MARITIME SECURITY

The Past – For centuries maritime transportation interests have addressed the risks posed to their crew, property and cargo. The threats included piracy, smuggling, crime, specifically cargo theft and pilferage, and stowaways.

The Present -- All the threats of the past remain with us today though they have in some cases adapted to the modern environment, for example drug smuggling and human trafficking. In the case of piracy, there are significant changes to the way in which piracy is being conducted. Namely there is a shift from opportunistic smaller efforts, which of course still exist, to sophisticated piracy businesses with networked finance connections, sophisticated technical skills, modern weaponry, and near endless supply of human resources. There have been however significant 'game-changers' which have made the present maritime security environment differ from years past. The events surrounding 9/11 including specifically the USS Cole have shown us that the threats have changed or evolved. We now fully understand that the vessel, its crew, and its cargo may be employed as a weapon, may itself be a target, or may be used to introduce threats in its ports of call. We understand that the messaging of terrorists can be delivered through a variety of means which include loss of life, disruption of infrastructure and services, environmental impact, and industry reputational threats.

Responses to these threats by national governments have included preventative measures like regulatory solutions (ISPS), transparency requirements and schemes, and enforcement. The degree to which implementation of these measures is robust is quite variable therefore for example, the US Coast Guard is taking their programs beyond our borders to areas of high risk internationally to prevent these problems from arriving on our doorstep. Ports and facilities have been encouraged to collaborate and share information through the ACMS forums but competitive and economic issues serve to limit the effectiveness of their participation.

The Near Future – The maritime security issues on the horizon are many. While piracy in North Africa is beginning to show the effect of national efforts undertaken to combat it, other spots like Nigeria, and traditional areas like the Malacca Straits are surging forward. Enforcement of security regulations has been steady in particular regions but nearly non-existent in others. Vessels, terminals and facilities have essentially set security standards at the compliance level with a few notable exceptions.

Before treating the pressing issues of today and the future, specifically maritime cyber security and Ebola, it is interesting to look at the business environment in which our clients find themselves. That environment can be captured by the phrase 'Risk Management'.

The business, whether public or private, has an aim and obligation to protect the value of the business. This means that maritime security is another realm for the C-Suite to consider with regard to risk; identification, mitigation, transfer and insurance of risk. For those risks that we understand and are well defined risk management is a discipline. But when new undefined risks appear on the horizon, the job is not so easy. Two immediate threats we face now illustrate this point clearly, namely maritime cyber security threats and spread of disease (Ebola).

We need go no further than the last week's news report to see what the Ebola virus scare did to the operations of a cruise ship headed to Belize. It doesn't take much imagination to see what the situation could have become had the subject patient in fact been infected and perhaps

been contagious prior to isolation. Ebola is serving as an example of security threat which can impact the health and safety of the vessel and port operations—for which the companies, ports and indeed governments are largely unprepared. Planning, equipment, training, exercises and continuous measurable improvement is urgently called for. Economic interests are of course tied to the enormous potential for human impact.

But what about the threat we cannot easily see?

MARITIME CYBER SECURITY

The Problem - Gone are the days when the physical security described in the ISPS Code provided vessel operators with guidance for adequate protection needed to ensure safe transit of crews, cargo, and vessels. With today's sophisticated automation and communications capabilities, introduced to meet both regulatory and commercial requirements, new cyber-based risks have been introduced that vessel owners must now address.

The expanded utilization and connectivity of Supervisory Control and Data Acquisition (SCADA) equipment on vessel networks has replaced physically independent systems and while these newer systems are highly integrated and remotely accessible they have outpaced the security controls needed to secure vessels from cyber-attack. As it is, automated maritime systems are typically not managed to IT best practices. Instead, they are relegated to the traditional physical security practices stipulated by the ISPS and ISM regulations and have not yet adapted to address emergent cyber threats. In short, cyber risks exist with Internet access point, every email opened, every attachment downloaded, every file exchanged on a flash drive, every un-patched software application, and every time a third party contractor accesses to your company's network.

Cyber threat actors, regardless of their political or ideological motivations, no longer require physical access to vessels or facilities in order to commit harm, to steal information for criminal purposes or perhaps worse. In today's hyper-connected world, vessels are hack able from anywhere.

The Vulnerability – While maritime trade connotes the streamlined movement of cargoes and mariners across oceans, cyber risks, such as malware, DDoS attacks, and botnets can be easily and unknowingly introduced at any point in the ecosystem. As a result, maritime companies are acutely vulnerable to cyber risk. Organizational and network vulnerabilities can be easily exploited by hackers intent on disrupting shipboard systems such as navigational and operational systems, Global Positioning Satellites (GPS), marine Automatic Identification System (AIS), and the Electronic Chart Display and Information System (ECDIS). The Security Association for the Maritime Industry (SAMI) is constantly monitoring potential security threats and recently reported[1] that of the world's top 20 container carriers, 16 were found to have serious security gaps. Moreover, cybersecurity capability 'maturity' on vessels and at ports is 10 to 20 years behind typical office-based network environments. Lloyd's Register (LR) further discovered that cyber threats can extend beyond software, impacting non-related operational issues, such as misuse of systems which contain software critical to vessel safety.

What's at Risk? - Unlike office network environments, compromised SCADA devices or an ECDIS system can result in environmental damage, property losses and/or physical injury, or in the worst cases death. Negative impacts to policy, compliance and finances may also trigger class action lawsuits. Specifically, networked navigational and loading management systems, which represent vulnerable, high impact points of compromise, are prime targets for terrorists. Vessels, representing the most expensive asset in most maritime companies, are particularly vulnerable to cyber threats since operators regularly access the vessel's network and related management information systems from remote sites. While such access introduces cyber risk to the vessel, it represents operational risk to the business.

Crews and cargos are also increasingly at risk of piracy and theft because of the escalating and expanding nature of cyber threats. Poorly protected access endpoints, including human input devices, become virtual gateways, exposing SCADA devices and networks to probing cyber threats.

FAST FACTS

- ISM and ISPS compliance do not equate to security, the focus is physical rather than cyber security
- ICS-CERT received and responded to 257 incidents as voluntarily reported by asset owners and industry partners. In 2013, attacks against the Energy sector represented over 56 percent of all incidents reported to ICS-CERT[2].
- The scope of incidents encompassed a vast range of threats and observed methods for attempting to gain access to both business and control systems infrastructure, including:
  - Unauthorized access and exploitation of Internet-facing ICS/SCADA devices
  - Malware infections within air-gapped control system networks (impacting operations)
  - SQL Injection and application vulnerability exploitation
  - Lateral movement between network zones
  - Targeted spear phishing campaigns
  - Watering hole attacks (one of which utilized a zero-day vulnerability)

HIGH-IMPACT ACTIONS

- Instill a culture of cybersecurity awareness
- Champion all cyber-security activities from the top
- Develop common risk language
- Update operating policies and procedures
- Build awareness through audits and feedback

CONTACT US

HudsonTrident MCS
2 Aquarium Drive, Suite 300
Camden, NJ 08103 USA

+1 856 342 7500
info@hudsontrident.com

The Solution – We best serve our clients, whether as legal counsel or risk management consultants, by bringing the best cybersecurity expertise and solutions to the table, helping them to solve their cybersecurity challenges, facilitating understanding of how to protect critical systems and confidential data, and to implementing a sustainable cybersecurity program.