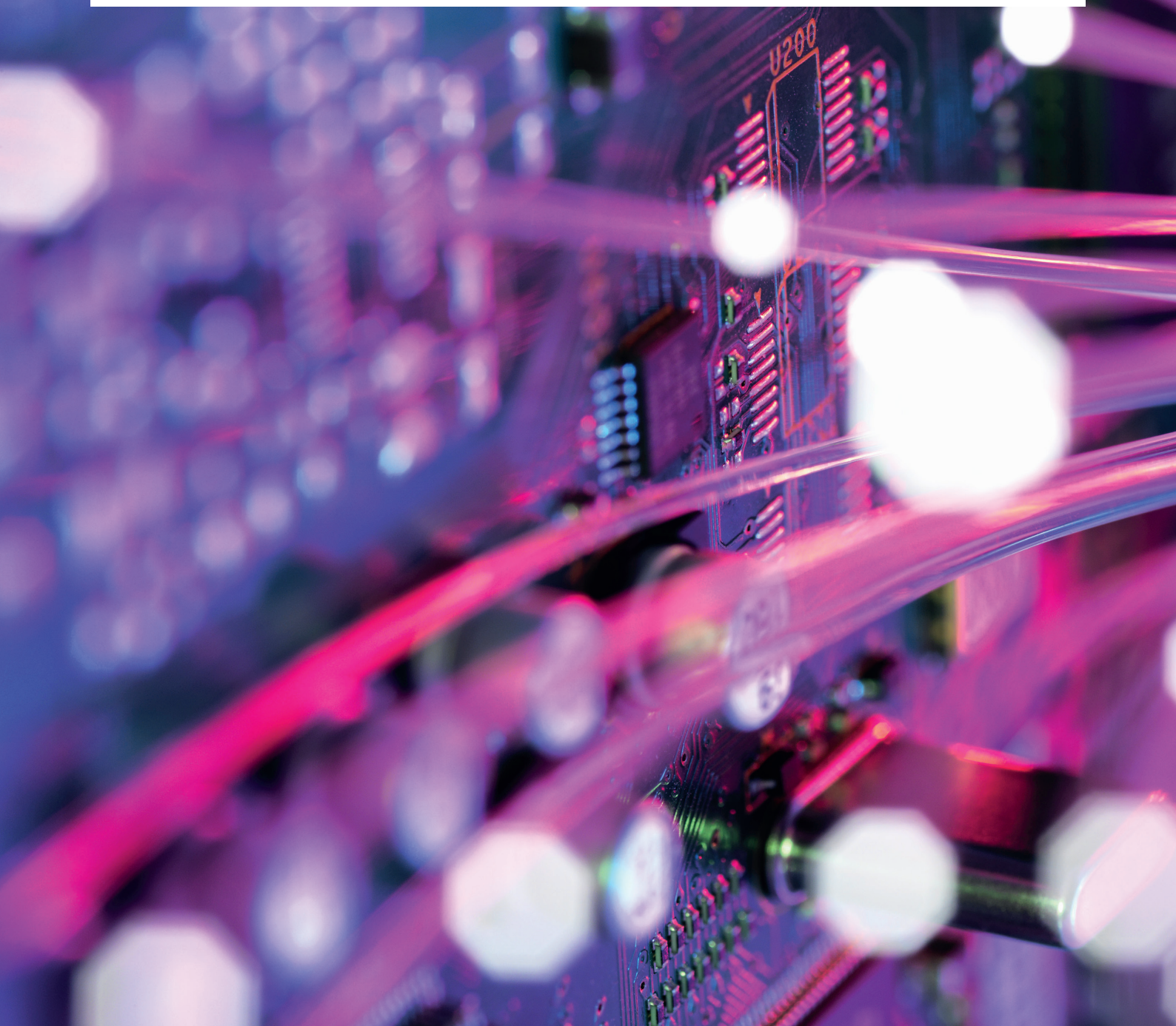
Tackling complexity: Protecting against cyber risk in the marine industry.

Lloyd's Register

NETTITUDE



Elisa Cassi
Lloyd's Register Group Ltd

Paolo Scialla
Lloyd's Register EMEA

John Paul (JP) Cavanna
Lloyd's Register Group Ltd

Abstract.

Recent years have seen high-profile security incidents involving information and operational assets in several industry and business sectors.

With innovative technologies in use across a broad range of production and business processes, it has never been more urgent to consider the associated risks. The maritime sector, like many others, is exposed to potential hazards that need to be understood and addressed. Any effective international cyber risk assessment must consider all the relevant elements. As information and communication technologies (ICTs) are applied widely to information processing and in support operations, these elements include passenger and cargo ships, yachts, supply and offshore vessels, water transport, and harbour facilities and infrastructures.

As with other technologies and activities, the new cyber environment requires a suitable process for assessing risks and appropriate measures to mitigate them. Maritime operators and owners are naturally more attracted to digital and information technologies that improve their business, but such technologies are always evolving. Protective techniques and testing procedures must keep pace. In this paper, we will explore the complex cyber risks that the marine industry faces and will continue to face, and we will focus on the most effective ways of managing them.

Introduction.

Over the last few years, transformational technologies, with their promise of improved key performance indicators (KPIs) for stakeholders, have been highly influential in the maritime sector.

Here, the impact of the digital age has been tangible. Modern technologies can integrate real-time monitoring and control of ships' systems and machinery, while acquiring data about weather, sea conditions and a wide range of other information.

Integrating, analysing and processing the mass of data from navigation systems, machinery, cargo, passengers, safety and other systems makes it possible to optimise ships' operations and develop improved performance models. The technology can be exploited to provide accurate and optimised voyage schedules, reduce fuel consumption, warn crews about potential system or component failures, and help and support emergency decision-making. Advanced automation can also minimise the effect of human error, acknowledged as the main cause of most hazardous incidents in the shipping sector (1).

Several technologies have been identified as the top drivers for the commercial shipping industry over the next few years. These are shipbuilding, propulsion and powering, smart ships, advanced materials, big data analytics, robotics, sensors and communications. All are linked to, or influenced directly or indirectly by, digital and communication technologies. On a modern ship, most, if not all, of the installed machinery and systems are already monitored and controlled by supervisory control and data acquisition (SCADA) systems. These transfer data from sensors to processing units – i.e. distributed control systems (DCSs) and programmable logic controllers (PLCs) that combine sensors and control electrical, mechanical and hydraulic components and actuators.

The computer-based technology used by a ship's industrial control systems (ICSs) is shared by other onboard systems. In other words, the navigation, propulsion, steering and power management, dynamic positioning, cargo handling, bilge and ballast, and safety systems use the same or similar processing unit technologies as the ship's internal and external

communications, passenger entertainment, ventilation and conditioning, lighting and other systems.

Each ICS sub-system is provided with a lower level of communication infrastructure based on a bus network. A higher level of communication is provided by a backbone local area network (LAN), often closed in a ring and sometimes duplicated and redundant.

In this LAN, data from sensors is exchanged between data concentrators, processed by PLC units and sent to actuators in both directions to monitor and control activities and processes. DCS central servers on the same communication infrastructure are responsible for data acquisition and controlling processes and operations, as human-machine interfaces (HMIs) inform the human operator and allow personnel to interface with machinery and processes. Data generated by the readings and operation of sensors, instruments, alarms and other events created by the sub-system are stored and logged.

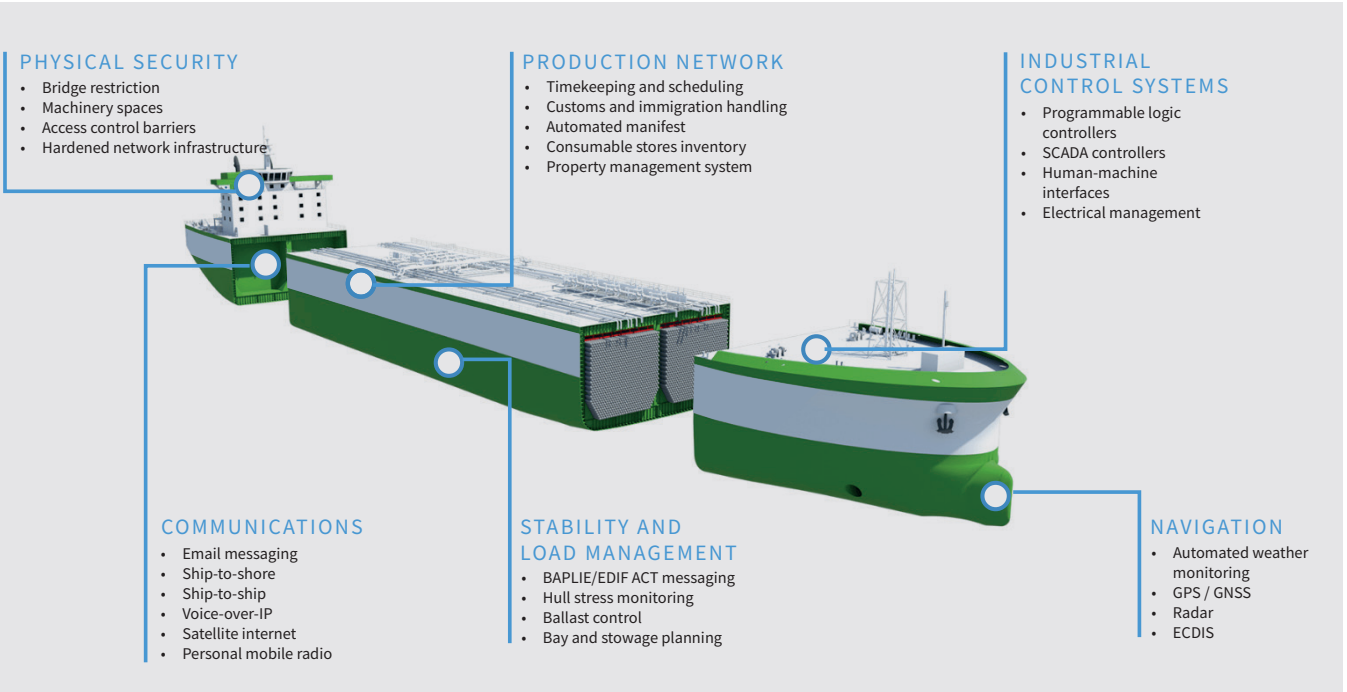
Most ships' systems use the same principles and architecture just described. This makes the interconnecting of different shipboard LANs, as well as the sharing of information and data between systems, technically straightforward. It also allows different HMIs to operate on different systems and to process different operations. Ultimately, it makes possible a higher level of data management that spans large geographical areas and connects to remote, land-based operation centres. This requires wide area network (WAN) technologies, offered by satellite technologies at sea, by mobile communication networks when within range in coastal navigation, and by Wi-Fi networks in port. All three depend on infrastructure provided by telecommunications service providers.

Then there's the Internet of Things (IoT), generally defined as the cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision (2). 'Things' are physical or virtual objects that can be identified and integrated into communication networks. Their interoperability is ensured by the exchange of data and information through gateways. This exchange can be wireline-based or wireless, with a large number of protocols existing for both media.

Given the clear benefits, it is no surprise that a number of shipowners have already invested in the external connection of shipboard systems. By remotely monitoring ships' data, as well as collecting data from ships' navigation systems and about fuel consumption, cargo and passengers, they have been able to provide feedback to the ships' crew and optimise operations. In addition, remote monitoring and diagnostics of machinery and complex shipboard systems by their original equipment manufacturers (OEMs) can ensure improved maintenance, the timely provision of software upgrades and 24/7 assistance in the event of failure. The cyber environment comprises the interconnected networks of both information technology (IT) and cyber-physical systems using SCADA computer-based and wireless systems. It also includes information, services, and social and business functions (3).

This environment is not limited to ships' systems. It extends to the shore-based activities of ships' operators and port facilities (4) and involves two main technology families: IT, where data is used for information; and operation technology (OT), where data is used for industrial processes.

In the past, access to data, information and the operation of processes was limited to the ships' personnel. In the new ICT environment consisting of interconnected internal systems that are also connected to external systems, that has all changed. Data access is now available at various levels and this poses new 'cyber risks'. These can be associated with the incorrect use or misuse of technologies and communications interference, as well as external attacks and intrusion aimed at harming assets, persons, systems or organisations. In this new cyber environment, security is a major concern.



Critical infrastructure protection: The US and European responses.

Governments worldwide take cyber risks and the threat they pose to public interests and security extremely seriously. The defence of critical infrastructure has become a priority and the maritime sector, along with other industries, is acknowledged as requiring appropriate protection.

On 12 February 2013, the US President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity (5). This was designed to establish a policy that would enhance the security and resilience of critical infrastructure in the US. The aim was to maintain a cyber environment that would encourage efficiency, innovation and economic prosperity, while promoting safety, security, business confidentiality, privacy and civil liberties.

The executive order called for the development of a voluntary, risk-based cyber security framework as a set of industry standards and best practice. The National Institute of Standards and Technology (NIST) issued such a framework (6) created by the government in collaboration with the private sector. It addresses cyber security risk in a cost-effective way based on business needs. The framework focuses on the use of business drivers to guide cyber security as an integrated part of an organisation's risk management processes.

The European Parliament and the Council of the European Union also issued an NIS Directive (7). This covers the measures needed to ensure a high common level of security among network and information systems across the EU, to improve the functioning of the internal market.

Both the US and EU programmes recognise that critical infrastructures make wide and increasing use of digital and communication technologies and so require defence. The water transport sector, encompassing port operations and seagoing traffic, is one of those critical infrastructures.

National cyber security programmes also aim to establish authorities that would be notified in the event of cyber incidents. These computer security incident response teams (CISRT) and computer emergency response teams (CERT) would have the technical and organisational capabilities to prevent, detect, respond to and mitigate network and information system incidents and risks.

The threat landscape.

Threats to the maritime sector's cyber environment can come from a range of sources, including:

Some cyber security guidelines.

Following the cyber security lifecycle outlined in the NIST cyber security framework, the International Maritime Organisation (IMO) issued Guidelines on Maritime Cyber Risk Management (8), recommending the following high-level actions.

Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to shipping operations.

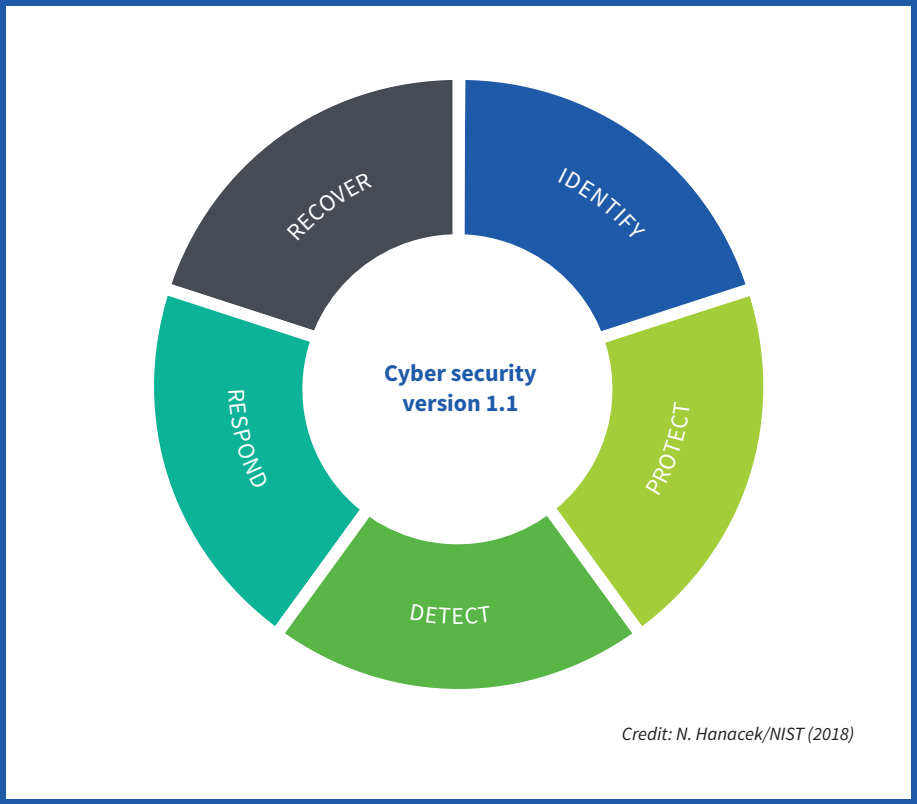
Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber event and ensure the continuity of shipping operations.

Detect: Develop and implement activities necessary to detect a cyber event in a timely manner.

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.

Recover: Identify measures to back-up and restore essential cyber systems impacted by a cyber event.

These activities form what the NIST calls the framework core and are common across all critical infrastructure sectors. Within this, organisations are free to create their own framework profiles. These identify and prioritise the organisation's own cyber security requirements, mission objectives, and the operating methodologies of their business environments. For example, the United States Coast Guard (USCG) developed a Cybersecurity Framework Profile (CFP) (9) for three maritime businesses: the Maritime Bulk Liquids Transfer (MBLT) mission area, the Offshore Operations, and the Passenger Vessel Operations. The mission objectives for each CFP make it possible to prioritise and allocate resources appropriately.



Credit: N. Hanacek/NIST (2018)

Identify: Revealing the vulnerabilities.

It is usual practice to adopt a risk assessment approach to identifying and quantifying potential cyber hazards.

Once a risk has been identified as unacceptable, the next task is to decide on the controls that will reduce or mitigate it. These controls may be across three possible categories: people, processes and technology. A technological solution may be the most appropriate. A process solution would change the way technology is used. A people solution ensures that personnel are trained to the necessary level of competence.

When the appropriate control is missing, whether it has been overlooked or not implemented, this is commonly defined as a vulnerability.

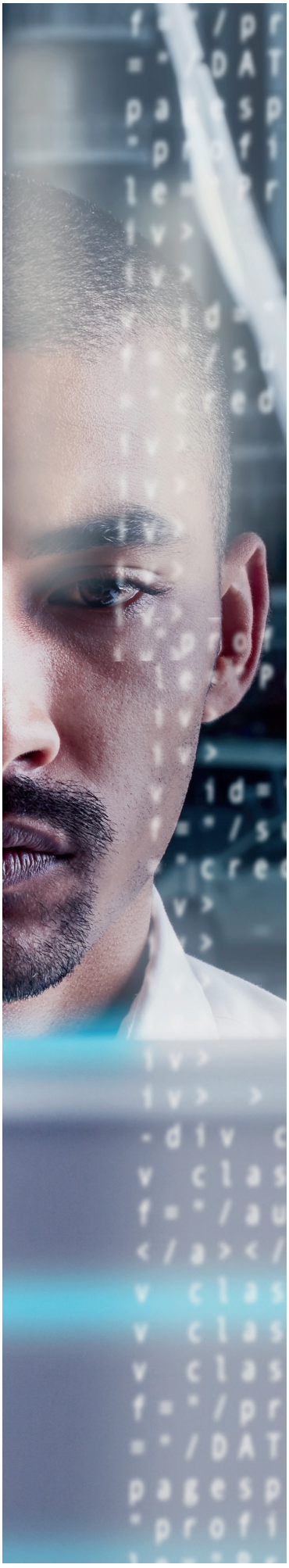
Take some examples from the maritime sector.

Studies in 2013 showed that navigation aids used at sea, such as Global Positioning System (GPS), Automatic Identification System (AIS), and Electronic Chart Display and Information System (ECDIS), represent significant vulnerabilities in a ship's cyber security posture.

With its lack of any inbuilt mechanism to encrypt or authenticate signals, AIS is easy for an attacker to exploit. In 2013, Trend Micro2, a cyber security firm, showed that they could compromise AIS by making 'phantom' vessels or structures appear, staging fake emergencies, and obfuscating the ship's actual location on the maps. They were even able to mislead the online services that monitor AIS data to track vessel positions.

ECDIS systems need periodic map updates and sometimes rely on physical access through a USB key to load them. It is easy to imagine a user inadvertently spreading malware that would give an attacker access to the underlying operating system. Needless to say, a number of these navigation systems are configured to operate with administrator rights and have no password protection.

GPS systems, like AIS systems, are not encrypted or authenticated, and offer an easy entry point for an attacker. Earlier in 2013, researchers at the University of Texas were able to demonstrate how they could send a superyacht off course by generating a fake GPS signal that overlaid the genuine one.



Protect: Creating appropriate defences.

As the proliferation of cyber-attacks in 2017 shows, the cyber threat landscape is complex and constantly changing.

In response, marine and offshore organisations need a much more strategic approach to protecting their critical assets and business drivers. This means deploying comprehensive and multilayered defences that are risk-based and threat-intelligence-led. It's the only way to build security approaches that are secure and scalable. The role of people and processes also needs consideration (not just the technology) in the face of increasingly complex challenges.

Various approaches can reduce the exposure of interconnected systems to common and sophisticated cyber-attacks.

As a general principle, the best starting point is to identify what ultimately needs protection, then design suitable perimeter security.

> Everything is hackable and no defence mechanism is 100% secure. So, don't attempt to build an 'impregnable fortress'. Rather, aim to develop effective security defences around the critical business and supporting infrastructure. And, since cyber threats are constantly evolving, make those network defences flexible enough to meet future needs.

The traditional approach: Perimeter security

The traditional first-line of defence is usually a firewall. This is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined rules. Traditional firewalls are binary solutions. Traffic is allowed in or it is blocked.

These devices have evolved. The next-generation firewall can include application control, identity awareness and other capabilities – such as intrusion prevention systems (IPSs), web filtering, and advanced malware detection – from the same appliance.

The IPS, as part of a next-generation firewall or as a separate device, is another important perimeter defence mechanism. It is an in-line device that blocks malicious traffic and, when properly optimised and monitored, is a valuable tool for catching attackers who have slipped past a firewall.

The increasing popularity of cloud computing has led to the development of new protection services, such as cloud-based malware detection and Distribute Denial of Services (DDoS). Unlike appliance-based solutions, these cloud-based services sit outside the architecture and analyse traffic before it hits the network.

These perimeter-based defences all assume that everything in the internal network can be trusted. They therefore deploy countermeasures at predefined entry points.

That assumption is no longer valid in the maritime sector. Onboard wireless technologies, the proliferation of partner connections and the need to facilitate interaction between headquarters and vessels all blur the internal/external distinction. And insiders, malicious or just careless, may present a very real security threat that perimeter defences could never detect.

The new model: Zero Trust security

Originally conceived by John Kindervag and presented by Forrester Research, Zero Trust addresses the shortcomings of perimeter-centric strategies by removing the assumption of trust from the equation (10).

Its guiding principle is 'never trust, always verify'.

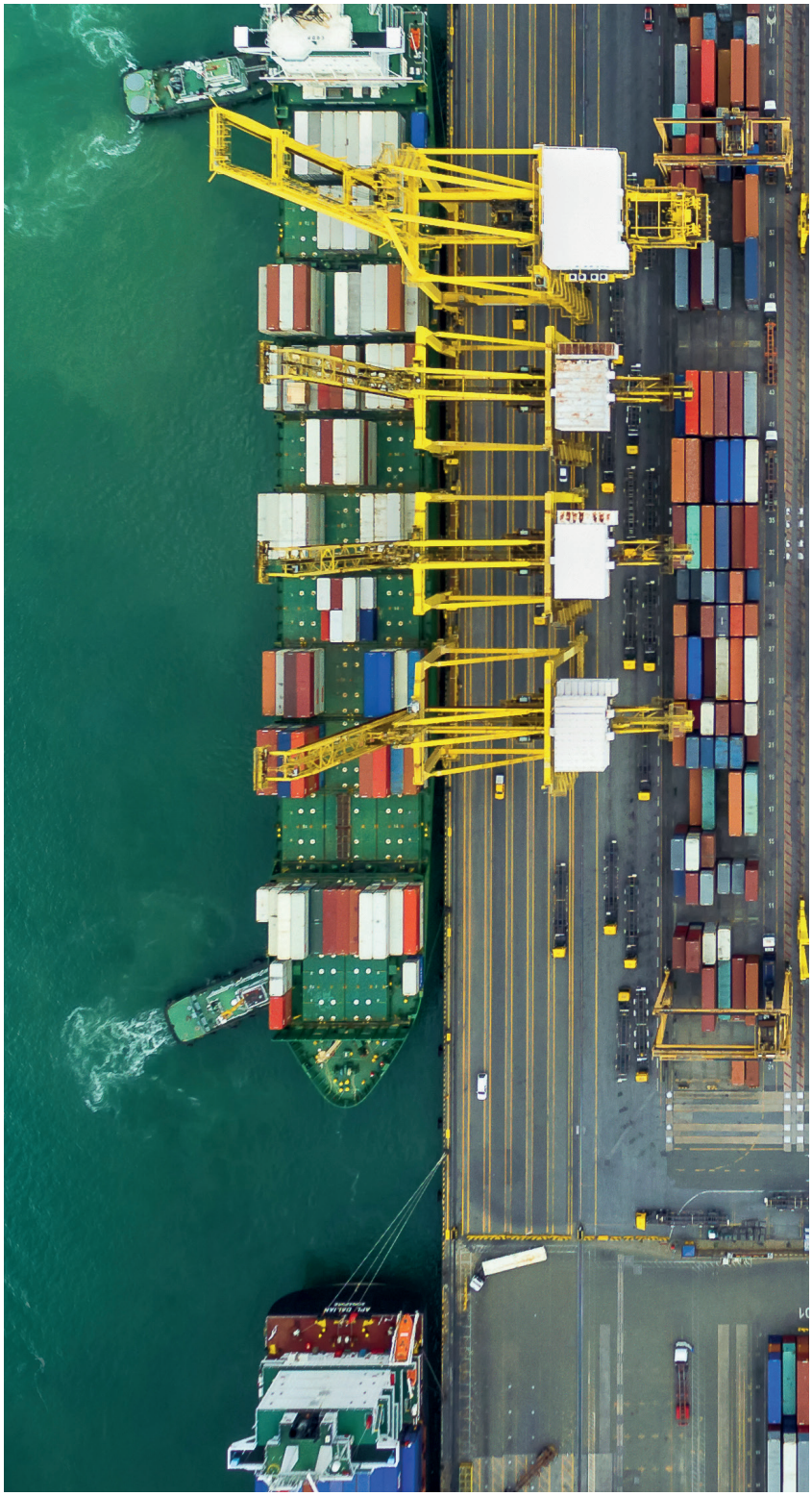
This means deploying the essential security capabilities in a different way. Its aim is to provide policy enforcement and protection for all users, devices, applications and data resources (onshore and onboard), as well as for the communications traffic between headquarters, vessels, providers and port authorities, regardless of location and user roles.

The basic concepts behind the Zero Trust approach are:

Concept #1: Ensure that all resources are accessed securely regardless of location.
This is not just a question of effective network segregation. It requires the increased use of secure access for communication between resources, even when sessions are confined to an 'internal' network, whether onboard or headquarter-based. It also means only allowing network access to devices with the right status and settings. When it comes to navigation systems such as the ECDIS (which is accessible through a USB stick), an online chart update, or other electronic onboard systems, a well-thought-out access control policy covering all connected systems and the ship-to-shore interface becomes increasingly important. And this should be extended to the various actors in the marine supply chain.

Concept #2: Adopt a least-privilege strategy and strictly enforce access control.
Minimising permitted access reduces the pathways available for malware and attackers. That helps to prevent them gaining access, then spreading laterally and/or infiltrating sensitive data. Lateral movement, phishing attacks and other commonly successful cyber threat vectors are less effective, if not completely blocked, under the Zero Trust model.

Concept #3: Actively inspect and log all traffic.
A range of tools can be used for traffic inspection. These include network discovery tools for finding and tracking assets, flow data analysis tools to analyse traffic patterns and user behaviour, and network forensic tools to assist with incident response and criminal investigations.



Detect: Recognising a cyber incident.

All organisations that store clients' personal and financial data have a legal obligation to record and declare cyber security breaches. Since May 2018, the General Data Protection Regulation (GDPR) has required security breaches involving others' data to be reported to the authorities within 72 hours. Fines for failing to do so may amount to 4% of worldwide turnover or up to €20 million.

Early detection, however, is challenging. In fact, it is not uncommon for successful cyber-attacks to remain undetected for six months or even longer. And attackers are constantly searching for new vulnerabilities in evolving digital environments.

Intrusion detection tools

Deploying intrusion detection tools can be highly effective in the early detection of threats, the control of breaches and the mitigation of damage.

These tools are software or hardware products that can identify active threats and generate alerts to prompt remedial action.

Many different products exist in the market, from open source tools to commercial packages. Some are also able to detect advanced, targeted attacks.

A first category is based on rules and signatures.

Rules and signature-based detection systems

These systems identify threats, such as intrusions and viruses, by performing a network traffic inspection to look for signatures, or patterns of events, that match documented attacks. A second category is based on the analysis of the attack and normal behaviour.

Behaviour-based detection systems

On the assumption that attack behaviour differs from normal activity, malicious actions can be identified by detecting anomalies in user or system behaviour. One advantage of these systems is that they can identify advanced, targeted attacks without having to recognise their signatures.

The challenge of advanced attacks

Advanced, targeted attacks are very different from the more opportunistic kind. Advanced attackers possess the ability, and the willingness, to dwell in the targeted network in order to learn how best to exploit it. They are motivated and well-resourced, and will use techniques such as social engineering and zero-day exploits to infiltrate enterprise networks and compromise the network infrastructure or IoT devices. Once inside, they can use the exploited entry point as a pivot to go deeper into the network in a process called 'lateral spread'.

The detection of such attacks requires event correlation over time and from multiple sources. This technique analyses 'attack metadata', the indicators attackers inevitably leave as they exploit a network, even if they have penetrated the first-line of defence.

All cyber-attacks follow the same basic pattern: infiltrate, establish command and control, move laterally and exfiltrate data. Various events can be correlated with these different stages. Failed login attempts are a common sign of infiltration; unusual utilisation of resources and the execution of unknown processes are indicators of the 'command and control' stage; increased network traffic from a particular host can be associated with the exfiltration of data. Logging and inspecting these 'attack metadata' over hours, days or months can detect the onset of sophisticated cyber-attacks, especially with recent advances in analytics technology.

Behavioural and predictive analytics tools use metadata as an input feed to estimate the location of the threats, making in-depth investigation more focused and accelerating the process of discovery. They significantly enhance the detection capabilities of any cyber-defence strategy.

Respond and recover: Limiting the impact of cyber incidents.

Having an incident response plan in place is a clear legal requirement. Under the EU's GDPR (11), which came into force in May 2018, organisations holding data from EU subjects need an effective plan they can implement in the event of a data breach, to contain any damage and prevent future incidents.

The Cyber Security Incident Response Guide from *CREST* (12) provides valuable advice on preparing for, responding to and following up any incident in a fast and effective manner. It helps organisations to determine what a cyber security incident means and to build capability for an appropriate response.

If you decide to delegate the implementation of your incident response plan to a third party, the guide also offers advice on selecting a suitable supplier. There are clear benefits of using experts from commercial suppliers, as they will have specialist skills and well-defined processes in place to effectively respond to and manage security incidents.

After any cyber security incident, action must be taken to limit damage to the organisation and to return operations to normal. This should include an assessment of what caused the incident and how effectively it was managed, as well as a consideration of the best way to communicate the lessons learnt.

Fundamental to the respond and recover phase are the following actions:

CONTAIN THE THREAT

to prevent it from spreading laterally within the targeted network.

INVESTIGATE

to identify the size of the breach and the systems affected and to establish how the threat actor managed to exploit the network.

RECOVER

by restoring data and operations.

REPORT

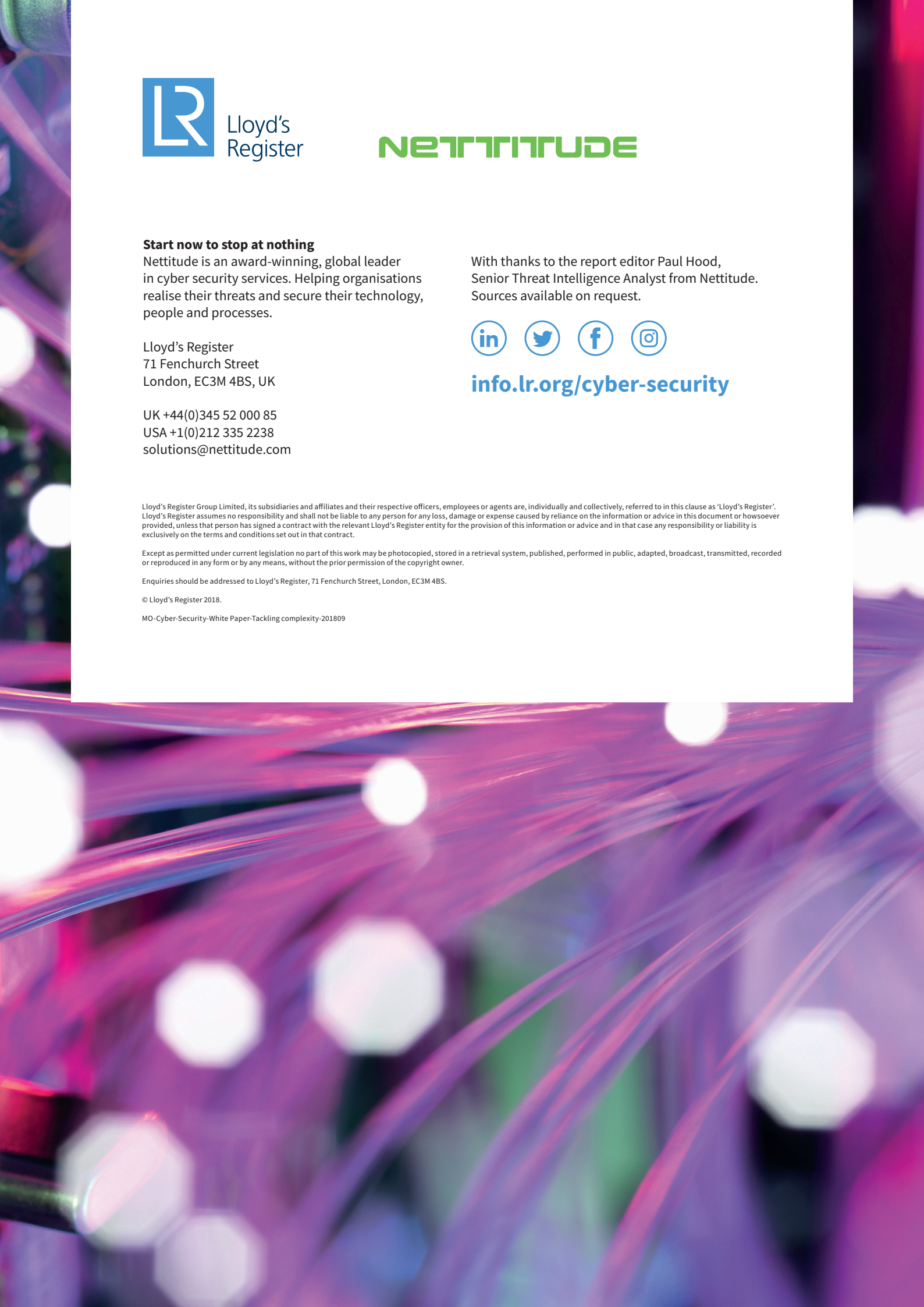
the incident and alert the wider cyber community by sharing threat data with law enforcement and other shipping companies.

Conclusion.

Cyber-attacks are becoming increasingly complex, and interconnected technologies are significantly expanding the threat surface. As a result, organisations are far more exposed and at risk. Directing the appropriate security focus to critical business drivers and assets is of vital importance. No business can make itself impregnable. What it can do, however, is seek to temper any attack on its critical business drivers by creating a scalable security posture – based on risk and driven by threat intelligence – and applying the correct security controls and technologies. It is then in a position to assure its board and its shareholders that, should a breach occur, the adverse effects can be mitigated, and any disruption and loss to the business minimised.

REFERENCES

(1) Lloyd's Register, 'Global Marine Technology Trend 2030', 2015.
(2) ENISA, 'Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures', November 2017.
(3) IET Standards, 'Code of Practice: Cyber Security for Ships', The Institution of Engineering and Technology, London, United Kingdom, 2017.
(4) IET Standards, 'Code of Practice: Cyber Security for Ports and Port Systems', The Institution of Engineering and Technology, London, United Kingdom, 2016.
(5) The White House, 'Executive Order 13636: Improving Critical Infrastructure Cybersecurity', 12 February 2013.
(6) National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity'.
(7) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
(8) International Maritime Organization, 'MSC-FAL.1/Circ. 3', 5 July 2017.
(9) US Coast Guard, 'Maritime Bulk Liquids Transfer, Offshore Operations, and Passenger Vessel Cybersecurity Framework Profiles', version 3, December 2017.
(10) NIST, 'Critical Infrastructure Cybersecurity', Forrester Research, Inc., Cambridge (MA), 2013.
(11) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),
(12) CREST (GB), 'Cyber Security Incident Response Guide', 2013.



Start now to stop at nothing
Nettitude is an award-winning, global leader in cyber security services. Helping organisations realise their threats and secure their technology, people and processes.

Lloyd's Register
71 Fenchurch Street
London, EC3M 4BS, UK

UK +44(0)345 52 000 85
USA +1(0)212 335 2238
solutions@nettitude.com

With thanks to the report editor Paul Hood, Senior Threat Intelligence Analyst from Nettitude. Sources available on request.

info.lr.org/cyber-security

MO-Cyber-Security-White Paper-Tackling complexity-201809