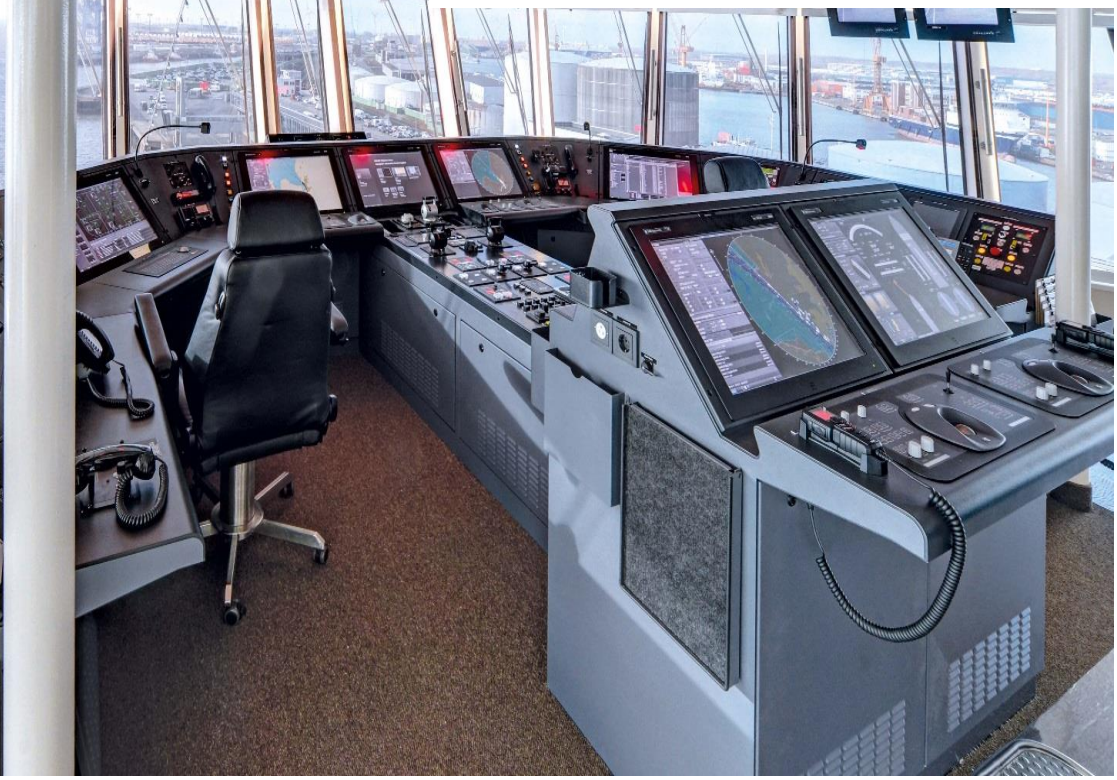
Building Maritime Cyber Assurance

1 February 2015



USMRC

UNITED STATES MARITIME RESOURCE CENTER

Authors

Captain Alexander N. Soukhanov, AFNI

Vice President, International Shipping and Maritime Operations, USMRC

Alex is a Full Branch State Pilot in the Commonwealth of Massachusetts and licensed Master Mariner (unlimited tonnage) with extensive and diverse global operational experience. He has developed and directed research projects involving maritime operations, global logistics, and supply chain security for a wide variety of complex industry and government clients. Alex is also a serving Commander in the United States Navy Reserve with command experience. He holds a Bachelor of Science degree in Marine Transportation from the Massachusetts Maritime Academy.

Mr. John Bos

President, Cybrex LLC

John is a career cyber operator with fifteen years of advanced network offensive and defensive experience primarily associated with network penetration and Vulnerability Assessment. He is also a 23 year veteran of the US Navy, serving with distinction as an Information Warfare Officer, Surface Warfare Officer/Navigator and computer and radar technician. For 9 years, John led a highly successful competitive hacking team consistently placing within the top 4 percent against US and international adversaries. John holds a Master's Degree in Information Warfare from Naval Postgraduate School and is a Certified Information Systems Professional and Certified Ethical Hacker.

Executive Summary

Much has been written about the vulnerabilities to industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems of commercial ships and marine terminals; the integration of those systems with information technology (IT), and the dependency on Global Positioning Satellite systems. IT-dependent critical shipboard systems is the reality of modern maritime operations. Modern ships are built with Ethernet and LAN configurations, supporting electronic navigation, engine control, cargo management, and other systems. Dynamic Positioning (DP) systems integrate navigation and engine control systems with positioning sensors to hold station and navigate along precise tracks. Vessels across the globe, in numerous sectors of the maritime industry ecosystem, are equipped in this manner.

Organizations from European Union agencies, maritime law firms, the Nautical Institute, Royal Institute of Navigation, universities, and maritime consultancies have published scores of papers and have made compelling arguments on the need to deal with the apparent weaknesses to maritime cybersecurity. Others rightfully argue that cyber vulnerabilities may constitute serious threats to seaworthiness, while invoking aspects of maritime law, citing the carrier's duties in "exercising due diligence"…"to make the ship seaworthy" and "to properly man, equip, and supply the ship".[1]

However, common wisdom and traditional risk management methodologies pose a potential challenge in moving forward, countering with the questions, "Where is the threat?" and "What has been reported?" Although only a few specific cases have been reported to the public, the questions must still be answered and the hypotheses tested through technical research. As mariners, we are trained from the beginning to continuously observe activity on the sea and aboard our vessels, monitor trends, anticipate, and take proactive action. It is apparent to us at USMRC that indeed the abstract spectrum of the cyber world and security standards for protecting mariners, cargo, and the environment have not maintained pace with the continuous advances in technology.

USMRC seeks to conduct research, raise awareness, and develop technical solutions solve the problem. The end state is to develop sensible and relevant maritime cyber assurance standards through collaborative work with industry stakeholders, such as class societies, flag states, insurers, ship operators, and other organizations. We believe real technical solutions are the imperative, vice traditional risk management approaches.

The Maritime Operations Perspective

Mariners are trained to mitigate risk in maritime operations and proactively deal with a wide variety of safety scenarios, from firefighting and lifesaving, oil spill and pollution prevention, medical care and first aid, communications, collision avoidance and

[1] Hague Visby Rules, Article III, Rule 1 (a) and (b).

navigation safety, enclosed space entry, engineering and cargo operations, stability and ballasting, bunkering, physical security, and so much more. Safe operations best practices are codified in many international regulations, such as Safety of Life at Sea (SOLAS), International Convention for the Prevention of Pollution from Ships (MARPOL), International Ship and Port Facility Security Code (ISPS), International Regulations for Preventing Collisions at Sea (COLREGS), and the International Safety Management Code (ISM). Compliance of safety standards is verified through numerous types of periodic inspections by companies, port state, classification societies, P&I, and more. Astonishingly, despite global regulations covering all aspects of industrial safety aboard ships, nowhere do global standards for maritime cyber assurance exist. Not even in marine terminals.

Further, mariners are not trained to recognize active cybersecurity breaches to critical systems, and are not trained to recognize the difference between intentional and unintentional interruptions. Software in critical equipment varies and none are known to exist that actually alert the mariner of a cyber-disruption. Mariners are trained to react to malfunctioning or inoperative systems by dedicating resources and personnel to respond, troubleshoot, and take corrective action or schedule shoreside repair. Yet, any response and capability to deal with on board maritime cyber disruptions, if actually recognized, is nearly non-existent in the maritime industry, with the exception of some specialized vessels.

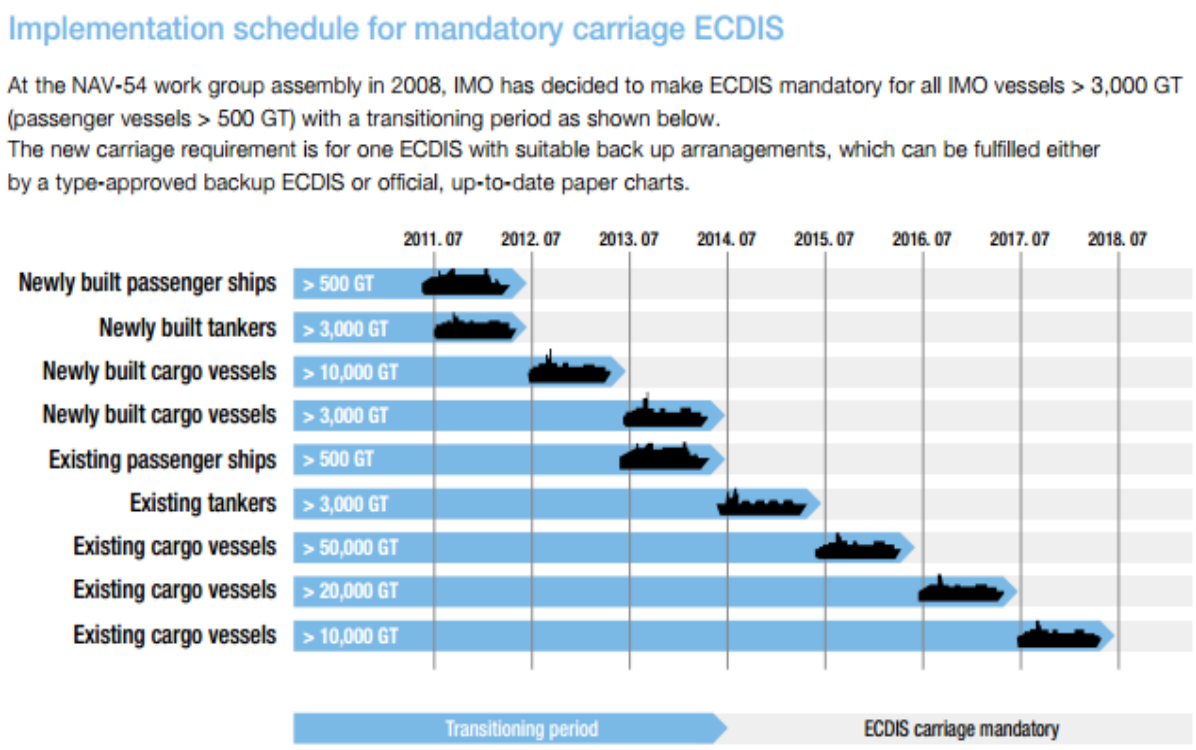
The July 2010 Manila Amendments to the International Convention on Standards for Training, Certification, and Watchkeeping for Seafarers (STCW 1978, as amended) contains new requirements for the training of shipboard engineering department positions with the endorsement as Electro-Technical Officer (ETO) and Electro-Technical Rating (ETR). The ETO endorsement will require certification of competency "to operate computers and computer networks on ships".[2] The Electro-Technical Rating (ETR) "must satisfactorily complete courses in computer systems and maintenance"[3]. The 2010 Manila Amendments will be effective 1 January 2017. As of printing on 1 October 2014, 46 US Code of Federal Regulations (CFR)[4] specifies that an ETO candidate must provide evidence of completion of professional training in "Onboard Computer Networking and Security". Yet specific IMO and USCG-approved training courses do not appear to exist, with limited guidance available. In the United States, there is no equivalent path for the national endorsement outlined in 46 CFR.

Some critical IT-dependent shipboard systems are mandated to be installed aboard vessels, and operated by officers trained in its use. Dependency on mandated navigation and situational awareness tools, such as Electronic Chart Display Information System (ECDIS) is therefore natural and expected, but also assumes the systems to be true and reliable. ECDIS is increasingly integrated with all systems in the navigation bridge. Cyber disruptions to equipment essential for maintaining a proper lookout, navigation, and determining if risks of collision exist could certainly contribute to

[2] STCW 1978, 2010 Manila Amendments, Regulation III/6, Section A-III/6, Table III-6.
[3] 46 CFR §12.611(a). Also see USCG NVIC 24-14, 02 September 2014.
[4] 46 CFR §11.335. Also see USCG NVIC 23-14, 25 August 2014.

a transportation safety incident. ***Doubt*** as to one's navigation and collision avoidance situation requires immediate action to be taken in accordance with the COLREGS.[5]

Many ship systems are also able to connect to the Internet to perform a wide variety of functions, such as monitor engine performance through Remote Access Monitoring (RAM), fuel consumption, DP performance monitoring, Electronic Navigation Chart (ENC) download and updating, engineering maintenance, and spare parts inventory. Uncontrolled access to the Internet, via any communications medium, requires security considerations for all the obvious reasons.



Source: Furuno

Although shipping companies may possess varying information assurance policies, there are no known best practices or IMO-mandated certifications of shipboard IT-based critical systems. There are no mandated IT security audits, aside from those conducted ad hoc. In fact, USMRC's team thoroughly researched international maritime regulations and classification society standards, and found no standards for maritime cyber assurance, resilience, or security. Additionally, there is little evidence of hardware and software manufacturers developing assurance and resilience standards to include basic and regularly updated software security patches for shipboard systems, and routine tests of security boundaries after the equipment has been installed.

[5] COLREGS Rules 5 and 7.

Our Approach

While the US Coast Guard has recently issued its imperative for risk management approaches to dealing with maritime cybersecurity, USMRC has chosen to take a more direct and holistic technical approach to cyber risk mitigation through assurance via the following methodologies:

1. Partner with a maritime cyber-defense firm to develop an understanding of threats and vulnerabilities to critical shipboard systems.

2. Build an evidence-based aggregate model of ship IT configurations and dependent critical systems to tell the complete story of vulnerability.

3. Develop best practices of cyber security and resilience through the discoveries of our research, while supported by industry stakeholders.

4. Develop and implement cyber security audit standards for classification societies.

5. Amend the ISPS to incorporate global minimum cybersecurity standards.

6. Develop education for mariners, company, and facility personnel for basic cybersecurity best practices.

7. Develop an International Maritime Organization (IMO) and US Coast Guard approved professional training course in “Onboard Computer Networking and Security” in accordance with 46 CFR §11.335 and STCW 1978, 2010 Manila Amendments, Regulation III/6, Section A-III/6, Table III-6.

8. Achieve certification for development of standards, regulations, and training.

First Steps Taken

It was important for us to understand the vulnerabilities to our equipment through onboard examination of actual systems with the help of appropriate subject matter experts. USMRC partnered with Cybrex LLC, a firm specializing in “Red Team” and “Blue Team” vulnerability assessments and mitigation work for IT systems aboard naval vessels. The Cybrex team fully understands the complexities of maritime IT systems and their integration with critical industrial controls. To drive a concerted effort in understanding the weaknesses of maritime cyber, it was first necessary to merge the languages and experience of maritime operations with cyber operations.

The first step was to conduct an actual assessment of critical systems aboard a vessel. Over a three day period in January 2015, USMRC and Cybrex performed a limited pilot assessment of a vessel classed by a member class society of the International Association of Classification Societies (IACS), equipped with dynamic positioning, an integrated navigation bridge (to include ECDIS), and an automated engineering power

plant with Remote Access Monitoring (RAM). Our major discoveries, from basic cyber hygiene to severe issues, include:

- Consoles in main engineering room only have administrator accounts. This means any person has unlimited ability to create new accounts, modify critical configuration, install/uninstall software, and conduct any operation. This could be potentially catastrophic.

- Consoles in main engineering control have potentially unsafe Internet-based third party remote administration software. This is a Virtual Private Network (VPN) software which can be unsafe to the system, depending on the version. It is used as a Remote Admin Tool (RAT), which should not be on an ICS to connect to the Internet. Again, this is potentially very dangerous to operations.

- Version of installed software is unknown. The consequences could be malicious remote control, with denied or degraded engineering operations.

- Engineering control computer consoles have persistent unauthorized Internet connection, with no detected security boundaries or firewalls. Sensitive engine controls may be accessed globally by malicious actors. The consequences could be catastrophic, not to mention denied or degraded engineering operations.

- Cumulative effects of the above three discoveries of engineering consoles could lead to potential remote exploitation of engineering consoles, adverse effects to seaworthiness, unexpected shutdown, or manipulation of important engineering processes. Ship is potentially dead in the water when engineering console servers fail. Local and manual backups existed but would only be effective after a shutdown or disruption in operations.

- A wireless router, of a type normally found in a home, was found disconnected inside engineering console. Careless or malicious connectivity creates substantial vulnerability, leading to potential denied or degrade engineering operations.

- All ICS/SCADA and ECS cabinets were unlocked, yet keys were readily available. A malicious insider or careless user could install convenience devices, disrupt the system or lock out the authorized users. This could lead to the degradation or denial of engineering operations.

- Engineering watch officer computer was logged on and open for use by anyone; persistent access available. Someone other than the watch officer can impersonate the watch officer or directly access the critical functions as if it were the person actually logged on, and potentially degrade or deny use of engineering functions.

- Unapproved keyboard installed by crew due to failure of original, introducing microphone, headphone, and USB interface availability outside the lockable

console. Easy to use the console as an entertainment device inviting misuse and unauthorized data and software. Easy access to USB flash drive enabled malware or surveillance devices.

- Numerous unsecured and unlocked engine performance monitoring cabinets throughout the ship, with easy access to USB ports.

- Recent class society inspection did not include cyber/IT survey or inspection. While apparently not a requirement by Class societies (ABS, Class NK, Lloyds, etc.), this discovery verifies current lack of policy for IT security from a key industry stakeholder.

- Motor drive cabinets unlocked with easy unauthorized access. Degraded/denied engineering functions possible.

- Evaporator auto control computers/monitors not physically secured. Unauthorized access to control networks on same subnet as Program Logic Controllers (PLC) and associated computers running engineering control software.

- The “Powershell” program was installed on main engine control computers. Large numbers of built-in capabilities exist in this program and are useful to an attacker. A malicious attacker could use these built-in capabilities to strengthen the intended access and impacts.

- Fuel management and reporting system has unsecured database access. Data is easily corrupted.

- Bridge console software crashed during testing and appears to be in use in many places throughout the ship. This is a shared instability problem with shared risk of denied engineering functions.

- Dual-homed computer on bridge console shares vulnerability of the obsolete Windows XP operating system across subnets. This could lead to degraded engineering and loss of subnet redundancy.

- Transas ECDIS box acts as the National Marine Electronics Association (NMEA) to USB connection. This is a critical node for navigation data. There is significant potential for disrupted or degraded electronic navigation.

- Computer used for downloading charts was a laptop, and not a permanent ship’s computer. Dangers of portable laptops and removable media are well-known and could render ENCs unreliable.

- ECDIS USB port reliability: no identification on thumb drive utilized for downloading and transferring ENCs from laptop to the ECDIS. No security for

USB which could be open to malware. Unreliable ENCs could be employed. Potential for malware infection by careless flash drive usage.

- ENC's for ECDIS are downloaded through an unsecured connection and protocol ("Wget" script); this invites the potential for Man-In-The-Middle (MITM) attacks on the traffic and the potential for eavesdropping or corrupted files. Again, downloaded ENCs could be rendered unreliable and be a potential factor in a transportation safety incident (TSI).

- Keys to dynamic positioning panels hanging near locked panels. Potential for unauthorized access, which could disable or manipulate DP system.

Next Steps

1. Continued Research. USMRC and Cybrex LLC seek support from maritime industry stakeholders in continuing cyber research assessments aboard a wide variety of ship types and classes. This research is necessary to build an aggregate model of discoveries and patterns of configurations. We also seek to understand and record the current levels of cyber security hygiene and awareness from crews, vessel operators, and companies.

2. Through industry supporters, such as class societies, registries, and other groups, USMRC and Cybrex LLC will develop best practices and guidelines for onboard IT security, to include amending ISPS.

3. Develop the cyber assurance certification process to involve equipment manufacturers, naval architects, shipbuilding, and shipyard activities aboard vessels.

4. Develop approved standards for maritime cyber auditors through collaborative work with class societies and other organizations.

5. Provide cybersecurity awareness for mariners, designated persons ashore, company security officers, and other key personnel. With the amendment of ISPS must also come changes to the Vessel Security Officer (VSO), Company Security Officer (CSO), and Facility Security Officer (FSO) requirements and certifications. Cyber assurance must be certified.

Conclusion

The burden of cyber security and resilience must not be solely on the mariner. It must originate as integral to the systems installed on the vessel, ingrained in the mariners operating the systems through advanced training, and maintained through routine – and secure – methods of upgrades and updates as supported by vessel operators and owners.

"As the maritime transportation system carries approximately 90% of international commerce, a successful cyber-attack against a maritime stakeholder could have significant negative effects on the global economy and disrupt international trade."

- IMO FAL 39th Session, Letter Submitted by Canada, July 2014

About the United States Maritime Resource Center

The United States Maritime Resource Center (USMRC) is a 501(c) (3) independent nonprofit organization specializing in navigation safety, maritime risk mitigation, human capital development, and raising awareness of international shipping and trade. For more than three decades, our business has focused on the safety of mariners, ships and cargo and the protection of the marine environment, through the extensive use of modeling, simulation, research, consulting and a deep global network of strategic advisors. Our projects range from new port and channel design testing and maritime consulting, to specialized training in navigation and LNG bunkering. Our team is comprised of senior maritime operations practitioners, and supported by a robust Advisory Board of global trade executives and professionals. Each of USMRC's senior staff holds a government security clearance.

About Cybrex LLC

Cybrex LLC is a Service Disabled Veteran Owned Small Business (SDVOSB) and Cleared Defense Contractor (CDC) established in 1999, specializing in maritime-centric cyber security and information operations. Based in Southeast Virginia, we serve customers primarily within the Mid-Atlantic Region. Our services include maritime information assurance, adversary emulation, security consultation, research and development, and specialized software development. Our team of experts offers combined expertise of over forty years of experience in information assurance, cyber security and maritime operations. All current members of the team are recognized subject matter experts with government security clearances.