Nick Shaw Partner
njshaw@reedsmith.com
Christian Ayerst Associate
Reed Smith LLP, London

Image: Enrapture Media / Unsplash.com

The UK's Cyber Security Code of Practice for Ships

During London International Shipping Week 2017, the UK Government launched the 'Cyber Security Code of Practice for Ships' (the '2017 Code'). The 2017 Code presents a framework and a series of steps which it recommends those operating in the maritime industry take to make the industry more resistant to cyber attacks and more attuned to cyber security threats. Nick Shaw and Christian Ayerst, of Reed Smith, provide a breakdown of the 2017 Code and shed some light on the cyber security vulnerabilities unique to the shipping industry.

Key issues

Who does it apply to?
All those involved in protecting ships, persons, cargo, cargo transport units and ship stores against the risk of a security incident.

I'm not a UK national and I don't sail on a UK-flagged vessel. Should I care about the new code?
Yes! The 2017 Code certainly applies to UK registered ships and subjects. The 2017 Code also applies to (i) foreign subjects on UK ships; and (ii) foreign ships and subjects in UK waters.

Is the 2017 Code legally binding?
No - there is no defined penalty for non-compliance. However, failure to carry out the steps recommended may affect your insurance and may leave you exposed to allegations of unseaworthiness if a claim is made.

Does the 2017 Code sit comfortably with other legislation?
Yes. Its provisions are complementary to those of the International Convention for the Safety of Life at Sea, the International Safety Management Code, the International Ship and Port Facility Security Code ('ISPS Code') and other rules and regulations. The 2017 Code assumes the existence of several pre-existing actors in setting down its framework.

Why has the Code been introduced?

In 2014, the Government published the 'UK Cyber Crime Strategy,' which sought to place the UK at the forefront of the technological community, by promoting four key values:

1. Making the United Kingdom one of the most secure places in the world to do business;
2. Making the United Kingdom more resilient to cyber attacks and better placed to protect its interests;
3. Shaping an open, vibrant and stable cyber space; and
4. Developing the United Kingdom's security knowledge, skills and capabilities.

Shipping has traditionally been one of the slower industries to adapt to changes. This may be due to several factors, including the large amount of data transfer between various stakeholders (owners, charterers, managers, service providers, cargo interests etc.) in the cyber security chain; the use of different systems and platforms between those stakeholders; and the disparity between those using modern technology and those not using it at all.

The Code recognises that cyber attacks come in many guises, for example weapons of revenge for disgruntled employees, avenues for cash-hungry fraudsters to forge invoices and opportunities for smugglers to alter the cargo manifests to hide illicit goods being carried in a container. The shipping industry is slowly realising that its future lies in digitisation, network based systems and the automation of vessels and processes. If this rapid uptake in new and sophisticated technology is to continue, the expenditure in time and money needs to be matched in less visible but nonetheless critical cyber defences and training of those working in the industry.

As a response to the upturn in technology - and as a platform for British industry to show off its credentials as a sophisticated cyber nation - the Government has introduced the 2017 Code, reaffirming its commitment to the cyber revolution. It is not a prescriptive checklist which promises an attack

continued

free operation to those who comply with it. Rather, it sets out a series of best practice steps which those in the industry should take to minimise the risk of a cyber attack, mitigate the impact of an attack and maximise the effectiveness of the response, as well as demonstrate compliance at a national and international level.

What does the 2017 Code require me to do?

1. Carry out a 'cyber security assessment' ('CSA'). The International Ship and Port Facility Security ('ISPS') Code already requires that a ship security assessment be carried out to identify physical vulnerabilities to a vessel. From this, a ship security plan should be developed. The 2017 Code requires that - on top of these - a CSA be carried out. The aim of this is to 'adopt a risk-management approach to the threat posed by cyber security.'

   In layman's terms, this means a comprehensive review of the ship's and company's facilities and procedures, evaluation of the risks posed to these by cyber attacks, an analysis of what steps can be taken to reduce these risks and an evaluation of the 'residual risk' which - despite the steps taken - still remains. It is essential that an organisation identifies its most important cyber assets and allocates resources to protect these assets accordingly. This will vary from company to company and requires an objective evaluation of the risks posed to each company, from the generation of electronic documentation and manifests by an exporter of goods, to sensitive customer information held by a large container operator.

2. Use the CSA to draw up a 'cyber security plan' ('CSP'). This requirement aims to eliminate as many risks identified through a variety of measures, such as physical barriers to sensitive systems and data, initial and periodic screening of employees, training drills and education in cyber security. In addition, the CSP should record and monitor use of the computer and data systems, as well as a plan for the regular monitoring of hardware and software for viruses and malicious programmes.

   This is where the company should allocate resources to protect particular systems. It is important to also consider where information is stored, particularly where this information may be subject to other laws and regulations, such as employees' personal data which will be the subject of data protection regulations. The data that is most critical or sensitive to a company will likely need the most protection and monitoring.

3. Appoint a 'cyber security officer' ('CySO') who is responsible for all cyber security on the ship. They should liaise with the company security officer ('CSO') to develop, implement, monitor and regularly review the CSP. They should be conversant with any legal and/or regulatory change in the sphere of cyber security, and understand jurisdictional issues relevant to the policing of cyber crime. The 2017 Code does not set out who the CySO should be, but instead promotes competence based compliance with each step. They should therefore be conversant with the CSP, with the technologies used by the company and the ways that the different business units deploy that technology (and expose themselves to cyber risks). A CySO who has a limited appreciation of the CSP and the ways the company manages its risk is unlikely to be considered compliant with the 2017 Code.

4. Establish a 'security operations centre' ('SOC'), which should be a centralised unit dealing with issues relating to cyber security. It may be integrated into the pre-existing operations centre, but it should respond to potential, emerging and present cyber threats faced, take proactive steps to manage cyber security threats and liaise with other stakeholders (such as third party suppliers) to ensure that they are equally conversant with the risks and responses required.

Does it work?

The 2017 Code laudably recognises that limiting 'cyber crime' to instances of hackers obtaining money by forging invoices or amending bank account details is not accurate in the current climate. Instead, it recognises that 'cyber crime' exists in many guises, from sophisticated and targeted attempts to divert funds, to forging documents and to disgruntled employees seeking revenge by corrupting the system. The 2017 Code also recognises that the outcome of a cyber attack is not limited to just financial loss. It goes further and acknowledges that control of a vessel/operation for malicious purposes, long term diversion of funds and the ability to report information for the distortion of markets and completion are all current goals of cyber criminals.

The practices preached and the steps to be taken to achieve compliance are set out unequivocally in the 2017 Code. However, only time will tell whether these are adopted in practice by the industry, or treated as a box-ticking exercise and either ignored or subject to minimalist compliance. The more interesting question is perhaps how the authorities will react - will a Liberian-flagged cargo ship discharging at London Silvertown come under additional scrutiny, and will the UK flag be performing spot-checks and compliance audits on those flying the Red Ensign to ensure that the steps outlined in the 2017 Code have been adopted.

In the meantime, much of the success of the 2017 Code is likely to be governed by the industry and how it self regulates. A good precedent for this is sanctions: since the hardening of US, EU and UN sanctions in recent years,

The practices preached and the steps to be taken to achieve compliance are set out unequivocally in the 2017 Code. However, only time will tell whether these are adopted in practice by the industry, or treated as a box-ticking exercise and either ignored or subject to minimalist compliance.

sanctions compliance has become a hot topic at all levels. It is now rare to see an agreement which doesn't contain a commitment to sanctions compliance, and many companies avoid entities unable or unwilling to match their compliance through words and actions. In essence, whilst the ultimate penalty of governmental action for non-compliance still exists, much of the day-to-day enforcement is performed organically by the industry players.

The authors of this piece hope that the 2017 Code will encourage the industry to react in a similar fashion. Although the specifics of the CSA and CSP will be commercially sensitive to each entity, the development of a framework will lead to a more harmonised approach by the industry towards the risks and remedies, and a consistent approach to what needs to be done to secure a system. This in turn should develop industry specialism, which in turn should spread to other companies through the organic changing of roles and employment.

In an industry which has undergone recent hard times, the natural inclination of a business faced with a further checklist and cost is to either shoehorn the requirements into the portfolio of a pre-existing department or individual portfolio, then comply to the minimum standard or ignore it entirely. The 2017 Code imposes the positive obligation upon companies to create the role of the CySO, for that individual to be competent in the sphere of cyber security and for that individual to positively interact with others involved in the security project to ensure compliance. On its face, it will be difficult for a company to plead compliance unless it has given a competent individual the proper tools to perform the tasks, and the objectives and follow-ups set out in the 2017 Code have been met.

The 2017 Code also demonstrates that the Government's commitment to double the UK Merchant Navy is a serious one and supported by the acts (and not just words) of Parliament. It envisages a technologically competent post-Brexit merchant navy competing on a global scale with other sophisticated fleets. This vision is a commendable one, and will no doubt resonate with owners in other jurisdictions where the central government has been less forward in offering its support to the industry in recent difficult times.

Could it go further?

Many industries have become collectively stronger through the sharing of information. Piracy in the Gulf of Aden has been significantly reduced largely due to the exchange of intelligence between governments, supranational organisations and commercial actors. The same can be said for sanctions where - as mentioned above - a consistent flow of information has led to a largely self-regulating industry. It is therefore a surprise that the UK Government has not taken a bolder stance on the reporting of cyber crime. The sharing of information about cyber crime - from suspicious email addresses to sophisticated cover-ups on cargo manifests - would benefit the industry immensely. Even if obliged to report anonymously, a weekly circular listing suspicious activity and innovative steps taken to combat cyber crime would surely benefit the CySO.

Of course, a company suffering a cyber attack can still report it to one or all of the entities listed in the 2017 Code. However, in the authors' experience, the chances of redress are extremely limited due to a lack of resources, which is perhaps unsurprising where the 'action fraud' reporting service ranges from scammers purloining £100 by imitating police officers, to sophisticated cargo heists involving forged bills of lading and amended cargo manifests. At present, the reporting and recovery system is struggling to make real inroads into the problem due to the lack of resources - the shipping industry would benefit from its own dedicated service. In that respect, the private sector has of course sought to fill this vacuum.

The CSO Alliance, built in partnership with Airbus, has established a maritime cyber crime reporting portal. The portal creates a community of CSOs who can anonymously submit reports on all crime information, opinions and best practice. Beyond disseminating current threats, the Alliance also provides approaches to combat these issues. However, its use is not universal throughout the maritime industry and companies will naturally be nervous about admitting their exposure to competitors, even when under conditions of anonymity.

The future?

The 2017 Code is a best practice framework which makes a positive demand for the shipping industry to redouble its efforts to combat cyber crime. It sets out a framework which clarifies the positive steps individual companies within the industry should now take in order to protect themselves and others against the malice of nefarious keyboard warriors.

However, the authors hope that the industry will now seize the opportunity to take the initiative in the fight against cyber crime. First, those receiving a service should require their providers to have in place policies and procedures which reflect the requirements of the 2017 Code. Secondly, influential players in the industry - the owners, charterers, insurers, brokers etc. - should as a matter of course now ask their clients and counterparties to demonstrate both creation of and compliance with the steps set out in the framework.

Thirdly, the Government should now consider how best to take the fight to the cyber criminals, be that through compulsory (albeit anonymised) reporting of the cyber incidents, to a dedicated taskforce charged with investigating and proactively bringing to justice those who perpetrate crime, on a national and international level. The 2017 Code is the starting point the industry desperately needed. Its success will now be defined by the steps taken to build upon it.