nccgroup
freedom from doubt

Batten down the hatches: Cyber threats facing DP operations

Andy Davis, Research Director NCC Group

Agenda

- What are the threats?
- Incidents that could have been caused by cyber attack
- Short and longer term solutions to increase cyber security
- The importance of security awareness

The threats

- Control systems are becoming more complex
- Older, less secure control protocols are being wrapped in IP
- There is more of an expectation of remote access
- Attackers are becoming more interested in non-conventional IT
- The technical competence of attackers is increasing

Image: www.grtcorp.com

Control system failure

- IMCA Safety Flash 02/13 - Serious DP Diving Incident:
  - Loss of all analogue and digital RBUS Input / Output (I/O) signals
  - Loss of positioning references and environmental signals
  - Subsequent loss of DP control, resulting in a vessel position drift-off
  - Problem was contained in the DP control system rather than the thrusters
  - Power to DP was recycled and the vessel was able to return to full DP auto mode
  - The vessel had drifted off a distance of 240m from the original position
- Investigation determined that the RBUS jammed involving faults in one or more RBUS I/O modules in the DPC-3 cabinet
  - No definitive cause of the jamming was identified
  - A firmware upgrade has now resolved the problem

Image: www.smp-ltd.co.uk

Unconfirmed cyber security anecdotes

- “An attacker managed to tilt a floating oil rig to one side off the coast of Africa, forcing it to shut down”
- “One rig was so riddled with computer malware that it took 19 days to make it seaworthy again”
- Attacks could “do damage to an offshore drilling rig that could lead to an oil spill.” and “Such threats now have the potential to cause environmental damage, energy-supply outages for weeks or months, and even the loss of human life.”

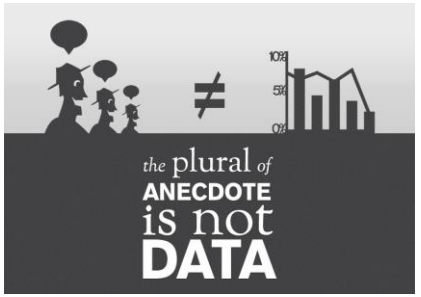

Image: line-in.co.uk

Short term solutions

- The active threats to DP 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

Longer term solutions

- DP systems developers need to implement an SDL (Secure Development Lifecycle)
- System components and fully integrated solutions should be security regularly tested
- The “bigger picture” should be considered when remote connectivity to any component is required

Image: www.trickedbythelight.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 DP operations.

Image: www.eci.com

Questions?

UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Milton Keynes

North American Offices

San Francisco

Atlanta

New York

Seattle

Australian Offices

Sydney

European Offices

Amsterdam - Netherlands

Munich – Germany

Zurich - Switzerland

Andy Davis, Research Director NCC Group

andy.davis@nccgroup.com