ABS CyberSafety™ Program

Marine and Offshore Cybersecurity

Jan Otto de Kat
Director Energy Efficiency and Vessel Performance

Genoa
18 April 2016

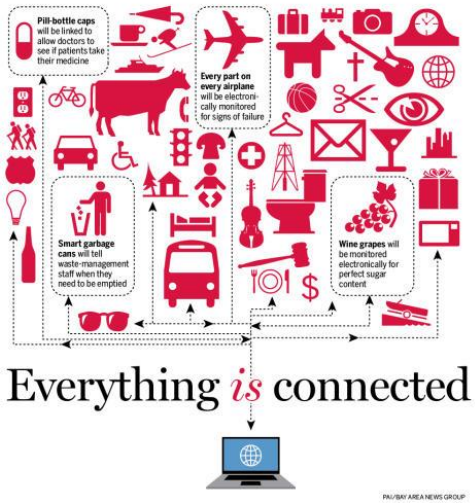
Agenda for Today's Discussion

- Cybersecurity Key Issues in Marine and Offshore Industry
- ABS Latest Development on Cybersecurity
- IACS Activities on Cybersecurity
- ABS Key Services on Cybersecurity

Areas of Concern for Cybersecurity

- Industrial Control Systems (ICS)
- Software Applications
- Data Stores and Intellectual Property Assets
- Data Transmission Paths

Priorities change by industry and according to levels of investment



Source: http://www.mercurynews.com/business/ci_24836116/internet-things-seen-bonanza-bay-area-businesses

RISK ASSESSMENT / SECURITY & HACKTIVISM

Analysis confirms coordinated hack attack caused Ukrainian power outage

BlackEnergy was key ingredient used to cause power outage to at least 80k customers.

by Dan Goodin - Jan 10, 2016 11:42pm CST

Share Tweet

~1 Week Outage

Source: http://arstechnica.com/security/2016/01/analysis-confirms-coordinated-hack-attack-caused-Ukrainian-power-outage/

Potential Losses:

- *Functions*
- Trust
- Money
- IP or Assets

Cybersecurity is Required *Everywhere*
Examples in Marine and Offshore Industry

- SAFETY: Diver tender stationkeeping system “blue screened”; resulting drift-off severed diver umbilical
- DOWNTIME: Tidal turbine hacked, operating software encrypted, utility held for ransom, 15 days to fix
- DESTRUCTION: Steel mill OT system hacked, mill burned to the ground
- CONFUSION: Ship’s manifest modified to benefit perpetrators, containers weren’t where the operator expected

What is the risk?

Attacks in cyberspace are generally done…

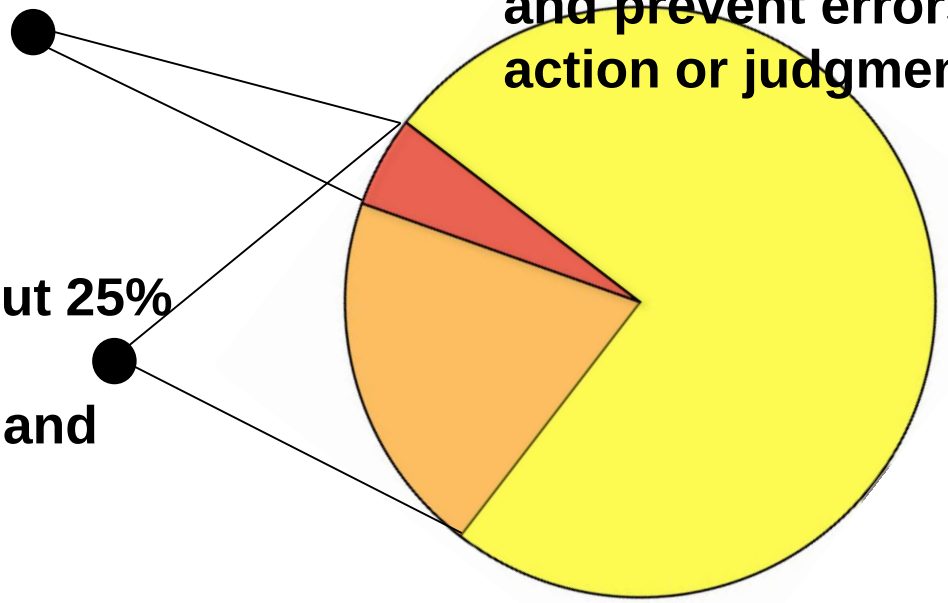
1. **For financial gain**
2. **To extend a personal agenda**
3. **To extend a political agenda**

<u>Takeaways</u>:

1. **Train your people**
2. **Put policies and procedures in place to guide their actions – and prevent errors of action or judgment**

<u>Most targets</u>: about 5% of the attacks are from bad actors, and 95% from mistakes carelessness and poor practices

<u>Very attractive targets</u>: about 25% of the risks come from bad actors, 75% from mistakes and accidents



Marine Cyber-Physical Environment

- Automation is Everywhere on Marine and Offshore Assets
  - Crew management systems
  - Voyage management systems
  - Communications systems
  - Emission monitoring
  - Navigation system
  - Ship control system
  - Equipment control systems
  - Cargo management system
  - Propulsion control system
  - Power distribution management system
  - Machinery control systems
  - Alarm management system
  - Sensor management system
  - Ballast management system
  - Maneuvering & positioning systems
- “Smart” Adds a System Integration Dimension

Offshore Cyber-Physical Environment

- Ubiquitous and Pervasive – Multiplying Functions, Reducing Crew Numbers
- Systems are More Often Networked (i.e., Industrial Ethernet) Than Standalone
- Internet Standards Are Slowly Replacing Proprietary Protocols in ICS
- Remote Accessibility is Often the Rule, Rather Than the Exception

ABS Latest Development: ABS CyberSafety™

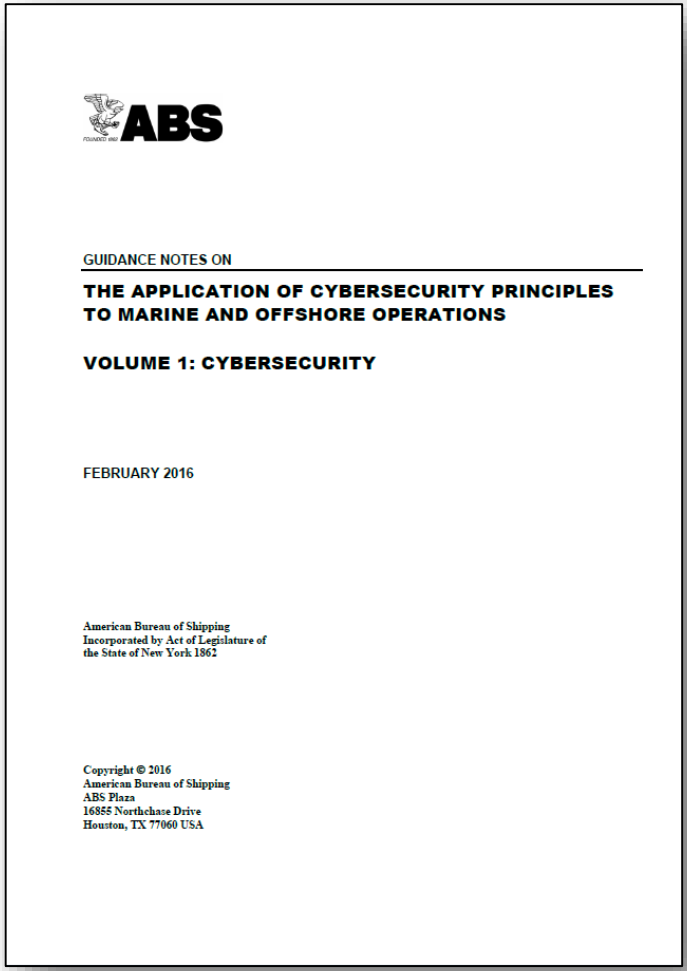
- ***ABS CyberSafety™****:* Measurable implementation of CyberSafety that tailors cybersecurity and systemic safety to assets in order to enable and encourage risk-based asset management as a systemic outcome.

- ABS CyberSafety™ will provide deterministic outcomes when implemented within managed environments that include appropriate processes, policies, system test and audit, and data management.

ABS Guidance Note – Volume 1: Cybersecurity

Starting to Link Systems Engineering & Cybersecurity

- This cybersecurity guidance note provides best practices for cybersecurity as a foundational element of overall safety and security within and across the marine and offshore industries.
- First volume in the ABS CyberSafety™ series.
  - Series is the industries' first risk-based management program for four key cyber areas: cybersecurity, automated systems safety, data management and software assurance.


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

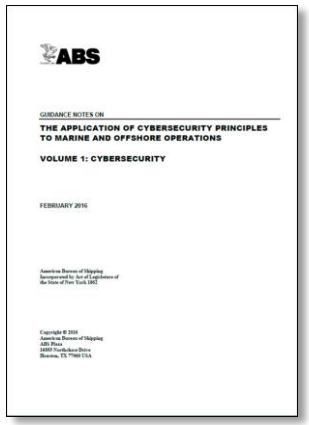
Available at: http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/221_Guidance_Notes_Cyber_Safety_Principles_Maritime_Operations/Cyber_Security_v1_GN_e.pdf

IACS Recent Activities on Cyber Topics

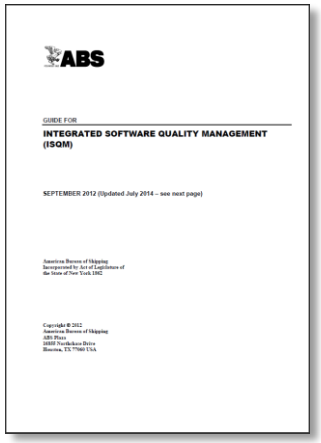
- Complex systems working group changed its focus to Cybersecurity in 2016
- Actions for this year include
  - Manual / local backup capabilities for integrated machinery systems – interpretation of SOLAS - SOLAS II-1/Reg. 31.2 (Machinery controls) and SOLAS II-1/Reg. 49 (Unattended machinery spaces)
  - Identification of information required to be recorded in the system documentation to ensure robust system design, functionality and security
  - Identify an initial range of cybersecurity practices and needs which could be integrated into a UR (Unified Requirements)
  - Develop an IACS paper on Cybersecurity for submission to MSC 97

ABS Key Services

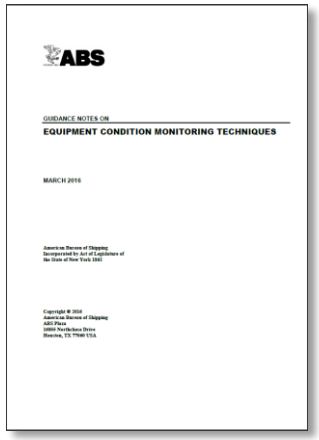
- Integration of Cyber, Data and Software assurance
  - Machinery and sensor monitoring give us an opportunity to gauge efficiency and effectiveness
  - Cyber to be integrated with the machinery
  - Software assurance to be part of system testing and sensor management to ensure proper safety throughout the system of systems.



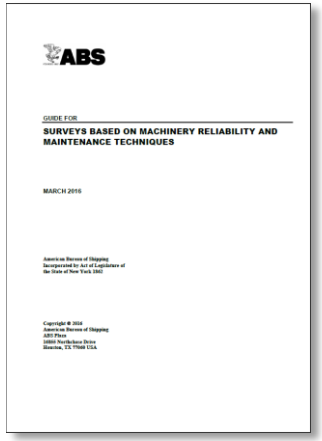
Cybersecurity



ISQM



Equipment Monitoring



Machinery Reliability & Maintenance

Available at www.eagle.org

www.eagle.org