Transport Assurance: Maritime
Services, Capabilities and Research
NCC Group Company Overview

- 2,000+ Employees worldwide
- 35+ Offices across Europe, North America, Asia-Pacific & Middle East
- 1999: NCC Group was formed in June 1999
- 15,000: Helping 15,000 organisations worldwide to manage risk & limit threat of cyber crime
- £244.5m: Group Revenue for year end May 2017
Agenda

• Maritime Cyber Attack Surface
• Potential Impact
• Common Maritime Cyber Themes we have observed
• Our services
• Secure Development Lifecycle
• Q&A
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 money every day
Attack Surface Overview: Maritime

- Harbours
  - Office IT systems connected to the Internet
  - AIS (Automatic Identification System) gateways
  - VTS (Vessel Traffic Services)
  - ICS (Industrial Control Systems)

- Navigation
  - GNSS (Global Navigation Satellite System) data
  - Electronic chart data
  - ECDIS (Electronic Chart Display Information System)
  - eLoran
  - AIS transceivers, LRIT (Long-range Identification and tracking)
  - Fleet broadband
  - DSC (Digital Selective Calling), Man-in-water beacons
  - Data sharing between systems via USB memory sticks
  - Lack of segregation between systems

- Rigs
  - DP (Dynamic Positioning) systems
  - Malware inadvertently introduced via Internet browsing and USB memory sticks

- Ships
  - Data sharing between systems via USB memory sticks
  - Lack of segregation between systems
Maritime – Common themes observed

- 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 increasingly targeting non-conventional IT
Cyber Guidelines

NCC Group were a key contributor to the BIMCO Guidelines on Cyber Security Onboard Ships.

Guidelines include:

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

IMO Guidelines on Maritime Cyber Risk Management

- International Guidance
- References BIMCO and ABS Guidelines
- NCC Group Contributed
Our Approach

Strategic

- Strategy and Policy Review
- Strategy and Policy Development
- Process and Control Guidance

Technical

- Penetration Testing
- Product Assurance Testing
- ‘Red Team’ Scenarios
- Technical Security Training
- Research-led Engagements

Operational

- Cyber Defence Monitoring Services
- Incident Response and Forensic Services
Partnerships

Comité International Radio-Maritime (CIRM)
- International Trade Association for Maritime Electronics Manufacturers and Suppliers
- NCC Group Holds a Directorship – Brendan Saunders
- Chair Cyber Security Working Group
- Advisors to the IMO and other International Bodies

Kilo Marine Electronics
- Reseller of NCC Group Maritime Cyber Security Services
Contact info

+44 (0)161 209 5200
TransportSecurity@nccgroup.trust
www.nccgroup.trust/transport

A global practice offering the full range of Cyber Security and Assurance services to the Transport industry

North America
- Atlanta
- Austin
- Boston
- Chicago
- New York
- San Francisco
- Seattle
- Sunnyvale

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

Canada
- Waterloo

Middle East
- Dubai

Australia
- Sydney

Asia
- Singapore