Circular From LONDON

Date: 8 September 2016

Cyber Risk
- A new area of vulnerability for the maritime industry

The risk of cyber-attack is potentially the biggest threat to both Shipowners and their ships as the use of information technology spreads into all areas of the business. A Ponemon Institute Research Report in 2015 found that cyber losses increased by 14% over the year and against 39 benchmarked organizations calculated that the mean annualised cost for such organizations was £4.1m per year (ranging from £628,423 to £16m).

Financial and data risk

For shipping companies, this type of loss is currently faced by the "back office" part of the business - accounting, payments and banking. Financial data, crew information, and counterparty confidential material are all vulnerable to hacking, and there is increasing regulation in this area - principally by the EU which will require companies to take precautions and report loss of data. Good cyber hygiene, up-to-date firewalls, penetration testing and staff training are routinely deployed to counter this threat.

Even then, risk will continue to be presented by third parties, such as port agents, whose computer systems may be vulnerable to attack and whose staff receive little training. Several recent cases have shown how easily such systems can be hacked resulting in the use of spoof emails to divert payments to a fraudster's account. Basic precautions, such as making telephone calls to verify payment instructions go a long way towards preventing frauds of this nature.

Physical risk

Where the risk is less well understood is the physical risk to the ships themselves. We have found that this is particularly the case for traditional ship owning companies and their fleets. Although it might be said that the risk is currently low, cyber-attacks potentially pose a serious risk to the overall operability of a ship because of the increasing use of IT onboard, even where there is no single network controlling numerous systems and where internet connectivity is low. Examples of such technologies in common use are the Automated Identification System (AIS), Electronic Chart Display & Information System (ECDIS), Global Navigation Satellite System (GNSS) and E-Navigation Systems (E-Nav). Main and auxiliary propulsion systems rely increasingly on computers to operate efficiently.

Although cyber-attacks can occur deliberately, it seems that currently the risk is principally from inadvertent introduction of viruses and the like into key systems. For example, a crewman charging a mobile phone from a USB port in the ECDIS system caused a virus to render the system entirely inoperable. An expensive mistake. The ship's maintenance and propulsion systems are exposed to the same hacking/malware risks and the consequences of cyber-attacks might be potentially severe if key systems are lost at crucial times. All successful attacks incur significant expenditure to fix.

The number of cyber-attacks that have caused physical damage are still, thankfully, rare. There are a number of reasons for this but currently it seems to be the general invisibility of shipping to the general (hacking) public and the number of far easier targets for cyber criminals. But we have heard instances of pirates manipulating GPS data to lure ships off course; pirates hacking ship management systems to identify which ships are sailing without armed guards; and the hacking, by drug runners, of a terminal's container management system so they could monitor and control the movement of containers in which drugs were hidden to avoid detection.

As the "internet of things" is adopted by shipping such that ship's systems are centrally controlled, connectivity with the shore is continuous and maintenance and diagnostics increasingly done via USB ports in equipment, the risk will only increase. The rise in the amount of cyber-crime is, on any view, shocking and shipping will be targeted as other sectors improve their security. It is time therefore for shipping to consider these issues proactively.

The way forward

As with any operational issue, it is a matter of applying tried and trusted risk assessment methodology. Consider the risks, weigh the consequences and put proportionate steps in place to reduce that risk. The difference from the usual types of marine risk is that IT and cyber are outside most marine professionals' experience and so help has to be sought from experienced IT consultants. Training will be key as it is the ship's crew inadvertently introducing a virus into equipment or clicking on a bad link that is currently the highest risk. But if risk assessment is thorough, crew are trained and vigilant, and thought has been given to how to respond to an attack, then ships and shipping companies will be better protected when the cyber-criminals turn their attention to your company.

Source of Information: London P&I Club