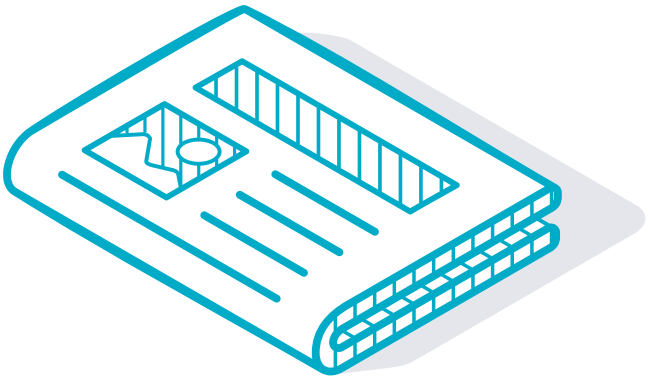

12 CASE STUDY 2: POORLY PROTECTED ON-BOARD NETWORKS - LACK OF NETWORK SEGREGATION - CORRUPTION OF ECDIS SYSTEM

Case study narrative:

- Shipowner has satellite communications capability installed on their fleet and ships broadcast an IP address.
- Hackers accessed on-board networks using this IP address
- Hackers hop from external to internal networks to access chart and navigation systems, as well as accessing essential telemetry systems for e.g. engine management, ballast control etc.
- Hackers Altered ECDIS software to render inaccurate position
- Ship veered off course, wasting fuel and time
- Bridge management team had to resort to dead reckoning and non-GPS navigation techniques (a paper chart)

Investigation identified

- A lack of segregation (physical and logical) between on-board OT network, internal email network and satellite feed
- A lack of proper configuration of firewalls between these networks to permit only known types of traffic
- Access control systems inadequate

Recommendations & Remediation

- Gap analysis identified material shortcoming in vessel cyber security and related vessel safety management
- An agreed work programme would:
  - » Improve network segregation to improve operational resilience
  - » Improve network monitoring and security to improve vessel safety management
  - » Improve core defences by implementing a structured patching programme
  - » Improve access control and password management

SUMMARY

Client contacts ACL after a navigational incident

Poor network security allowed vessel to be vulnerable

Investigation identified that a programme of co-ordinated activities is required

Improvement in cyber security posture of client

OUTCOME:
Improved cyber hygiene and security