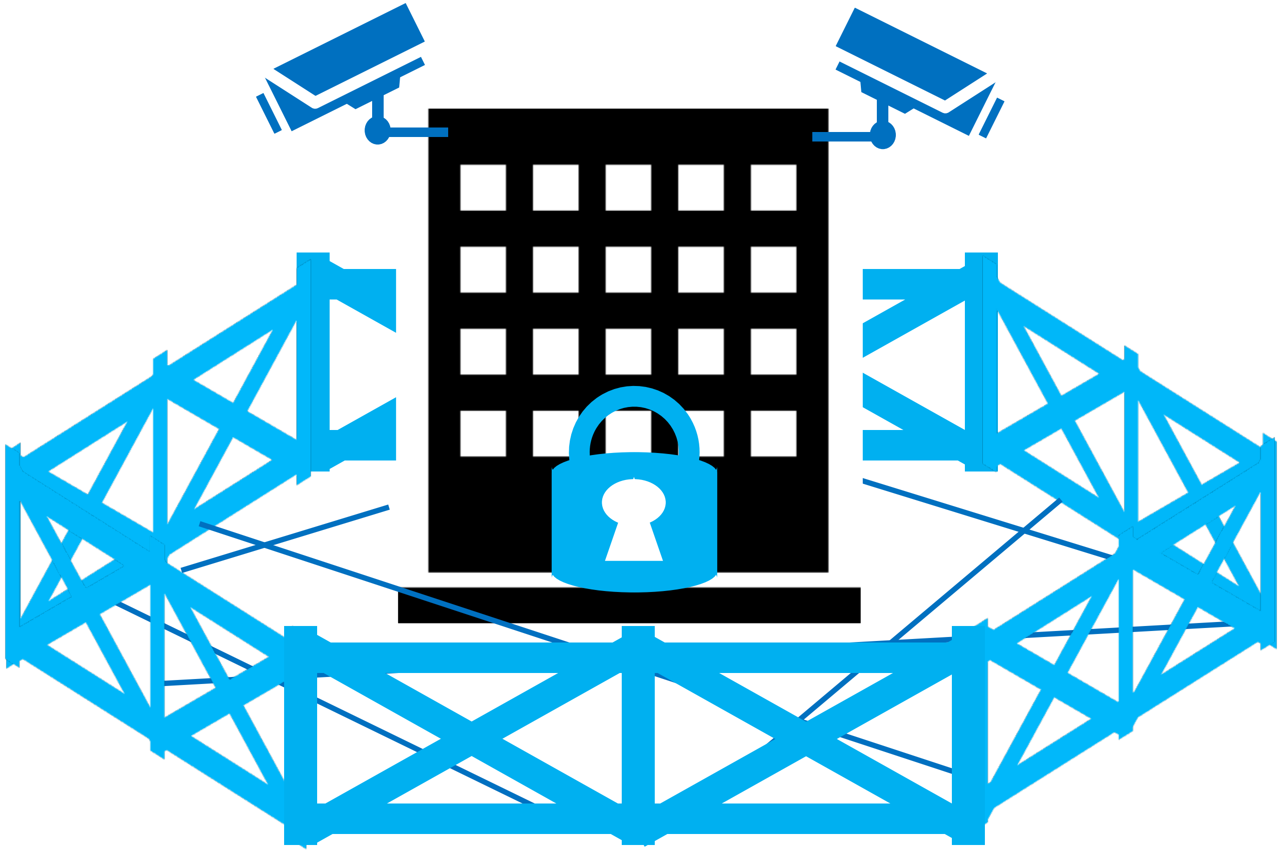


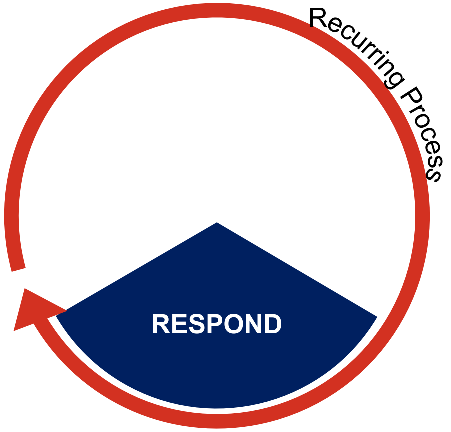
…ensure you can detect intrusions…



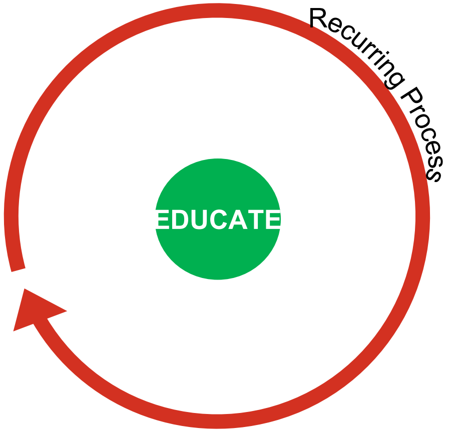


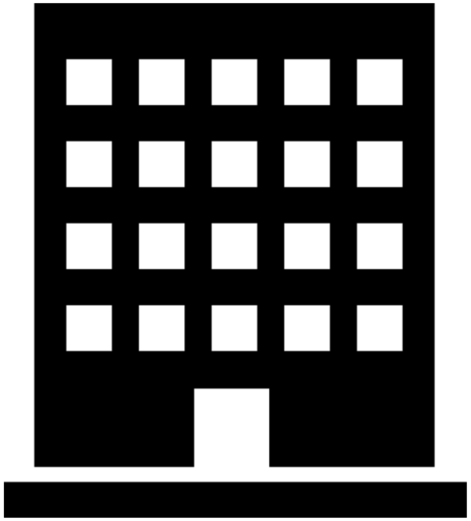
…and get support when required!

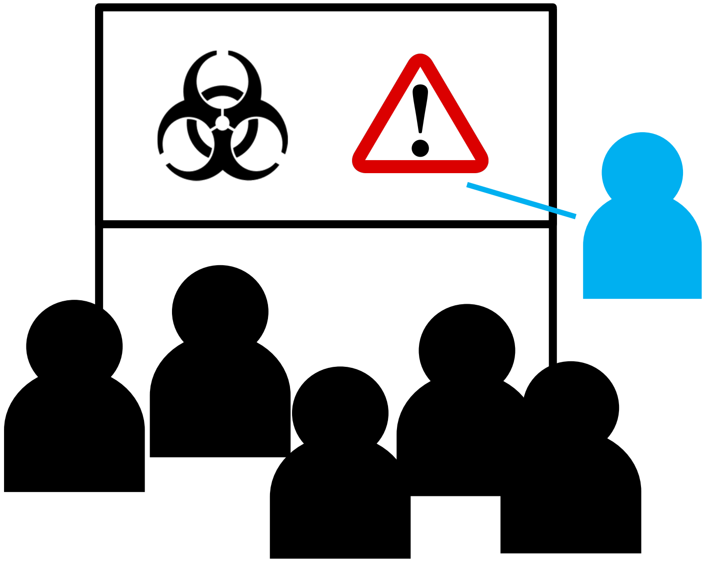




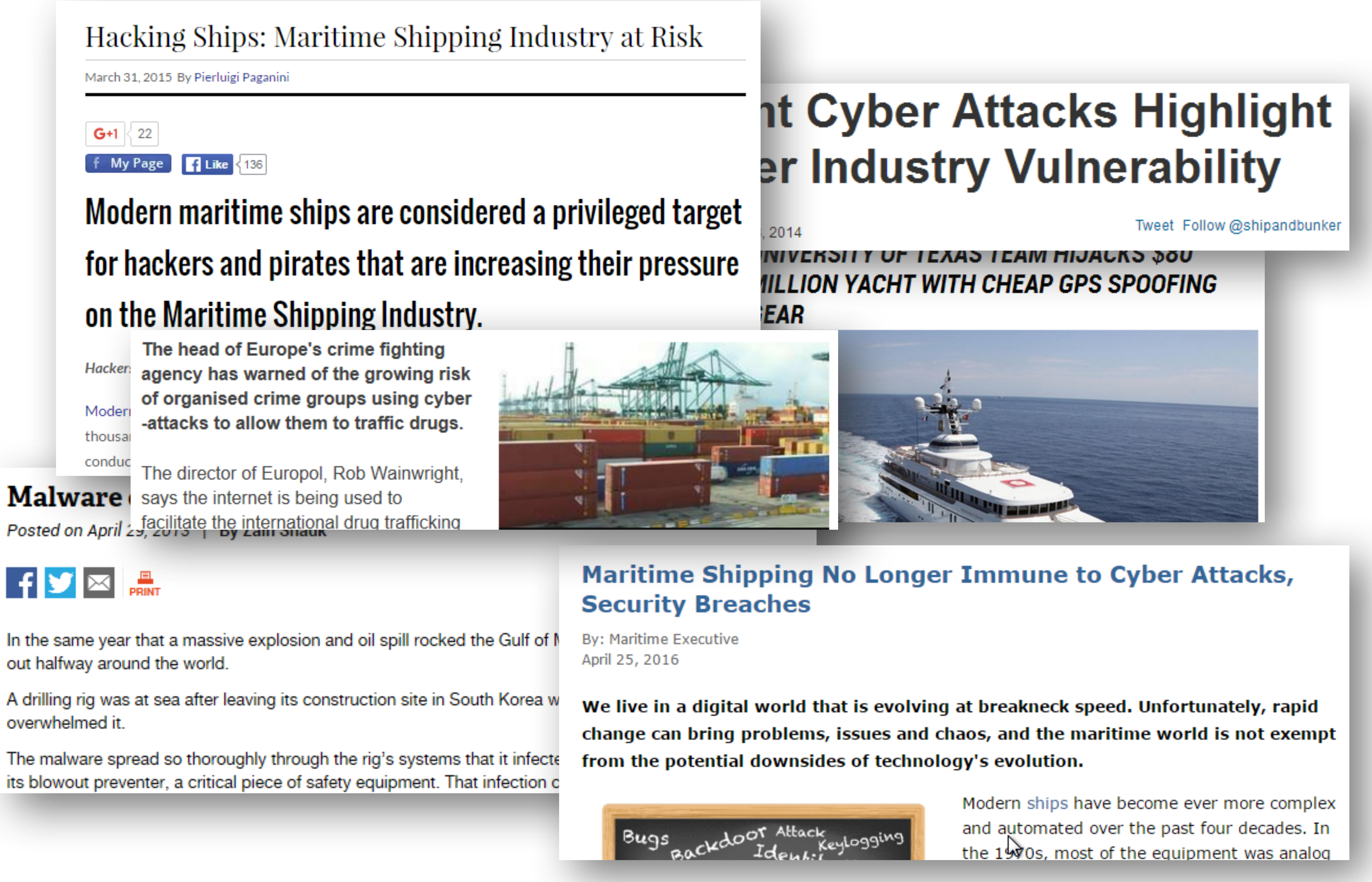
But it is also about limiting risks made by ignorance or negligence!







The Reality of Cyber Security for Maritime!



Hacking Ships: Maritime Shipping Industry at Risk

March 31, 2015 By Pierluigi Paganini

Modern maritime ships are considered a privileged target for hackers and pirates that are increasing their pressure on the Maritime Shipping Industry.

Hacker

Moderr

thousar

conduc

nt Cyber Attacks Highlight er Industry Vulnerability

, 2014

NIVERSITY OF TEXAS TEAM HIJACKS $80 ILLION YACHT WITH CHEAP GPS SPOOFING EAR

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

Malware

Posted on April 29, 2015 | **By Zain Shauk**

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

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

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

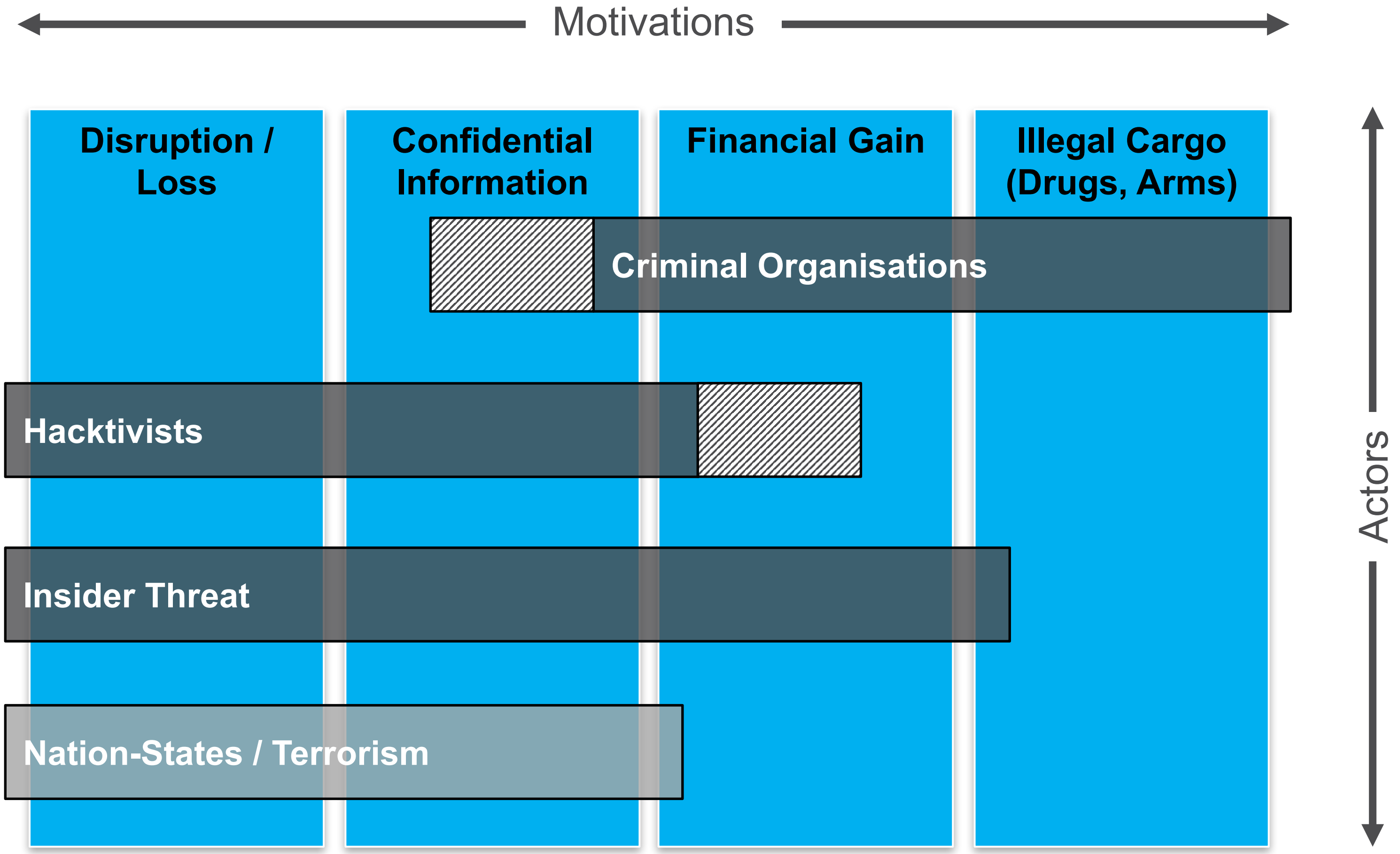
Maritime Shipping No Longer Immune to Cyber Attacks, Security Breaches

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

Motivations & Actors



Motivations

Disruption / Loss

Confidential Information

Financial Gain

Illegal Cargo (Drugs, Arms)

Criminal Organisations

Hacktivists

Insider Threat

Nation-States / Terrorism

Actors

BIMCO Survey

story in numbers

Fairplay.IHS.com

Get access to integrated maritime intelligence:
Shipping data offerings available. For more information or to discuss the information you are interested in please contact out sales team:
✉ marketing@ihsmarkit.com ☎ +44 (0) 1344 328155

www.maritime.IHS.com
Integrating the power of Sea-web & AISLive

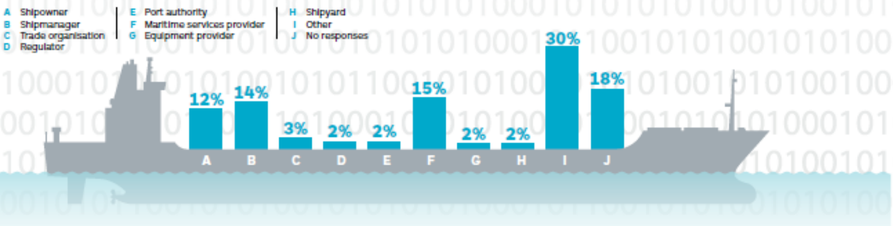
story in numbers

2016 cyber security survey

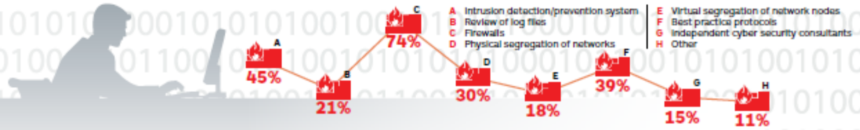
in association with BIMCO

IHS Markit and BIMCO launched the maritime cyber security survey on 22 July. The survey, which ran for four weeks, was promoted on social media and via email. More than 300 industry players responded. Of the 300 respondents, 65 had been a victim of a cyber attack. Here are some of the highlights of the insights gathered from respondents to the maritime cyber security survey.

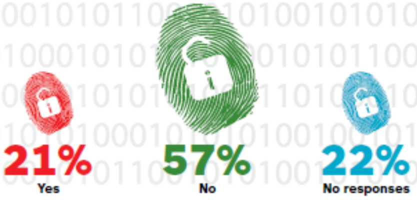
Who responded?



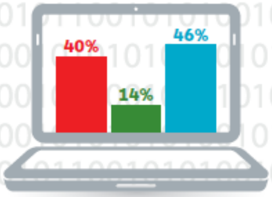
What is in place to protect against cyber attack?



Have you been a victim of cyber attack?

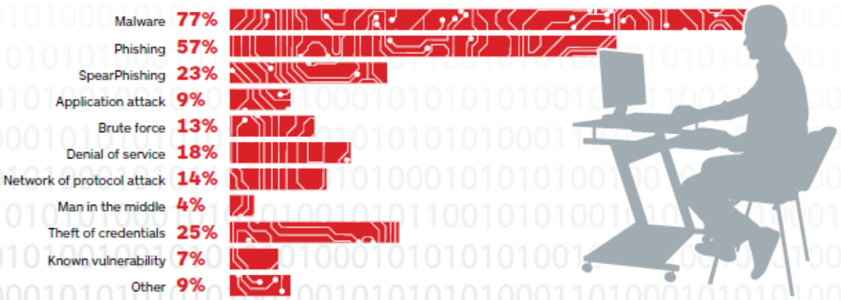


Were protection strategies in place?

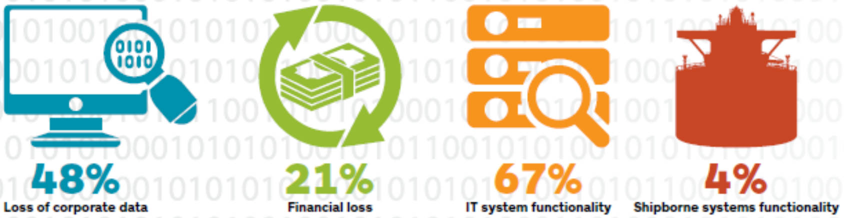


Data Source: IHS Markit in association with BIMCO
Image source: Shutterstock

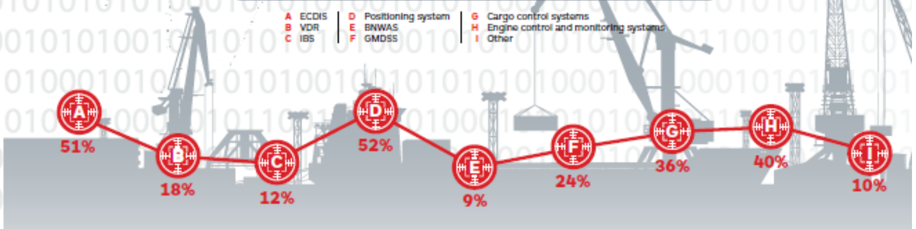
What was the nature of the attack?



What was the extent of the attack?



Which shipborne systems are most vulnerable?



Guidelines & Future Regulation

EU General Data Protection Regulation (GDPR)

- To come into force May 2018
- All organizations must appoint a Security Officer
- 72-hour notification period for all persons / entities whose data has been breached
  - ➢ Penalty: up to 4% of revenue !

BIMCO

HOME CHARTERING

ABOUT CONTACT EVI

HOME ➔ NEWS ➔ NEWS ARTICLES 2016 ➔

SEARCH

CYBER SECURITY GUIDELINES

BIMCO PRESS RELEASE

4 January 2016

Cyber security guidelines for ships laun

BIMCO, together with other leading shipping
global shipping industry prevent major safet
cyber incident onboard a ship.

The cyber guidelines launched today are a f
associations, comprising BIMCO, CLIA, ICS,
range of stakeholders. The Guidelines on Cy
download from the BIMCO website.

OUT NEWS CONTACT EMPLOYMENT

+372 507 6406
ESCGS@ESCGS.COM

te Papers

ugh increased

he use of targeted phishing
dential information. No one is

ure of more than 150 million
users of infidelity site Ashley
y companies today.

sing on specific areas could
s resulting from a successful

E

.1526
2016

2016),
bilities,
annex.

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

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

***

Digital Ship –Cyber-Resilience Topics: 2017

1) Responsibility and liability for a cyber security breach, incident or loss

2) Possible or available solutions, standards, networks, designs

3) Guidelines and best practices

4) Systems protection, transparency of risks/resilience, access/confinement

5) Awareness, training, the human element, crew and management responsibility

Some thoughts for your Ship Digitalisation…

Secure remote access solutions to manage all your fleet IT from shore *(working over any satellite service, with no public IP address)*

Managed IT solutions to ensure resiliency of on-board networks *(keeping all your computers / software up-to-date without human interaction)*

Embarked cloud service to facilitate software deployment & maintenance *(no dedicated and unmanaged 3rd party computers)*

Managed content distribution services to limit necessity to provide Internet access to 3rd party computers *(distribution of eCharts, eLearning, eforms, M2M…)*

Advanced cyber solutions to detect targeted hacker attacks *(APT / zero day attacks)*

Proper Defence Controls include:

Restricting portable media and implementing antivirus software

Policy for Secure operations and maintenance of system

Secure design and deployment of applications and system

Employee awareness

Securing the ports which are primarily using automated systems for cargo handling.

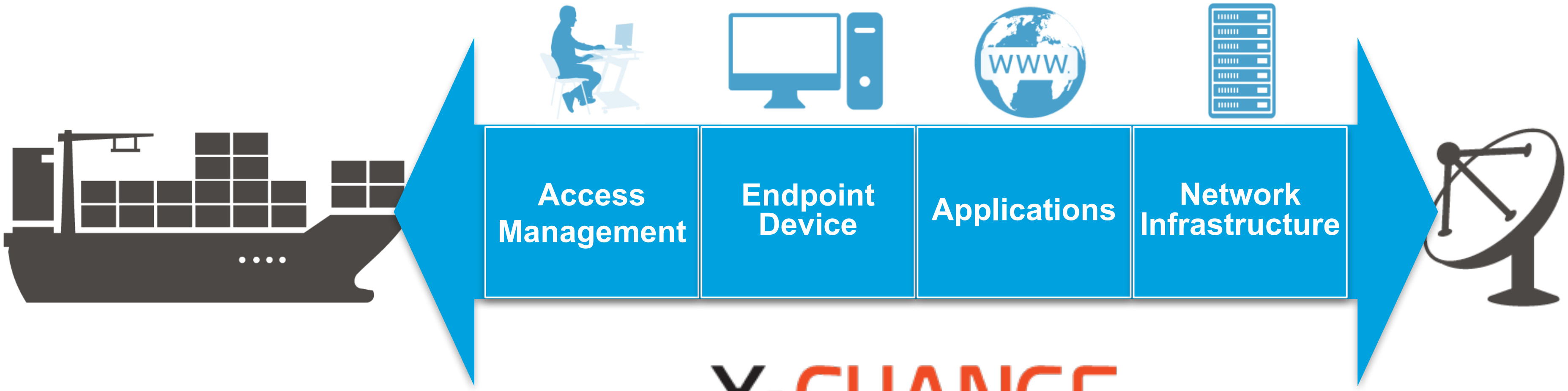
http://securityaffairs.co/wordpress/35504/hacking/hacking-maritime-shipping-industry.html

Some questions for your Satcom Provider…

- Describe your Maturity level on Information Security (ISO?)
- Do you perform periodic audits of your infrastructure (penetration testing)?
- Do you separate traffic on-board (i.e. crew vs. corporate vs. operations)?
- Do you block data communication between vessels (vessel-to-vessel)?
- How do you secure against DoS attacks?
- What Security Options do you offer?

Marlink’s Security Portfolio

Multi-Layered Security Solutions



X·CHANGE

SKYFILE ANTI VIRUS

KeepUp@Sea

palantir

PORTAL360

SEALINK

Maritime Cyber Security Check List

MARLINK

PREVENT

- Onboard Network Management
- Multi-Satellite Services
- Multi-Layer Firewall
- Antivirus Solutions
- Corporate VPN
- Web Filtering
- User Management

DETECT

- Network Surveillance / DPI
- Zero Day Attacks
- File scanning

RESPOND

- Critical Systems Backup
- Secure Remote Access
- On-board IT Resilience

EDUCATE

- Information Portal
- Training Academy
- BYOD Adapted Environment

Information Sources

DNV·GL

RECOMMENDED PRACTICE

DNVGL-RP-0496 Edition September 2016

Cyber security resilience management for ships and mobile offshore units in operation

The electronic pdf version of this document, available free of charge from http://www.dnvgl.com, is the officially binding version.

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

Produced and supported by
BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO

BIMCO
CLIA
INTERNATIONAL CHAMBER OF SHIPPING
INTERCARGO
INTERTANKO

MARLINK

Connect smarter. Anywhere.