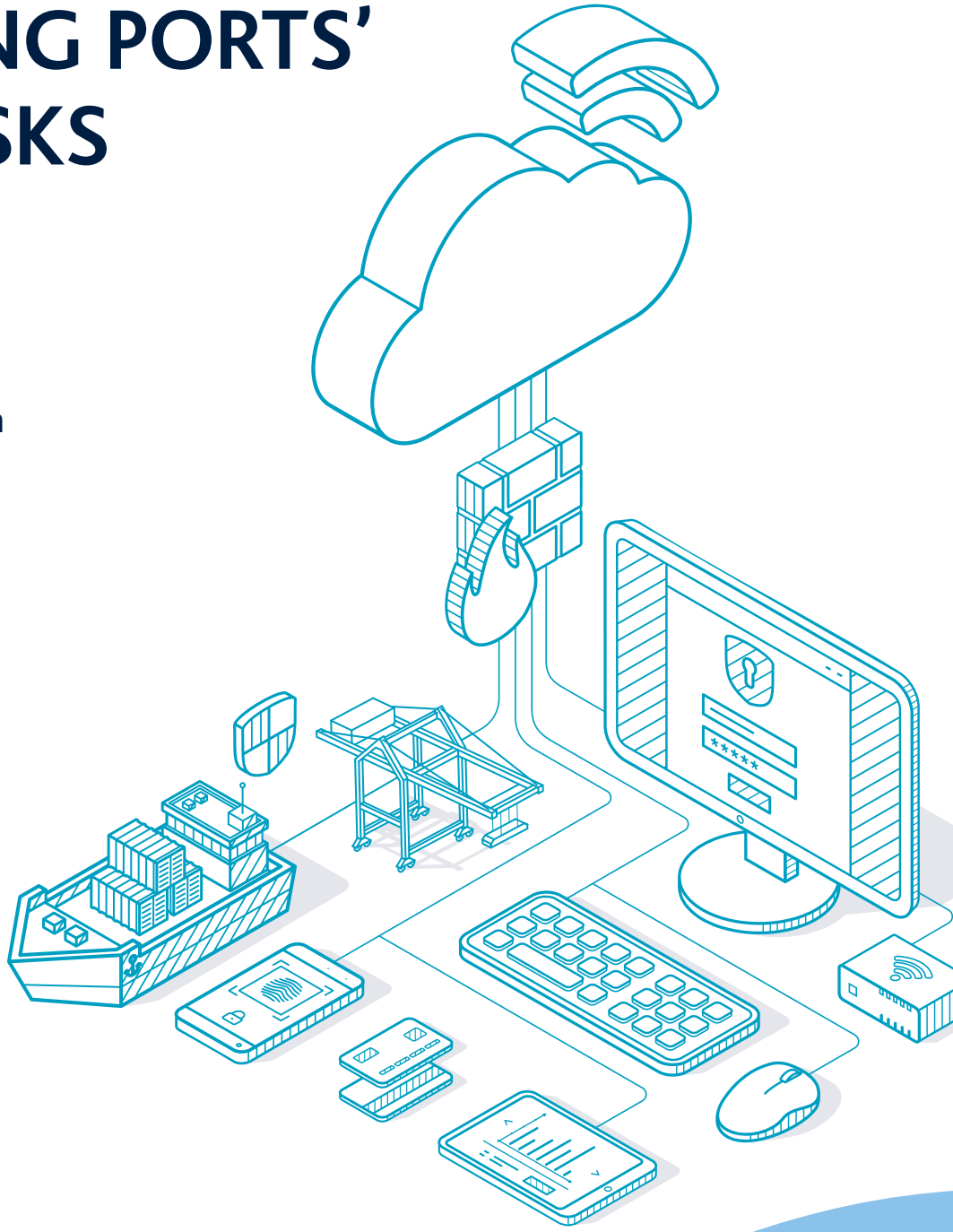
British Ports Association

ASTARA COMPANY LIMITED

MANAGING PORTS' CYBER RISKS

WHITE PAPER

in partnership with
British Ports Association



British
Ports
Association

CONTENTS

1	**EXECUTIVE SUMMARY**	4
2	**OBJECTIVES OF THIS PAPER**	5
3	**CYBER SECURITY: WHAT IS EXPECTED OF A PORTS**	6
3.1	It's the law	6
3.2	Now wash your hands, please!	6
3.3	Know your network	7
3.4	You are not alone	7
3.5	It's everything – not just IT	8
4	**SO, I RUN A PORT. WHAT DO I DO ABOUT THIS?**	9
4.1	Lead by example	9
4.2	Demonstrate and document what you have done	9
4.3	Suppliers' risk = my risk	9
4.4	Responsibilities and accountabilities.	10
4.5	It's the users, stupid.	11
4.6	Invest, invest, invest	11
CONCLUSIONS		12
4.7	Take this seriously	12
4.8	Train your people	12
4.9	Get the basics right first	12
4.10	Lead by example	12
4.11	Recognise your position in the ecosystem	12
4.12	If you're going through hell, don't stop	12
ABOUT ASTAARA		13

1 EXECUTIVE SUMMARY

The life of a port authority/operator is becoming ever more complicated. Increased regulation, the prospect of attracting government ire for failing to resist a cyber-attack, the increasing digitisation of the fleet and the growing importance of connectivity between hinterland, port and vessel, all mean that ports are and will remain the subject of close interest to cyber criminals, as well as essential points of resilience for countries.

And therein lies the tension: what designates sufficiency of protective measures? How much is the right amount to spend? When and how does the Port know they are doing the right thing and that they are secure? In simple terms, there are no yardsticks. Each port must assess the threats and risks they face, and respond accordingly. The key is that they must respond – and document their response – preparing for the worst, while hoping they never have to demonstrate their proficiency at business continuity planning or disaster recovery.

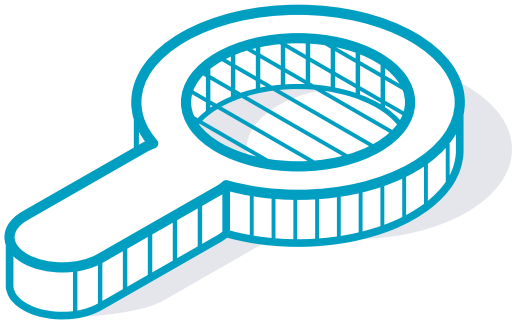
Laws and regulations are getting tougher. Regulatory fines are increasing in size. Technology is getting more complex, requiring significant investment both in the platforms themselves and in the technologies, processes and people necessary to keep critical data secure.

There is no right answer to the question about how much should be spent on security. The only sensible answer is 'more than the bad guy is prepared to spend to attack you'. But there are things you can do in the short term that are relatively cheap to achieve, and which will give you a measure of confidence that you have mitigated the obvious risks. These basic steps have usefully been codified in the UK by the National Cyber Security Centre as "Cyber Essentials". Other frameworks are available in varying degrees of complexity, for example the "Cyber Assurance Framework" in the UK and the NIST framework from the US. Whatever you decide to deploy, be sure you have clearly documented what you have done.

Your people will ultimately be the determining factor of your success. Train them well, imbue them with a sense of responsibility towards the collective, help them understand the threat and their part in dealing with it, and you will have a motivated workforce sensitised to the threat and observant of their surroundings. Underinvest in your staff, their training and the capabilities that they need to do their jobs, and you will more likely suffer a breach, whether from inside or outside your organisation.

No board wants to spend any more than they have to on things like information technology. But the alternative is worse: cyber-crime bleeds the world economy of $2 trillion a year because we only spend $150bn a year on cyber defence. While every dollar spent on security might not be necessary, the asymmetry is still stark. It will persist unless and until every corporation brings its cyber security up to at least a minimum standard.

The ability of ports to withstand most cyber-attacks is critical to national prosperity. Investment in cyber defences enables global trade and protects national sovereignty. While the burden of regulation on ports is not trivial, there is help available to get it right. This white paper seeks to explore the challenges ahead and identify sources of support for these important elements of our national economies.



2 OBJECTIVES OF THIS PAPER

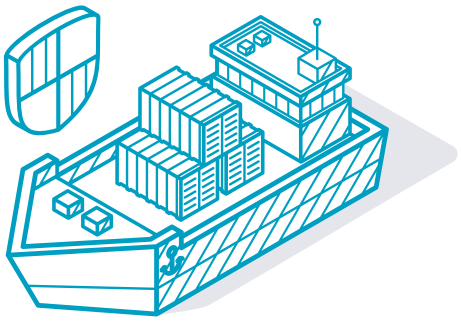
Our objectives in writing this paper are threefold. First, we wanted to illustrate the implications for ports of their current obligations and responsibilities as far as their data is concerned, and to identify for them some of the key requirements placed upon them by legislation and regulation.

We want both to inform and support ports in their deliberations on how to run their business while at the same time meeting the requirements of legislation, and ensuring that they were mindful of other parties involved in their enterprise, be they clients or suppliers. There needs to be a dialogue inside the organisations to tie together the issues that often link together and to encourage their exploration at a senior level so that boards and stakeholders understand what ports and operators intend to do with regard to keeping their operations running and their data secure.

Secondly, we want to tease out some of the issues in cyber security that readers will face in the future. There is a lot that can be done relatively quickly and cheaply to bring down risk levels to a manageable residual risk level. These may not be rocket science, but they are intricate and need to be managed appropriately. Boards can no longer stand by and hope the breach doesn't happen on their watch; responsibilities and accountabilities need to be taken seriously. The role of management is particularly important in this arena as organisations buckle under the weight of spam and other attack vectors. Companies need to be disciplined in addressing cyber security. Individual board members need to be responsible for their actions, and work collaboratively with colleagues in ways that they are not used to. Organisations will need to spend considerably more on protecting their assets than hitherto partly as a response to decades of underinvestment, and partly in the realisation that without this investment breaches become far more likely and loss of business far more expensive.

Finally, we encourage ports to engage both their user population and their suppliers in active defence of their businesses. We discuss insider risk. And we suggest ways in which organisations might want to take the assessment of their cyber footprint seriously.

We would welcome any feedback readers might have on this document as we prepare for another issue later in the year.



3 CYBER SECURITY: WHAT IS EXPECTED OF A PORT

3.1 It's the law

Governments understand how important information is to the economy and are becoming increasingly intolerant of organisations that lose personal or business critical data. In recent years, progressively stronger legislation has been brought forward to increase the incentives for industry to behave better with respect to the information systems they control and the data that resides on them. The twin canons of the General Data Protection Regulations (GDPR) and the Network and Information Systems Regulations (NIS) present a formidable set of legislation, with which, in the case of GDPR/DPA 2018, companies have no choice but to comply. For now, only the largest ports that the government regards as critical to national resilience are within the scope of the NIS regulations. For a port designated as an Operator of Essential Services (OES), regardless of ownership model, there are three key areas of concentration which these laws require: personal data must be kept secure; systems must be resistant to and resilient in the face of an attack; and must be able to recover quickly after an attack. Ports not currently designated OES under NIS are still urged to up their cyber game and are expected to follow the Government's port-specific cyber security guidance, Our view is that over time, the scope of the NIS regulations will widen to include more UK ports and also to raise the bar for compliance.

Under NIS, Ports and terminals designated as OES are expected to use as modern technology as possible to keep their networks running in the face of most types of cyber-attack and other threats to operations. This therefore means that not only do systems have to comply at a point in time with government regulations, but there needs to be regular investment to ensure they stay up-to-date and capable of defeating all but the most sophisticated attacks emanating from either hackers or nation states. Government also requires OES ports to maintain the ability to recover quickly, so business continuity planning and disaster recovery are both critical components of any strategy to meet the cyber threat. Assessment frameworks like Cyber Essentials and the Cyber Assessment Framework should both be deployed. Indeed government and regulators will be looking for evidence of good practice, if ports are attacked. Whether your Port has been designated OES or not, the challenge is significant. This is where the cyber assessment framework and the associated security controls come in. These range from training and education through to concrete, specific cyber security steps including anti-virus, network monitoring, identity and access management, firewalls, secure configuration through to security event management and proactive threat and vulnerability identification.

While government doesn't expect industry to achieve the most mature levels at the start, it is expecting pretty quick action from those it has designated as OES. And you need to check whether or not you fall within the definitions of OES, if they have not already informed you.

3.2 Now wash your hands, please!

Cyber security is like infection control: basic hygiene makes a huge difference. Getting a few simple things right will prevent the majority of viruses and infections. We have to remember that the internet is a vast domain populated by a lot of people, and that like society as a whole, there will be those looking to cause harm. They are adept at circumventing the most obvious security systems. But if they find an environment is too difficult or toxic, they will go somewhere else. It should be your objective

(and ours) to make your environment very unattractive for the potential hacker. This can only be done if the basics are observed, and this is why tools like Cyber Essentials exist. At very minimum, Organisations should:

- Remove default passwords and use strong passwords everywhere
- Ensure firewalls are properly configured and turned on
- Ensure antivirus is up-to-date
- Control access management and identity
- Know networks, monitor them for anomalous activity
- Keep software updated and your patches current
- Test business continuity and disaster recovery plans regularly and learn the lessons from those tests

In addition, you need to ensure that all your staff, from Chief Executive downwards, are properly trained and that awareness of the threat is maintained. Make sure that management are co-opted into this process, and that there is somebody visibly accountable for the risk.

These basic measures will protect you from the majority of attacks. Depending on your size, criticality and proportionality, you may wish to go further and use such frameworks as the Cyber Assessment Framework (CAF) or the US NIST framework as the basis for your security posture. Whatever you choose, you have to make sure you invest appropriately and do not short-change the process.

3.3 Know your network

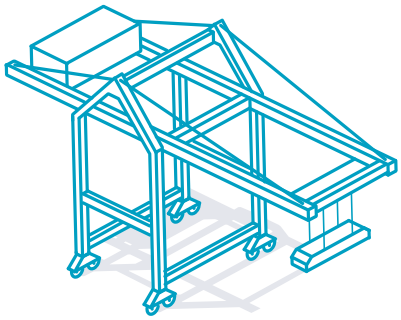
One of the most important elements for protecting one's data is to understand the full nature of one's network. Very often, when organisations first review their computer networks, they find they have extended much further afield than they thought, hosting previously unknown applications, different devices and different and numerous ungoverned points of intersection with the internet. Without an accurate understanding of your network topology, you cannot defend your network or your endpoints. Whilst you may apply a 'zero trust' architecture to your network, unless you know where your endpoints are, you cannot protect them either. It is therefore vital that you know, and can control, how your network is configured, where your data resides, and if you've outsourced any part of it, how your outsourcer treats your data, where it stores it and how it looks after it.

3.4 You are not alone

There is a measure of comfort to be derived from the fact that ports are not alone in worrying about this problem. There is helpful guidance available from the Department for Transport and from the European Agency for Cyber Security (ENISA) . In particular, the ENISA work on taxonomies is very useful for identifying the intersections between the Port, its customers and suppliers, both in the hinterland and those on the wet side. Work on taxonomies is particularly important since it goes into some detail about the interfaces that modern ports operate whether back into the hinterland or offshore. These reveal how interconnected ports now have to be both in terms of physical and data interconnections. Even the smallest port will have some measure of connectivity back into the society that surrounds them. And it is important to recognise that connectivity implies vulnerability, unless you have done your homework. But remember, guidance, advice and support are all available.

3.5 It's everything – not just IT

In your activities to secure your enterprise. you need to recognise that it's not just about information technology and office systems. Operational technologies, including industrial control systems, SCADA systems and ship-borne non-Internet facing systems are all vulnerable. These vulnerabilities will have a bearing on how you design your security architecture and your network, and protected they must be. Attacks on industrial control systems can have a catastrophic impact, and may be easier to perform as they are often disregarded as threat vectors. Remember – you probably have more touch points to the internet than you imagine and a hacker can get just as lucky within an unprotected industrial control system as they can trying to break down the front door of your IT system. You need to ensure that both are protected and not one to the exclusion of all others.



4 SO, I RUN A PORT. WHAT DO I DO ABOUT THIS?

4.1 Lead by example

The obvious answer is you can't do nothing. Whatever you do has to come top down in order to demonstrate the necessary leadership to the organisation that you take this seriously. The worst-case scenario would be a bottom-up approach where you could end up spending more and everybody would be acting in their own silos. Ports are now integrated both with their hinterland and with their vessels. You cannot afford to be an island amidst this traffic; you are linked and therefore you have to protect those links and know to whom you are connected.

4.2 Demonstrate and document what you have done

You have to be able to demonstrate what you've done and that what you've done is a legitimate approximation of the right thing to do. Everybody will treat the subject differently. That doesn't mean that everybody is wrong or right; what's important is that things are done in accordance with good practice and that the appropriate documentation is maintained, up-to-date and available for review. Being able to demonstrate that you have taken the appropriate steps, and that any damage suffered as a result of attack was by bad luck, or zero day, will help mitigate the worst of the fines. Managers need to understand their organisation's technology and empower the CIO and CISO to bring issues to the Board for resolution. There are too many cases of IT departments swearing blind that everything is under control when in fact it's not. Management has to lead by example.

4.3 Suppliers' risk = my risk

There's an old saying in the outsourcing industry that you never outsource a problem. The reason being that the supplier fixes the problem, saves the money and takes the benefit. But it also could be that the problem you're outsourcing is so great that the supplier never has a chance to deal with it properly.

In this time of outsourcing, it is critically important that the users of outsourced services understand what is being provided, how, and where their data lives. This means being very careful about the contracts that you agree with your suppliers, ensuring that the indemnities are in the right place and that there is a valid backup plan should their service go down. That backup plan needs to be owned, tested and improved by the suppliers just as you curate your own plan.

Many companies only realise how important their suppliers are to them when there's a problem. Business continuity planning is just that. If a supplier goes down and takes your systems down with them, you need to know what to do – and what your suppliers will do. Once the contract between you and your critical suppliers is agreed, it does not preclude you from managing that contract. You need to ensure that they are taking steps to make certain that they and you are at similarly high levels of cyber readiness. You need to be capable of protecting your data in the event of an attack on them (or you). Ensuring the resilience of your supply chain is critical to minimise downtime. You don't know when an attack might occur, but you will know what to do in the event of one, and therefore your ability to return to full operating capacity is increased and the time delay reduced.

4.4 Responsibilities and accountabilities.

In these days of collective responsibility it is easy to say that the board is responsible and leave it at that. But as we see in multiple breaches of major companies, it's not as simple as blaming the IT director. The CEO is responsible for the performance of the business. They are both responsible and accountable to the shareholders, the board and the stakeholders. The CEO needs to show that the shop is in safe hands and that business is being taken care of. The CEO will not be thanked if a cyber-attack damages the business, reducing earnings, dividends and the stock price. The CEO needs somebody to be responsible for this angle of risk management.

There are a number of different options for this sensitive role. Some argue that there needs to be an empowered Chief Information Security Officer on the Board. Others argue that a decision set of the magnitude of cyber security must be dealt with by a Board or near-Board Committee of empowered people capable of decision making across business lines including their own. Some other observations:

1. Good practice suggests that the CISO should not be the IT director. This makes the IT director conflicted between the need to do things efficiently and the need to secure them. Furthermore, making the poacher the gamekeeper puts responsibility for the checks and balances into the role of the individual against whom they need to be applied. They are conflicted from the start. The advantage is that the IT director has the money and can therefore divert resources to protecting the infrastructure, should the need arise.
2. Make the finance director responsible. The advantage of the FD is that they know where the money is buried, and if they need to free up some resource to plug risk gaps, they can do so. They are an independent voice, who can work with the IT director to identify opportunities and means of risk reduction. It leaves the CEO as final arbiter.
3. Give it to the corporate risk person. It could well be argued that the chief risk officer should take on the cyber risk portfolio. This will allow insight between different portfolios of risk, and permits a fuller debate about trade-offs than might otherwise be possible. It is likely that the risk director will not know much about cyber. Prevention will allow them to see the different types of risk involved and try to articulate the trade-offs to support the case for risk reduction mechanics. The Chef Operating Officer could also be a reasonable candidate.
4. Don't appoint one person. In some cases, collective responsibility works better than individual responsibility simply because the dynamics of the business. But having nobody responsible for this issue at the board is irresponsible. If we look at all the breaches that occurred in major companies, particularly the listed ones, constant top-level communication and the ability to explain the issues, as well as what was being done about them, were vital to the survival of the business. Those that failed, required too much of the CEO and there appeared to be nobody responsible on the board.

In our view, the CEO is ultimately accountable. But they have a full day job, as do the IT director and CISO. Each of these roles needs to be filled by a competent individual in their own right at the board level, reporting to the CEO.

4.5 It's the users, stupid.

System users are your biggest headache. Never satisfied with current systems, they are always looking for workarounds. They become frustrated by limitations and lazy about security. This makes your users your prime risk. They need not be, of course; they can be your eyes and ears, a reliable set of agents looking for anomalous behaviours, both in system and in users. Insider threat is the nightmare scenario, but if your business is well managed, precursor signs to insider threat will be more easily identified.

None of this happens by osmosis. There are multiple different levels at which organisations need to be briefed, trained, educated, or simply made aware of the cyber threat and their role in protecting themselves from that threat materialising. Whether it's half an hour of e-learning, a full day of face-to-face or a senior executive briefing, it needs to happen regularly, and be done and received professionally.

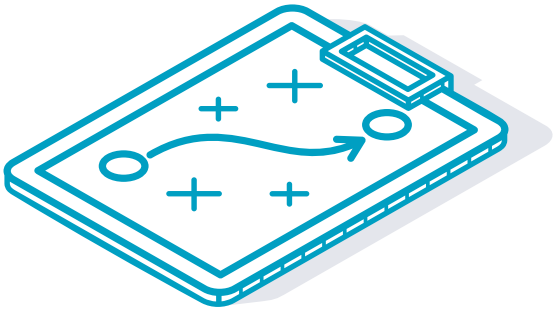
Boards need to understand both the risks and their role in combating them. Likewise, senior management must understand how they fit into the equation. System users need to be trained on the systems they use, both in terms of what they're allowed to do and what is prohibited. No one should be allowed onto a system before they've been trained in its use. Specialist users need to understand the cyber implications of their role. Staff who have roles on the system need to be managed to ensure that their privileges do not exceed their role. It is critical that access rights are amended accordingly for leavers, movers and joiners. Education needs to be provided to those whose role it is to defend the organisation, be they in the security operations centre or the IT department. You cannot protect your enterprise with an understaffed team with the wrong qualifications.

Insider threats are particularly difficult to detect, and, when the team is close-knit, particularly disappointing. Once the ring of trust is breached, it is very difficult to detect the anomalies and find those individuals without proper system and human resource management. There is research that has established that there are important precursor signals to an insider threat materialising. Management staff need to be aware of these and ensure that the appropriate individuals are made aware.

4.6 Invest, invest, invest

Wars are won generally because one side massively outspends the other, and that's how it has to be in cyber security. Currently, the figures run the other way – cybercrime nets around $2 trillion per annum for the criminals and less than $150 billion a year is spent in protecting systems. This asymmetry puts legitimate users at a big disadvantage. Management have to understand that the security of data and technology are THE key enablers and protectors of the business. If they underinvest, a hacker will find a way to breach the defences, and unfortunately these days this kind of error cannot be easily hidden. This expenditure needs to be judged against risk appetite for proportionality, but organisations also need to recognise that they are probably not as good as they think they are. Self-assessment tends to bias for optimism. When you have ever more stringent regulations, a user population that is innovative in breaking the rules, and an external environment that is hostile to say the least, you cannot afford not to invest in your security, and to protect those aspects of business that depend on others for their delivery.

To be a truly connected enterprise, you need to be a secure enterprise. Ports are the very model of a connected enterprise, and must be managed securely to deliver what they need to for their customers, staff, shareholders and stakeholders.



CONCLUSIONS

4.7 Take this seriously

We expect in the fullness of time that government will seek to treat information assets as they would any other class of asset on a company's balance sheet. This requires a change in the law which will mean that directors will have a fiduciary responsibility to look after the digital assets as well as the physical and financial assets of a company. Breaches will possibly lead to prosecutions. The more seriously a company can take the legislation now, the better prepared they will be for more severe penalties in the future.

4.8 Train your people

Your people are your biggest risk - but they can be your strongest line of defence. Give them the tools, training and the understanding of the threat, and let them help you protect your data, your balance sheet, your company.

4.9 Get the basics right first

You can go a long way to mitigating the risks to your business by adopting the approaches outlined in Cyber Essentials. Whatever you decide, getting the basics right will reduce your risk profile. If you can't do the basics properly there is little point in investing any further in technology security. You will be breached and fined, and the fine will probably be far more than you would have had to spend on security in the first place. Be proportionate and measured in your response – but don't shortchange it.

4.10 Lead by example

Management's role is clear: lead by example, let the workforce see that you are taking this seriously, and ensure that they are aware and receive proper training. Nothing undermines the cyber security effort more than management visibly adopting a cavalier attitude to information security, or worse saying that it's important but not investing to mitigate the risk.

4.11 Recognise your position in the ecosystem

Ports are becoming important parts of a bigger ecosystem. Each component of this ecosystem, be it logistics, transportation, passenger safety, navigation or safety at sea, needs confidence that the other is respectful of and competent in handling data belonging to other. There are dependencies up and down the value chain that need to be recognised and managed. If you all recognise your contributions to other people's success as much as your own, you will develop mutual strength and better situational awareness of the threat. United, you will succeed.

4.12 If you're going through hell, don't stop

Winston Churchill was right. The same can be said of the cyber environment - cybercrime is dynamic and needs to be met with a dynamic, adaptive and robust response. For the most part this is not rocket science. But it requires

constant investment to preserve your licence to trade, and to safeguard a critical part of your nation's critical infrastructure. You will get no thanks for getting it right. Failure on the other hand will be your responsibility, particularly when the tools to protect yourself were within your reach. Don't be a victim: don't let them win. Make the investments necessary to secure your enterprise and you will have done the right thing in the right way.

ABOUT ASTAARA

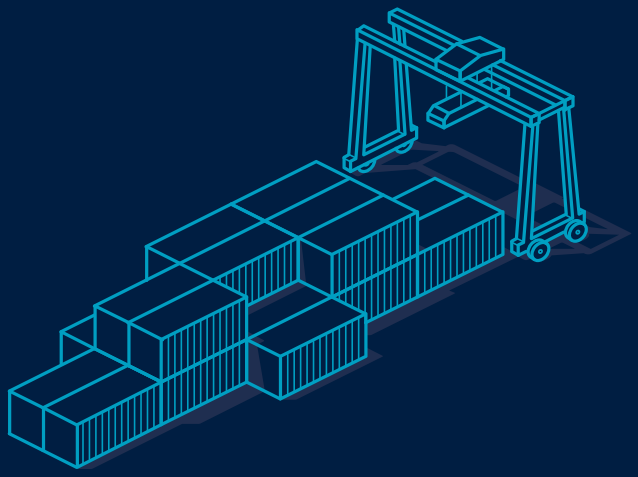
Astaara is a company designed to meet the needs of the Marine, offshore and Port sectors.

First, to assist in risk management and loss prevention, by advising boards and management how to make their companies more resilient to cyber incidents and faster to recover from them.

Secondly, to provide risk transfer solutions to the maritime community on terms of cover which are broad and reflect the actual risks of the insured, through adherence to high levels of underwriting discipline and understanding of the insured's operations and cyber maturity.

The Astaara team is composed of experienced and leading marine, energy and ports underwriters. The risk management team are leaders in cyber risk management. Combined the team has more than 95 years of experience.

Please see **astaara.co.uk** for further product information and team contact details.



APPENDICES

APPENDIX A: REGULATORY ADVICE – HOW TO MAXIMISE VALUE IN YOUR BUSINESS 15

ENISA Port Cyber Security 15

APPENDIX B: CYBER SECURITY FOR PORTS AND PORT SYSTEMS 17

MANAGEMENT RESPONSES 18

What are the consequences of doing nothing? 18

Does management engagement improve the cyber risk profile? HOW? 18

LEGISLATION AND OTHER GUIDING STANDARDS 19

1. Network & Information Systems Regulations 2018 ("NISR") 19
2. Data Protection Act 2018 21

THE CAF 23

CYBER ESSENTIALS AND CYBER ESSENTIALS+ 24

i. Cyber Essentials 24

ii. Cyber Essentials Plus 24

iii. Technical Controls 24

ENISA'S ASSET TAXONOMY 26

APPENDIX A: REGULATORY ADVICE – HOW TO MAXIMISE VALUE IN YOUR BUSINESS

ENISA: The European Union Agency for Cybersecurity, based in Greece.

IET: The Institution of Engineering and Technology, UK engineering trade body

NCSC: The UK National Cyber Security Centre.

CAF: Cyber Assessment Framework – The UK Department for Transport model for assessing an OES against NISR

ENISA Port Cyber Security

Summary

In their 2019 report, ENISA seeks to create a standard taxonomy of port activities and systems and so reduce the likelihood of inconsistent approaches to port security. It also outlines the main dataflows and interfaces that need protecting, presenting a reference model of port systems and their interfaces with external entities such as local authorities, other transport providers and satellite systems. It goes on to describe the various threats that could affect a port operator and the potential impacts such threats might have on a port, particularly given the historic weaknesses in port cyber security. The report further describes some cyber-attack scenarios e.g. ransomware and describes security policies ports should define and implement.

Key points that management should recognise

A. Make cyber security a priority and engender more of a security culture

B. Institute training, education and awareness raising, especially at Board level

C. Allocate appropriate time and budget across the business

D. Appoint SQEP (Suitably Qualified and Experienced Personnel)

E. Simplify and manage technical complexity of convergent IT & OT

F. Achieve better balance between efficiency and security

G. Manage and protect weaker legacy systems

H. Potential confusion on regulatory requirements – beyond relatively narrow confines of NIS

I. Understand the Dynamic nature of the threats and the new threats arising from vulnerabilities due to digitisation

J. Supply chain and 3rd party interdependency – work with suppliers to define good practices; recognise the interdependencies and work accordingly

K. Ensure right information is shared with interested parties in good time.

Key policies and practices that management should adopt

A. Security Policy and governance of systems

B. Risk and Threat management

C. Security and privacy by design

D. Asset and Inventory management

E. Cyber Resilience (BCM)

F. Protection of Endpoint and IT Lifecycle Management

G. Vulnerability Management

H. People Security Management

I. Supply Chain Resilience

J. Incident Detection and Response

K. Physical Protection for IT and OT

L. Network Security

M. Port System Access Control

N. Administration and Configuration Management

O. Threat Management

P. Cloud and Machine-To-Machine Security

Q. Data Protection Measures – In Transit, At Rest or In Use

R. Patch and Update Management

S. Monitoring System Health and Attack Detection

T. Industrial Control Systems Security

U. Back Up and System restoration

V. Control and Audit

APPENDIX B:
CYBER SECURITY FOR PORTS AND PORT SYSTEMS

Summary

In conformity with the UK's implementation of the Network and Information Systems Directive, the Department of Transport has engaged with the IET to update a 2016 good practice code. This was reissued in 2020. While it does not seek to go across NISD and provides actionable advice on:

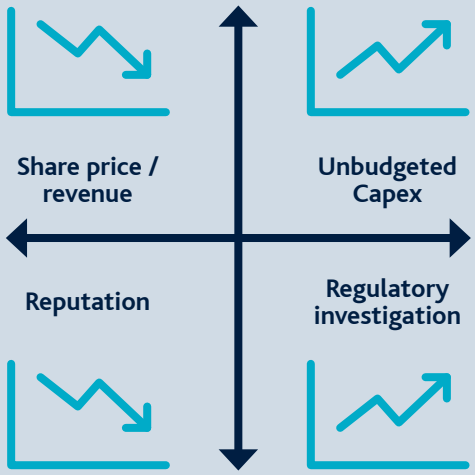
A. Developing a cyber security assessment and plan for important assets, processes and potential vulnerabilities
B. Devising the most appropriate mitigation measures
C. Having the correct governance structures, roles, responsibilities and processes
D. Handling security breaches and incidents
E. Highlighting national and international standards used and the relationship to existing regulation
F. Information to be used with DfT cyber security for ships guidance.

Key points that management should adopt

A. Understand the requirements of the NISR and seek to go beyond
B. Integrate cyber security planning into other planning interventions
C. Understand attacker motivation and identify critical systems
D. Implement appropriate and proportionate measures to combat the threat
E. Train people to reduce human error
F. Develop policies that set out the definition of a critical asset
G. Identify critical assets and processes relying on them
H. Identify risks arising from particular threats to those assets and prioritise
I. Identify controls and mitigation for those threats
J. Ensure residual risk is acceptable and accepted by the organisation
K. Draw up a Cyber Security plan, monitor and audit it
L. Staff cyber security appropriately, starting with a Senior cyber Security Officer
M. Create a port security committee and where necessary a Security Operations Centre (SOC)
N. Define what constitutes a breach or an incident and put plans in place to deal with scenarios

MANAGEMENT RESPONSES

What are the consequences of doing nothing?



- Share price slump, slow recovery
- Unbudgeted Capex (non-budgeted spend)
- Loss of Revenue (negative cashflow impact)
- Regulatory investigation (management time, expense, uncertain of outcome)
- Regulatory Fines (GDPR, NISD, NISR etc.)
- Reputation (management time, client relationships, employee confidence)

Does management engagement improve the cyber risk profile? HOW?

LEGISLATION AND OTHER GUIDING STANDARDS

1. Network & Information Systems Regulations 2018 ("NISR")

The UK implementation of Network & Information Systems Directive ("NISD")

The Directive is focused on protecting critical national infrastructure from cyber caused attacks/ disruption. The nation states divide the critical state infrastructure into sectors and establishes the idea of an Operator of Essential Services (OES). As an OES there is a legal requirement to maintain continuity of supply in the event of a cyber incident. This is now implemented in all EU member states. Marine Aviation and Transport is one of the sectors.

NISR Enforcement key points

The enforcement authority of the DfT is the Maritime and Coastguard Authority. THE MCA has broad scope to sanction Operators. However, the regulations are designed to operate in a proportionate manner and are therefore escalating in severity:

A. Information order

Service of an order on Operators to retrieve information in relation to:

A. the NIS security and

B. the implementation of the NIS security plan

B. Inspection order

To assess whether the OES is fulfilling its obligations under the NIS Regs, where the MCA suspect a potential breach of the NISR.

C. Enforcement notice

Where the MCA finds or has reasonable grounds to suspect a breach or failure of the obligations imposed by the NISR.

The enforcement notice, among other things, must specify the alleged failure by the recipient and what steps, if any, must be taken to rectify the failure

D. Penalty notice

Where an Operator fails to rectify a failure under an Enforcement Notice the MCA may then service a penalty notice.

E. Fine

Financial penalties may be attached to the penalty notice and the Regs require the fine to be appropriate and proportionate to the failure in respect of which it is imposed. Financial penalties will only be levelled as a last resort where it is assessed appropriate risk mitigation measures were not in place without good reason.

F. Fine scale

The NIS Regulations set out caps on the penalties which can be imposed reflective of the breach; from a limit of £1 million for any contravention which could not cause a NIS incident; to £17 million for the most severe breaches, being a material contravention which has the potential to cause an incident resulting in an immediate threat to life or significant adverse impact on the UK economy.

G. Enforcement forum

Decisions taken by the MCA will be enforceable by civil proceedings, and appealable through the court system.

A competent authority must have regard to whether the breach would also be result in liability under another enactment or regime. As such, there may be reason for an operator to be penalised under different regimes for the same event, such as the GDPR, because the penalties might relate to different aspects of the wrongdoing and have different impacts. This will not limit a competent authority's ability to apply the penalty it feels is appropriate to the circumstances, but will encourage it to factor in other regimes if this is appropriate.

NISR 2018 key points

The UK implementation of NISD. There will be a difference of approach in standards and enforcement across the EU however key principles that apply in the UK are:

A. Application to Ports in the UK

The following are specifically identified within the NISR (Schedule 2 s5(5):

Harbour authority has the same meaning in section 313(1) of the Merchant Shipping Act 1995.

Port Facility has the same meaning as in regulation 2 of the Port Security Regulations 2009.

Vessel Traffic Services has the same meaning as in regulation 2(1) of the Merchant Shipping (Vessel Traffic Monitoring and Reporting Requirements) Regulations 2004.

B. Application to ports within the EU

Ports operators are often owned by group companies domiciled in other jurisdictions which may own other ports operations within the EU. As such UK ports operators will be captured under UK NISR. Note however, that each EU Member State has to identify essential operators with an operation on its territory. The practical consequence is that if an enterprise operates ports with in more that one jurisdiction within the EU one or more other Member States could have jurisdiction over the legal same entity.

C. Proportionality

NIS is targeting the prevention or mitigation of disruption of the economy – the larger enterprise you are the more likely you will be captured by the Regs (there are defined thresholds). Inversely if you are small operator you may not be captured by the NIS unless there is a unique element of national economic dependency of your operation.

D. Best practice

Compulsory Reporting for defined large incidents. However if you have incidents that are reported (which fall below the compulsory threshold) and you respond in accordance within the NIS security plan then this will assist in evidencing you are operating in conformity of the regulations in particular when DfT or others are considering the effectiveness of risk management and incident management systems.

E. Competent authorities

In the case of marine aviation and transport it is the Department for Transport.

If the Operator straddles more than one CSI sector then that will also include the other government department as applicable – however they will be encouraged to cooperate, to ensure that they do not put an unnecessary burden on the Operator.

NCSC has a significant supporting role, providing expert advice to competent authorities, including but not limited to publishing guidance and assessment tools to enable them to undertake duties effectively and providing incident response capability to cyber-attacks.

F. Reporting

is to the competent authority for the relevant sector.

Reporting is also possible and encouraged directly to the NCSC however NB the NCSC is a separate and distinctly separated entity to the competent authority. Reporting to the NCSC is not reporting to the competent authority.

Voluntary reporting to other agencies may also evidence conformity and may be taken into account by the competent authority.

2. Data Protection Act 2018

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018.

DPA 2018 sits alongside the GDPR, and tailors how the GDPR applies in the UK - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

What is the GDPR?

The GDPR is the General Data Protection Regulation (EU) 2016/679. It sets out the key principles, rights and obligations for most processing of personal data – but it does not apply to processing for law enforcement purposes, or to areas outside EU law such as national security or defence.

The GDPR came into effect on 25 May 2018. As a European Regulation, it has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

Cyber Assurance Framework

Designed by NCSC to cover the most critical sectors of the economy, particularly those organisations forming part of the Critical National Infrastructure; those subject to regulation under the NIS Directive or those covering risks to public safety.

The CAF is based on NCSC cyber security and resilience experience. It is comprises 14 principles written in terms of outcomes, i.e. specifying what needs to be achieved, rather than dictating 'how' the outcomes be achieved. The CAF provides further detail, augmenting the top-level principles, including providing structured sets of Indicators of Good Practice (IGPs). The CAF itself can be found here.

Why these matter

The GDPR, the Data Protection Act 2018 and the Network and Information Systems Regulations are all extremely powerful pieces of legislation. They give governments the ability to fine companies huge amounts if they feel they have egregiously breached the code. In the case of GDPR, fines can be up to 4% of turnover; under NISR, the fine can be up to €17 million. This is neither trivial nor ignorable: most importantly these laws apply globally. If a company not domiciled in the UK loses data about European citizens, the local authorities are empowered take action on behalf of any of their citizens who might be affected. If the lost data belongs to UK national, they can expect information Commissioner to come knocking. It's too early to say whether the extra-territorial aspects of this legislation will be enforceable, but for the moment the year jury is out.

THE CAF

Objective	Description	Sub-objective	Description
Objective A: Managing security risk	Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.	A.1 Governance	Putting in place the policies and processes which govern your organisation's approach to the security of network and information systems.
		A.2 Risk management	Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management.
		A.3 Asset management	Determining and understanding all systems and/or services required to maintain or support essential functions.
		A.4 Supply chain	Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers.
Objective B: Protecting against cyber attack	Proportionate security measures are in place to protect the network and information systems supporting essential functions from cyber attack.	B.1 Service protection policies and processes	Defining and communicating appropriate organisational policies and processes to secure systems and data that support the operation of essential functions.
		B.2 Identity and access control	Understanding, documenting and controlling access to networks and information systems supporting essential functions.
		B.3 Data security	Protecting stored or electronically transmitted data from actions that may cause an adverse impact on essential functions.
		B.4 System security	Protecting critical network and information systems and technology from cyber attack.
		B.5 Resilient networks and systems	Building resilience against cyber attack.
		B.6 Staff awareness and training	Appropriately supporting staff to ensure they make a positive contribution to the cyber security of essential functions.
Objective C: Detecting cyber security events	Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.	C.1 Security monitoring	Monitoring to detect potential security problems and track the effectiveness of existing security measures.
		C.2 Proactive security event discovery	Detecting anomalous events in relevant network and information systems.
Objective D: Minimising the impact of cyber security incidents	Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.	D.1 Response and recovery planning	Putting suitable incident management and mitigation processes in place.
		D.2 Lessons learned	Learning from incidents and implementing these lessons to improve the resilience of essential functions.

CYBER ESSENTIALS AND CYBER ESSENTIALS+

i. Cyber Essentials

The self-assessment option. Gives users protection against a wide variety of the most common cyber attacks. Important because vulnerability to simple attacks can mark organisations as target for more in-depth unwanted attention from cyber criminals and others.

Certification gives peace of mind that defences will protect against the vast majority of common cyber attacks - simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place.

Cyber Essentials shows users how to address those basics and prevent the most common attacks.

ii. Cyber Essentials Plus

Cyber Essentials Plus has the simplicity of the CE approach; the protections required are the same as CE, but for Cyber Essentials Plus a hands-on technical verification is carried out.

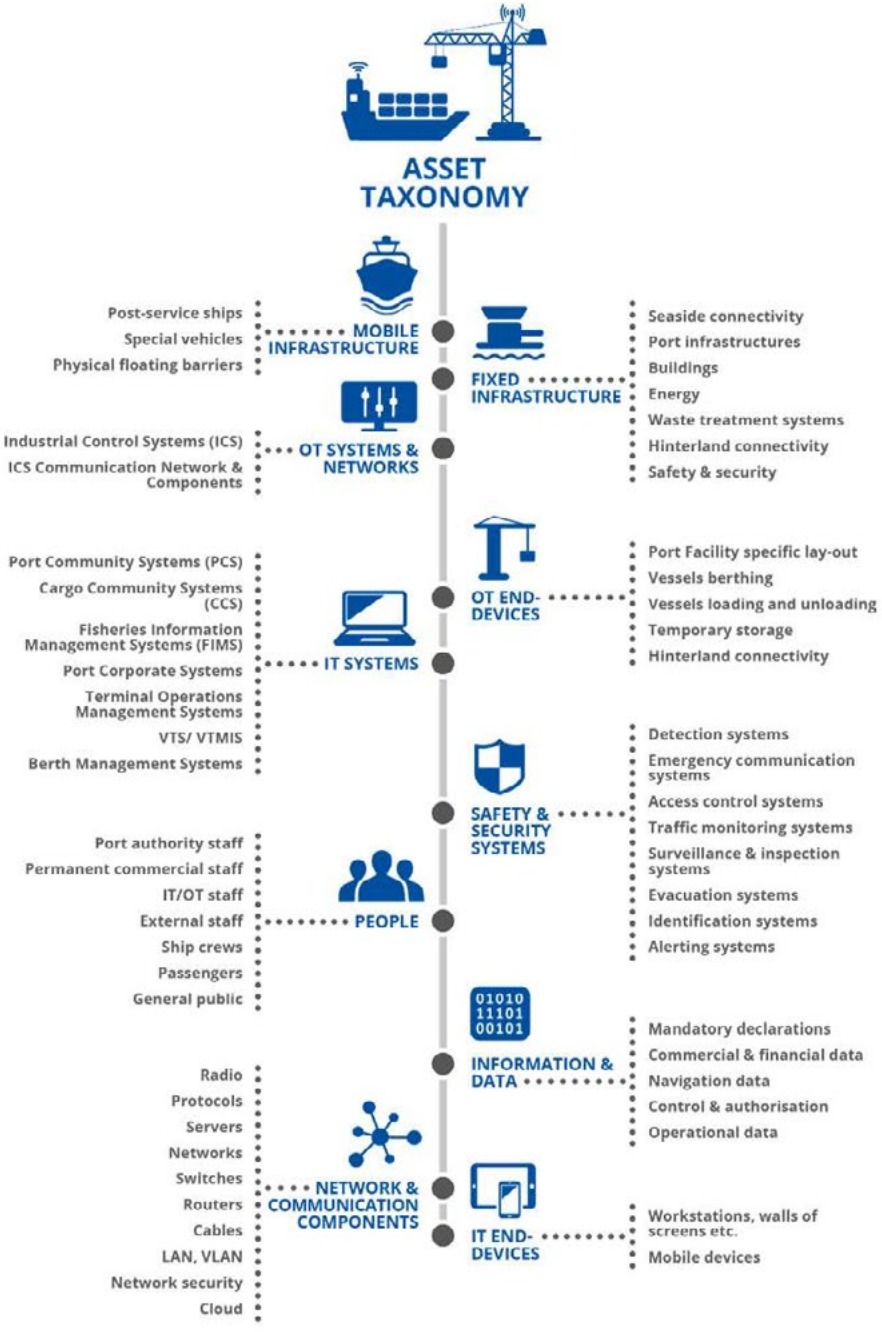
iii. Technical Controls

The controls required:

- Use a firewall to secure your internet connection
- Choose the most secure settings for your devices and software
- Control who has access to your data and services
- Protect yourself from viruses and other malware
- Keep your devices and software up to date

CE/CE+ Element	Description
1. **Use a firewall to secure your internet connection**	• understand what a firewall is • understand the difference between a personal and a boundary firewall • locate the firewall which comes with your operating system and turn it on
2. **Choose most secure settings for your devices and software**	• know what 'configuration' means • find the Settings of your device and try to turn off a function that you don't need • find the Settings of a piece of software you regularly use and try to turn off a function that you don't need • read the NCSC guidance on passwords • make sure you're still happy with your passwords • read up about two-factor authentication
3. **Control who has access to your data and services**	• read up on accounts and permissions • understand the concept of 'least privilege' • know who has administrative privileges on your machine • know what counts as an administrative task • set up a minimal user account on one of your devices
4. **Protect yourself from viruses and other malware**	• know what malware is and how it can get onto your devices • identify three ways to protect against malware • read up about anti-virus applications • install an anti-virus application on one of your devices and test for viruses • research secure places to buy apps, such as Google Play and Apple App Store • understand what a 'sandbox' is
5. **Keep your devices and software up to date**	• know what 'patching' is • verify that the operating systems on all of your devices are set to 'Automatic Update' • try to set a piece of software that you regularly use to 'Automatic update' • list all the software you have which is no longer supported

ENISA'S ASSET TAXONOMY



(Asset Taxonomy Infographic © ENISA 2019)

British
Ports
Association

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