SEMAPHORE

Newsletter of the Maritime Law

Association of Australia and New Zealand

Cyber Marine Attacks: the New Shot Across the Bow?

Introduction

Cyber-attacks represent one of the most significant threats facing the marine and energy sectors. The increasing interconnectivity of devices and the growing reliance on technology brings with it increasing vulnerabilities. It is a not a new concept. However, the potential exposures have transcended far beyond the simple data loss scenarios that were initially contemplated. Catastrophic scenarios now envisioned include significant business interruption, total loss damage to property and even loss of life.

The Target

With over 90% of international trade and transport estimated to be based on maritime transport, the safety of shipping vessels, port operations, marine facilities and other elements of the maritime transportation system are critical to the global economy.

Industrial control systems (ICS), which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and programmable logic controllers (PLC), are almost universal in industrial and maritime operations.

Merchant ships rely upon hundreds of ICSs to manage propulsion, support navigation and communications, provide fire protection, operate safety systems, and manage cargo loading and discharge. ICSs are also found in support vessels and onshore, in container cranes, autonomous vehicles involved in loading operations, port security systems and automated cargo tracking systems.

With many of these systems being designed in the days before cyber security became an issue they are ideal targets for hackers.

The State of Play

It is increasingly likely that hackers will take advantage of cyber security exposures for malicious ends. In fact, there have already been a number of notable marine cyber-related incidents. To name a few:

- Somali pirates have been known to infiltrate digital shipping systems so as to identify ships carrying high value cargoes with minimal on-board security.
- In 2003, a denial of service attack froze a US port's web service.
- In 2011, hackers working with a drug smuggling gang infiltrated a computerised cargo tracking system at the Belgium Port of Antwerp in order to identify containers in which drugs had been hidden.
- In 2012, criminal syndicates penetrated cargo systems operated by Australian Customs, and the Chinese military was reported to have allegedly hacked a commercial ship on contract to the US military.
- In 2013, a major fuel supplier fell victim to an online bunkering scam.
- In 2014, a hacker caused a floating oil platform off the costs of Africa to tilt to one side, forcing a temporary shutdown, and a US port facility suffered a denial of service disruption that shut down multiple ship-to-shore cranes for several hours.

Further, researchers have identified significant holes in the three key technologies sailors use to navigate ships: GPS, the Automatic Identification System (AIS) and the Electronic Chart Display and Information System (ECDIS).

In 2013, researchers at the University of Texas demonstrated that it was possible to change a ship's direction by faking a GPS signal. Additionally, 'Trend Micro', an internet security firm, was able to use a $100 VHF radio to exploit a weakness in a ship's AIS. It was able to tamper with data, impersonate a port authority's communications with the ship, shut down all communications between ship and onshore stations and even create 'phantom' ships.

Developing Dangers — Groundings and 'iShips'

It is now not inconceivable that a cyber-attack could result in a ship's grounding. The Rena grounding in 2011 resulted in estimated losses totalling $1 billion and the salvage operation took several months. It isn't difficult to envisage the devastating economic impact that would be felt globally if a ship passing through the Panama Canal was attacked resulting in a blockage of the canal.

With ships getting bigger, crews are getting smaller, and companies are increasingly exploring the possibility of autonomous vessels, 'drone ships' or 'iShips'. For example:

- the European Union is currently funding a 3.5 million-euro study into drone ships;
- in early 2014, Rolls-Royce Holdings Plc released a virtual reality prototype of an unmanned cargo ship; and
- more recently, satellite communications group Inmarsat signed up to a research project, launched by Rolls-Royce, to provide expertise on how drone ships can be controlled from the shore, when they are not navigating themselves.

These unmanned ships will be remotely controlled and use dynamic positioning systems, with data collected from satellites, gyrocompasses and stabilizing sensors to hold position in rough seas. The susceptibility of unmanned ships to cyber-attacks is another risk that needs careful consideration.

The increasing number of potential loss scenarios poses significant opportunities as well as challenges for insurers and brokers in the energy and maritime sector. The cyber insurance market is forecast to grow to over $20 billion by 2020 and experts estimate that hacking attacks against the gas and oil industry alone will cost energy companies upwards of $2 billion by the year 2018. There is no shortage of risk that needs cover. However, the increase in business also gives rise to conceptually challenging risk scenarios involving multiple types of coverage and underwriting disciplines.

Identifying the proximate cause of a loss may be challenging. Often hackers will try to cover their tracks. A cyber-attack may not be readily apparent at the time of the loss and may only be discovered, if at all, after a long, expensive and comprehensive investigations.

Slipping Through the Gap

In the event of an incident, what policy will respond? Is the loss a product, professional, general or cyber liability? Typically, marine insurance policies exclude computer related liability and losses arising from computer and network security failure.

One such exclusion is the 'Institute Cyber Attack Exclusion Clause CL380' (CL380) which is well-established and widely adopted across marine and energy policies. Generally, CL380 operates to exclude cover for loss arising from a cyber-attack. The effect being that an insured is left uninsured for bodily injury, property damage and any associated business interruption stemming from cyber-related incidents.

Filling the Gap

Given that standalone cyber insurance policies typically exclude, or significantly limit, third party property damage and personal injury loss, up until recently, this left marine and energy companies significantly exposed.

The market has recently responded with a number of insurers offering 'cyber-gap' insurance aimed at covering situations that are excluded by reason of CL380 type exclusion clauses. One such policy acts to indemnify an insured in the event that indemnification under a normal property, business interruption, liability, terrorism, or package policy is denied solely due to the existence of a CL380 type exclusion.

Final Comment

Navigation systems are just one element of integrated and complex digital information processing systems. Whether manned or unmanned, land or sea based, whenever there are electronic components and computer systems, there is always a threat that the system can be the subject of a cyber-attack.

While insurance cover for cyber-attacks in the marine and energy sectors is an emerging risk market, there is no doubt that cyber-attacks continue to evolve at a rapid pace. It is the new shot across the bows that cannot be ignored.

Peter Craney
Lawyer, Kennedys

September 2016