Maritime Cyber Security

Threats and Opportunities

Brendan Saunders – Maritime Lead, Transport Cyber Security Practice

Agenda

- Maritime Cyber Threats
- Attack Surface Overview
- Potential Impact
- Reported Incidents
- Solutions
- Guidance
- The NCC Group Approach

About Us

Brendan Saunders

Brendan is an Executive Principal Security Consultant and the Practice Lead for Maritime Cyber Security at NCC Group. A CREST accredited Penetration Tester, he regularly acts as the lead for large-scale consultancy engagements as well as leading research and mentoring junior consultants.

Brendan is a Director of CIRM, the international organisation for Maritime Communications and Technology and has a broad experience of the maritime environment. Most of his spare time is taken up as serving as an officer the Royal Navy Reserve specialising in communications and information systems.

NCC Group

NCC Group is a global consultancy and our assurance division boasts the world's largest cyber security consultancy team with over 300 consultants active across Europe, North America and Asia-Pacific. We are committed to creating a safer Internet for all and our research activities form the core of our business.

Maritime Cyber Threats

- Increasing connectivity of ships
- Ever-greater integration of ICS into onboard networks
- Pre-Internet systems and protocols wrapped in IP
- Widespread use of USB memory devices for data sharing
- Greater use of remote access capability
- Attackers increasing targeting non-conventional IT
- Lack of Leadership in the Maritime Cyber Security Space

Attack Surface Overview: Ships

AIS transceivers, LRIT (Long-range Identification and Tracking)

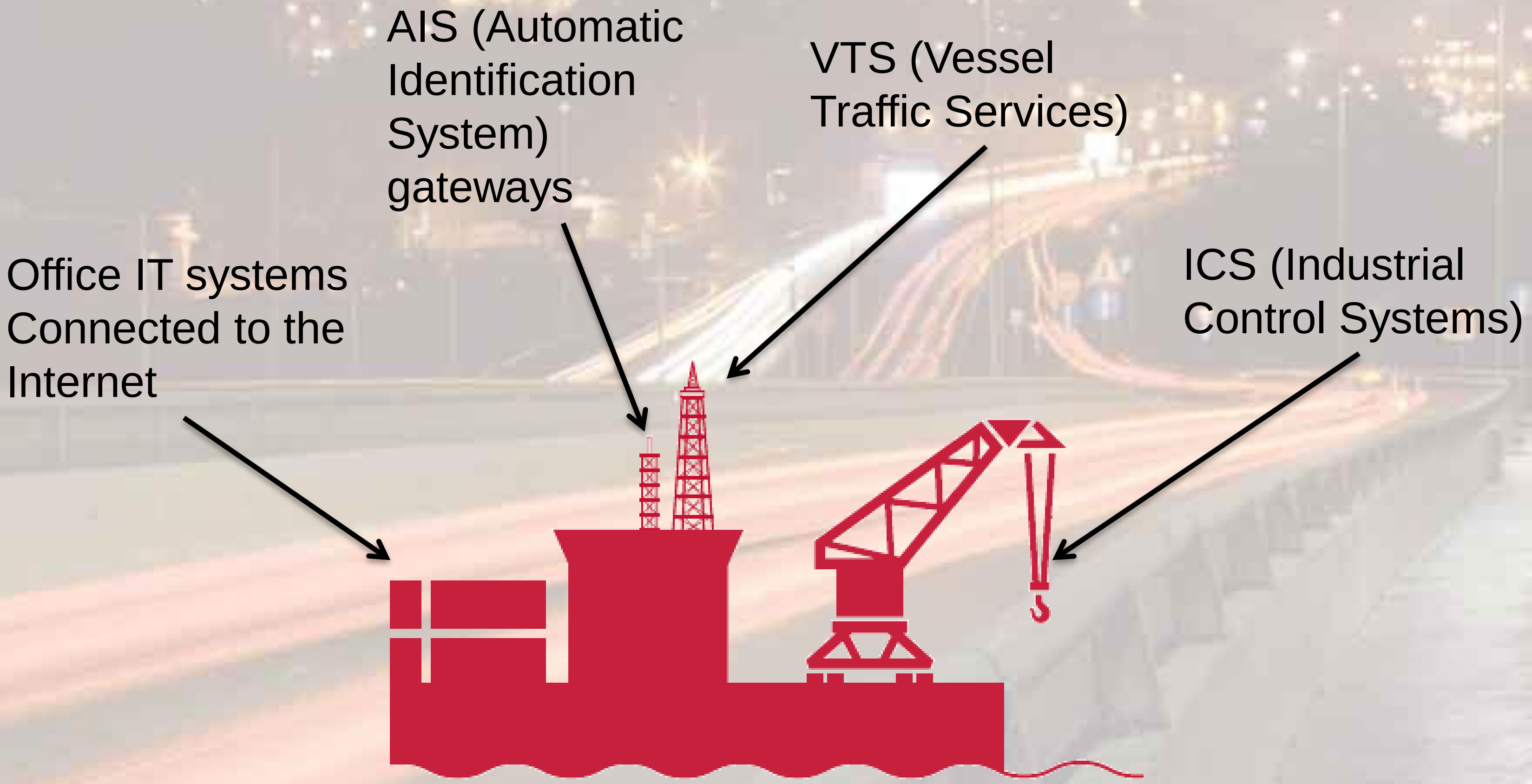
IT systems connected to the Internet

DSC (Digital Selective Calling), Man-in-water beacons

Data sharing between systems via USB Memory sticks

Lack of segregation between systems

Attack Surface Overview: Harbour



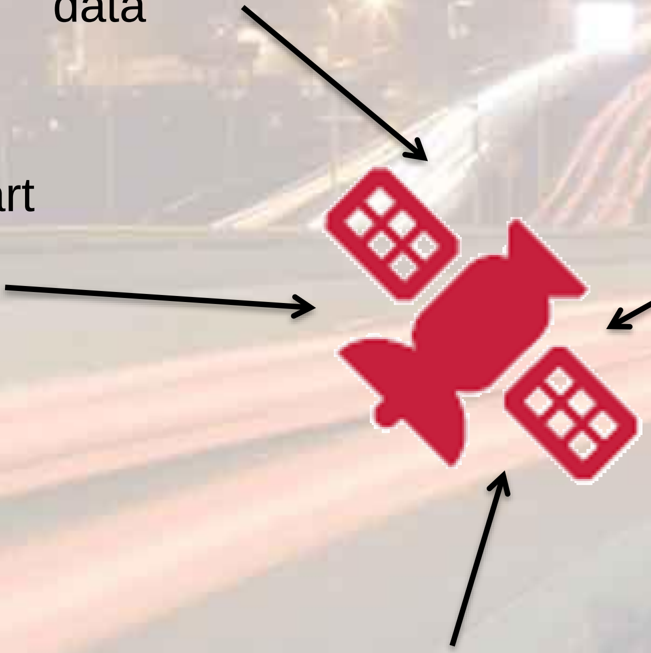
AIS (Automatic Identification System) gateways

VTS (Vessel Traffic Services)

Office IT systems Connected to the Internet

ICS (Industrial Control Systems)

Attack Surface Overview: Navigation



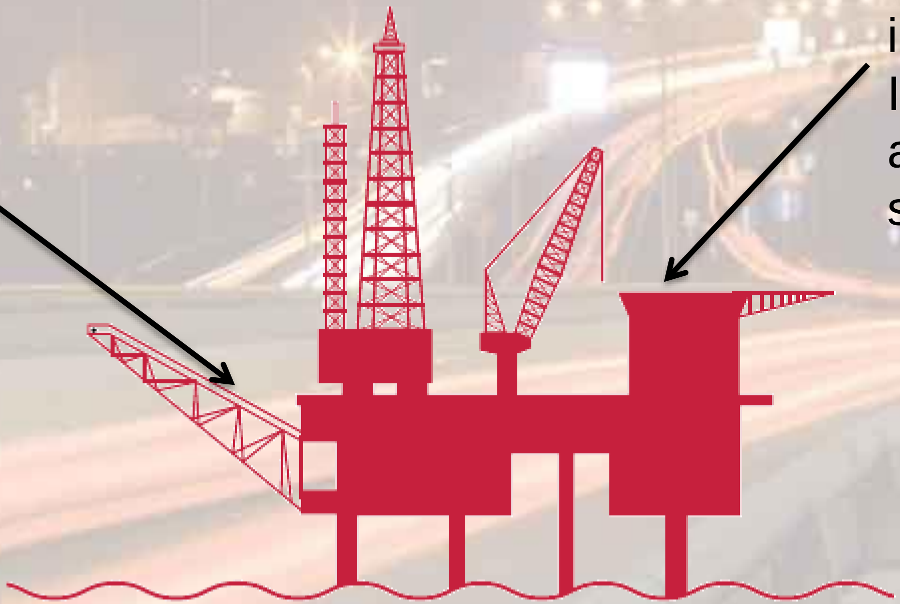
GNSS (Global Navigation Satellite System) data

ECDIS (Electronic Chart Display Information System)

Electronic chart data

eLoran

Attack Surface Overview: Rigs



DP (Dynamic Positioning) systems

Malware inadvertently introduced via Internet browsing and USB memory sticks

Potential Impact

- Technical safety controls in ICS systems and procedural controls make ‘catastrophic’ scenarios unlikely, but possible.

- More likely: Failure of a critical system (e.g. Engine Management or ECDIS) leaving a ship ‘quarantined’ in harbour losing $$$ every day

Impact: Some Reported Incidents

- In 2012 criminals penetrated the cargo systems operated by the Australian Customs and Border protection, allowing them to check whether their shipping containers were regarded as suspicious by the police or customs authorities.

- Drug traffickers reportedly hacked into the computer controlling the location and movement of shipping containers at the port of Antwerp

- In 2012, North Korea uses lorry-mounted devices to block GPS signals in South Korea for 16 days, causing 1,016 aircraft and 254 ships to report disruption

- In 2016, pirates worked together with hackers to identify high-value cargo on ships in order to target their attacks.

Image: gcaptain.com

Short-Term Solutions

- The active threats to marine systems should be identified through threat modelling
- If software/firmware can easily be fixed to mitigate vulnerabilities this should be done
- More complex design-related vulnerabilities need to be contained using segregation technologies

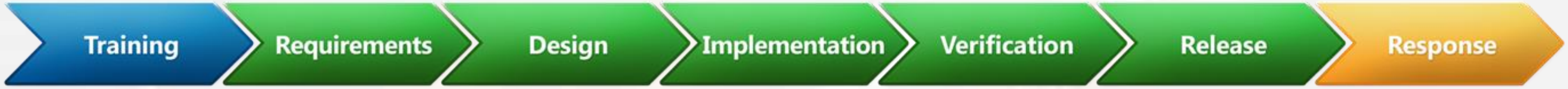
Image: www.trickedbythelight.com

Medium-Term Solutions

- Standards and Guidelines:
  - BIMCO and ABS Guidelines for Cyber Security Onboard Ships
  - IMO Draft Guidance on Maritime Cyber Risk Management
  - IEC Standards and Guidance development. IEC TC80 61162-460 in particular provides good guidelines on how to implement security into shipboard network infrastructure.
  - DNV Classification society documentation and DNV Nautical Safety (Network Based Integration of Navigation Systems (ICS)).
- Policy and Strategy Best-Practice Development
  - Further Development of Industry Best-practice guidance for process and technical activities

Long-Term Solutions

- Marine systems developers need to implement an SDL (Secure Development Lifecycle)



- System components and fully integrated solutions should be subject to regular security assessment.

- Remote connectivity solutions should be tailored to the specific environment and the risks fully evaluated.

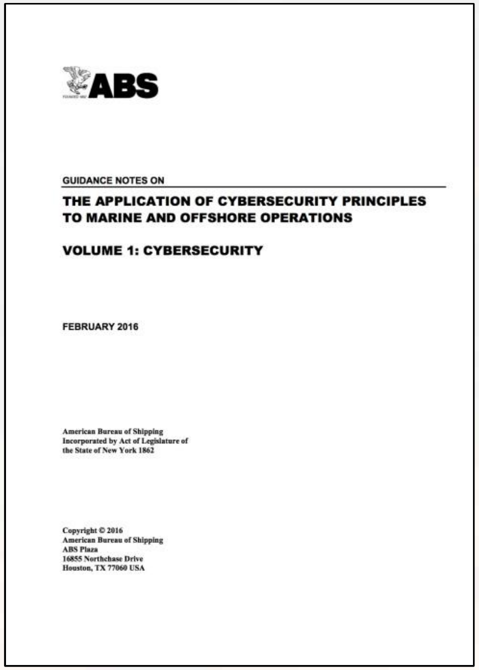
Image: msdn.microsoft.com

Raising Security Awareness

- Effective cyber security starts with Security Awareness
- Understanding the fundamentals can make a huge difference: You don’t need to be an expert to spot potential security risks
- Processes need to be implemented to enable people to raise potential security issues/risks from systems development through to operations.

Image: www.eci.com

Guidance



ABS

GUIDANCE NOTES ON

THE APPLICATION OF CYBERSECURITY PRINCIPLES
TO MARINE AND OFFSHORE OPERATIONS

VOLUME 1: CYBERSECURITY

FEBRUARY 2016

American Bureau of Shipping
Incorporated by Act of Legislature of
the State of New York 1862

Copyright © 2016
American Bureau of Shipping
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA

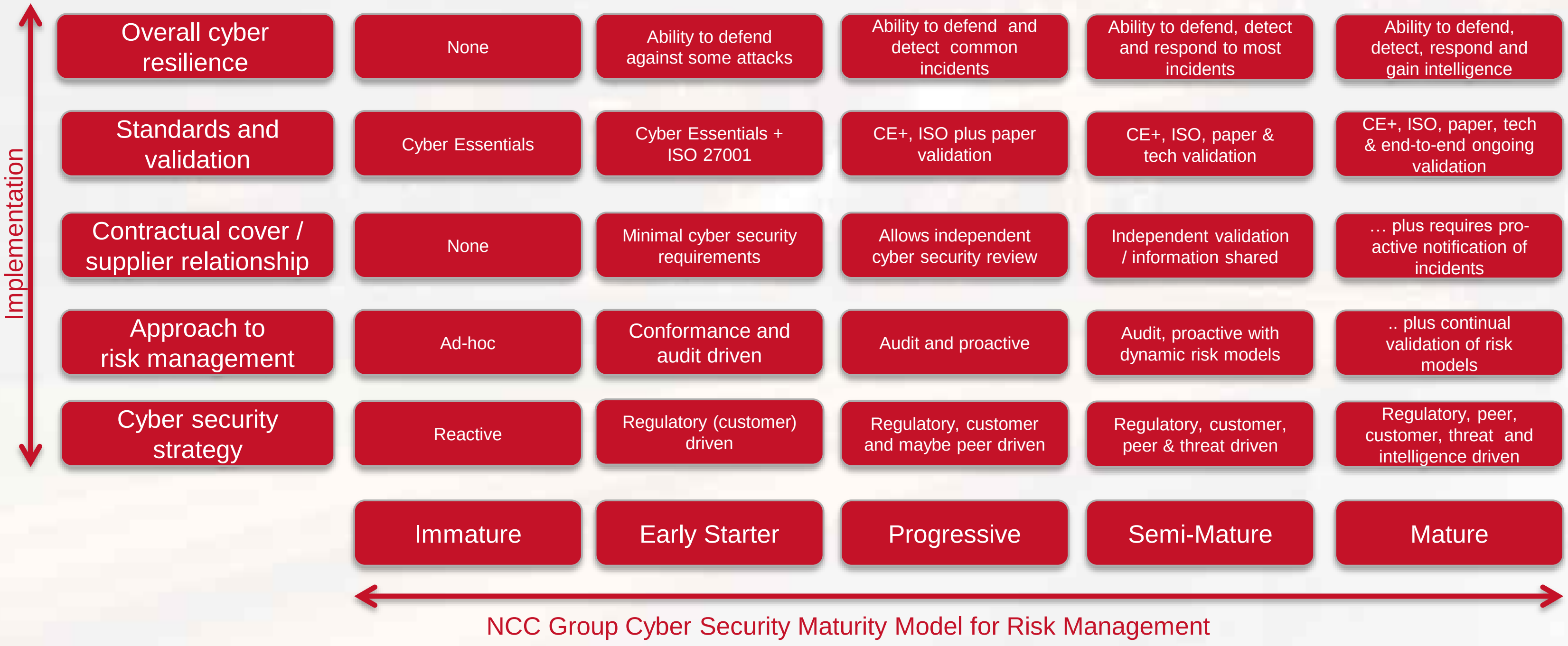
NCC Group were a key contributor to the BIMCO *Guidelines on Cyber Safety and Security On Board Ships*.

Guidelines include:

- Understanding Cyber Threats
- Risk Assessment
- Cyber Security Controls
- Incident Response and Recovery Plans

American Bureau of Shipping have released similar guidelines.

Introducing the Cyber Security Maturity Model



	Immature	Early Starter	Progressive	Semi-Mature	Mature
Overall cyber resilience	None	Ability to defend against some attacks	Ability to defend and detect common incidents	Ability to defend, detect and respond to most incidents	Ability to defend, detect, respond and gain intelligence
Standards and validation	Cyber Essentials	Cyber Essentials + ISO 27001	CE+, ISO plus paper validation	CE+, ISO, paper & tech validation	CE+, ISO, paper, tech & end-to-end ongoing validation
Contractual cover / supplier relationship	None	Minimal cyber security requirements	Allows independent cyber security review	Independent validation / information shared	… plus requires pro-active notification of incidents
Approach to risk management	Ad-hoc	Conformance and audit driven	Audit and proactive	Audit, proactive with dynamic risk models	.. plus continual validation of risk models
Cyber security strategy	Reactive	Regulatory (customer) driven	Regulatory, customer and maybe peer driven	Regulatory, customer, peer & threat driven	Regulatory, peer, customer, threat and intelligence driven

NCC Group Cyber Security Maturity Model for Risk Management

NCC Group Approach

- The NCC Group Approach to Maritime Cyber Security tackles the challenges facing maritime businesses at three levels.
- **Strategic:** At the Strategic level, NCC Group leverages years of experience in developing information security strategy and a broad understanding of the maritime environment to help businesses develop strategies and policies.
- **Technical:** NCC Group is well-known as a centre of excellence for security assessment and research. We have a highly-skilled technical consulting team holding many UK Government security testing accreditations.
- **Operational:** NCC Group provides real-time and rolling monitoring to detect security incidents and provide rapid Incident Response.

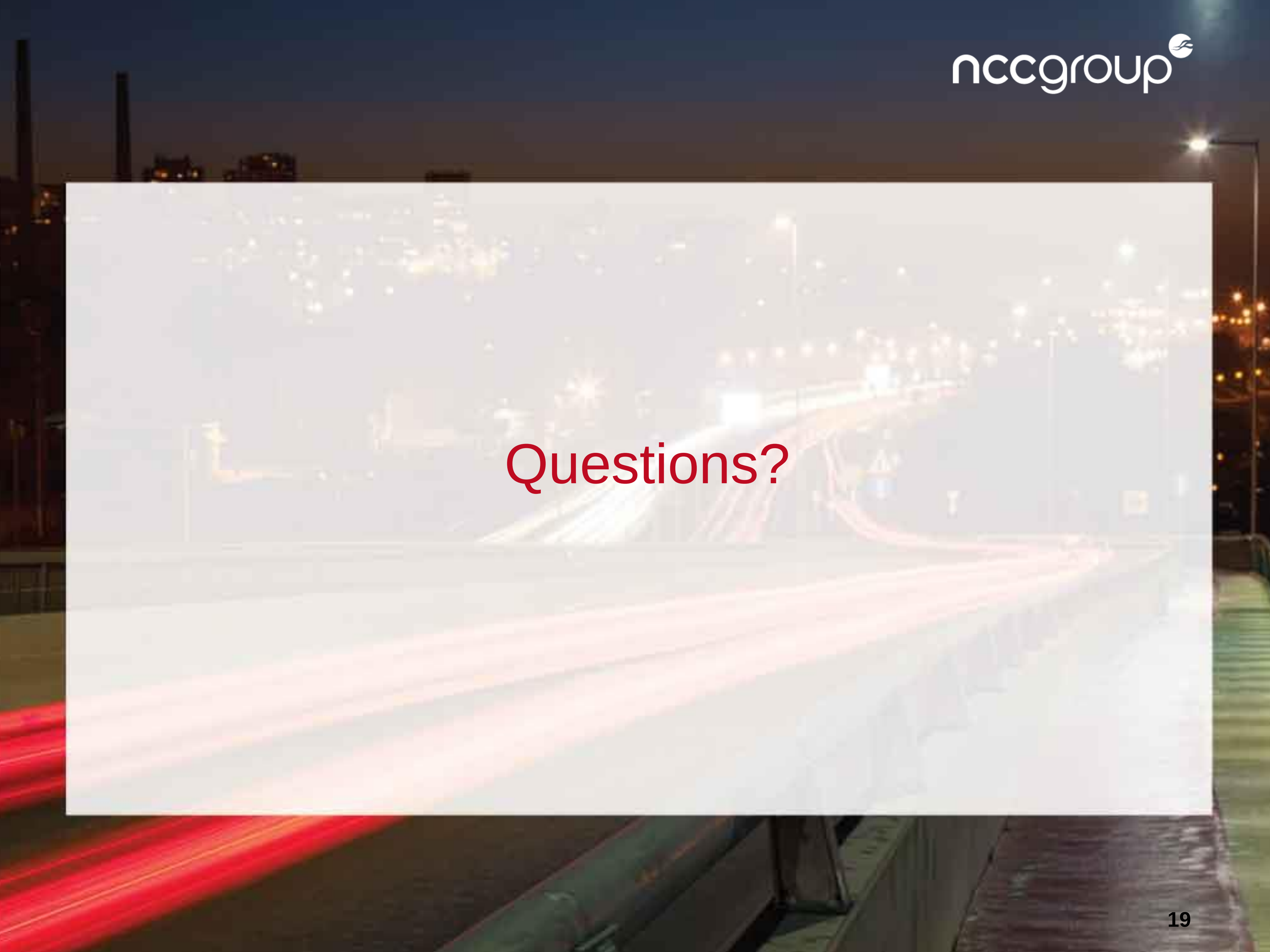
Strategic

Technical

Operational

Conclusions

- The potential impact of marine cyber attacks includes potential revenue loss, environmental damage and loss of life
- Development and implementation of agreed standards and guidelines is required
- More security testing of marine systems, networks, hardware devices and any associated software is required
- The ultimate solution is to embed security into the development lifecycle of products and systems
- The most important step is to ensure staff are aware of cyber security threats through appropriate training so that they can be identified and reported



Questions?

Contact us

+44 161 209 5200

maritimesecurity@nccgroup.trust

www.nccgroup.trust/maritime

North America

- Atlanta
- Austin
- Chicago
- New York
- San Francisco
- Seattle
- Sunnyvale

Canada

- Waterloo

Europe

- Manchester - Head Office
- Amsterdam
- Basingstoke
- Cambridge
- Cheltenham
- Copenhagen
- Edinburgh
- Glasgow
- Leatherhead
- Leeds
- London
- Luxembourg
- Madrid
- Malmö
- Milton Keynes
- Munich
- Vilnius
- Wetherby
- Zurich

Australia

- Sydney