Maritime Security: IMO Secretary General and the MSC Prioritise Cyber Security

At the MSC's 95th meeting in early June 2015, IMO Secretary General Koji Sekimizu opened with an address that elevated cyber ahead of all the other security risks facing the industry[1]. When you consider that the headline grabbing issues of migration, ecology, safety and piracy have been seemingly ever-present in the national media throughout recent years, it is interesting and encouraging to the security professional to note that the MSC placed cyber 4th on the meeting's agenda and made a distinct statement by having a separate discussion on piracy[2].

Historical Underexposure

Piracy has long been in the limelight because of the scale, the violence involved, its links to international terrorism and its accessibility to mass media. Then there's the matter of the multi-state-sponsored physical response to piracy in the form of the naval task forces with embedded journalists. By comparison, cybercrime has no public face, operates under a cloak of mystery and attacks do not result in images of casualties being broadcast on 24-hour news.

It's not just media underexposure that has kept maritime cyber security in the shadows - actual events are very hard to come by. Taking capability and intent into consideration, why would a pirate resort to technical methods of attack when only a few colleagues, a small vessel and some firearms are required for a small operation?

Why Now?

A small but growing body of academics[3][4] and professional commentators[5][6][7] are at pains to point out that maritime cyber security is an underdeveloped area that, if not coherently addressed, will likely result in a significant failure of critical infrastructure or loss of life in the near future as over 50% of European goods are transported by maritime carriers[8]. The exact figure was up 4% from the previous decade and is projected to grow. The operation of digital navigation systems and other radio communication equipment at sea and in port are vulnerable.

Evidenced Weaknesses

Demonstrations by interested security parties have been successful in evidencing that a ship can be remotely operated by injecting radio signals into a GPS antenna, spoofing an Automatic Identification System to mimic the movements of other vessels in the area or forecast weather conditions that would likely make a ship change its course, penetrating 74% of the largest container carrying company websites to highlight security flaws and penetrating maritime satellite communications using Inmarsat and Iridium SATCOM terminals to expose critical security issues.

In 2014, NCC Group published its findings on the vulnerabilities of a commercially available ECDIS used by ships to navigate in place of hard copy charts[9].

NCC Group noted that it is common for ECDIS to be connected to a ship's internal network as well as the Internet, thus providing a greater attack surface. The paper pointed out that some manufacturers of ECDIS devices advise operators to maintain an Internet link so that the latest charts and data can be immediately available.

[1] IMO (2015). Address of the Secretary-General at the Opening of the 95th Session of the MSC.
[2] IMO (2014). Provisional Agenda for the 95th Session of the MSC.
[3] Lancaster University (2014). The Future of Maritime Cyber Security.
[4] Security Association for the Maritime Industry (2014). Seaworthiness & Cyber Security: The Hidden Threat to Shipping.
[5] Gooding, N (2015). Maritime Cyber Attack: A Clear and Present Danger.
[6] IBM (2014). Implications and Threats of Cyber Security for Ports.
[7] Marsh & McLennan Companies (2014). The Risk of Cyber-Attack to the Maritime Sector.
[8] ENISA (2011). Analysis of Cyber Security in the Maritime Sector.
[9] NCC Group (2014). Preparing for Cyber Battleships: Electronic Chart Display and Information System Security.

Also in 2014, Cyberkeel and ClearSky compiled a paper detailing their evaluation of the risks to maritime cyber, identifying 3 reasons why cyber security is not as advanced in the maritime industry as it is in other sectors: it is viewed as a technical matter customarily delegated to the IT Manager or the CIO, a lack of awareness of actual occurrences exists and there is a wide-held belief that the threat is theoretical (there are insufficient suitably equipped and motivated threat sources) [10].

Current Methods of Actual Attack

The Cyberkeel and ClearSky paper detailed some of the attacks to date such as barcode scanners being used as hacking devices, deleting carrier location information, gaining backdoor access to steal information, the amendment of cargo details with the aim of transporting illicit goods undetected and GPS jamming.

The Regulatory Situation

There are no maritime cyber regulations or industry-sponsored best practices in circulation, resulting in a culture of companies failing to report incidents for fear of reputational damage[11]. A best practice is being developed by a body of companies[12] but this measure was only just announced on 15 April 2015[13].

There is presently no IEC standard for the safe implementation of digital navigation systems or radio communications systems, although IEC TC80 is in development and due to be published in early 2016.

MSC 95 Outcomes

The MSC urged member states and international organizations to collaborate on proposals for guidance on maritime cyber security and submit them to the next session in 2016[14], as its own Round Table Working Group continues to make progress on regulatory and best practice proposals on: cyber awareness and education, developing a risk-based framework, protecting business critical assets, establishing information system policies, integrating holistic security and business continuity, identifying third-party relationships that could compromise cyber security, monitoring systems and network management, developing contingency plans and continuous review and assessment of cyber systems for robustness[15].

Filling the Gap in Security

Although it could be up to another year before the MSC and IEC announce their respective security solutions, companies can take action now. Regency IT Consulting offers strategy, design, delivery, assurance and audit of the technical, procedural and physical aspects of security. The Managed Services include a Secure Data Centre, Managed Encryption, SCADA security and Credential Management as a Service.

Our security consultants are all senior people with long track records of delivering security services within the public and private sectors. All have gained their experience either within Central Government where they held roles either within CESG (the UK National Technical Authority for Information Assurance), the military, as IT Security Officers for Government Departments or with blue chip suppliers providing secure IT systems to Central Government and the MoD. All are security cleared to the highest UK Government levels and where necessary are members of the CESG Listed Advisor Scheme (CLAS). The majority of our security consultants are ISO/IEC 27001:2013 Lead Auditors.

In August 2010, Regency IT Consulting was acquired by Airbus Defence & Space to further strengthen their presence in the UK Information Assurance and Cyber Security market. Airbus Defence & Space is a world-leader in global security solutions and systems, providing lead system integration and value-added products and services to civil and military customers around the globe including naval, land and joint systems, cyber security, secure communications, test systems, services, support solutions and intelligence and surveillance.

What Next?

Visit www.regencyitc.co.uk to see what we have already done for others and can offer you, or call 01242 225699 to speak to a member of the team.

[10] Cyberkeel (2014). Maritime Cyber-Risks.
[11] Panda Security (2015). Operation Oil Tanker: The Phantom Menace.
[12] Baltic and International Maritime Council (BIMCO) - an independent international shipping association; International Chamber of Shipping (ICS) - the principal international trade association for merchant ship owners and operator; INTERTANKO - an independent body that provides leadership to the tanker industry; INTERCARGO - a global cargo transporter; Cruise Lines International Association (CLIA) - North America's largest global cruise industry organisation; Comité International Radio-Maritime (CIRM) - the principal international association for marine electronics companies.
[13] BIMCO (2015). Round Table Press Release.
[14] Maritime Safety Committee (2015). 95th Session, 3-12 June 2015.
[15] IMO (2015). Measures to Enhance Maritime Security.