As readers of this journal know, technology and innovation are everywhere in the marine industry, and are key drivers in making global supply chains more efficient, safe, secure and sustainable.

Cybersecurity has sometimes taken a backseat to all of this innovation. In 2012, when I first began looking into cybersecurity issues related to the maritime industry, it was a challenge to convince some companies that cybersecurity was even a concern. While most maritime companies were taking responsible measures, a significant portion believed that they were not targeted by cyber attackers, or that their proprietary, air gapped or simply out of date systems somehow made them immune.

The industry’s recognition of cybersecurity is now much more widespread, and for good reason, as cybercrime continues to grow. For example, Juniper Research estimates that the cost of data breaches will reach $2.1 trillion globally by 2019. Well-publicized cyberattacks have impacted every industry imaginable, including the maritime sector. Last year the notPetya incident impacted container terminals around the world, causing significant shipping delays and an estimated $300 million in costs.

In the face of these threats, industry groups, classification societies, private firms, and organizations including the U.S. Coast Guard, The Institution of Engineering and Technology, and the International Maritime Organization have developed cybersecurity guidance and products for the maritime industry. Smart companies are requiring evidence that contractors and business partners abide by appropriate cybersecurity standards before connecting to the network.

While these efforts are encouraging, no one should believe that these emerging standards and best practices are comprehensive, or that abiding by them will provide complete protection against cyber threats. Indeed, a recurring refrain is that organizations must be resilient, and develop strong cyber response and recovery plans.

The maritime sector has many attributes that make it vulnerable to cyberattack. Consider that the marine industry:

- is mobile, necessitating wireless connections,
- is global, bringing in international players and transactions,
- is high volume, meaning that even where profit margins are small, financial transactions are large, creating incentives for cybercriminals,
- requires and provides connections to global customers, contractors, government agencies, and other players in the supply chain,
- faces cost-control and customer service pressure to add new technologies quickly, often in advance of prudent risk analysis and configuration management practices,
- uses Operational Technology (OT) for industrial control activity, information technology (IT) for business operations, and the Internet of Things (IoT).

IoT represents a qualitative and quantitative growth in how the industry uses cyber technology. IoT devices are used for information sharing (routers, modems), decision making, and industrial processes. They are quite literally integrated everywhere from the propeller shaft to the stack emissions. Ships and port facilities are moving to an operating environment rich with sensors, controllers, in-house analysis and complex communication nodes. These devices improve safety and efficiency.
Properly employed, the “big data” generated by these systems combined with artificial intelligence create value for companies and enables a more flexible and customer focused supply chain. Emerging “Smart Ship” technology uses onboard analysis, real-time collection, transmission, and analysis to improve safety and efficiency, and meet customers’ needs. INMARSAT estimates that smart ships will generate up to 60 GB of data per day, and process much of that data onboard (via “fog” computing) to optimize autonomy.

The downside is that every new connected device, be it a small sensor or a sophisticated industrial control system, creates some level of cyber risk. Given the ease at which individual devices can be added, few organizations are even fully aware of what IoT systems they employ, much less how well they are protected. The Internet Security Threat Report for 2017, published by Symantec, notes a 600% increase in IoT attacks from 2016 to 2017.

One might wonder why cyber crooks are targeting IoT devices. While a terrorist might try and disable a security camera or hazardous gas sensor, there are also more routine reasons why hackers attack IoT devices.

First, it is important to understand that some of these devices do not have a simple method for updating firmware, or the memory or processing power to host security features. In other words, many are inherently insecure. As such, they provide a gateway to more valuable assets of a computer network. Also, hackers can use compromised IoT devices to launch distributed denial of service attacks, or exploit them for crypto-currency mining.

Regardless of why or how, IoT security breaches can lead to the same consequences as other systems: fraud, theft of intellectual property or privacy data, business interruption, liability and reputation impacts. For some IoT devices, compromise could lead to significant safety, security, or environmental consequences. Terrorists and criminals may even target IoT devices as part of a combined cyber-physical attack to disable critical infrastructure or disrupt trade.

**BLOCKCHAIN**

IoT devices are perhaps the most tangible systems in the cyber world. That is not the case with another mover and shaker, the blockchain. Typically described as a “shared ledger”, blockchain technology underlies bitcoin and other crypto currencies – an abstract concept if ever there was one.

Blockchain technology works by creating an online record of transactions that are jointly shared and verified. Unlike other aspects of cyber technology, blockchain is designed to promote security, albeit in a very different way from, say, firewalls. Criminal ingenuity being what it is, I’m sure there are ways of manipulating blockchain for ill intent, and some studies have shown vulnerabilities in blockchain enabled smart contract applications. Nonetheless, blockchain is well suited to information sharing among networks and supply chain partners, and is arguably much more secure than many other options.

IBM and Maersk have formed a company to use a blockchain to help share information between shippers, ports, customs offices, and others in trade. Dupont, General Motors, Toyota, Walmart, and other major shippers are also getting in the act. Blockchain will improve transparency and help these organizations to streamline and authenticate record keeping, whether it is for the movement of cargo, or the associated financial and administrative transactions. Note that blockchain can be used with IoT – for example an IoT device senses stack emissions and sends the data to a blockchain.

The tangible world of IoT and the abstract field of blockchain both represent opportunities for the marine industry. These technologies are changing the way companies operate, connect with customers, and create value. They promote agility, proficiency, and efficiency.

These benefits are at risk if we don’t address the corresponding cybersecurity concerns. We are now giving cyber technologies primary control over processes that control huge financial transactions, day to day operations, and even the safety of human lives. Cybersecurity is not a technical responsibility of the IT department, it is a risk management and governance responsibility at the highest level of an organization. It should come as no surprise that the U.S. Securities and Exchange Commission recently updated its guidance concerning the disclosure of cybersecurity risks to investors.

New cyber technologies represent both risks and rewards for the marine industry. Organizations must train, empower, and instill a sense of responsibility in the people who operate, monitor, and rely on these systems. It is people who will decide whether to delete a suspicious e-mail, report suspicious activity, or incorporate a cybersecurity provision into a routine maintenance contract. For all of its technical complexity, cybersecurity is ultimately about people.

---

**CYBER THREATS AND DEFENSES**

The volume and sophistication of cyber attacks continues to grow, with crypto-coin mining and ransomware being especially prevalent in the last year. In addition to financially motivated exploits, industrial, energy, and transportation sectors can expect intelligence gathering exploits that lay the groundwork for future disruptions. The presence of such intruders in an infected system is difficult to detect. Despite the much-publicized Advanced Persistent Threats, most attackers use simple tools to exploit known vulnerabilities, simply seeking those systems without the right patches. Keep your systems updated, use complex passwords and double-factor authentication, and train your employees to not click on suspicious links or e-mail attachments, and to be alert for phishing and spear phishing attacks.

---

**ABOUT THE AUTHOR**

Captain Andrew Tucci is an officer in the U.S. Coast Guard. He is retiring this summer after 28 years of service as the Sector Commander and Captain of the Port in New Haven, Connecticut where he was responsible for all Coast Guard operations in Connecticut, Long Island, and the surrounding waters. In his previous tour at Coast Guard Headquarters in Washington DC he developed national policy related to port and facility safety and security, and was one of several key authors of the Coast Guard Cyber Strategy.

**ABOUT THE ORGANIZATION**

The United States Coast Guard is a branch of the U.S. Armed Forces and is responsible for maritime safety, security, and environmental stewardship in U.S. ports and waterways. The Coast Guard is also a first responder and humanitarian service that provides aid to people in distress or impacted by natural and man-made disasters at sea or ashore. The Coast Guard is a member of the Intelligence Community, and is a law enforcement and regulatory agency with broad legal authorities associated with maritime transportation, hazardous materials shipping, bridge administration, oil spill response, piloting, and vessel construction and operation.

---

**ENQUIRIES**

Email: Andrew.E.Tucci42@gmail.com

---


**https://www.sec.gov/spotlight/cybersecurity**