CYBER SECURITY – UNDERSTANDING RISK SIMPLY

ABS

CYBER SECURITY – UNDERSTANDING RISK SIMPLY

INDUSTRY AWAKENING TO CYBER SECURITY

Inviting a cyber incident takes no more than a flash drive plugged into a ship system USB port, or a phishing e-mail containing a malicious link – unfortunately clicked on a company laptop. Once inside one computer, the demon can spread to any other it contacts. In 2017, a malicious update to a popular Ukrainian accounting program released ransomware, which ultimately ended up inside several global organizations including shipping giant Maersk, where it caused some $300 million worth of trouble and interfered with operations in several of the world's major ports.

While the maritime industry has been slow to acknowledge cyber security as a relevant issue, a growing number of companies are now working on addressing cyber risks. Historically, ships and offshore units were remote from a company's main information technology (IT) systems. Clearly, now they are increasingly connected – to maintain ship functions (propulsion, thrusting, ballast), which rely on industrial control systems; provide internet access to crew; or stream data ashore to monitor vessel health.

Over the past two years, ABS invested significant resources to close a critical gap in cyber security capabilities for the maritime industry. ABS has developed an industry-leading capability that empowers owners and operators to *identify and measure* cyber risk in their Operational Technology (OT) environments.

A PRACTICAL APPROACH

Until now descriptions of cyber security risk, and resulting management plans, were anecdotal and largely an educated guess made by vessel OT environment managers – which characterized risk based on abstract concepts – perceived threats and vulnerabilities. Fundamentally, we were using educated guesses as the foundation for maritime OT risk assessment.

A new, *practical and quantifiable* model to define maritime OT risk analysis was badly needed. ABS began this effort as basic research with the US Department of Homeland Security, the US Coast Guard, and the Stevens Institute of Technology. ABS' work with clients demonstrated that available guidance for developing the required Cyber Security Risk Management Plan was insufficient (C2M2 CERT-RMM[1] specifically calls for implementation actions based on a detailed Risk Management Plan).

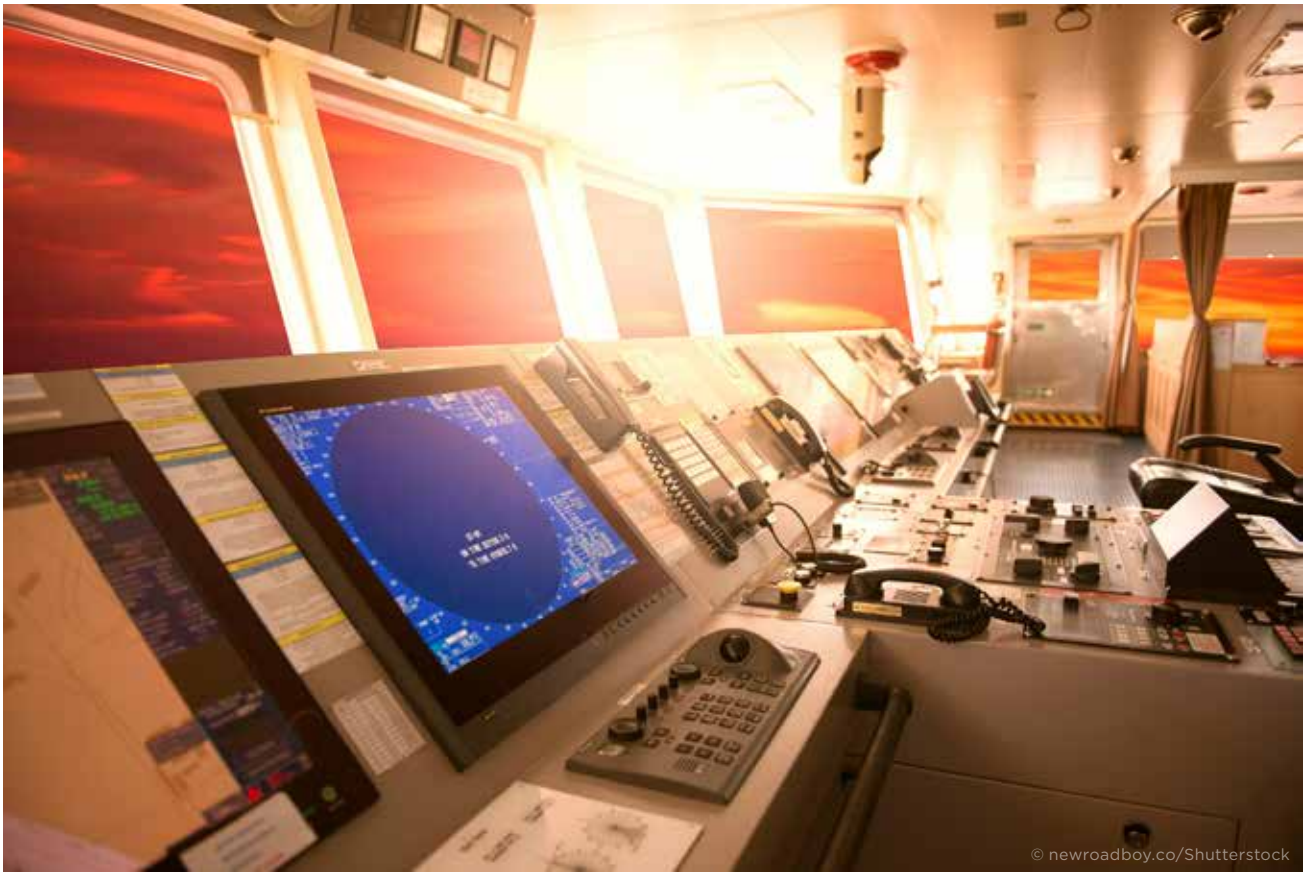
Following on from the joint research effort, ABS applied research and development resulted in methods and tools that describe cyber risk on vessels as readily observable and quantifiable cyber risk constructs. In contrast to commonly used risk elements in the cyber security risk equation defined by the FBI **Risk = Consequence x Vulnerability x Threat**[2], ABS defined OT risk elements to reflect countable maritime OT realities: Functions, Connections, and Identities respectively.

ABS FCI CYBER RISK MODEL

The FCI Cyber Risk™ model is simple in its structure, but sophisticated in its application. The FCI Model "transforms" the abstract constructs of the commonly used risk equation into physical constructs that are observable and countable in a vessel OT system. The revised equation for maritime is, **Risk = Functions x Connections x Identities**.

Using the ABS FCI Cyber Risk equation, we can calculate a cyber risk index for clients that is actionable and easily understood by senior management and "C-Level" executives. From the risk index, an actionable report details how to reduce cyber risk enabling owners and operators to prioritize OT cyber security design and investments across their assets.

1: C2M2: US-DHS Cybersecurity Capability Maturity Model; CERT: Computer Emergency Readiness Team; RMM: Resilience Management Model
2: This model is often referred to as the "FBI Risk Equation"



First, consider *Functions* of an OT system, which represent Consequences in the original equation. Failure of critical *Functions*, like navigation, steering, or engine management controls, has serious consequences. Solutions to reduce risk for vessel *Functions* are basically constrained to network architecture management activities, such as distributing critical functions to segmented and protected networks, which reduces risk that a single cyber incident could impact several critical *Functions* simultaneously.

Second, consider *Connections* to potential cyber threats which represent Vulnerabilities. Digital Connections are the pathways to critical functions that must be operational, and therefore protected from a cyber incident. The gateways to connections are network nodes. Logically controlling access to critical Functions through digital *Connection* nodes, reduces risk.

In the end, what are we protecting Functions from? In the common risk equation, Functions must be protected from Threats. The concept of "Threat" is widely assumed to be malware, software viruses, ransom-ware, and the like. A "Threat" has an agenda that may, or may not, be malicious. Most importantly, a Threat has an *Identity* that is either known or unknown. "Threats" are merely methods by which *Identities* impose a Threat. Untrusted *Identities* introduce threats into connection nodes that can, or are intended to, impair critical Functions.

Controlling access to important *Functions*, through vulnerable *Connection* nodes, by untrusted *Identities* capable of delivering an infinite number of potential threats, reduces or eliminates Cyber Risk. So there it is – cyber security in a nutshell. Once described in these terms, cyber security becomes simple to understand; and just detailed and tedious to define and design. By applying the FCI Risk constructs to an OT system, risk elements can be observed, defined, counted, and reduced or eliminated within the risk tolerance limits of the concerned organization. All risk management requirements imposed by international cyber security guidance standards and regulations can be prioritized and clearly explained in real risk elements using ABS the FCI Cyber Risk model. Finally, with the results of the FCI Cyber Risk process, clients can apply a cost-effective risk mitigation strategy across their assets and fleets.

CONTACT INFORMATION

North America Region
16855 Northchase Drive
Houston, Texas 77060
United States

South America Region
Rua Sao Bento, 29 - 11° floor, Centro
Rio de Janeiro 20090-010 Brazil

Europe and Africa Region
ABS House, No. 1 Frying Pan Alley
London E1 7HR United Kingdom

Middle East Region
Al Joud Center, 1st floor, Suite # 111,
Sheikh Zayed Road
P.O. Box 24860, Dubai
United Arab Emirates

Greater China Region
5th Floor, Silver Tower
No. 85 Taoyuan Road, Huangpu District
Shanghai 200021 P.R. China

North Pacific Region
11th Floor, Kyobo Life Insurance Bldg.
7, Chungjang-daero, Jung-Gu
Busan 48939, Korea, Republic of

South Pacific Region
438 Alexandra Road
#08-00 Alexandra Point
Singapore 119958

ABS