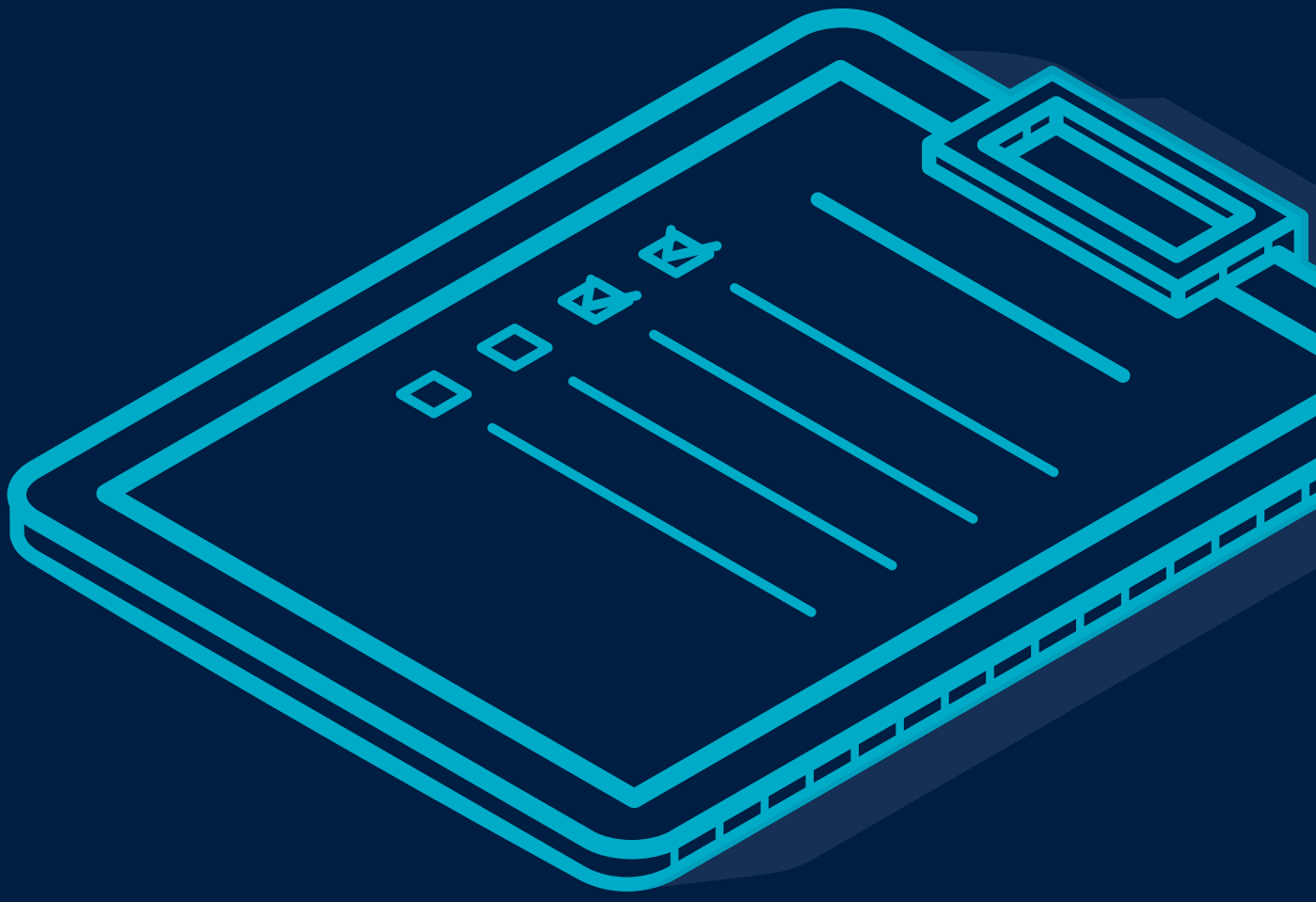
ASTARA
COMPANY LIMITED

The IMO's cyber security regime

meet the challenge, make the change



#ResilienceandRecovery

#ResilienceandRecovery

The IMO's cyber security regime: meet the challenge, make the change

The decision by the Maritime Safety Committee of the International Maritime Organisation (IMO) to include cyber security in ship safety management system[1] will soon be put into practice. An important step to improve security aboard ships, it brings a necessary, if slightly belated, focus on the cyber security of vessels as part of the essential underpinning of their seaworthiness. Done properly, the implementation of the standards and the audit thereof can become a focal point of the shipping companies' licence to trade. It recognises that a cyber-attack could be the root cause of a safety incident or environmental event. And it points to a future where more digitised ships, possibly with increased autonomy, will require continual improvements in security to guarantee their ongoing seaworthiness.

The IMO has wisely taken the standard Network and Information Systems Directive 'identify-protect-detect-respond-recover' cyber security framework categories as its core. It has had to rationalise the content in a way that will be understandable in a marine environment, by focusing the cyber measures on events that could threaten the safety of the vessel, or the environment. While shipping companies have had three years to consider the implications of these requirements, the regulations take effect on 1 January 2021 and there is still a long way to go.

What does this mean for ship owners and managers?

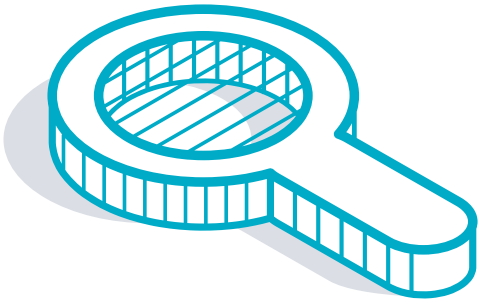
The audits will identify areas of strength and weakness. As with safety, the leadership of the organisation will have to be prepared to adopt measures and/or technology to meet the audit requirements. But in order to understand where you are now, you will need certain information capabilities: only then can you identify where you need to get to and how.

1. Identify the risks you face and the critical systems you depend on
2. Make people responsible - from the board downwards
3. Train your staff
4. Understand data flows, protect and monitor
5. Plan for an incident, practice and learn

What is involved?

The IMO cyber requirements are non-trivial, and most shipowners will need help to comply. And comply they must, to obtain their document of compliance (DOC). For others, the IMO requirement will be but the starting point for a more stringent set of standards that shipowners will have to meet if they have been designated as Operators of Essential Services (OES) under the Network and Information Systems Directive that became law in Europe in May 2018.

[1] The Maritime Safety Committee, at its 98th session in June 2017, adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021. The IMO also released Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) in July 2017.



There will be a number of implementation issues:

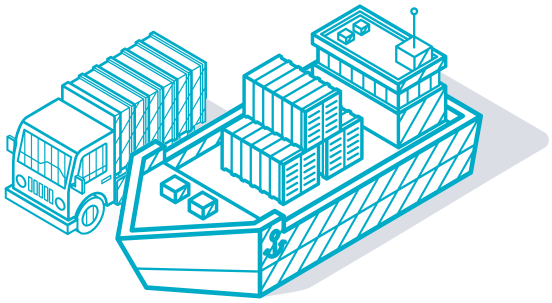
- Flag states will have to find sufficient numbers of suitably qualified and experienced people to conduct the audits objectively. To start with there will be wide varieties in the quality of the audits, since currently the standards are couched in such a way that suggest that some of the standards are less than mandatory
- The standard, when talking about the detection of a cyber event, talks about 'non-conformities' but only gives examples as to the scope of a monitoring system (begging the question of how an audit in this area could reassure anyone about the efficacy of network monitoring)
- Shipping companies will need to train their people both to work in cyber security aware way, and to be able to deal with the cyber requirements placed upon them by the standards (e.g. cyber risk management or system monitoring for instance)
- Masters and technical managers will need to recognise when an event is occurring that there might be a cyber element to it, and that it is incumbent on them to understand the root cause
- The guidelines, and the accompanying compliance audit, are not just about getting to a certain level. Since the cyber threat is dynamic, shipowners will have to continue to invest in their capabilities in order to remain current and capable of resisting future attacks to their systems and infrastructure

One audit does not secure make...

Audits are a useful device to check compliance at a point in time. While it would be reasonable to assume that a safety plan could remain valid for a number of years, assuming no any major changes on the ship, it would be a mistake to think that a single ISM audit would be sufficient to provide the shipowner – and the flag state – with the assurance that the cyber security relevant to the safety and environmental protection of their vessel is now guaranteed, until the next DOC. It cannot – and it won't. Seafarers of every rank (and owners, managers) need to realise that this is not a one-off but the start of a new way of working. While an ISM audit may traditionally consider a range of options against a defined number of situations, cyber threats will manifest themselves in different ways depending on the maturity of the attacker and the recipient. Cyber threats will mutate in how they act and how they get into your systems, and how they will affect ship systems. It will be important, therefore, to ensure that audits are accompanied by regular and ongoing monitoring systems, processes and technology to ensure they continue to operate as intended.

What will the audit mean?

While still focused on issues of safety and environment, the audit will be looking for evidence that shipowners and operators will have considered cyber security as a key risk factor for potential damage to vessels. They will expect to see cyber risks identified and encapsulated in operational policy and risk management activity. Some of those risks will need to be managed by technical means, whether through protective capability or monitoring. Either of these will require new capability both at head office and on board. They will also expect to see cyber security issues taken into account in the response and recovery plans that each ship must have. There will need to be better



system logs, better access control systems and a range of other steps taken render both IT and OT environment is more secure there will need to be more stringent security applied to critical systems on board a vessel so that they are more difficult to corrupt and/or otherwise endanger. The audit will wish to see ongoing consideration of cyber issues at senior levels of the organisation. And they will expect to see masters of vessels similarly engaged in the issue.

People, People, People

The pre-eminent issue is to ensure that their people are well trained to understand the requirements and are able to implement them. This investment in people cannot be underestimated, nor its importance understated. Without competent, trained people, shipowners will not be able to understand what is occurring on their systems and networks nor understand the implications of potential attacks.

More than Safety or Environment

While the IMO has sought to integrate cyber into the important areas of safety and environmental protection, given the existing focus of the ISMS, they, the shipowners and the operators, will need to understand that cyber threats range more widely than this. They include financial theft, extortion through ransomware and other attacks, which may not necessarily threaten the safety of the vessel at sea but can inhibit it or its owners from trading profitably. In short, this is not just about safety, it is about the ability of a vessel to ply its trade securely in an increasingly threat driven environment.

A floor not a ceiling

On the positive side, the standards will require shipowners to take a more proactive stance on cyber security and ensure that their vessels are capable to a certain degree to meet the threats and to resist attacks. But the standards must not be regarded as merely a ceiling or a target to achieve. They are but a baseline, a sensible point of departure from which shipowners and operators need to progress over time to ensure that their ability to counter and to minimise the risk from cyber-attack becomes part of the way they do business rather than a separate annual exercise.

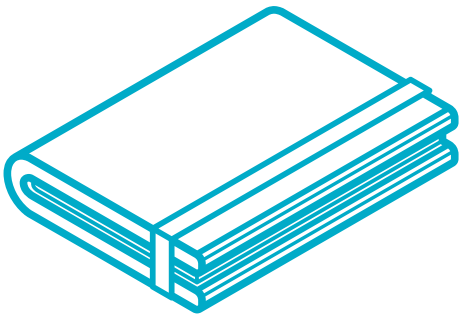
It's not just about the ships

Shipowners will also need to get to grips with those elements which do not necessarily form part of the ISMS requirements.

A. This is not just about the ships, but it is about the head office and the linkages between land-based and sea-based assets. Ships may not be the target themselves; it is possible that an attack on land-based infrastructure will affect the ships indirectly.

B. Ports and terminals will be attacked, and may seek to use shipboard systems to attack head office

C. Crew may inadvertently bring malware aboard which could attack shipboard IT and OT



Cyber is not just for Christmas

There is a is a temptation to think of these audits as an annual exercise, which you can forget once they are finished. Both this and the required cyber activity are continual: you need to forget the prospect that cyber is a one-hit activity. Just as the criminals are always active, so must you be. This process embarks you on a journey which will continue as long as you are in the shipping business. In planning your engagement with the standards therefore to treat them as an ongoing way of doing business rather than as a project with a finite end.

Shortening the cycle – or 'what's the plan, Stan?'

The big costs in a security breach involving a successful cyber-attack come in the recovery phase. Your business is off-line, your systems are not functioning, and you may need a large-scale replacement of hardware and software to get the business back. But if your backups were frequent and are accessible, the amount of data lost is relatively small: hours or days rather than weeks.

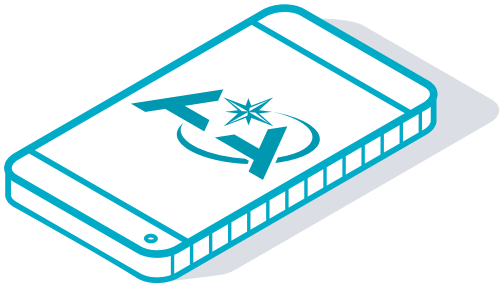
You can only shorten the recovery phase if you have planned for it. Your disaster recovery (DRP) and business continuity plans (BCP) will be seminal documents for the business. You will know how they operate, who is responsible for what, and that the options described in the plans actually work. Your planning will enable you to understand the financial impacts of a shutdown of some or all of your business.

At this point you can have a more meaningful conversation with insurers over the support you can expect from them. If you and they understand the financial cost envelope that a breach would entail, and how you would shorten the recovery cycle to as low as reasonably practicable, they, the insurance community, can more easily play a meaningful role in ensuring that you get back up to full profitability as quickly as possible.

So, what should a shipowner do now?

It is important to recognise that the changes introduced by the IMO to deal with cyber risk management are here to stay. They will require new ways of working, the deployment of new skills and investment in training, equipment and processes. These changes start with the board: without resolute board leadership, compliance with the standards will not be possible. The board is ultimately responsible for the safety of the vessels, and will be required to decide how much and on what to invest to mitigate significant risks. There are a number of actions that the board will have to take as a matter of priority. The list that follows, in our view, indicates the first few steps that need to be taken by the company's leadership to start this process, and to prepare the business to change the way it looks at cyber risk for the future. These actions include:

1. Review the corporate risk register;
2. If not already, put cyber security as a standing item of main and risk board agenda;
3. Identify a senior board member to be responsible for cyber risk, and empower them with the necessary authority and budget to discharge that mandate;
4. Initiate a full risk review to define, validate or identify both the risks and the critical functions, processes and technology;
5. Review protective measures currently in place;
6. Review staff competency and develop a training needs analysis;
7. Identify gaps in terms of outcomes required by the Standard; and
8. Identify options to fill the gaps.



How we can help

Astaara provides multi-faceted cyber risk management support to shipowners and operators, ports, terminals and other components of the marine ecosystem. From risk analysis through to risk transfer, we can help you identify the risks, the threats, the activities you need to undertake to mitigate the risks and provide you with cost-effective risk transfer mechanisms. We combine experienced insurance professionals with advanced cyber expertise. We provide access to what we believe to be best in class capability, whether for training, risk management, technology deployment, system monitoring and incident response. Our insurance solutions are built around your requirements rather than simply removing buybacks. We believe in helping you become resilient against cyber-attacks, capable of recovering quickly and reducing business losses. Specifically:

- We work with you on the development of the policies necessary to underpin your cyber security regime;
- We assess your status under the standard, identify the key gaps and recommend means to fill up whether through people, process change or technology;
- We identify the key risks to your business and your vessels and most effective means of mitigating those risks;
- We help you optimise your organisational structures to deliver effective business continuity and disaster recovery planning;
- We access cutting edge capabilities whether technical or training to help educate and inform your people;
- We mentor your leadership as they develop the cyber skills necessary to fulfil the role; and
- We can shape insurance cover to meet your risk transfer requirements

ASTAARA
COMPANY LIMITED

www.astaara.co.uk

robert.dorey@astaara.co.uk william.egerton@astaara.co.uk james.cooper@astaara.co.uk tom.graham@astaara.co.uk