The Reality of Shipboard Cyber Vulnerabilities

Cyber threats are pervasive across ***ALL*** industries. There isn't a day that passes without news of a cyber-attack in the private and government sectors. These attacks contribute to significant business impacts and financial losses, such as the recent hacking of the software in the SWIFT banking platform, resulting in the loss of $81 Million from the Central Bank of Bangladesh. And this particular investigation continues.

While much has been written about these vulnerabilities in shipping and marine terminal operations, little ***validated*** and ***current*** evidence of cyber disruptions to shipboard operations is available or apparent, except for a few overly-referenced and dated incidents. Moreover, the frequency of reported and validated incidents in maritime doesn't remotely compare to that of other industry sectors. This is peculiar: why is the cyber threat obvious across all industry sectors, but not so apparent to maritime? What's wrong with this picture?

The United States Maritime Resource Center (USMRC), an independent non-profit maritime risk research organization, and its maritime-centric cybersecurity partner, Cybrex LLC, developed the Maritime Cyber Assurance^{SM} research program to understand the vulnerabilities to IT- centric critical marine systems and industrial control systems (ICS) aboard ships and in marine terminals. This program is now recognized at the highest levels of international shipping. The objective of this research program is to assist our industry in *achieving* an acceptable and certifiable level of cyber awareness, safety, security, and resilience through evidence-based research.

USMRC specializes in maritime risk research and the development of operational best practices and specialized human capital development. Much of this work features maritime simulation, particularly in the human-machine interface, to aid in proving concepts and conducting specialized training. Human integration with machines and computers has been a traditional focus as a performance assessment and unique training tool. However, we are concerned with the risks presented by a systemic over-dependency on IT-based equipment and shipboard systems, whereby situational awareness and the mariner's "sixth sense" is either underdeveloped, or atrophied, by a false sense of trust in systems that can fail at any time – because they can and do fail.

We are also concerned that this trust is blind to cyber disruptions that may manifest themselves unbeknownst to the mariner, and that the ability to "trust but verify" in all aspects of daily operations becomes increasingly more difficult, particularly in stressful circumstances, or if doubt exists. For mariners, there are very clear and long standing rules on doubt, particularly in navigation.[1] Lastly, we are extremely concerned with the inconsistent and relatively low prioritization of security in shipboard and marine terminal IT environments, new technologies, and software as validated through our in-depth research.

To get a better understanding of international shipping's perception of cybersecurity, USMRC interviewed many principals across industry sectors, to include insurers, class societies, flag state, pilot groups, ship ownership and management, marine terminals, and many others. The responses varied, and while many viewed a growing concern, most key stakeholders had reservations of believing in cyber threats to maritime and ships, because it cyber didn't manifest itself as a "tangible risk". While cyber vulnerabilities and attacks have been common across the private sector, the vast majority of maritime principals acknowledged that the maritime industry has had little concern or understanding of the cyber threat. Common replies to our surveys and interviews of industry stakeholders are:

- "Why would someone want to attack my business? We own and operate ships? They're not connected to the internet."
- "Who would want to attack this little marine terminal? Besides, we have followed the advice of our lawyers and insurers. They provide us with the compliance direction."
- "What's the threat?" Or "Where's the threat – Nothing has happened yet!"

Although the reasons for this perception may be the lack of incident reporting, and no known insurance claims for shipboard incidents, we felt this was unsatisfactory and that a larger research effort was required. Knowing that cyber threats are pervasive (by whom, from where, or why is largely irrelevant), we focused our research on helping industry identify the vulnerabilities across systems, vessels, and terminals first.

USMRC's partnership with Cybrex LLC led to the creation of the Maritime Cyber Assurance Team (MCAT), allowing us to translate cyber vulnerabilities into understandable risks to shipboard operations. This translation of technical cyber vulnerabilities into operational and business impacts is critical to conveying the true risks that face every business.

[1] COLREGS Rules 5 and 7.

Major Discoveries

During the course of our shipboard cyber research over the past year and a half, vulnerability discoveries ranged from basic cyber hygiene issues to severe operational impact vulnerabilities. The following are some of the most poignant findings:

- Little to no evidence of cybersecurity policy
- Little or no crew cyber awareness
- Unsupported/obsolete operating systems, ***even in new-build ships***
- Many unpatched systems
- Many systems without anti-virus software or updated anti-virus definitions
- Dangerous crew modifications to IT networks and hardware configuration
- Removable media access on shipboard PCs
- No known cyber auditing occurring as a shipboard and safety management procedure
- Ethernet-connected Industrial Control Systems (ICSs)
- Critical systems connected to the internet without protections or segregation

The Imperative for This Research

In the business of shipping, risk management practices, conventions, and standards are pervasive across nearly every aspect of maritime operations. These exist because of a documented history of hard lessons learned: incidents, casualties, fatalities and injuries, losses, and near misses. These are real events with real outcomes, requiring serious attention to revising or creating new operational best practices and policy.

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 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 conventions and 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 is verified through numerous types of periodic inspections by companies, port state, classification societies, P&I, and more. It wasn't until January 2016 that BIMCO released the international shipping industry's first *Guidelines on Cybersecurity Onboard Ships*.

Indeed, mariners are not trained to recognize active cybersecurity breaches to critical systems or identify the difference between intentional and unintentional interruptions. Software in critical equipment varies and none are known to exist that effectively actually alert the mariner of a cyber disruption. Mariners are trained to react to malfunctioning or inoperative systems by shifting to an alternate mode of operation, and 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 nonexistent in the maritime industry, with the exception of some highly specialized vessels. Moreover, and in the case of the widely-publicized Stuxnet virus, IT-dependent systems appeared to operate normally for a long period of time while the worm made its way through the systems before the disruption was obvious.

Some critical IT-dependent shipboard systems are mandated to be installed aboard vessels and operated by officers trained in their 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[2], particularly as a mandated system for carriage. Cyber disruptions to equipment essential for maintaining a proper lookout, navigation, and determining if risks of collision exist could certainly contribute to a transportation safety incident. ***Doubt*** as to one's navigation and collision avoidance situation requires that immediate action be taken in accordance with the COLREGS. [3]

The vulnerabilities associated with Automated Identification Systems (AIS) and Global Positioning Systems (GPS) are old news, and little, if any action, has been taken using traditional risk management approaches to mitigate them. Mariners are typically able to manage AIS and GPS issues with sound traditional navigational practices to ensure safe navigation. While much has been written about these two areas, there are a multitude of other vulnerabilities that pose a much more significant and persistent threat to industry.

Many ship systems are also able to connect to the Internet to perform a wide variety of functions, such as monitoring engine performance through Remote Access Monitoring

[2] On 1 September 2016, the new IMO Performance Standards for ECDIS will take effect. Astonishingly, the new standards did not include provisions for ECDIS hardware and software to demonstrate any level of cybersecurity or resilience.

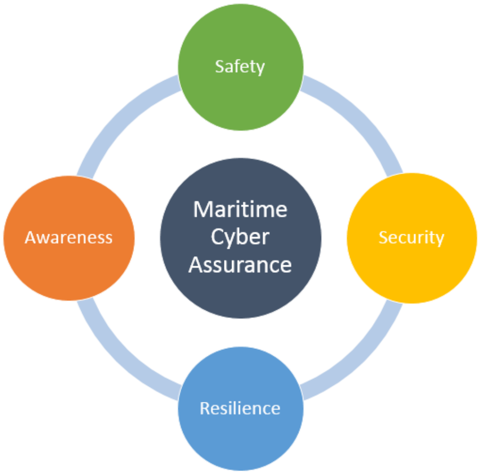
[3] COLREGS Rules 5 and 7.

(RAM), fuel consumption and efficiency, Dynamic Positioning (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 significant security considerations for all of the obvious reasons. In most cases, remotely accessible systems involve third parties to not only perform core functions of the service, but also maintain and update the software from remote locations. Additional security practices and procedures are required here as well.

Although shipping companies may possess widely divergent information assurance policies, there are no known global standards or IMO-mandated certifications for shipboard IT-based critical systems. There are also no mandated IT security audits, aside from those conducted in an ad hoc manner by some highly motivated companies. It wasn't until January of 2016 that the first industry guidelines were published for cyber safety, resilience, or security.[4] Additionally, there is little evidence of hardware and software manufacturers developing and implementing safety 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.

What We Have Found

With little validated evidence of maritime cyber disruptions available prior to our efforts, it was necessary to create an alternative plan to understanding cyber vulnerabilities through evidence-based research (Figures - 1 & 2, next page). Our research discoveries are comprised of cyber vulnerabilities across multiple ship types. The most prevalent of these vulnerabilities are categorized as unauthorized network access vulnerabilities and are the result of network configurations that lack segregation and allow for excessive transfer of risk between network nodes.



[4] In January 2016, BIMCO led the release of the industry's first guidelines, "Guidelines for Cybersecurity on Board Ships". In March 2016, ABS published its guidelines on cyber safety.

Figure-1

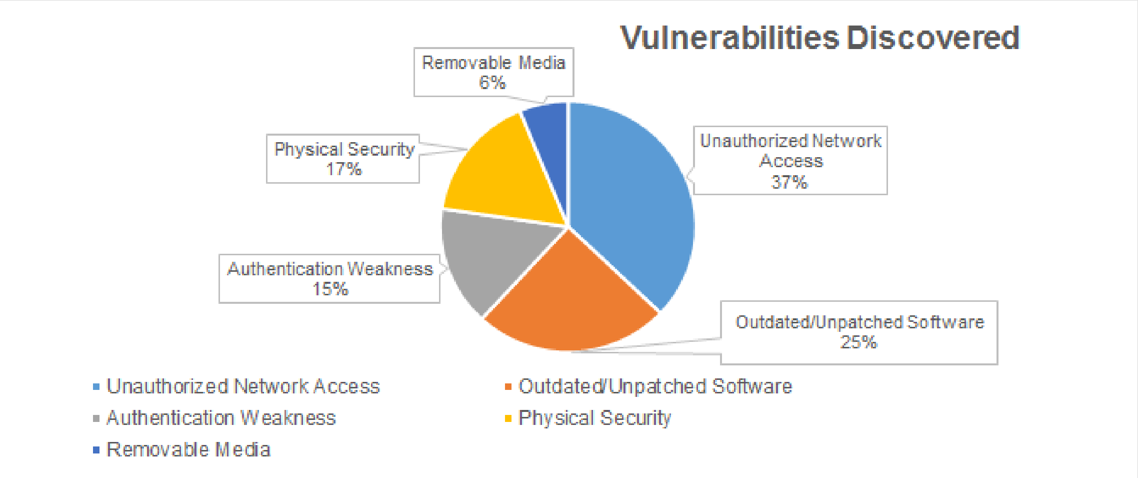
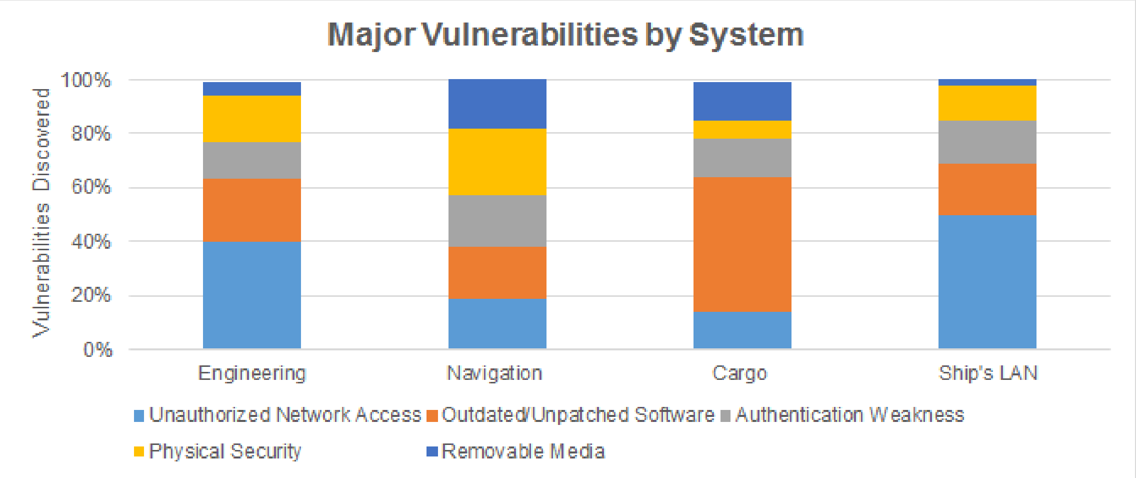


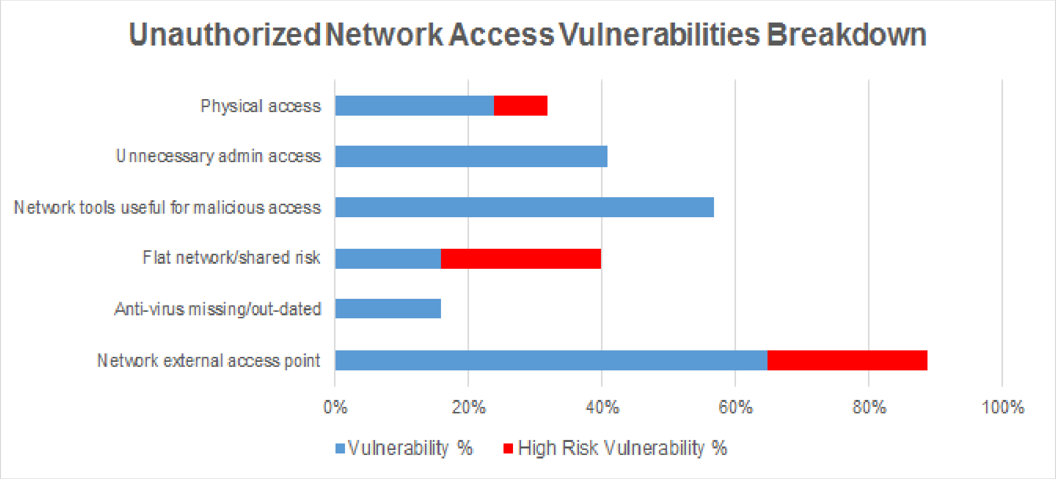
Figure - 2



The large scope of vulnerability discoveries related to unauthorized network (Figure - 3, next page) access required us to break down the types of accesses that were discovered and determine whether these vulnerabilities were assessed as high risk. Unsecured USB ports are an inherent design weakness across systems and all vessels assessed. They also presented the greatest vulnerability and opportunity for unauthorized network access.[5] This is especially true when coupled with nonexistent policies for handling of removable media and specific rules concerning which individuals were provided permissions to access shipboard network computers via removable media.

[5] Available and unsecured USB ports is highly common because security in marine system hardware is generally not by design.

Figure - 3



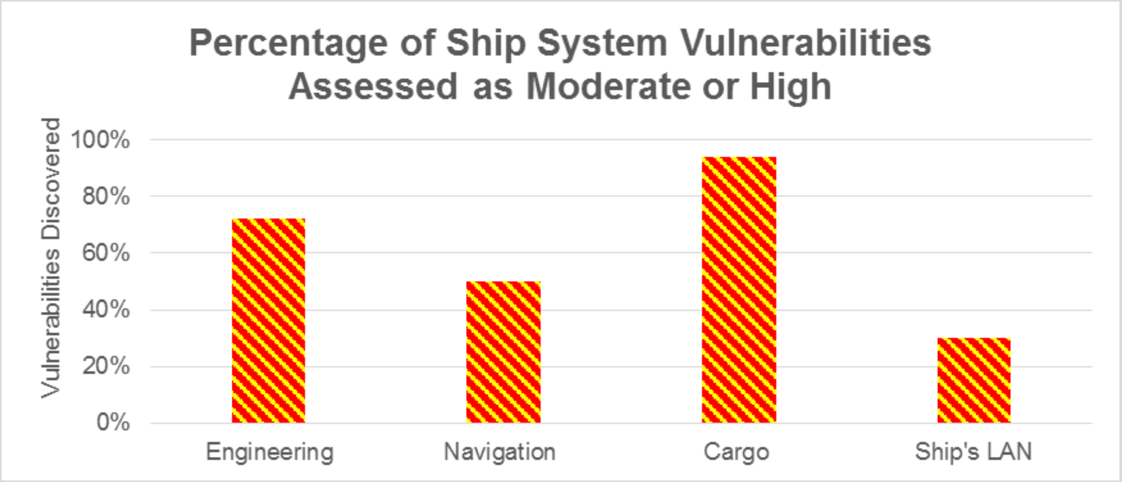
Operational Impact of Cyber Disruptions

The center of gravity of this research was not only to prove that cyber vulnerabilities exist aboard vessels and marine terminals, but also to translate the technical observations into potential or actual operational and business impacts. To close this gap, the MCAT devised a proprietary means of translating the technical observations to operational and business impacts and risk analyses. It's the only way to articulate an understandable risk message to mariners, management, ownership, and other stakeholders.

To conduct thorough risk analyses during the assessments, the MCAT developed a proprietary risk scoring system. Aspects of the National Institute of Standards and Technology (NIST) were incorporated in the risk model. While this is a highly objective scoring process, some aspects of subjectivity are also included. The cross-functional nature of the MCAT provides the experience and knowledge of maritime business and maritime operations with cyber, to a point where the discoveries can be discussed, assessed, and scored accurately.

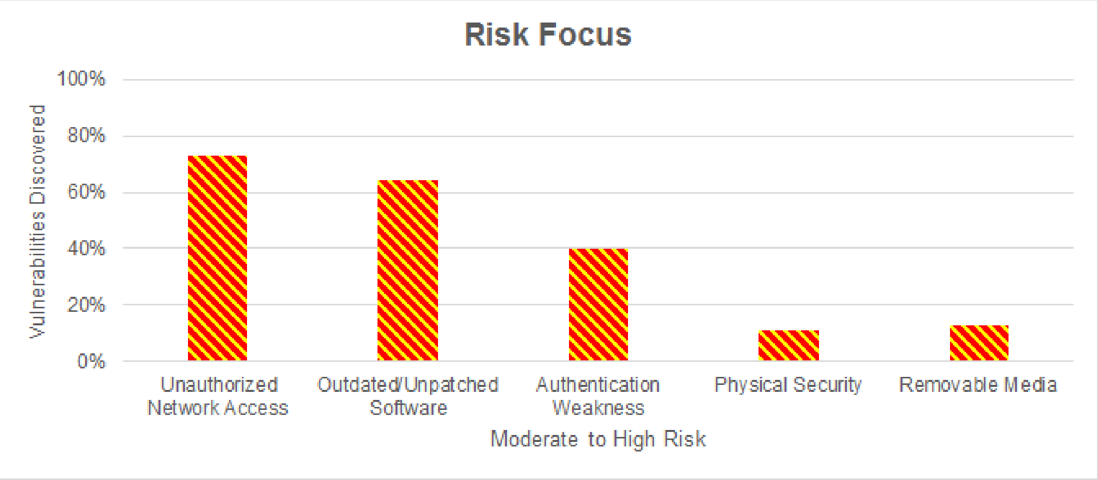
The most concerning takeaway is that engineering and cargo systems (Figure - 4, next page) were assessed to have more than 60% of the vulnerabilities identified to be of moderate to high risk, and would have serious to catastrophic adverse effects, not only the ship's operation, but also the shipping companies' operations.

Figure - 4



Unauthorized network access vulnerabilities and outdated and unpatched software created the highest levels of risk **<u>across all systems</u>** (Figure -5), due to the vulnerabilities they present to the operating capabilities through pervasive access and inability to protect against viruses and malware.

Figure - 5



Research Discovery Vignettes

The following sample vignettes are provided as proofs of concept derived from a number of key vulnerabilities discovered in our research across numerous vessels. Without *validated* evidence of a real cyber-attack in maritime operations, it is necessary to provide our partners and research sponsors with a plausible and convincing story from the vulnerabilities of highest severity.

Loss of Engineering Monitoring from the Bridge

In this example, the engine monitoring computer, located on the bridge, malfunctioned under load. The computer cabinets had to be opened and power manually removed to get the computer rebooted. It was an unsupported O/S on the bridge, with shared risk and vulnerability of a dual homed computer. This vulnerability decreased reliability of engineering system control from the bridge. This system is directly connected to the engineering control system and the effect of this computer malfunction on main control is unknown, but potentially catastrophic. Our team was able to demonstrate the ability to crash the O/S through manipulation of the touch screen for the bridge engineering control. This test also triggered numerous alarms and created a major distraction to the crew.

This issue was prevalent on the specialized vessels we assessed. The severity of this vulnerability discovery was ranked as “medium”, as the crew would shift control of the engines from the bridge to the Engine Control Room. However, it could be a potential distraction to a bridge team, especially in a restricted maneuvering or restricted visibility situation.

Cargo System Disruption

In this scenario, a vendor technician boards the vessel with a company laptop to perform software upgrades and testing of cargo management computers. Unbeknownst to the technician, this laptop is already infected with malware, and when it is connected to the ship’s network, the ship’s critical cargo management systems also become infected. The malware, known as ransomware, immediately locks the systems and encrypts all files. Once the systems are locked and the files are encrypted, the cargo loading system stops responding and begins to behave erratically, and finally shuts down completely.

The systems can only be unlocked after paying a ransom to an unknown hacker, or by hiring experienced (and expensive) computer security consultants to regain access to the systems. The cargo loading system remains offline until the computer security consultants arrive and spend several days reloading the system. The delay also caused days of backups throughout the cargo supply chain, causing dissatisfaction amongst customers and suppliers and financial losses that adversely affects business.

This issue was unique to cargo ships with quality control parameters set in the cargo management systems we assessed. The severity of this vulnerability was high due to the impact it had on the quality assurance limits of the cargo onboard.

Widespread Exploitation of Critical Data and Systems

Flat network infrastructure leads to widely shared risk across all operations. Malware spreads faster and has more effect when there are no network segregation boundaries or security barriers. This consists of hardware, such as switches, routers, wireless access points, and wiring typical of Small Office-Home Office use. Combine this with varying degrees of cyber awareness and compliance by the crew, access to an entire ship's network and data is possible.

Crew ad-hoc network - there was significant evidence of multiple IP networks on the ship's LAN. No network or baseline documentation exists to justify existence of these multiple networks.

This issue was prevalent on all vessels assessed. The severity of this vulnerability discovery was moderate as accidental or unintentional release of business sensitive, private, or personal data across the network. Though there was no direct operational impact, the business impact could be significant.

Conclusion

The USMRC Maritime Cyber Assurance^{SM} research program went from concept to fully operational in less than six months and launched an evidence-based research framework for the industry six months prior to the U.S. Coast Guard's release of its Cyber Strategy. This was made possible by the effective presentation of the facts to key industry principals, such as BIMCO and the Liberian Registry, and their ardent and committed support of USMRC's research.

Yet, as the industry continues to experience additional business downturns, including the greatest depressed freight rates and overcapacity in the bulk and container sectors seen in decades, the incentive by industry principals to invest in maritime cybersecurity is also at risk. In our opinion, it is absolutely necessary for shipowners, ship management, and class societies to fully commit to ongoing and evolving cybersecurity research. Every industry sector in the world has felt the brunt of cyber-attacks and disruptions. The financial, technology, and healthcare sectors have experienced at least fifteen years of cyber lessons learned, many of which apply to maritime and offer a glimpse of that potential magnitude of consequences to both business and operations.

Further, technology vendors and "control system vendors don't see a business opportunity in improving the cybersecurity of their products if it's not a selling proposition."[6] This must change, because no action is inexcusable. Regardless of industry downturns and economic difficulties, industry leadership must see that it keeps its own house clean regarding cyber. In this case, ignoring or deferring action on cyber risk and the specter of disruption is wrong and very dangerous.

Before procuring new optimization and remote access monitoring technologies, industry must exercise the due diligence and prioritize security. Blindly assuming the vendor will provide secure and resilient technologies to be outfitted aboard ships and in marine terminals is no longer acceptable. The industry should prioritize maritime cybersecurity in a call to action as follows:

- Invest in a cyber research assessment now. The cost of doing nothing and experiencing a cyber disruption could be far higher than taking proactive measures.
- Take responsibility for your vessels' IT and cybersecurity. Physically survey your vessels' IT networks; understand and document.
- Have an independent cyber research assessment conducted, by experienced cyber operations professionals who understand maritime and can clearly translate highly technical vulnerabilities into operational impacts for the Master and the CEO. USMRC has pioneered a program that is well-tested and recognized at the highest levels of international shipping.
- Take the initiative and amend your Safety Management System with initial cybersecurity policy for your operations. Basing this on your cyber research assessment is even better, as it will be evidence-based. Don't wait.
- Train and educate everyone, not just the mariners. This is from the CEO level to the deck plates, no exceptions.

The burden of cybersecurity 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 education and training, and maintained through routine – and secure – methods of upgrades and updates as supported by vessel operators and owners. This can only be accomplished by effecting positive change on industry operations and culture, from the executive level to the deck plates.

[6] "Bound to Fail: Why Cybersecurity Risk Cannot Be Simply Managed Away", Ralph Langner and Perry Pederson, Cybersecurity Series, Brookings Institute and Foreign Policy, February 2013.

Authors

Captain Alexander N. Soukhanov

Vice President, International Shipping and Maritime Operations, USMRC

John Bos

President, Cybrex LLC

David P. Polatty IV

Senior Associate for Strategic Development, USMRC

Terence M. Nicholas

Program Manager, USMRC

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 proven risk mitigation methodologies center on proactive and comprehensive approaches from practitioners' perspectives.

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 cybersecurity 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, cybersecurity and maritime operations.