Cyber security worries mount

Operators reveal real-world threats while trying to avoid placing reputations at risk

John Gallagher, senior Americas reporter

Maritime transport is moving swiftly from the theoretical to the practical when addressing the risk of cyber attacks, with threats rising across all shipping sectors.

The Baltic & International Maritime Council (BIMCO) – whose shipowner, operator, broker, and affiliated member companies represent about 60% of the world's merchant fleet – began scrutinising electronic threats to cargo vessels in 2013.

BIMCO stepped up that analysis further in 2015 to include a pilot project that gave maritime researchers access to some members' vessels to investigate such attacks. The council intends to use this information to help create the first informal guidelines on cyber security for shipowners and vessel operators; these will be sent to the International Martime Organization (IMO) in January 2016.

"Almost every industry has been responding to cyber attacks, usually because an incident has affected their business," BIMCO deputy secretary-general Lars Robert Pedersen told *IHS Fairplay*.

"What's really the case is that not much seems to have happened surrounding cyber issues and ships yet, so you could say we're at the forefront of the issue because we're proactively trying to prevent incidents in the first place.

"As ships become increasingly more computer controlled and an increasing number connect to shore, it will gradually make the industry more vulnerable. That's why we're responding now," he explained.

Developing guidance for commercial vessels on identifying cyber risks is one of the objectives of the US Coast Guard (USCG) maritime cyber strategy, unveiled in June.

Key points

- The maritime sector is preparing cyber-security guidelines based on real-world disruptions
- Pilot project gives maritime researchers access to some members' vessels

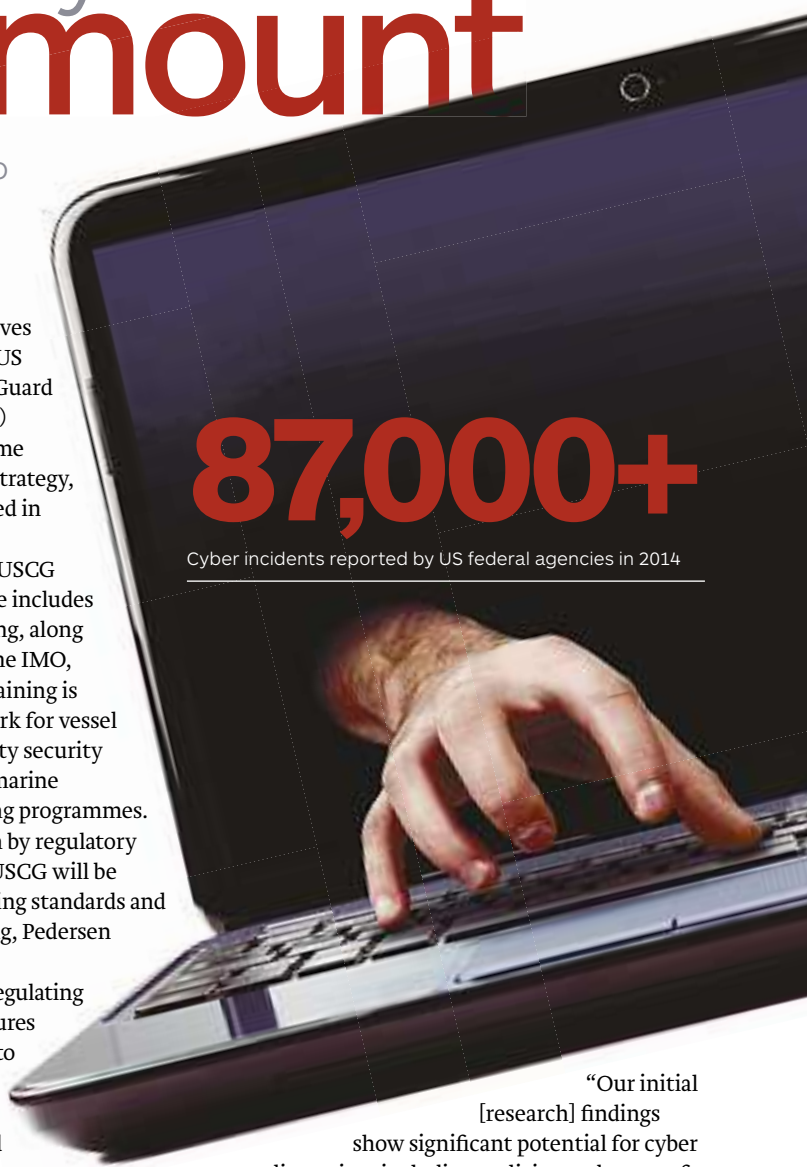
The USCG scheme includes ensuring, along with the IMO, that cyber-security training is included as course work for vessel and shore-based facility security officers at merchant marine academies and training programmes.

Increased attention by regulatory agencies such as the USCG will be invaluable in developing standards and guidelines for shipping, Pedersen pointed out.

At the same time, regulating cyber-security procedures "is a very tricky piece to embark on, because cyber is a very fast-moving issue, and we have a concern if countries want to regulate it due to the time it takes to develop them and then amend them if they become inadequate", he told *IHS Fairplay*.

For BIMCO, the key to remaining on the leading edge of real-world prevention will be its recently formed alliance with the US Maritime Resource Center (USMRC). It is a nonprofit research group based in Middletown, Rhode Island, seeking to advance navigation safety and mitigate risk.

The Liberian flag registry has joined with USMRC and BIMCO to use data gathered from shipboard operations to raise understanding of cyber-security risks.



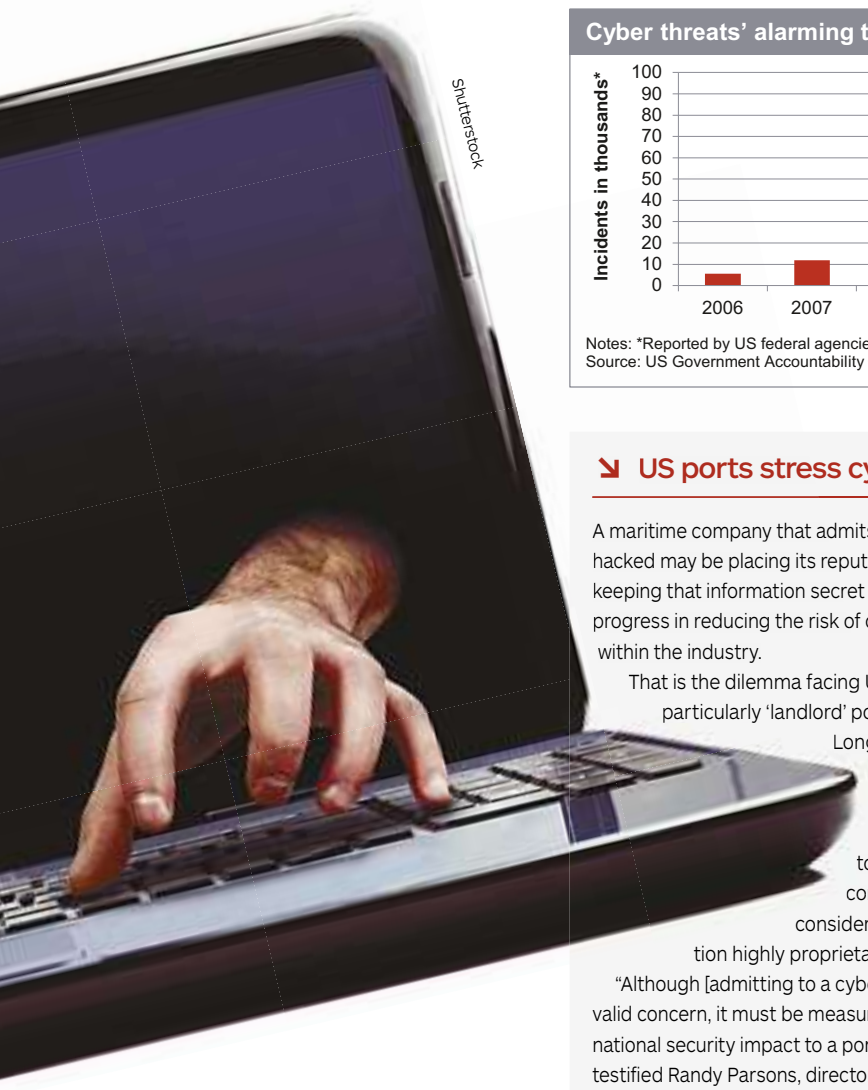
87,000+

Cyber incidents reported by US federal agencies in 2014

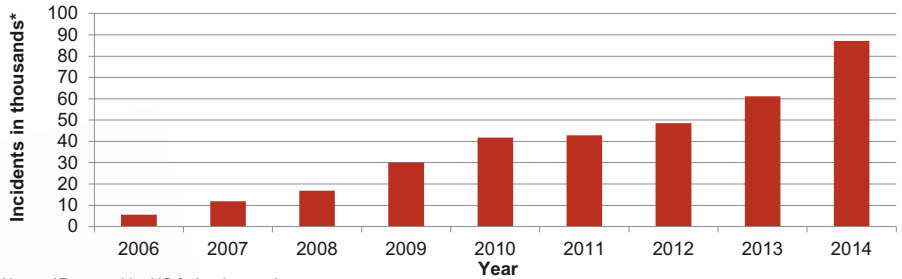
"Our initial [research] findings show significant potential for cyber disruption, including malicious takeover of engineering controls, widespread exposure of critical data and systems, and corrupted electronic navigation charts, to name a few," Alexander Soukhanov, a USMRC vice president, commented during BIMCO's annual conference in Hamburg in November.

USMRC investigated a recent cyber incident involving a critical piece of equipment on a large cargo carrier that delayed the vessel for several days in port.

Soukhanov declined to give out specifics about the incident but noted that "a shipowner can run the numbers to find out that this type of delay can be very expensive".


Shutterstock

Cyber threats' alarming trend



Notes: *Reported by US federal agencies
Source: US Government Accountability Office

US ports stress cyber data sharing

A maritime company that admits to being hacked may be placing its reputation at risk, but keeping that information secret could impede progress in reducing the risk of cyber attacks within the industry.

That is the dilemma facing US ports, particularly 'landlord' ports such as Long Beach in California, where terminal space is leased to private companies that consider such information highly proprietary.

"Although [admitting to a cyber attack] is a valid concern, it must be measured against the national security impact to a port complex," testified Randy Parsons, director of security at Port of Long Beach, during a hearing in October in Washington DC on port risks.

"Not sharing cyber-security information makes it difficult to identify the nature of threats or establish lessons learned and best practices to mitigate them," he warned.

Jonathan Sawicki, security officer at Port of Brownsville, Texas, noted at the hearing that his port oversees several private terminals, but "it's hard to get them in one room to discuss these issues because they all compete".

Gregory Wilshusen, representing a government oversight group, suggested that a "secure mechanism" should be set up so private terminals can provide sensitive cyber information to the government.

"There should be ways to make that information anonymous so that individual companies do not have to be identified," he said.

Soukhanov told *IHS Fairplay* that USMRC's shipboard research is revealing very little "security by design" in laptop software used by crews, which can make carriers vulnerable to cyber disruptions.

"With the advent of remote access monitoring and optimisation technology such as remote fuel efficiency monitoring, remote maintenance, and record-keeping, we're finding more internet connectivity," he said. "Optimisation is fine, but we're not really seeing security as a priority yet."

He added, "We're not interested in scaring the pants off the industry, what we want to do is protect reputations while raising awareness."

Pedersen emphasised that creating guidelines on cyber security "helps shipping companies avoid reputational risks, which can be quite damaging, [caused] by not being prepared".

A cyber attack could be even more damaging to a company's brand reputation on the passenger side of shipping, given the large number of people involved.

"The cruise industry is unique in that we have the same sort of commercial security interests that any resort or retail operator might have, with regards to personal information, financial data, credit card information, and things of that nature, but we also share the common interests of the rest of the maritime community when it comes to operational cyber security," Bud Darr, senior vice-president of technical and regulatory affairs for the Cruise Lines International Association (CLIA), told *IHS Fairplay* earlier this year.

In terms of operational risks to cruise ships, he cited concerns over "remote access to onboard computer systems that could potentially lead to vulnerabilities that need to be identified and protected against, affecting navigation systems, engineering systems and many other systems.

"When you look at the complexity of the systems and the scope and volume of data exchange, it tends to be on the high end for cruise ships relative to the rest of the maritime community," he added.

CLIA will join BIMCO, INTERTANKO, INTERCARGO, and other maritime groups in presenting guidelines on cyber-security management practices at the IMO's Maritime Safety Committee in spring 2016. F

john.gallagher@ihs.com