NO SAFE HARBORS

January 2018

Charting a smarter course for the maritime industry with Cyber Risk Management

By:
Mark R. DuPont
Executive Director of the National Maritime Law Enforcement Academy
President of Merrick Maritime Security

Chris Coyle
Managing Director, Business Development Services
CBC Group

No Safe Harbors

CHARTING A SMARTER COURSE FOR THE MARITIME INDUSTRY WITH CYBER RISK MANAGEMENT

INTRODUCTION

Last year saw an unprecedented, tectonic shift in our increasingly cyber-dependent world. Especially in the maritime domain. This is best illustrated in Royal Caribbean's plan to make a big bet on technology – and how they are "connecting" to their passengers with unique digital offerings. (You can read that article here: https://finance.yahoo.com/news/royal-caribbeans-big-bet-tech-170804676.html.)

At the same time, we are seeing an increase in risks. From the major hacks including Equifax and the attack on Maersk that cost them as much as $300 million[1], the risks associated with cyber threats have only escalated. With virtually every device including printers, cameras, mobile phones and the expanding world of IP connected devices and systems (e.g. the Internet of Things/"IoT"), the openings for cyber-attack are increasing. Especially in the maritime domain, as outlined in the April 2017 Article "Industrial Internet of Things use cases: The IIoT at Sea.[2]" From route optimization, to asset tracking, to equipment monitoring and crew member wellbeing… the maritime industry is "connecting." And by default, the threat surface, the risk landscape, is increasing exponentially with each "connection."

Can we be "secure?"

In the cruise line industry, the lynchpin of the cruising value proposition is personal security. That became very clear after 9/11 when you see U.S. Coast Guard boats and local law enforcement agencies escorting ships in and out of ports. It became clear when there were threats of a virus on board ships. Now we have something that we really haven't seen before, an existential threat that has emerged so quickly at the same time that technology and the cruise industry itself is expanding faster than any other segment of the

[1] https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html
[2] https://www.ibm.com/blogs/internet-of-things/the-iiot-at-sea/

economy. In an industry that is evolving and innovating to attract the next generation of customers, entertainment is at the core, as evidenced in the Royal Caribbean investment in technology[3]. This requires (and the customers expect) 24x7 connectivity for all devices to the web. Couple this with the fact that the maritime shipping industry as a whole, including port authorities and the ships themselves, are increasingly connecting for things like route planning, cargo operations, human resource management, equipment monitoring and for crew comfort. You begin to see how exponentially fast this digital surface is growing. And like the cruise ship passenger on deck 5, the industry itself expects that flow of information as quickly as you can ask Google or Siri where the closest Starbucks is.

If the security in place last year did not stop the attacks, will it stop them this year?

Can organizations truly build a defensive shield big enough and strong enough to ensure protection? The quick answer is "no." You will never stop the attacks, and if you focus on putting up a good wall or guards at the barbed wire fence, someone will always be working on a plan to get around all that. If your cybersecurity plan is solely focused on the defenses you put up, someone will get by the gate keepers. So, what do you do? Especially when you consider we are all suffering some degree of "cyber fatigue."

> **"We do have to worry about the same thing that a lot of the industry is worrying about and corporations, and that is the – you know, the cyber fatigue is starting to set in. You know, sort of across our – across our nation and in boardrooms and others, this sense of it just keeps coming, this sense of victimization and helplessness that's out there, and not really knowing exactly what to do. So we kind of have to guard against that[4]." – Vice Admiral Jan Tighe, Deputy Chief of Naval Operations for Information Warfare/Director of Naval Intelligence, and former commander, U.S. Fleet Cyber Command.**

The Merriam-Webster dictionary defines "security" as "the quality or state of being secure: such as freedom from danger (safety), freedom from fear or anxiety, or something that secures (protects)." With ever-active and more sophisticated cyber threats emerging, the phrase "cybersecurity" can be interpreted as a misleading oxymoron. Why? As soon as one believes their organization is in a "state of being secure" a new cyber threat emerges. ***Organizational leaders can't really have "freedom from fear or anxiety," if they rely on the traditional defensive oriented cybersecurity posture.***

There is a way to defend your company, your assets, and your customers by taking a slightly different offensive approach, and a way to ease that cyber-fatigue.

"The best defense is a good offense."

To coin an old adage that has been used in many sports discussions and is also known as a principal of war, "The best defense is a good offense." Today's cyber threats require organizations to go on the offensive; to become proactive, addressing what we call - The Four "Ps" of Public Safety and Port

[3] https://finance.yahoo.com/news/royal-caribbeans-big-bet-tech-170804676.html
[4] https://www.csis.org/analysis/cyber-warfare-maritime-domain

Security; People, Platforms, Processes and Performance. This is a higher-level strategy that goes beyond and above the traditional cybersecurity tool box.

According to a recent article summarizing cybersecurity, ***What is Cyber Security? How to Build a Cyber Security Strategy***[5], the author describes cybersecurity as "the practice of ensuring the integrity, confidentiality and availability (ICA) of information". In addition to the expected IT availability expectations, this means having the ever-ready capabilities to defend against and recover from cyber-attacks by adversaries, including business continuity and disaster recovery.

The article goes on to zero in on the key issue facing us in 2018; "A good cybersecurity strategy needs to go beyond these basics, though. Sophisticated hackers can circumvent most defenses, and the attack surface — the number of ways or "vectors" an attacker can gain entry to a system — is expanding…Similarly, the trends toward cloud computing, bring your own device (BYOD) policies in the workplace, and the burgeoning internet of things (IoT) create new challenges."

Cyber threats can be generally classified as;

- ✓ Gaining access to confidential information for some type of political or financial objective.
- ✓ Sabotage, which is focused on corrupting, damaging, or destroying information and/or systems. These cyber-attacks seek to undermine integrity and trust of you and your company.

DISTRIBUTED DENIAL OF SERVICE (DDS) ASRE NOT YOUR TYPICAL RANSOMWARE ATTACK. THESE ARE CAREFULLY PLANNED WHOLESALE ATTACK THREATS THAT CAN SHUT DOWN SERVICES AND SYSTEMS FROM NORMAL CUSTOMER USE.

- ✓ Denial-of-service, which attack your availability and are often associated with Ransomware which encrypt the target's data while demanding ransom to free it.
- ✓ Distributed denial-of-service (DDoS) attacks which use 3rd party devices to

[5] https://www.csoonline.com/article/3242690/data-protection/what-is-cyber-security-how-to-build-a-cyber-security-strategy.html

flood systems making them unavailable for the intended users.

- ✓ And what is emerging in 2018 is a whole new level of cyber threat including "Advanced Persistent Threats" or "APTs." These threats slowly and carefully test cybersecurity defenses, often seeking to access and observe an organization's cybersecurity tools and procedures well before executing the cyber "kill chain." Increasingly, these APTs utilize artificial intelligence ("AI") to automate and accelerate the cyber-attack sequences from spying and testing defenses to distributing malicious code elements over time and erasing digital fingerprints. This means your organization could be in the process of being violated and attacked, you just do not know yet - who, how, when or where.

Today, given those cyber threats, it is time to change the game to an active approach. Going on the offensive means becoming proactive, with a more comprehensive battle plan. It is time to change to **Cyber Risk Management**.

Addressing Legacy Operational Models

Today's organizational and operational models - how your company or organization is run - are usually based on a combination of the company's objectives, the market demands and its internal operational capabilities. The "4 Ps" offer a useful way to consider the current state of your organization's cybersecurity posture (and many other things for that matter,) and how you can move to a cyber risk management approach.

People:

In any business, regardless of size or industry, people are our biggest asset…and our biggest vulnerability. As many a manager, leader or owner can attest, the People part of a business occupies the bulk of their activities and operations. What we called the old 80-20 rule: 80% of your time is taken up by 20% of your people. And, as outlined in our White Paper ***Navigating the Changing Seascape of Maritime Public Safety***[6], the changing dynamics of the workforce are magnifying the concerns and challenges. The Boomers are retiring at the rate of 10,000 per day (institutional knowledge going out the

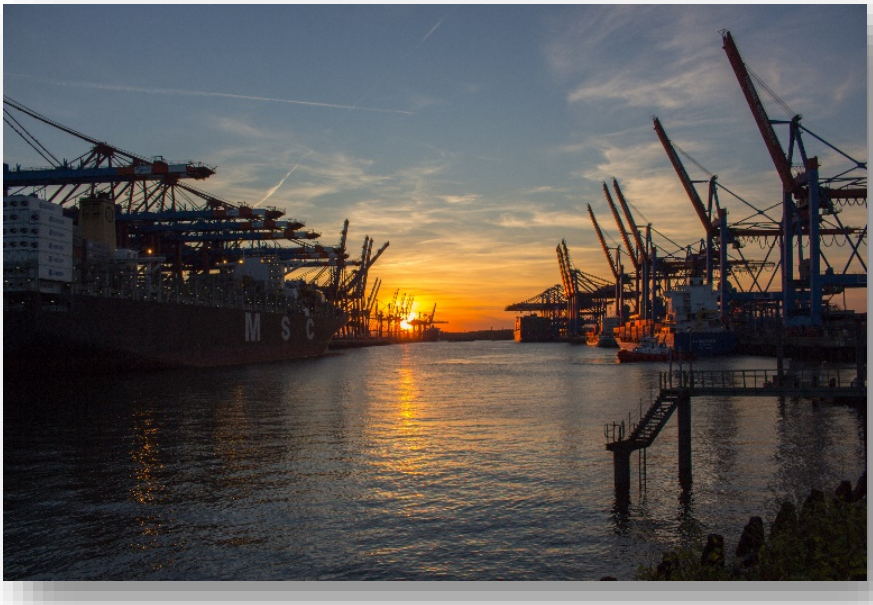
[6] https://docs.wixstatic.com/ugd/7c4db2_cab29f1b559e4166b15a8ae6900dab20.pdf

door with them), and Millennials occupy more than 40% of the personnel pool. (This shift, and loss of skill sets, is why outsourcing specific functions is coming back in vogue.)

People challenges become increasingly overwhelming when you consider the fact that 78% of people claim to be aware of the risks of unknown links in emails. And yet they click anyway. This was reported in two studies conducted by Dr. Zinaida Benenson about mock phishing attacks at Friedrich-Alexander University (FAU) of Erlangen-Nuremberg, Germany.[7]

Let's look at how the People part of the 4 P's and its relevance to evaluating your current Cybersecurity Strategy.

Organization: What does your org chart look like, especially as it relates to cybersecurity? Who in your organization is responsible for cyber risk? This means more than simply having current positions assigned to cybersecurity related tasks such as IT and security personnel. By the way, if you've placed the responsibility of your cybersecurity on the desk of either of these individuals or departments, you've already lost the battle. Cybersecurity should be a "whole of company" approach… especially when we talk about the importance of the People part of the puzzle.



Who will ultimately be held accountable in the face of a cyber-attack that jeopardizes the company's brand of trust? For example, many organizations have created a best practice of separating the role and functions of Chief Information Security Officer (CISO) from the role of the Chief Information Officer (CIO). Other organizations now have regular oversight briefings, such as regular board of directors or chief executive officer reviews, such as the state of Arizona whose Governor is briefed monthly on the cyber risk status of all agencies.

Expertise: As the scale, scope and sophistication of the cyber threat advances, do you have the people with the skill sets and experience to keep up? If you think you do, there are several important considerations.

- First, how will you keep them up to date with the new skills and tools required by a far more challenging cyber threat environment? And, with the expansion of your retail point of sale

[7] https://blog.barkly.com/cyber-security-statistics-2017

footprint, web, mobile networks and applications, do you have enough of the right people to keep up with the expanding threat surface?

- How deep is your "bench" and how will you keep your **best cybersecurity personnel** in the face of the exploding private sector job market for cybersecurity professionals? Many organizations find it hard to retain talented individuals whose skills can command significant compensation in the new world of escalating cybersecurity threats.

- How will you keep your cyber expertise up to date, and in the event of turnover, what is in place to ensure your **institutional cyber knowledge** base does not walk out the door?

- In the event of a cyber-attack, who comprises your **"Crisis Response Team"**? Do they have the availability without compromising their day-to-day responsibilities, and do they have the skills and experience to handle the potential size and scope of the impact to your organization?

Platforms:

Another critical part of the 4 P's are Platforms – what piece of equipment or tools will you use to execute the mission. And in this discussion, platforms mean the physical, virtual, internal and external resources that are available for addressing the cybersecurity risks.

IT infrastructure: IT infrastructure refers to all the IT components; desktops, laptops, tablets, mobile phones, routers, printers, retail networks, consumer facing websites, applications, etc. (everything with an IP address). Often called the "Threat Surface", how is yours changing and what is your strategy for scaling up your cyber strategies and resources in a cost-effective manner?

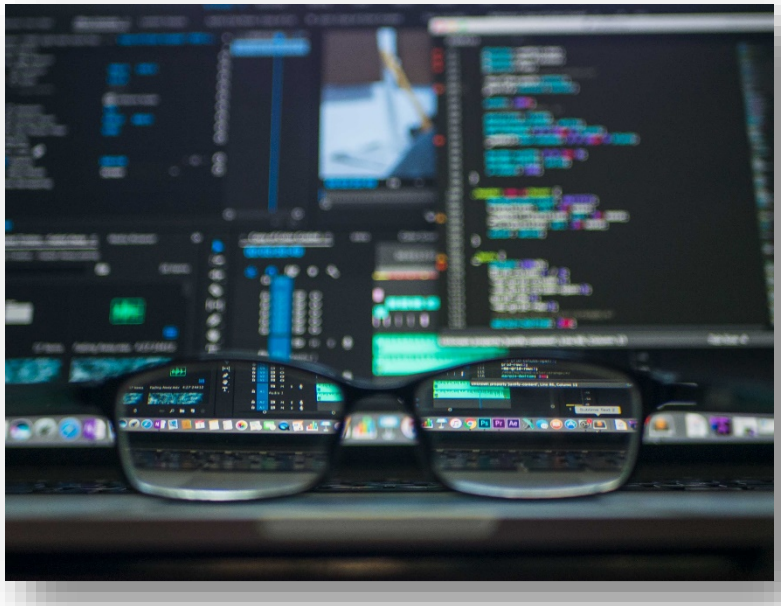
If your organization is managing an expanding universe of IT assets, with the usual scanner technology (e.g., Qualys, Rapid7, Tenable Network Security, IBM, HP, Intel Security) what level does this go to (Web Apps, Databases, Operating System, etc.?). How do you know it is fully comprehensive and complete? What is the coverage area for your vulnerability scans (i.e. sampling, 100% coverage, etc.)?

External Resources: Does your organization or another agency conduct external threat analysis? If so, how up to date is it (e.g. do they subscribe to commercial threat feeds such as iSIGHT, Verisign iDefense, CrowdStrike, etc.). If not, what is the extent of your exposure to increased risks?

Process:

While most organizations can check off the basic lists of cybersecurity readiness, in terms of basic tools and customary personnel, the processes for evaluating and prioritizing all your risks across all your IT assets is often an important area for improvements in efficiency and effectiveness. Which threats are the most serious and what criteria is used to make those judgments? Is your criteria "threat-centric" or "business criticality" based?

For example, some notable national organizations who infamously made national news for epic breaches were aware of their vulnerabilities, but lacking a "Threat-centric" approach to managing cyber risk, put a low priority on remediating those vulnerabilities.



Other critical process related considerations include how are cyber risk issues escalated and how your vulnerability remediation is prioritized? How does your organization categorize or prioritize remediation actions (e.g., by the database of Common Vulnerabilities Exposures (CVE), business criticality, or risk), and how do you handle remediation "ticket management" (e.g. Excel spreadsheets, email, or is it automated)? Are you able to track the outcome of an action that the Security Operations team initiated or the status of an action plan?

Performance:

How your organization performs in terms of managing cybersecurity risk is the ultimate consideration. While performance is often dependent upon and a by-product of your People, Platforms and Processes, the standard of performance you deem applicable is often the single most critical management decision. If your benchmark is past performance, is that really a viable standard for a far more challenging and threatening cyber risk environment? In some case, industry standards or regulatory mandates may be driving your current cybersecurity strategy; but is that the level of performance your specific organization should plan for?

Is the frequency and scope of your cyber risk monitoring keeping pace with the threat trends, and how many open vulnerabilities do you have and what is the aging trend?

Going on the offensive in 2018

When maritime organizations (and any business) carefully consider their current cybersecurity posture across these "4Ps", it is likely they will conclude a more proactive approach is required. Maritime customers, from the boardroom to the cruising enthusiast, from ship captains to port managers, all expect the highest level of integrity across the entire operational enterprise, including the emerging universe of web apps, 3rd party devices and BYOD. A compromise to any element of the delivery chain in any country in the world may result in national media attention and a challenge to the confidence of your customers and impact your brand dramatically.

It's about Situational Awareness

According to the US Department of Homeland Security, "Situational Awareness" is a human experience[8] defined as:

- *Knowing and understanding what is happening around you*
- *Predicting how it will change with time*
- *Being unified with the dynamics of your environment*

TODAY, THERE ARE NO "SAFE HARBORS" WHEN IT COMES TO DEFENSIVE MARITIME CYBERSECURITY METHODOLOGIES. IT'S TIME TO CHANGE COURSE, WITH A MORE COMPREHENSIVE AND INTEGRATED APPROACH. IT'S TIME TO NAVIGATE THROUGH THE STORM WITH A PROACTIVE CYBER RISK MANAGEMENT SOLUTION. IT'S TIME FOR **RISKSENSE**

These are important concepts for understanding which solutions and/or technologies are required to achieve desired results. Situational awareness and its dynamic nature are "new knowledge" as well as "spatial knowledge." Ever-changing circumstances mean a constantly evolving situation or event. Having the ability to understand the severity of those circumstances in advance of or during an emergency can mean the difference between safety and breach.

The ability to predict and/or model and [most importantly] visualize how the circumstances of a pending or evolving emergency may change over specific time(s), allows emergency-managers to allocate resources to priority areas before further damage or loss of life/livelihood occurs.

[8] https://www.esri.com/library/whitepapers/pdfs/situational-awareness.pdf

IN CONCLUSION

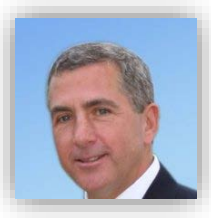
In 2018, your organization can move to a proactive and predictive posture with a Cyber Risk Management strategy. And we can help. From providing a "bench" of cybersecurity experts that are recognized internationally for their knowledge and skills[9] as an extension of your staff, to a Risk Management platform that can give you the "Situational Analysis and Awareness" that you need in today's rapidly expanding and complex environment, we can provide you the same resources that the Department of Defense, NASA, and other federal agencies use and trust, RiskSense[10].

A simple next step is to initiate an objective, expert review of your current cyber risk management posture. For no-cost, a Cyber Risk Management Questionnaire and a Self-Assessment Session with leading, national Cyber Risk Management experts can begin to shape your future and provide navigational guidance in today's challenging seas. Contact us today at cyber@nmlea.org or cbcg@risksense.com.

ABOUT THE AUTHORS

Mark DuPont is the Executive Director of the National Maritime Law Enforcement Academy (NMLEA), and provides expert consultation, assessments, intelligence, predictive analysis, training, exercises and evaluation for the port security, maritime law enforcement and emergency responder community. With over 35 years of organizational and entrepreneurial leadership, as a maritime law enforcement/military/port security specialist, he provides a unique blend of federal, state, local, private, and non-profit sector perspective and knowledge.

As a Master Trainer, facilitator, and instructional designer, DuPont contributes to the enhancement of the response, prevention and protection capabilities of maritime public safety professionals throughout the world, having developed and implemented a national standard of training and certification recognized by all 50 United States and six territories, and the United States Coast Guard. Mark's positions and achievements as the Chief Intelligence Office for the State of Florida's FWC (the largest conservation law enforcement agency in the world), and as a Homeland Security and Intelligence Officer for the United States Coast Guard, give him a wealth of experience to share.



Chris Coyle is the Managing Director of Business Development Services for Creative Business Collaborative Group (CBC Group), a women-owned, business development consultancy based in Connecticut. Chris leads a team spread across multiple time zones, who collaborate seamlessly to assist a diverse array of businesses and organizations, both large and small, with mission critical solutions tailored to the needs and strategic objectives of the organizations.

From global brands to local non-profits, Chris's proven experience and success has been applied in varied business sectors including defense, education, IT solutions, non-profit, publishing, retail, telecom, healthcare, aerospace, medical device, automotive and heavy industry markets. From business development to legal affairs, from channel partner management to strategic account oversight, Chris has provided a breath of services that have helped domestic and international clients achieve higher levels of organizational success.

---

[9] http://risksense.com/news/awards/

[10] As part of a think tank that advised the U.S. Department of Defense and U.S. Intelligence Community, RiskSense developed Computational Analysis of Cyber Terrorism Against the U.S. (CACTUS), Support Vectors Intrusion Detection, Behavior Risk Analysis of Vicious Executables (BRAVE), and the Strike Team Program.