**Introduction**

Security is a hugely important element of cyber risk management but it is part of something more substantial – it’s about ensuring that our industry is prepared for the challenges of an increasingly digital world.

We need ships which are robust and resilient industrial systems maximise their safety, efficiency and environmental sustainability through careful and deliberate implementation of technology.

**Why?**

Connectivity and data.

Connectivity creates networks, known and unknown. The benefit of connectivity is that it brings ships and shipping closer to those we want to have positive relationships with. The problem is that it also brings us closer to those that might want to do us harm. And it magnifies small actions and the probability of disproportionate consequences.

Data flows are important. ECDIS is data driven navigation to improve safety. Ship management and performance systems are data driven means of minimizing inefficiencies and reducing fuel and maintenance costs. Your shipping company’s customer relationship management system or booking service are data driven means of enhancing the quality of the service you provide to shippers and passengers. Inevitably it will be the currency of regulation in the future.

If we like the opportunities of connectivity and data; if we anticipate that we are going to be using data to demonstrate our compliance with regulation; then we need to be prepared to manage the risks.

**IMO requirements**

MSC 98 adopted MSC resolution MSC.428(98) on incorporating cyber risk management into company safety management systems by the first verification of the company document of compliance (DOC) after 1 January 2021.

If you are planning to manage your cyber risk exposure effectively then you will be thinking about operational safety and environmental protection, and security.

It has been recognised by the IMO that there will be sensitive information relating to a company’s approach to cyber risk management which it would be more appropriate to include in the ship security plan, or elsewhere at the discretion of the company. This is important because it means that information about specific vulnerabilities that you have identified and technical and analytical information about your systems and networks can be restricted. This is a legitimate cyber risk management response.

The IMO has not issued specific guidance on what information should go in the safety management system documentation and what information can go in the ship security plan or other documentation. It may be worth considering that:

1. If it is a policy or procedure relating to the protection of OT systems on board which should be followed by all personnel to ensure the safe operation of the ship then it should be in the safety management system;
2. If it is a procedure on how to respond to the loss of availability or integrity of OT systems that compromise the safe operation of the ship or protection of the marine environment, then it should be in the safety management system; but
3. If it is information of specific vulnerabilities in IT, OT, network infrastructure and procedures, or detailed information about network configurations, then it should be somewhere else and the ship security plan (SSP) is an option.

I would like to urge you to be thinking about how cyber risk management could be incorporated into your safety management system efficiently. Do you want separate standalone procedures or do you want to embed cyber risk into your existing approach?

I believe there is a lack of information out there for shipping companies conducting cyber risk assessments or assessing the cyber risk assessments provided by a third party.

Threat assessments seem to be the first port of call for the security minded amongst us. Whether you do one is a matter for you. However I will leave you with this to think about: we are all at risk from the threat of random, untargeted attacks from any source and in addition, if you were a likely target for criminals, activists or governments before, then you can expect to be targeted through cyber space now. Does it need to be more sophisticated than that?

Your operational technology (OT) is your asset and it’s the loss of this during cargo loading and unloading, berthing and un-berthing, and each of the voyage phases which will determine the magnitude of the impact on your operations.

The impact of a cyber incident is likely to arise from the loss of availability of one or items of OT or loss of integrity of the data used by OT. So your existing operational risk assessments have value – you will already know the impacts of the loss of certain pieces of equipment or combinations or equipment.

The likelihood is rather more challenging to assess. There is little, if any usable data on the frequency with which OT on ships is affected by cyber incidents. To get around this, we should think about the most significant determinants of vulnerability: connectivity and unsupported / unmaintained software.

The more connected a piece of equipment is (by networks, by removable media and by users), the greater the expected frequency of loss of availability or loss of data integrity and/or the greater the likelihood that other connected systems may cease to function correctly. The likelihood is magnified if the software is no longer supported.

By taking the above into account, and on the assumption that existing SMS procedures are adequate and effective, connectivity and software support status become the main risk variables for you to really think about. In simple terms this means is that: a ship with limited connectivity between OT systems and the outside world, running supported software will have a lower initial risk level than a highly integrated ship, connected by multiple links to the outside work, running a combination of supported and unsupported software.

This is obvious but it’s important. Administrations will expect you to demonstrate that you understand your cyber risk exposure. I hope the above demonstrates that you already have much of the information that you need. You know the equipment that is important. You know the safety, environmental and efficiency implications of equipment becoming unavailable. And if you look at how connected and well maintained your systems are, then you will have an appreciation of the expected likelihood of a particular impact.

**IMO guidance**

The IMO has issued non-mandatory guidance in MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management. This is a simple document which outlines a general approach to cyber risk management based on the US NIST Framework which encourages the following practices:

1. **Identify.** Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations. This is all good safety management system information;
2. **Protect.** Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations;
3. **Detect.** Develop and implement activities necessary to detect a cyber-event in a timely manner;
4. **Respond.** Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event; and
5. **Recover.** Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

The approach which the IMO guidance recommends aligns with the industry Guidance on cyber security on board ships, but significantly for you is sufficiently broad that it would also cover any sensible approach to cyber risk management.

**National guidance**

The IMO Guidance on Cyber Risk Management is non-mandatory. You do not have to follow the guidance in MSC-FAL.1/Circ.3. I would therefore strongly advise that in addition to consulting the industry guidance, that you seek the guidance of your Administration on the requirements they have for incorporating cyber risk management into safety management systems.

One word of caution. I recently reviewed some guidance produced by one Administration that was completely focused on ISPS Code compliance and included quite detailed guidance on how to establish an appropriate cyber security organization within the company. The advice was all sound but it neglected to recognise that:

1. Different companies have different cyber risk profiles and therefore companies need guidance which is scalable to the level of cyber risk a company expects to need to manage; and
2. The international requirement is for compliance to be demonstrated through the safety management system required by the ISM Code, not the ship security plan required by the ISPS Code.

**Industry guidance**

The document is available from the ICS website and the websites of other associations involved in developing the guidance.

The development of the guidance was led by BIMCO with substantial contributions from other industry associations. The guidance is high level and covers a lot of ground.

**The 85% solution**

The industry guidance refers to the Centre for Internet Security (CIS) security controls as the basis for the recommendations. There are 20 vendor and technology independent recommended technical and procedural risk mitigation measures mapped to the NIST framework and ISO 27000 series standards.

The CIS and the SANS Institute identified 5 of these measures which are considered to mitigate 85% of cyber risks – the “should be done by everyone” measures. An interesting piece of information if you are looking for a steer on how best to progress your response to cyber risks.

**Inventory of Authorized and Unauthorized Devices and Inventory of Authorized and Unauthorized Software.** This means establishing and maintaining and understanding of what devices and software is running on your OT and IT networks, and the pathways for data to and from your systems. This is how you find our who you are really connected to. By understanding what is using your networks you can restrict access to authorised devices and hardware and prevent unauthorized and unmanaged devices are found and from gaining access.

**Secure Configurations for Hardware and Software.** The reality is that the default configurations for operating systems and applications, or those that are left by system installers and integrators may not be the best settings for minimizing the vulnerability of the system. OT and IT systems should be configured to support a balance between operational need and security. We do not want OT systems locked down so that only the Master can use them but neither do we want hardware which is so open that the potential for damage is unbounded.

**Continuous Vulnerability Assessment and Remediation.** Unless you are proactive in responding to reports of vulnerabilities then you will allow vulnerabilities to enhance your risk exposure. This means having procedures in place to scan on board networks for known vulnerabilities and for applying software updates and security patches as soon as they become available from OEMs. We have to think of the application of software patches in the same way we would a physical maintenance task on a physical piece of equipment – think section 10 of the ISM Code.

**Controlled Use of Administrative Privileges.** Think very carefully about the privileges that are granted to ship and shore based personnel. By controlling privileges effectively, and limiting the number of Administrators, you reduce the potential for malicious or unintended consequences of individual actions. The vast majority of people are users – not administrators.

Once you have these 5 measures in place (which can be mapped to the first 4 practices in the IMO Guidelines) then you can start to advance your work – continuous improvement is required by the ISM Code – based on additional technical and procedural measures which can be demonstrated to be cost-effective for your company. Remember, you do not have to eliminate the risk but you should manage it so that the residual is ALARP.

**Training and awareness**

Ship- and shore-based personnel are both your best asset and greatest potential weakness.

Ship- and shore-based personnel need to be aware of their ability to contribute to managing cyber risks and how they could also be a vulnerability. There are a number of campaigns ongoing that are trying to help companies with this through written and video media and there are well known training providers offering specific courses. These should all help shipping companies, provided that the training that is provided and the messages it includes match the company’s expectations of its personnel.

The most important message here is that training and awareness building, in combination with the 5 measures mentioned previously, can be the foundation on which much more sophisticated approaches to cyber risk management can be based. I would like you to remember that it does not matter how complex and robust your approach becomes one ill-considered action could easily introduce or expose a vulnerability.

Investing the time and resources in training and awareness will protect your future investments in technology to help you manage cyber risks.

Having a training and awareness programme is also an excellent way of demonstrating that you are taking cyber risk management as seriously as any other form of risk management.

**1 January 2021**

A gentle reminder that by your first annual verification of the company DOC after 1 January 2021, companies will have to demonstrate that cyber risk management is incorporated into the company safety management system.