Cybersecurity for UNOLS

An Introduction to Proactive Best Practices

satnag@unols.org

RVTEC 2017 - Duluth, Minnesota

Questions for UNOLS

Being Proactive vs Reactive

What are our Risks?

How big are the Impacts?

Are we prepared?

Per Institution or Fleetwide Approach?

How much overlap with Networking?

Overview

Parent Documents and Guidance:

- **The Guidelines on Cyber Security Onboard Ships** (http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16)

- **Center for Trustworthy Scientific Cyberinfrastructure** (https://trustedci.org/)

- **NIST FIPS PUB 199** (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf)

- **IMO Guidelines on Maritime Cyber Risk Management** (http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20%28Secretariat%29.pdf)

> *Cybersecurity is not a "one size fits all" silver bullet, but instead is a process, carefully tailored to a community to create trust while impacting the work as little as possible.*
>
> *-- https://trustedci.org/*

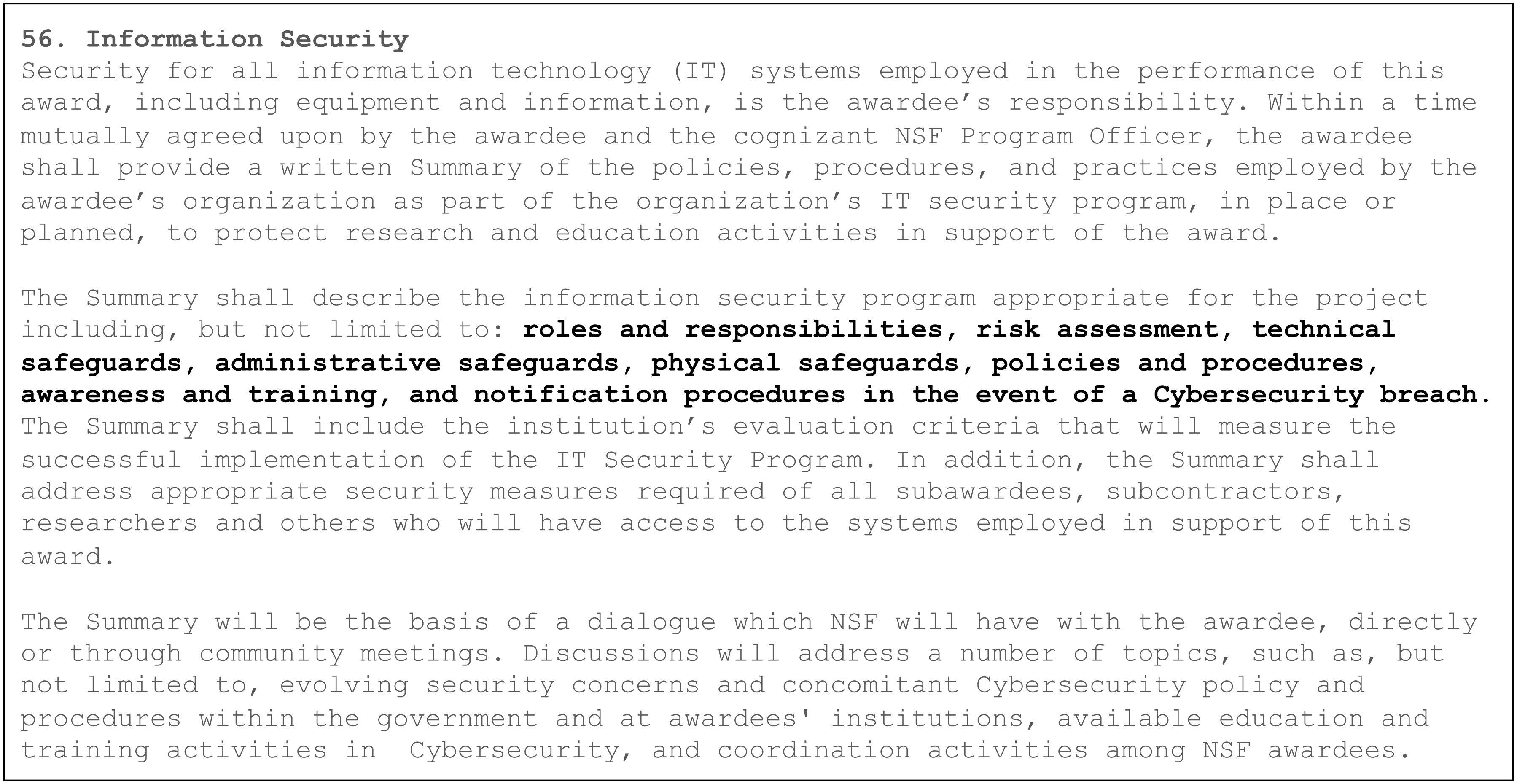
Why we care.

> ***Ships are increasingly using systems that rely on digitisation, integration, and automation****, which calls for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet.*
>
> *-- The Guidelines on Cyber Security Onboard Ships*

- Cybersecurity threats are complex, multifaceted and constantly changing.
- It is overwhelming to prevent cybersecurity incidents.
- A single successful attack can cripple your organization through:
  - Technical debt: IT Staff response and cleanup efforts
  - Compliance and regulatory response
  - Loss of data which could lead to loss of mission and loss of $$$
  - Erosion of trust by your customers
  - In-ability to securely reconstruct IT infrastructure

NSF Directives to Institutions

Cooperative Agreement, Supplemental Financial/Administrative Terms and Conditions - dated 02/12 Large Facilities
https://www.nsf.gov/pubs/policydocs/cafatc/cafatc_lf116.pdf



56. Information Security

Security for all information technology (IT) systems employed in the performance of this award, including equipment and information, is the awardee’s responsibility. Within a time mutually agreed upon by the awardee and the cognizant NSF Program Officer, the awardee shall provide a written Summary of the policies, procedures, and practices employed by the awardee’s organization as part of the organization’s IT security program, in place or planned, to protect research and education activities in support of the award.

The Summary shall describe the information security program appropriate for the project including, but not limited to: **roles and responsibilities, risk assessment, technical safeguards, administrative safeguards, physical safeguards, policies and procedures, awareness and training, and notification procedures in the event of a Cybersecurity breach.** The Summary shall include the institution’s evaluation criteria that will measure the successful implementation of the IT Security Program. In addition, the Summary shall address appropriate security measures required of all subawardees, subcontractors, researchers and others who will have access to the systems employed in support of this award.

The Summary will be the basis of a dialogue which NSF will have with the awardee, directly or through community meetings. Discussions will address a number of topics, such as, but not limited to, evolving security concerns and concomitant Cybersecurity policy and procedures within the government and at awardees' institutions, available education and training activities in Cybersecurity, and coordination activities among NSF awardees.

Industry Standard Best Practices

- Robust Backups with a routinely tested Disaster Recovery Plan

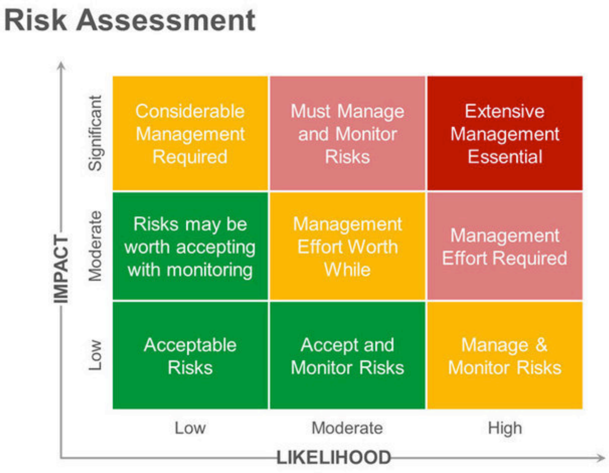
- Routinely updated Asset and Risk Management Plan

- Configuration and Change Managed IT Infrastructure

- Systems Health, Event, and Process Monitoring and Reporting

- Proactive Intrusion Detection Systems

- Routine Cybersecurity Awareness Training for crew and science parties.



Risk Assessment

IMPACT	LIKELIHOOD: Low	LIKELIHOOD: Moderate	LIKELIHOOD: High
Significant	Considerable Management Required	Must Manage and Monitor Risks	Extensive Management Essential
Moderate	Risks may be worth accepting with monitoring	Management Effort Worth While	Management Effort Required
Low	Acceptable Risks	Accept and Monitor Risks	Manage & Monitor Risks

The Guidelines on Cyber Security Onboard Ships

http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

Ships are increasingly using systems that rely on digitisation, integration, and automation, which calls for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet.

The International Maritime Organization (IMO) has developed guidelines that provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Guidelines on Cyber Security Onboard Ships are aligned with the IMO guidelines and provide practical recommendations on maritime cyber risk management covering both cyber security and cyber safety.

The National Institute of Standards and Technology, US Department of Commerce (NIST) framework has been used during the development of these guidelines. NIST aims to help understand, manage and express cyber security risks both internally and externally, for example within a ship's organisation. It can help to identify and prioritise actions for reducing cyber security risks. It is also a tool for aligning policy, business and technological approaches to manage the risks.

The Guidelines on Cyber Security Onboard Ships

http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

Ship to shore interface

Ships are becoming more and more integrated with shoreside operations because digital communication is being used to conduct business, manage operations, and stay in touch with head office. Further, critical ship systems essential to the safety of navigation, power and cargo management have been increasingly digitalised and connected to the internet to perform a wide variety of legitimate functions such as:

- engine performance monitoring
- maintenance and spare parts management
- cargo, crane and pump management
- voyage performance monitoring.

The above list provides examples of this interface and is not exhaustive. The above systems provide data which may be of interest to cyber criminals to exploit.

Bring your own device (BYOD)

It is recognised that personnel may be allowed to bring their own devices (BYOD) on board to access the ships' system or network. Although this may be both beneficial and economical for ships, because these devices may be unmanaged, it significantly increases the possibility of vulnerabilities being exposed. Policies and procedures should address their control, use, and how to protect vulnerable data, such as through network segregation.

The Guidelines on Cyber Security Onboard Ships

http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

- Defence in depth and in breadth
- Identify threats
- Types of cyber attack
- Stages of cyber attack
- Identifying Vulnerabilities
  - NIST FIPS CIA model
  - Bridge Systems
  - Propulsion and Power Control
  - Access Control Systems
  - Passenger Facing Public Networks
  - Communications Systems
  - Ship to Shore Interface
  - Bring your own Device
- Risk Assessment
- Protection and Detection Measures
  - Limitation to and control of network ports, protocols and services
  - Configuration of network devices such as firewalls, routers and switches
  - Satellite and radio communication
  - Wireless access control
  - Malware detection
  - Data recovery capability

- Procedural protection measures
  - Training and Awareness
  - Access for Visitors
  - Upgrades and Software Maintenance
  - Remote Access
  - Use of Admin Privs
  - Removable Media Controls
  - Equipment Disposal
- Establish Contingency Plans
- Incident Response

NIST FIPS PUB 199

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

FISMA - Federal Information Security Management Act of 2002

FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information security systems. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level.[2]

According to FISMA, the term ***information security*** means protecting information and **information systems** from **unauthorized access**, use, disclosure, **disruption**, **modification**, or destruction in order to provide **integrity, confidentiality** and **availability**.

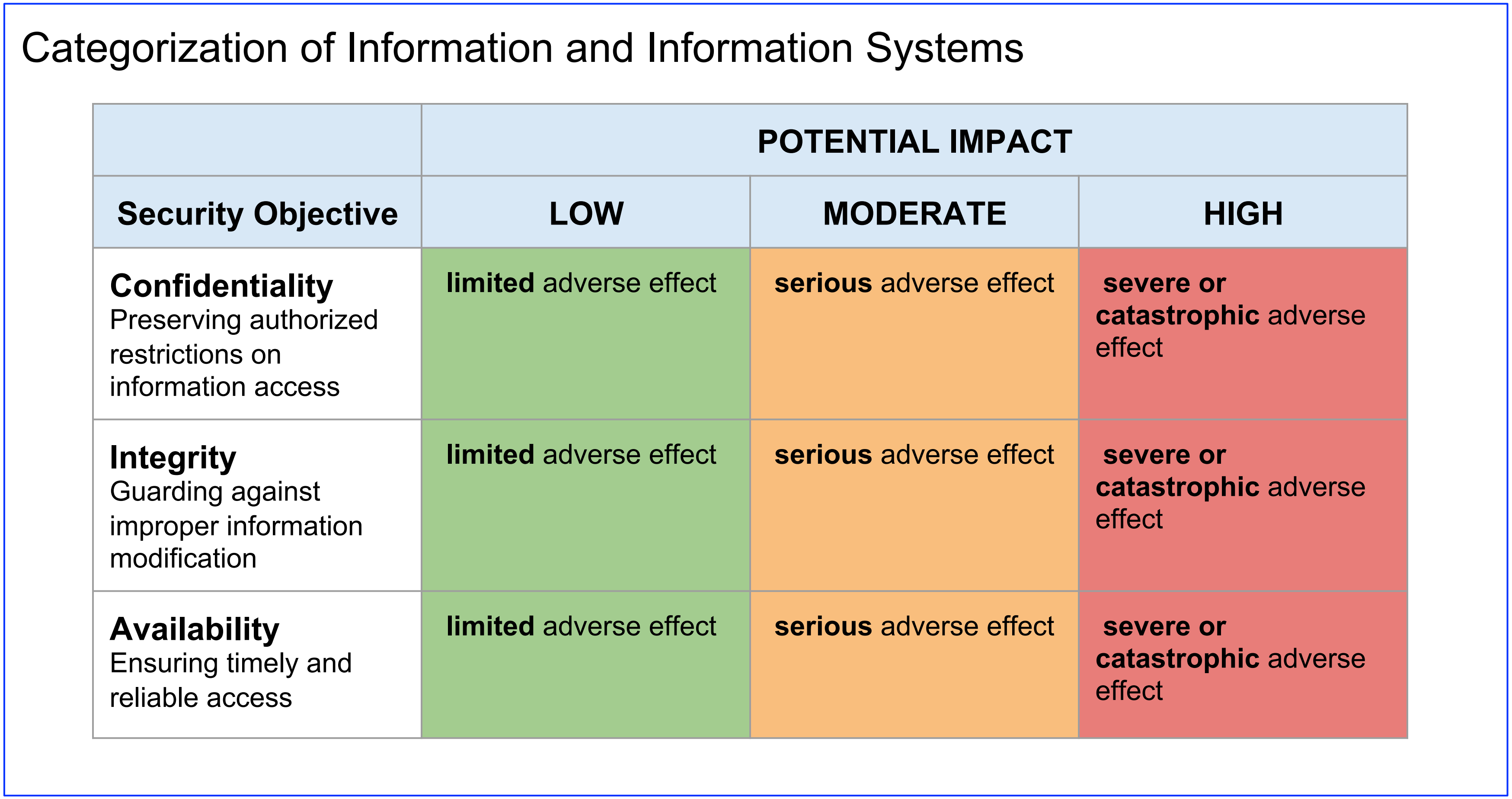
Title III FISMA tasked NIST with responsibilities for standards and guidelines, including the development of:

- **Standards to be used by all federal agencies to categorize all information and information systems collected or maintained** by or on behalf of each agency based on the objectives of **providing appropriate levels of information security according to a range of risk levels**;
- Guidelines recommending the types of information and information systems to be included in each category; and
- Minimum information security requirements (i.e., management, operational, and technical controls), for information and information systems in each such category.

FIPS Publication 199 addresses the first task cited—to develop standards for categorizing information and information systems. Subsequent NIST standards and guidelines will address the second and third tasks cited.

NIST FIPS PUB 199

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf



Categorization of Information and Information Systems

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access	**limited** adverse effect	**serious** adverse effect	**severe or catastrophic** adverse effect
Integrity Guarding against improper information modification	**limited** adverse effect	**serious** adverse effect	**severe or catastrophic** adverse effect
Availability Ensuring timely and reliable access	**limited** adverse effect	**serious** adverse effect	**severe or catastrophic** adverse effect

NIST FIPS PUB 199

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Categorization of Information and Information Systems Examples

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access	List of IP addresses Email addresses List of Persons on board and Citizenship	**Personally Identifiable Information (PII)** Passport Number, Social Security #, Birth Dates **Medical Information**	Administrative Passwords Ship Schedule and Navigation Plans ITAR Issues
Integrity Guarding against improper information modification	Defaced Website	Hijacked user account	Exploited Navigation Systems Compromised Engineering or Bridge Systems
Availability Ensuring timely and reliable access	Intermittent Internet Saturation from malicious traffic	Virus Infected Laptop	Denial of Service Attack Loss of Underway Data

Center for Trustworthy Scientific Cyberinfrastructure

https://trustedci.org/

The mission of CTSC is to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors.

This mission is accomplished through one-on-one engagements with projects to address their specific challenges; education, outreach, and training to raise the state of security practice across the scientific enterprise; and leadership on bringing the best and most relevant cybersecurity research to bear on the NSF cyberinfrastructure research community.

Center for Trustworthy Scientific Cyberinfrastructure

https://trustedci.org/

Getting Help from CTSC

The mission of CTSC is to ensure NSF cyberinfrastructure (CI) projects get the guidance they need regarding their cybersecurity challenges. From quick questions to collaborative engagements lasting months, CTSC tackles challenges of all sizes. This includes:

Getting started - You're running a project and you don't know if you have any cybersecurity issues. Or maybe you have something that makes you nervous, but you don't know where to start.

Asking specific questions - e.g., Should I being using OpenID or Shibboleth? What's a good tool for IDS? How do I check my code for security vulnerabilities?

Helping with cybersecurity planning in developing a program.

Assessing an existing cybersecurity program.

Is the piece of software secure? Maybe you want a user community to adopt your software but they aren't sure it's secure enough for them. An independent assessment can help.

Designing or reviewing a security feature of my software - e.g., you need to allow one user to authorize another user to access their data in a way that doesn't cause your PI to lose sleep about data privacy.

Maybe you are developing a new cybersecurity tool or researching a new technique and are looking for someone who could benefit from it.

Annual Conference - NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure August in Arlington VA

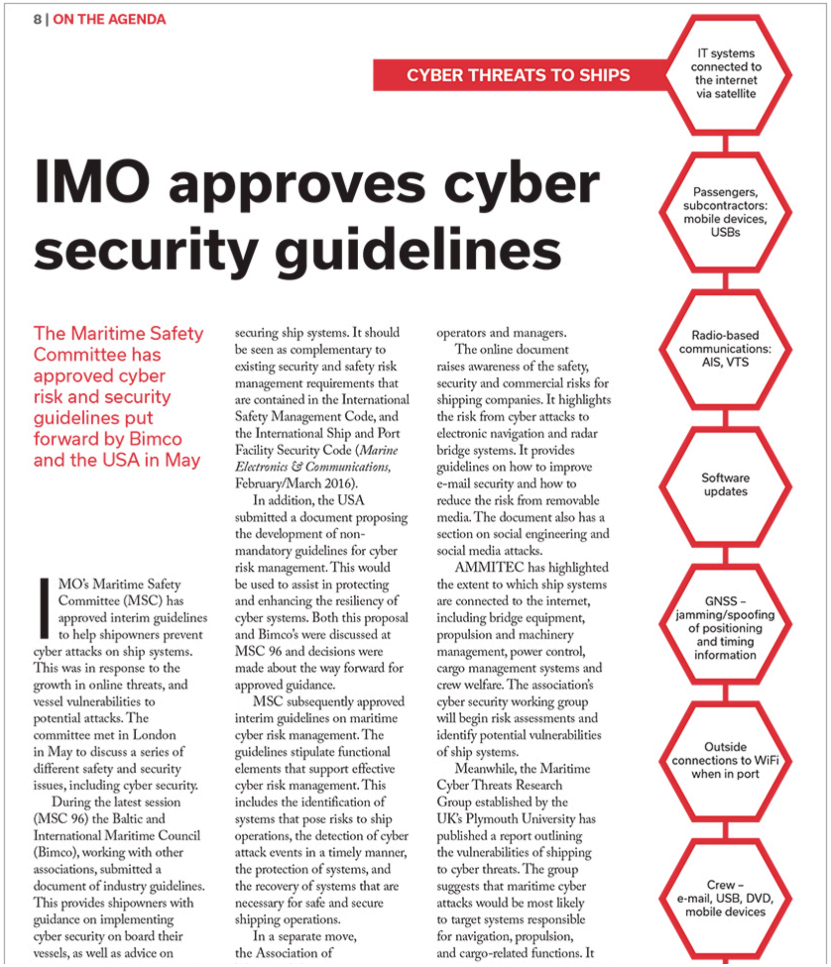
IMO Guidelines on Maritime Cyber Risk Management

http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20%28Secretariat%29.pdf

IMO Approves Cyber Security Guidelines - June 2016, Marine Electronics and Communications

Article: https://www.ammitec.org/index.php/news-and-events/news/98-imo-approves-cyber-security-guidelines-june-2016-marine-electronics-and-communications

IMO Website: http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/cyber-security.aspx



8 | ON THE AGENDA

CYBER THREATS TO SHIPS

IT systems connected to the internet via satellite

Passengers, subcontractors: mobile devices, USBs

Radio-based communications: AIS, VTS

Software updates

GNSS – jamming/spoofing of positioning and timing information

Outside connections to WiFi when in port

Crew – e-mail, USB, DVD, mobile devices

IMO approves cyber security guidelines

The Maritime Safety Committee has approved cyber risk and security guidelines put forward by Bimco and the USA in May

IMO's Maritime Safety Committee (MSC) has approved interim guidelines to help shipowners prevent cyber attacks on ship systems. This was in response to the growth in online threats, and vessel vulnerabilities to potential attacks. The committee met in London in May to discuss a series of different safety and security issues, including cyber security.

During the latest session (MSC 96) the Baltic and International Maritime Council (Bimco), working with other associations, submitted a document of industry guidelines. This provides shipowners with guidance on implementing cyber security on board their vessels, as well as advice on securing ship systems. It should be seen as complementary to existing security and safety risk management requirements that are contained in the International Safety Management Code, and the International Ship and Port Facility Security Code (*Marine Electronics & Communications*, February/March 2016).

In addition, the USA submitted a document proposing the development of non-mandatory guidelines for cyber risk management. This would be used to assist in protecting and enhancing the resiliency of cyber systems. Both this proposal and Bimco's were discussed at MSC 96 and decisions were made about the way forward for approved guidance.

MSC subsequently approved interim guidelines on maritime cyber risk management. The guidelines stipulate functional elements that support effective cyber risk management. This includes the identification of systems that pose risks to ship operations, the detection of cyber attack events in a timely manner, the protection of systems, and the recovery of systems that are necessary for safe and secure shipping operations.

In a separate move, the Association of operators and managers.

The online document raises awareness of the safety, security and commercial risks for shipping companies. It highlights the risk from cyber attacks to electronic navigation and radar bridge systems. It provides guidelines on how to improve e-mail security and how to reduce the risk from removable media. The document also has a section on social engineering and social media attacks.

AMMITEC has highlighted the extent to which ship systems are connected to the internet, including bridge equipment, propulsion and machinery management, power control, cargo management systems and crew welfare. The association's cyber security working group will begin risk assessments and identify potential vulnerabilities of ship systems.

Meanwhile, the Maritime Cyber Threats Research Group established by the UK's Plymouth University has published a report outlining the vulnerabilities of shipping to cyber threats. The group suggests that maritime cyber attacks would be most likely to target systems responsible for navigation, propulsion, and cargo-related functions. It

IMO Guidelines on Maritime Cyber Risk Management

http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20%28Secretariat%29.pdf

These Guidelines provide high-level recommendations for maritime cyber risk management. For the purpose of these Guidelines, maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework:

1. **Identify**: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
2. **Protect**: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
3. **Detect**: Develop and implement activities necessary to detect a cyber-event in a timely manner.
4. **Respond**: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
5. **Recover**: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

Questions for UNOLS

What are our Risks?

How big are the Impacts?

Are we prepared?

Per Institution or Fleetwide Approach?

How much overlap with Networking?