Human factors in maritime cyber security

10 June 2021 • 13:00-14:30 BST

Sponsored by

NEPTUNE
MARINE CYBER SECURITY

Presentation & sponsor documents:

Part of
Maritime Cyber
Tech & Ops
Webinar Day

10 June 2021

MARITIME
OPTIMISATION
& COMMUNICATIONS

#maritimecyber

Grant Thornton
An instinct for growth™

The Weakest Link

Staying Seafarer Secure

Vijay Rathour
Partner, Grant Thornton
Digital Forensics Group

Our Weakest Link?

The Human Factor

Operational Technology

Information Technology

Cyber Risks from Tele-Working

- Cyber Threats in Maritime are **increasing**
- **400% increase** in attempted hacks during 2020

  (Naval Dome)
- **10 fold increase** in home working focused attacks during the first half of 2020
- **Low %** of seafarers received **cyber training**

Cyber Risks from Tele-Working

- Attacks focused on **Human** and Configuration failure:
  - **Malware**: easy and sophisticated
  - **Ransomware/Hijack**: socio economics!
  - **Spear Phishing & Whaling:** CSO, CFO
  - **Vulnerability** IOCs (eg SolarWinds)
  - Ship & Crew **networks** not always segregated

Cause & Effect

Cyber Risks from Tele-Working

Cause:

- **Global travel restrictions**
- Social distancing measures
- **Hands off the tech:** not able to fly to the ship/rig
- **Economic pressures** resulting in lowered investment in Cyber and IT projects
- Furlough and **cost savings** for Service Engineers

Cyber Risks from Tele-Working

Effect:

- Ship and Offshore Rig Staff **remotely connecting OT systems to onshore networks** for servicing
- These can require operator to **bypass security protections** - creating an opening for a cyberattack
- Breakdown in segregation of **OT and IT systems**
- Our **remote/onshore** staff become **entry vector**

The Threat Landscape

Stopping Attackers Early

Colonial Pipeline

Our goal is to make money and not creating problems for society

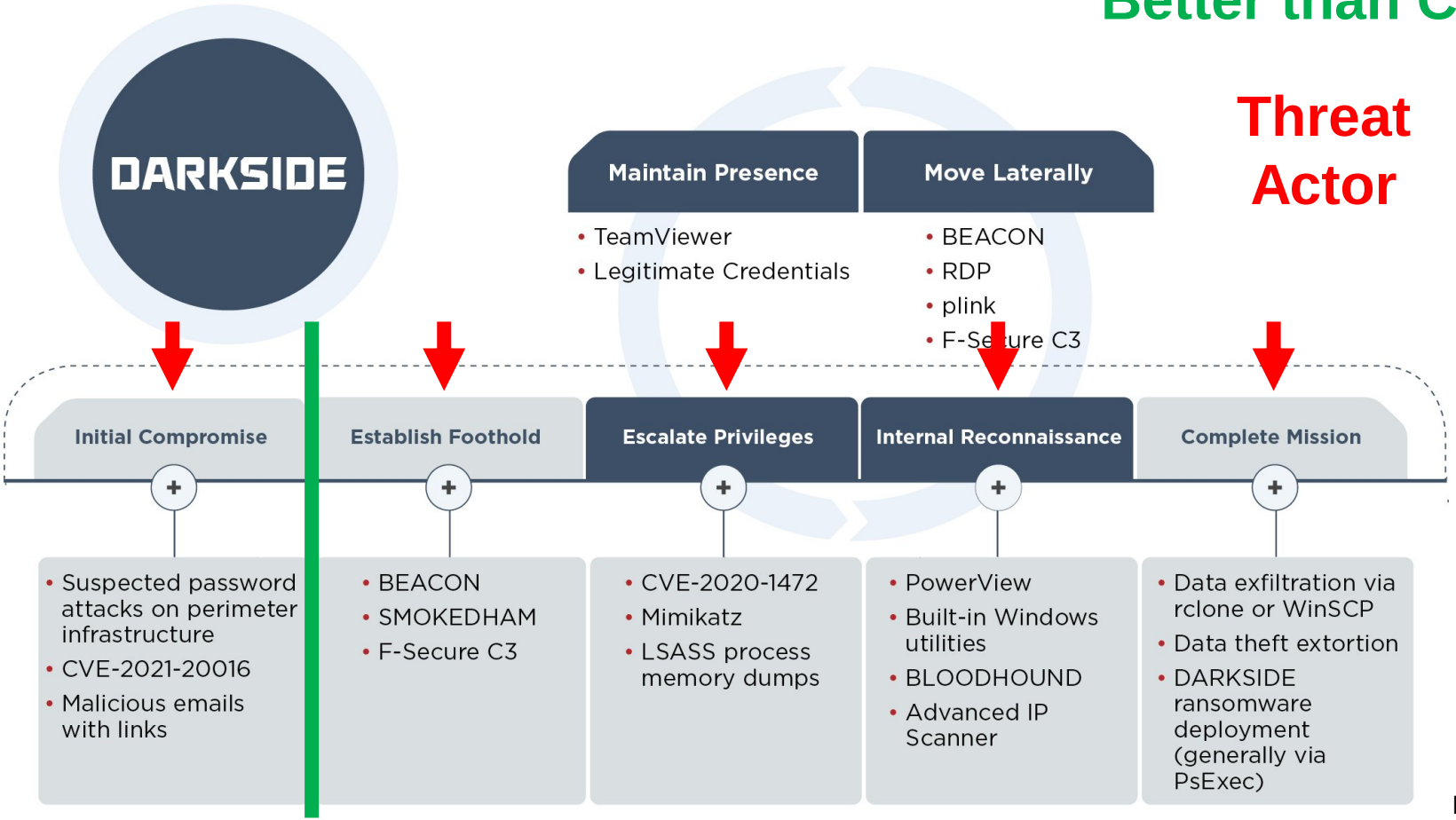
DarkSide

- **Ransomware as a Service**
- **Opportunistic attackers**
- **Highly disruptive**, highly visible, most likely to result in pay-outs
- **Leverages human Entry Vector**

Stopping Attackers Early

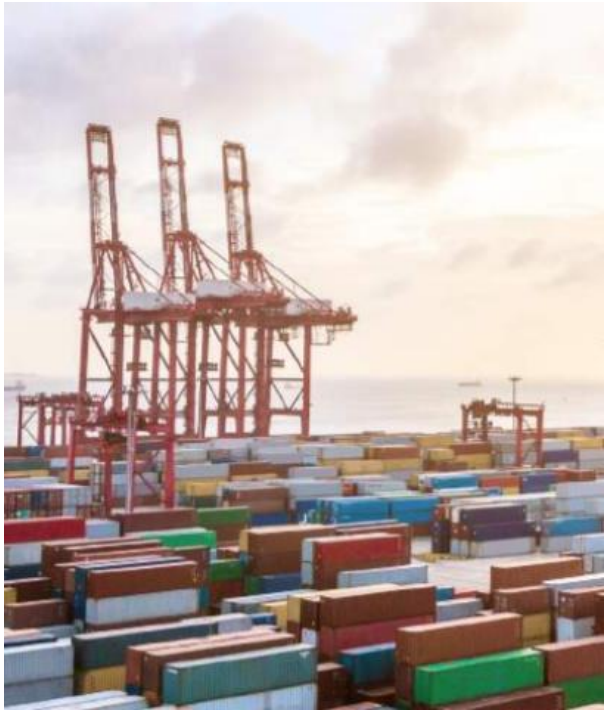
Prevention is Better than Cure

Threat Actor



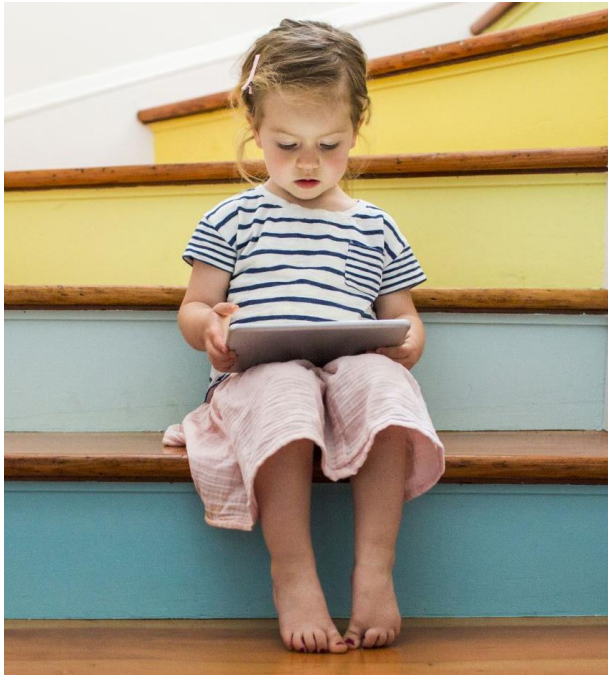
Mandiant

The Entry Point



- Our **Employees** are our greatest risk
- Less Predictable. Need training!
- They expose the business to **devices** and **behaviours** that increase risk to the business
- **Malware and Phishing** continues to be a leading form of system penetration
  - typically **social engineering**

Our Weakest Link & Strength



25 seconds: 7 char password

- More than 91% of all successful hacks and data breaches stem from **phishing emails**
- **Password theft** and reuse continues to be a major form of system “**stuffing**”
- **Training can improve behaviours** but nearly 50% of businesses train less than once per year.
  - **Much lower in Maritime**

Mitigating the Human Threat

Security by Design?

- Defensive **Infrastructure Design**
- **Minimise Access**
- **Monitor Access** – DLP, Firewalls, AIP
- Design Code & **Systems Defensively**
- Strong **OT and IT segregation**
- IOT and **SCADA hardening**

Onshore Staff: Collaboration Tech

- **Microsoft Teams**, Google Docs etc
- Is the Cloud Safe?
- **Shadow IT** – Dropbox, OneDrive
  - Increase in Bad Leavers
  - Remote Desktop risks
- **Phishing Risks:** Teams Spoofing

Security Mechanisms?

- **VPN & MFA – not always possible**
  - Single Sign On / Trusts
- **Security Monitoring**
  - Impossible Travel, USB sticks, File Access
- **Remote Response / EDR / MTTR**
- **Segregate Systems**
  - **onshore vs offshore, OT vs` IT**

Grant Thornton

Training!

Digital Forensics & Investigations
Electronic Disclosure Consultancy
Cyber Defence & Response

Data Breach Support Hub (24 Hours)

+44 20 7865 2552

cir@uk.gt.com

containment and response

Grant Thornton

An instinct for growth™

Vijay Rathour

Partner – Digital Forensics

Vijay.Rathour@uk.gt.com

Tel: +44 (0)7788 418 652

Human factors in maritime cyber security

Maritime Cyber Tech & Ops Webinar Day – Human factors in maritime cyber security

Thursday 10th June 2021

A quick introduction

- We are marine cyber security specialists
  - This is all that we do.
- Despite being technology geeks, we like to (try) and keep things simple
  - Everyone needs to be able to understand the ‘why’ in our advice
- Today’s presentation is not going to be technical
  - Reach out to us afterwards if you would like to get into detail, we’re always very happy to chat!

Minimising and mitigating the human factors in a maritime cyber attack

Minimising and mitigating the human factors in a maritime cyber attack

- Use IMO cyber compliance exercises to identify what would need to be done to recover if stuff goes wrong
  - Think in terms of technology failure, not just ‘cyber attack’
- Keep things really simple for recovery
  - Kill cards are a very useful tool
  - Worry about the cyber ‘part’ when things are safe to do so
- Train everyone. Repeat.

How to differentiate cyber security technology

How to differentiate cyber security technology

- Should one actually differentiate?
  - Making ‘cyber’ a separate thing can create barriers for understanding and adoption
- Be very clear that cyber security technology is not a magic bullet
  - It certainly helps but works best when everything else has been taken care of
- Implement what make sense for your individual circumstances
  - i.e. having 24hr monitoring tools sounds great in principle but isn’t so if there’s no one to interpret their output

Countering social engineering: defending against phishing attacks

Countering social engineering: defending against phishing attacks

- Train everyone (yes, this is indeed a recurring theme)
  - Training needs to be interesting and informative, not a mandatory module that ticks boxes
- Ensure people can safely report screw-ups
  - ‘Three strikes and you are out’ makes people hide things that you really ought to know about
- Get your overall technology set-up right
  - Most phishing attacks aren’t targeted, if you follow best practice for IT cyber security you can stop many from being successful

Summary

1. Invest in training, don’t just tick boxes
2. Treat cyber risk as you would all other risks, don’t set it apart
3. Follow IT and OT best practices in general, there are no magic bullets

Cyber-SHIP Lab

SECURING MARITIME

Seafarer Digital Competencies

Maritime Cyber Tech & Ops - Human Element

Rory Hopcraft

Industrial Researcher

UNIVERSITY OF PLYMOUTH

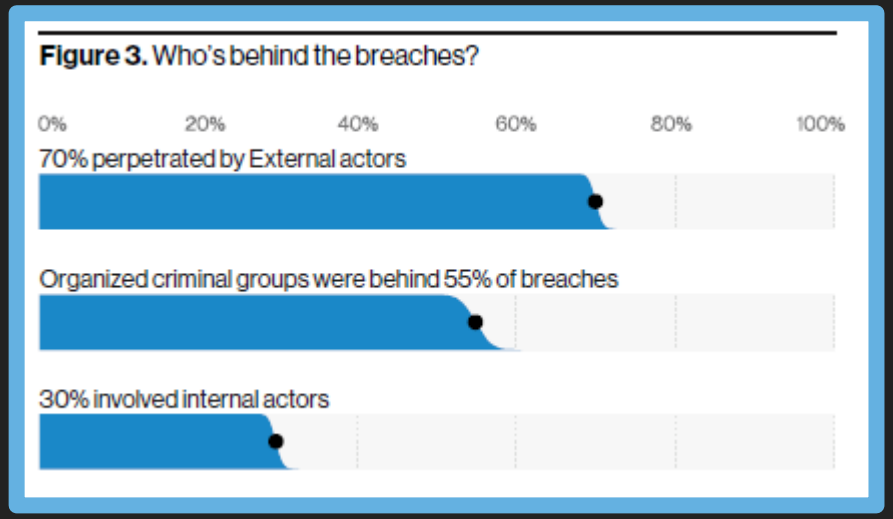
Resolution MSC.428(98)

AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

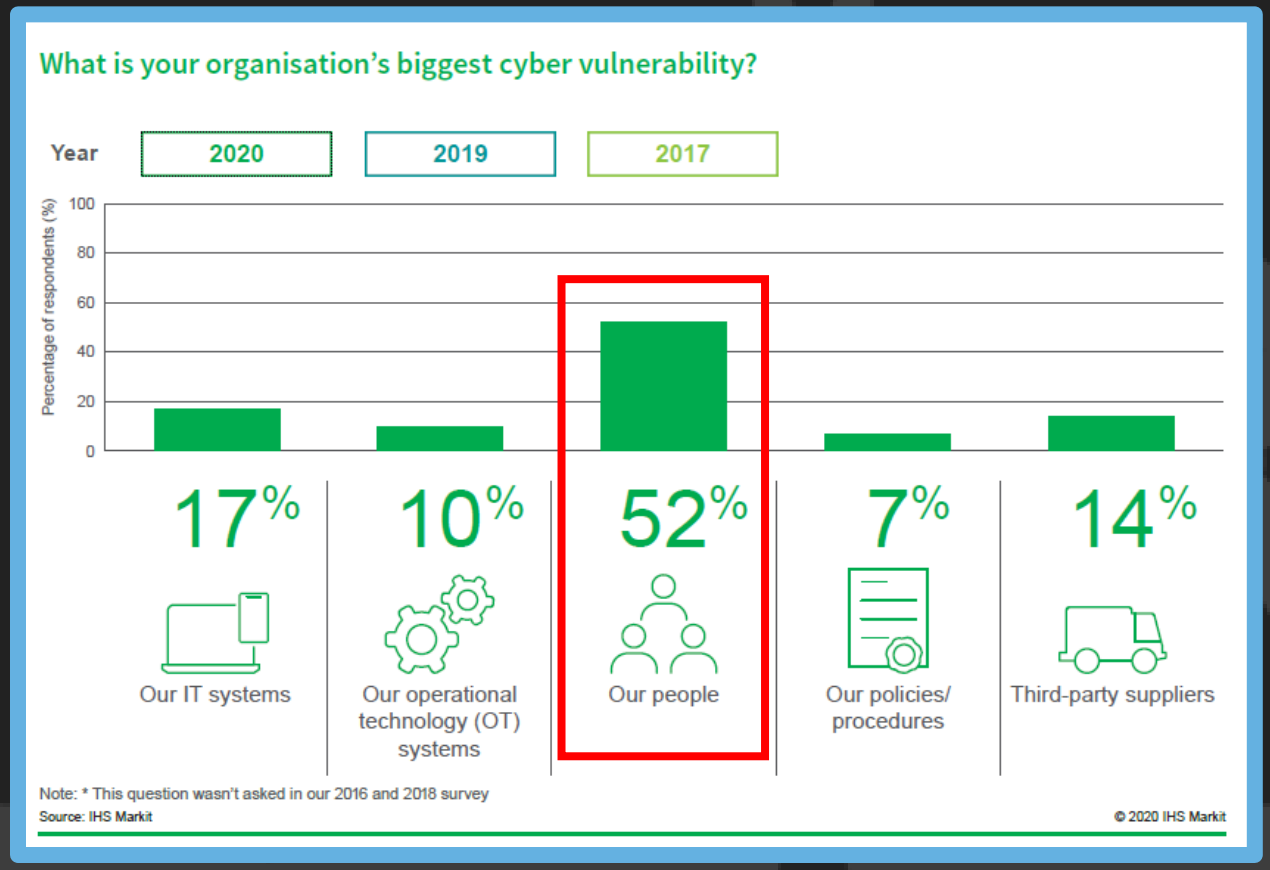
NOTING the objectives of the ISM Code which include… the provision of safe practices in ship operations… and the continuous improvement of safety management skills of personnel ashore and aboard ships.

The Human Element – The Biggest Risk?

- Humans often cited as the weakest link in cyber security
- Recent surveys highlight that without adequate training humans represent a significant risk to cyber security…



Source: *Verizon Data Breach Survey - 2020*

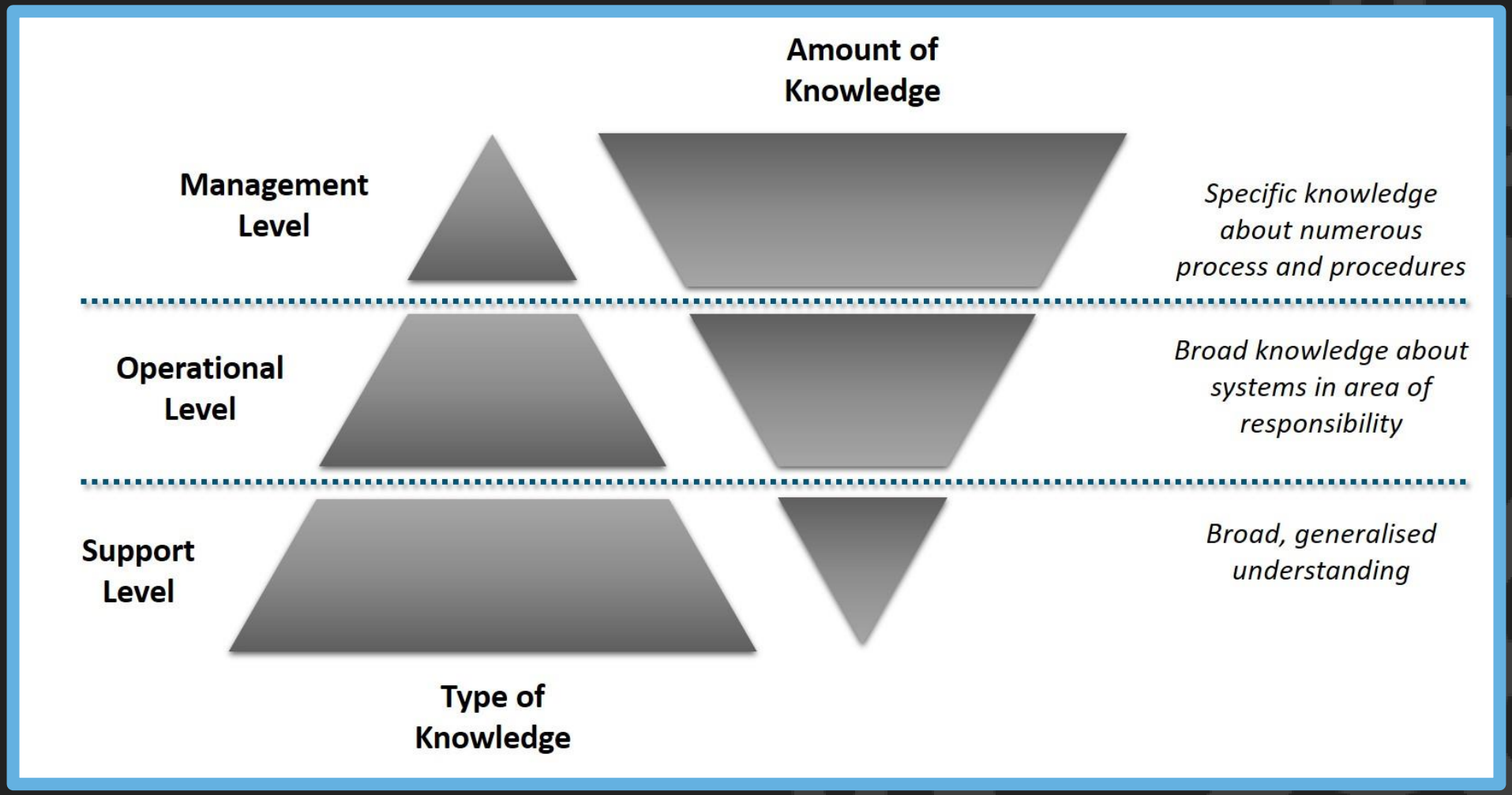


Source: *Safety at Sea and BIMCO Cyber Security White Paper - 2020*

Cyber Training Requirements

- Two regulatory instruments outline operational requirements for cyber security training to be provided:
  - STCW outlines the importance of seafarers being qualified for their duties, and places a minimum standard of competencies
  - ISM Code includes cyber risk management in SMS, meaning cybersecurity is a requirement for a safe ship.

Digital Responsibilities



Cyber-SHIP Lab

CyberMAR

One Size Does NOT Fit all...

- Ships have different functionalities
- Ships are equipped with different systems
- Ships travel through different locations

- Companies have different operational practices
- Companies are based in different locations
- Companies use different systems

- Attackers have different interests
- Attackers have different resources levels

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389.

Rory Hopcraft

Industrial Researcher

Maritime Cyber Threats Research Group

rory.hopcraft@plymouth.ac.uk

Thank you

NEPTUNE
MARINE CYBER SECURITY

A Company Overview

ABOUT US

- Founded in 2019
- Located in Lévis, Canada and London, UK
- Purely focused on marine cyber security
- Pragmatic approach to what we do and the solutions we provide Services offered range from security design to implementation
- Projects cover a wide range of industry sectors; from cruise lines to defense

SERVICES WE PROVIDE

- Cyber Audit
- Policy & Compliance
- Security Design
- Security Testing
- Crew Training
- Implementation

W neptunecyber.com E contact@neptunecyber.com T +1 514 476 6722

NEPTUNE

MARINE CYBER SECURITY

CYBER AUDIT

Have the IT systems onboard been installed, configured and maintained to be as secure as possible?

- Our cyber audit is a physical inspection of a vessel's IT systems and equipment and fully documents its current state.
- A cyber audit quickly highlights physical cyber security issues a vessel has and the risks they pose.
- Audits carried out quickly and at a time and location that suits your scheduling.

POLICY & COMPLIANCE

Are a vessel's policies and operations compliant with current IMO regulations and Classification Society requirements?

- Mapping and gap-analysis between what's currently in place and what is required to be compliant.
- Policy and process reviews and audits.
- Policy and process creation and cyber risk register updates.

SECURITY DESIGN

Reviewing proposed or existing systems to ensure they are designed to be as secure as possible.

- Reviews enable immediate issues to be addressed and plans made for future security.
- Review proposed designs, system upgrades or existing implementations.
- Doesn't require access to vessels or systems to add value.

SECURITY TESTING

Can a vessel or operations be hacked into and, if so, how can this be fixed to be secure?

- We use the same techniques as hackers to identify security weaknesses.
- The reports you receive provide technical and non-technical descriptions of any issues found, and the risks they create, together with details of how to fix them.
- Most security tests can be carried out remotely, even when at sea, and with no possible disruption to the vessel.

W neptunecyber.com E contact@neptunecyber.com T +1 514 476 6722

NEPTUNE
MARINE CYBER SECURITY

CREW TRAINING

Cyber security training for crew and other staff to help them understand the risks they face and how to protect against them.

- Enable crews to be the frontline of your cyber security.
- Training uses industry specific terms and examples to maximise its value Delivered in an accessible, interactive and non-technical format.
- Courses are designed to be equally valuable whether delivered online or in person

IMPLEMENTATION

Hands-on support to fix problems found and to ensure technology is installed correctly.

- Our implementation partners work with you to address issues found.
- Many issues can be fixed remotely reducing the time it takes to become more secure.
- We can also work with your existing teams and suppliers to fix issues and improve their skills.

NEPTUNE
MARINE CYBER SECURITY

CONTACT US

CANADA

1190B Rue de Courchevel
4th Floor
Lévis, Quebec
G6W 0M6
+1 514 476 6722

UK

Golden Cross House
8 Duncannon St
London
WC2N 4JF
+44 203 129 1878

NEPTUNE

MARINE CYBER SECURITY

A REALLY SIMPLE GUIDE TO:

Online Security For Crew

As great as it is, the Internet can be a dangerous place at times. In this guide we'll show you how to take a few simple precautions that will help you stay safer online, and protect your data and devices from harm.

NEPTUNE
MARINE CYBER SECURITY

01. STEP 1: CHOOSE BETTER PASSWORDS

Problem:

Choosing bad passwords is the easiest way to make yourself vulnerable online. If you don't want criminals to access your iCloud, DropBox, or PayPal accounts, choosing better passwords is your #1 priority.

Most people make two huge mistakes:
1. They choose poor passwords, or passwords commonly used by other people (e.g., Password123)
2. They reuse the same 2-3 passwords for all of their accounts

Why is reusing passwords a bad idea? Because if one of the online services you use is hacked (it happens all the time) and criminals gain access to your email address and password, they will immediately try to access other popular online services using the same login details. This is called a "password reuse" attack.

Solution:

Choose a unique password for each account that's easy to remember, but hard to guess or "crack" using brute force techniques. Rather than choosing a random string of characters (which you'll forget) choose a long, memorable passphrase. Edward Snowden's favourite example is MargaretThatcheris110%SEXY

Action Steps:	Complete:
Choose a strong, unique password for each of your online accounts	

02. USE A PASSWORD MANAGER TO KEEP TRACK OF YOUR PASSWORDS

Problem:

Remembering dozens of unique passwords is hard.

Solution:

If you struggle to remember passwords, a password manager like LastPass (www.lastpass.com) or KeePass (keepass.info) can help. Password managers securely store all your passwords, and allow you to autofill your login details when you access online accounts using any of your devices.

You'll need to choose a single master password to access your password manager, so make sure it's a good (and memorable) one. Once set up, password managers make it easy to assign extremely secure passwords for all of your online accounts, and save you from trying to remember passwords for sites you rarely use.

Action Steps:	Complete:
Choose a password manager and set it up on all of your devices	

03. BE REALLY CAREFUL WITH USB STICKS OR THINGS THAT PLUG INTO USB PORTS

Problem:

One of the most common ways that computers get infected is through hidden malware that's been accidentally installed on something that you plug into a USB port.

Lots of people that create malware don't care where it ends up so long as it goes somewhere. The really nasty stuff will encrypt any computer it's connected to and can only be removed by wiping what's infected clean and reinstalling everything from scratch.

Solution:

Painful as it sounds, do your best to avoid using USB sticks at all if you can. If you must use them, only use ones that you have purchased from new and never share them or plug them into anyone else's computer.

Action Steps:	Complete:
Throw away all your old USB sticks and buy a new one if you have to use one	

04. TURN ON AUTOMATIC UPDATES

Problem:

Most cyber attacks aren't sophisticated — They're just exploitations of known software vulnerabilities using simple techniques or pre-made hacking kits downloaded from the Internet. Unfortunately, many people fail to keep their software up to date, making it easy to compromise their devices.

Solution:

Turn on automatic updates. Most devices have an automatic update feature that finds and installs new versions of software as soon as they become available. Make sure this setting is turned on for all of your devices, and always accept updates when prompted.

Action Steps:	Complete:
Enable automatic updates on all of your devices	

05. BACKUP YOUR IMPORTANT DATA OFFLINE

Problem:

It's easy for your data to become lost or corrupted, even if you use cloud storage services.

Solution:

Keep offline backups, and update them regularly.

The simplest option is to regularly copy your important files, photos, and data onto an external hard drive. External hard drives are cheap to buy and easy to use – Just plug one into your computer and copy over everything that matters to you. When you're finished, unplug the drive until it's time for your next backup.

Having an offline backup of your important files will ensure that if your data is lost or corrupted (e.g., due to a ransomware attack or system failure) you won't lose everything. How often you should use your backup drive depends on the importance of your data. Weekly should be fine for most people.

Action Steps:	Complete:
Buy an external hard drive and use it regularly to backup your important data	

06. DON'T BE TOO TRUSTING

Problem:

The Internet makes it easy for bad people to do bad things. Most cyber attacks prey on human weakness – in particular, our tendency to assume communications and online content are legitimate. Email, websites, online ads, and even social media and dating services can all be used to trick unsuspecting people into compromising their security, or sending money where they shouldn't.

Solution:

Don't inherently trust things you find on the Internet, or things that are sent to you. Nobody really wants to send you money for nothing, and people who ask you for money through dating services – no matter how plausible their reasons or how nice they seem – are definitely scammers.

Never give away personal information unless you can be absolutely sure it's going to a person or service your trust. Similarly, you should only downloads attachments if you are sure they are from a trusted source.

If a website feels sketchy, get out of there. Malicious websites and ads often promise cheap goods or free movies and software to trick people into downloading malware or paying for things that will never arrive.

Remember – If something seems dodgy, it probably is. If something seems too good to be true, it definitely is.

Action Steps:	Complete:
Don't be too trusting. If something seems dodgy, assume it is	