STEPHENSON HARWOOD

Cyber Risk

A Joint Hull Committee paper in conjunction with Stephenson Harwood

September 2015

Joint Hull committee

Contents

Executive summary

An evolving issue
There is no single answer to the question of cyber exposure and the meaning of cyber as an issue is often misunderstood. Leaving aside the Iranian centrifuges sabotaged at the design stage, the only proven physical damage loss triggered by cyber to date has been at a German smelting plant which was damaged when a safety device was disabled.

No identified systemic risk to ships
The risk of a loss to a ship as a result of cyber disruption is foreseeable, but is not yet a reality. A systemic threat which could conceivably result in multiple losses on a scale which might impact the solvency of the world's insurers and reinsurers does not yet exist. For example, even if electronic navigation systems were disabled, a ship would still be able to manoeuvre and could either anchor or navigate using more traditional means (provided that the skills to do so exist on board). There is time for owners and operators to plan and ensure that computer systems on board ship and ashore are as secure as is reasonably practicable.

Growing exposure
Ships are mostly isolated units but as shipping embraces information technology, it becomes exposed to cyber risks some aspects of which are already well known in retail and banking. As the International Maritime Organisation's E-Nav programme gains momentum, the technologies required, as well as the aligned commercial demands of an ever more interconnected world, will increase the exposure to loss as a result of a cyber attack or intrusion.

Specialised vulnerability
This report argues that the risk of loss or damage caused to or by a ship as a direct result of cybercrime is currently low for bulk or general cargo shipping, but higher for specialised or technically advanced ships engaged in oil and gas exploration and exploitation by reason of remote systems access and the potential vulnerability of Dynamic Positioning.

Defence in depth
The defences against cyberattacks fall into two broad categories: People based, and design based. People based defences are generally easier to implement, unless the design defences can be incorporated at build. The concept is that multiple defences from both categories should be deployed to offer defence in depth. There is no single solution to the security problem.

Guidance for Underwriters
The report includes some guidance suggestions on cyber risk assessment which underwriters may wish to share with shipowners in an attempt to manage the risk.

JH2015/005

JHC Cyber Risk Assessment Guidance

Background checks:

1 Cyber security should be owned at Board level within the company, and there should be a demonstration of commitment to employees from the highest levels of the company to effective cyber security.

2 The company should have carried out a thorough threat assessment, contemplating the following;

2.1 The current level of actual or attempted security breaches recorded by the IT Manager

2.2 The current level of compliance with internal controls linked to the use of computer systems

2.3 The current level of compliance with international security standards (ISO 27001/2, NERC 1300, ISA/IEC-62443.)

2.4 The current level of compliance with the Critical Security Controls promoted by the Council on Cyber Security

2.5 The company's current reputation on social media.

3 The company should have established a coherent IT policy describing how IT will be used on board ship, and how it will be structured and supported.

4 The company should be able to provide a rationale for the design and arrangement of on board systems in the context of the Critical Security Controls.

5 The company should be able to demonstrate links between recruitment, training and vetting policies for sea staff and the company security policy as it relates to cyber security.

Control checks:

6 There should be clear links between ISM, ISPS and cyber security measures on board. Cyber security on board should be included in the scope of internal ISM/ISPS audits. The security measures should be fit for purpose and contemplate;

6.1 The age, vulnerabilities and arrangement of electronic equipment on board

6.2 The implementation of IT security policies and procedures

6.3 An acceptable use policy for the use of shipboard IT for social or recreational purposes

6.4 A social media policy for crew members.

7 If the company is not in compliance with an acceptable external standard, there must be an achievable action plan in place to achieve compliance within the policy year.

8 There should be sufficiently qualified and experienced people on board to implement the control measures that mitigate cyber risk.

9 The company should be able to demonstrate that it has assessed the cyber risk controls of sub-contractors and others in the supply chain that might impinge upon the risk on board ship.

10 The company should be able to demonstrate that his assessed the personnel vetting standards of sub-contractors and partners placing people on board ship.

11 The company should be able to provide a written security declaration from telecommunications providers on board.

Part 1 - The Anatomy of a cyberattack

Most of the current understanding of cybercrime operations is drawn from the lessons learned from attacks on enterprises of all sizes over the past 20 years. The hazards, risks and consequences to enterprises of all sizes are very poorly understood, and the current debate about the vulnerabilities of shipping has flowed from this discourse. The risk may be foreseeable but unquantified.

Because of the current limited level of technical sophistication on board, the modern ship may not yet be a tempting target for the cybercriminal in a way that puts the hull, machinery or cargo at direct risk of loss or damage. That does not mean to say that there is presently no scope for mischief or loss.

The rate of technical change, and the general desire by people to be more interconnected, and for business processes to be automated in the background, means that ship's systems are becoming increasingly interconnected on board, and those connections reach out in real time to the shore. As such the risk of loss or damage to ship, cargo or machinery is becoming more credible. The hacker employs three fundamental techniques that could be used in combination to target a ship:

"Social engineering", which is the ability to impersonate an employee, supervisor, maintenance engineer or customer over the telephone to dupe unwitting employees into handing over information.

"Brute force", which is the use of commonly available and easy to use software tools to identify targets and attack them. These tools use a general problem solving technique of identifying all of the possible encryption options and trying each one in sequence, and very rapidly.

Technical intrusions, which are the exploitation of deficiencies in system design, configuration, or management.

An attack on a ship could be mounted from ashore (the "outside") and intended to overcome defences in place, or from the "inside", where a person in a position of trust either on board or within the company office is induced to assist the criminal, either for gain or under some form of duress. The second "insider" scenario is more likely, and should not be confused with a social engineering technique used upon someone with no intention of assisting a criminal.

An attack is a three staged process that takes place over a period of days, or perhaps even weeks. The stages are Reconnaissance, Identification and Execution. The process is not clear cut, each stage may blend into the next and the attack might be iterative in nature; the attacker will move back and fore between Reconnaissance and Identification before deciding to strike. Figure 1 below illustrates the hierarchy and sequence of the stages.

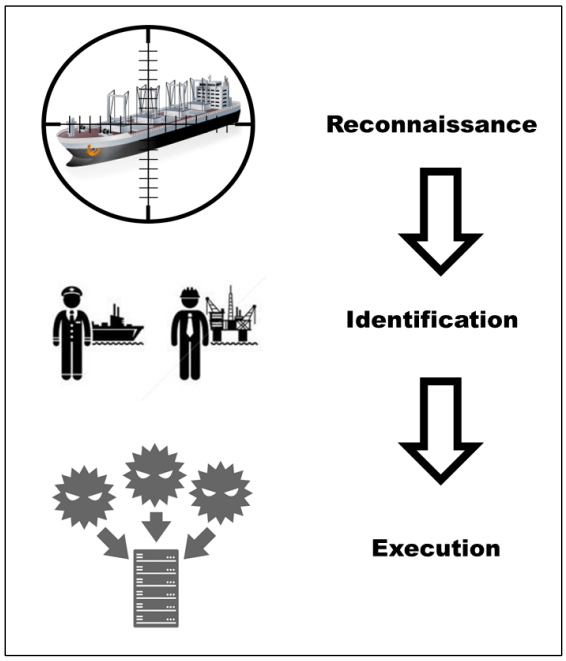

Figure 1: The three stages of a cyber-attack

Stage 1: Reconnaissance

Reconnaissance takes place over time, and is a process of acquiring information and intelligence about the target. Much of the initial information gathered is from open sources (OSINT). The kind of information sought could relate to the design of the target ship, the equipment specification, how authorised users interact with the equipment, how email addresses are assigned, any kind of encryption in use on email accounts, and the relationship between the internet and the intranet on board. There is a lot of OSINT available. Even source code attached to company websites, buried under HTML comment tags, can assist the attacker.

Related to OSINT is information in the public domain supplied via or by people; HUMINT. HUMINT is available from social media, specialised forums, professional publications and conferences.

The hacker can use anonymisers[1], metasearch engines[2], and DNS lookup utilities[3] to discover more information placed on line by key employees and /or crew members, some of which might reveal valuable clues as to the pattern of life on board, ship movements or procedures. IT administrators frequently go to bulletin boards when troubleshooting, and all of those discussions will have been recorded and be publicly accessible. Facebook and other social media platforms are a well-used source of HUMINT.

Finally, and armed with a wealth of information gathered freely from the public domain, the hacker will use some simple software tools to test the operation of the network. These tools scan and test the traffic moving in and out of the target company and to and from the ship, and these movements can say much about the disposition and configuration of security measures such as firewalls. This information will offer the hacker some choices as to where an attack should be made, and how. For example, when moving to the Identification stage, this

[1] Software tools that mask the identity or location of an intruder.
[2] Akin to browser search engines, these tools cast a much wider net.
[3] These tools identify computers and their addresses by exploiting information contained in website coding.

information can facilitate the stealing of passwords, the authentication of false email accounts and redirection of website traffic.

Stage 2: Identification

Stage 2 involves a more active probing or interaction with the target ship. The potential attack is now detectable and preventable, if countermeasures and procedures are sufficiently effective.

It may well be the case that the hacker contacts the company, or the ship, in an attempt to gain information or access to plan the attack. This is known as social engineering. Typical approaches might be to contact the system administrator on board (probably a junior deck officer, or on a larger ship the Electro Technical Officer) and pose as a user who cannot get access to his or her system, particularly if a company system is extended to trusted suppliers, like agents or stevedores.

These approaches can be bold. Using intimidation, or by seeking sympathy, the hacker might impersonate a client, passenger, crew member or manager over the telephone or by disguised email and coerce the administrator or the Helpdesk to pass on information, such as usernames or passwords or reset a password or username, or pass on an IP address or passcode. Other techniques, such as phishing[4] or spear phishing[5], can also obtain such information.

Impersonation by the hacker can be assisted using identity information garnered from the internet or simply from discarded documents, or by simply reading emails or security passes on public transport.

The hacker will also use software tools to scan the target network to discover IP addresses and open ports. Lapses in IT security, such as the registration of new, unsecured devices on the company network, will be detected and these devices will be targeted as recipients for spyware or backdoors for future use.

Brute force techniques, such as password guessing or password cracking are commonly employed. Password guessing is quick when used to check short passwords, but for longer passwords other methods such as the dictionary attack are used, because of the time a brute force search takes. Password cracking is the process of discovering password data stored in the target system. This can be done by manually guessing, or automating the process.

Stage 3: Execution

This is the process of identifying a valid user account or a poorly defended element of the network. Entering the target system will disclose the fact of the attack to an alert defender, but the competent hacker will cover their tracks by modifying the system log files and any record of their visit. When a hacker discovers a valid user account, brute force will be used to uncover the password if this has not been obtained by other means.

Once identified, the hacker can then fulfil the purpose of the attack. This may be either to access the system, copy large amounts of data and leave, or destroy large amounts of data and leave a calling card, or to plant a trojan or other malware to allow for continued and covert exploitation or use of the target system, extending as far as reconfiguring elements of the system to retain control and resist defences.

[4] Typically an unexpected email, broadcast widely, inviting the recipient to provide information by reply, or open an attachment.
[5] Similar to phishing, but directed at a specific internet user.

The insider attack is broadly similar in execution. Rather than look for unintended lapses (revealing information via eavesdropping on bulletin boards or other correspondence), the reconnaissance may flag up an employee willing to assist with the attack, or discover an opportunity to plant an accomplice in the office or on board. The motivation for assisting the hacker might be duress, financial gain or to further a grievance.

The insider may not be employed by the target company, or on the ship itself, but could be from a key supplier like a stevedore or agent with some access to the ship's systems. Specialist ships attending oil and gas fields may have hundreds of workers on board from a variety of employers, and some will be self-employed. Anybody could be an insider.

At the execution stage the insider can be used as a mule to transfer the malware via physical media such as a USB stick, or CD. It may be delivered as an attachment to an email, to be opened by the insider.

The extent of the involvement of the insider will depend upon the dynamic of the particular attack. However, the insider risk is probably the most significant when considering the construction of defences.

The insider risk extends to the careless or even reckless use of IT systems by employees, perhaps without criminal intent, but certainly without regard for the security implications. Such lapses will be detected by the hacker lying in wait, and will be exploited.

Part 2 – Defences

Ship control systems may be powered by a computer or microchip, but they are not interconnected or connected to the outside world. This does not mean that the systems currently in use are not vulnerable. Some are fitted with a modem, a communications port or a USB port. These are provided for maintenance purposes, and can provide a means of attack or damage. The causes could either be malicious (the insider attack) or negligence (poor procedures on board).

This section explores in detail the two categories of defence, technical and procedural. The first relates to system design, equipment resilience and the way that systems are interconnected. The second involves issues such as work processes and procedures, people management policies, security procedures and access controls. The two types of defence do not operate in isolation and are interdependent. The concept of an effective defence is that of depth; the integration of technical and procedural defences delivers a resilient system that can detect and defeat attack.

The list below is not exhaustive, but is prioritised from the industry standard critical controls to focus upon shipboard systems. The full text of the 20 standard Critical Security Controls are promulgated in the UK by the Centre for the Protection of National Infrastructure and in the USA by the SANS Institute.

Technical defences

1 *Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers*. Hackers can exploit well known weaknesses in operating systems intended for networking or maintenance. Accordingly, a secured system has the user profiles locked into a particular configuration that allows for legitimate use, but does not permit users to, for example, download or run executable files, or to make changes to the way in which the device or equipment communicates across a network.

2 *Secure configurations for network devices such as firewalls, routers, and switches.* Hackers can exploit the software routines widely used in devices that route data around the network. Secure configurations prohibit the connection of unauthorised devices, and change the generic password types to more secure structures.

3 *Malware defences.* These are automated tools that continuously monitor workstations, servers, and mobile devices. When malware is detected, the tools report the occurrence to IT administrators. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers. Anti-malware software should be installed that is ideally automatically updated with the latest definitions of malware. Computer systems should be designed to automatically conduct a scan of all removable media[6] when inserted to detect malware. Malware defences also scan and block all e-mail attachments entering the e-mail gateway if they contain malicious code or file types.

4 *Application software security (patch control).* Any software in general use, such as word processors, web browsers and operating systems become the subject of examination and experiment by hackers looking for a weakness to exploit with malicious code of some kind. The software producer and the hacker are therefore engaged in a struggle for security. Insecure software is commercially unviable, and so companies like Microsoft invest a great deal of money in making sure that their products are secure. Where vulnerabilities are identified,

[6] This includes USB memory cards, cameras, tablets and Dictaphones.

software producers release updates, or patches, to fix the issue. End users should have a means of identifying the latest patches and ensuring they are installed.

5 *Wireless access control.* This is a software solution that allows administrators to control access to the network by wireless devices, and to control the degree of access permitted to particular users based upon their password and the ability of the software to recognise the device being logged in. In practical terms, this allows the administrator to limit access for junior users and guests.

6 *Data recovery capability*. This is a means of having more than one copy of the data contained in the system, in a way that makes sure that the copy is updated from the live system in real time, and that the copy is in a secure, physically remote position. If the system is attacked or otherwise damaged so that critical data is damaged or destroyed, the disaster recovery copy can be used to restore the live system as quickly as possible. Remember that one way to damage a system is to change it to allow subsequent attacks, and so an authoritative and clean copy of the data and configuration files is essential. On a large system this can take hours. System resilience is not possible without a disaster recovery mechanism.

7 *Limitation and control of network ports, protocols, and services.* A hacker will be looking for remotely accessible network ports or services as a means to gain entry into the system. Some of these ports or services are installed by default at manufacture and in normal circumstances lie dormant and invisible to the user. Access routes that are not essential for the operation of the system should be identified and closed off.

8 *Secure network engineering.* The system should be designed so that the system architecture is zoned. An inner zone, most secure, should host critical ship systems for propulsion and control. The automation software resides here. Outside this zone sits another technical zone, typically containing the navigation network and other advisory systems. Outside this zone sits the ship intranet with low risk applications such as web browsing available to crew and passengers. The zones are partitioned with firewalls. A threat to secure networks is a requirement to add on or modify the network post build, and so a well operated network will guard against any unintentional breaches caused by such modifications.

9 *Physical security of critical hardware and cable runs.* The internal spaces inside a ship are complex and interconnected. Equipment is stored in places that are away from areas normally used by the crew as they go about their daily work. Cable runs can extend to every point of the ship. Critical equipment and cable runs should be physically protected from interference by concealment or physical security, i.e. locked compartments subject to strict access controls. This measure is one of the touch points with the existing Ship Security Plan, a statutory requirement under SOLAS Chapter XI-2.

Procedural Defences

Procedural defences are also defined by the CPNI and the SANS institute. The selected issues are considered to be the highest priority for shipboard application. In general terms, the "host document" on board for these defences should be the Ship Security Plan, a confidential document mandated under SOLAS Chapter XI-2. Additionally, the procedural issues described will map across into the International Safety Management Code Safety Management System on board, and into company HR and IT procedures.

1 *Access control on board.* The Ship Security Plan will already call for access control measures, such as proof of identity at the gangway, visitor passes, visitor escort, and the identification and securing off unattended spaces which should include spaces containing IT equipment. These requirements can break down when "trusted" people are on board, such as maintenance engineers, agents or port officials. Small crews and busy turnarounds can make escort and supervision duties a challenge. Alternatively, on a large passenger ship the number of people moving around the ship can cause some confusion. Extra vigilance is called for when any visitor requires or requests access to a technical space or the ship's IT equipment.

2 *Security skills training appropriate to job description*. The Ship Security Plan calls for one senior officer to be appointed as the Ship Security Officer. His post can only be held by an officer suitably qualified, and this qualification is mandated under the Standards, Training and Certification for Watchkeepers Convention. This training did not contemplate the particular demands of cyber security. On larger, more technically complex ships it may be the case than an Electro Technical Officer is assigned the role of system administrator. This is a responsible post and although no mandatory training might be called for, the system administrator should be trained and qualified to keep the system efficient and safe.

3 *Controlled use of administrative privileges and passwords.* Systems in shared use often have a shared password, which is very porous (especially if the password is "password"). Computer configurations should be set up so that password syntax is robust, containing at least 8 characters of which a number, an uppercase character and a special character are present. Passwords should ideally be assigned to individuals and changed regularly. Assigning passwords to individuals allows for fine tuning of access controls.

4 *Physical media controls and policies.* One of the greatest risks to system security is the accidental infection of a computer or system with worms, trojans or other malware present on physical media such as USB sticks. A recent examination conducted by the writer of a number of bridge and cargo office PC's on board several large cargo ships revealed the presence of Potentially Unwanted Programmes, or PUPs. The use of unencrypted and unscanned physical media should be prohibited. If it is necessary to receive information from the shore in this format, a "dirty" or quarantine standalone PC should be used as a gatekeeper to the system.

5 *Employee vetting.* One of the easiest ways to place an insider is to have them hired by the target organisation. For example, whilst large container ships operated by lines use crews from a trusted or in-house source, many ships engaged in oil and gas can have hundreds of workers on board, the identities of whom have to be taken at face value. Proper vetting, requiring the production of original documents before hire, references and background checks, should be considered prior to placing anyone in a position of trust.

Unintentional Defences

There are three common characteristics of computer driven systems currently fitted to modern ships that when combined, serve as an unintentional defence. Whilst this is, in the absence of a more structured approach, welcome news to ship operators, charterers and underwriters, a reliance on these three factors will prove to be unwise in the medium to longer term as systems become more sophisticated, interconnected and vulnerable. The three unintentional defence factors are;

- The stand-alone nature of ship systems and limited ship to shore broadband connections, and the defences that generally surround satellite systems. This makes it difficult for the average hacker to employ conventional brute force attacks with readily available tools.
- Even if the hacker could penetrate the ship systems via the broadband connection, the equipment that controls critical systems is not connected to the communications system, or organised on board across a Local Area Network.
- The time and effort required to attack a vulnerable ship or platform at present would probably not be for gain because the risk and effort is not matched by the reward. That level of investment might be more attractive to a hacktivist motivated socially or politically. Hacktivism requires media attention to provide the right reward. Much trade, exploration and exploitation goes on beyond the easy reach of broadcast media and so even for hacktivists, the effort may not be worthwhile.

Demonstrating Due Diligence

However hard an enterprise works to mitigate a risk, it is inevitable that either through some unforeseen circumstance, or the negligence of an individual, a loss will occur. An insurance policy will increasingly require a demonstration of active and ongoing due diligence by the Assured if it is to respond in the way that the parties intended at inception.

Part 3 – The Assessment of Risk

It is a challenge for those with management responsibility for the safety of ships and crews to accurately assess the risks and consequences of a cyber attack, particularly if they do not have a strong technical background in the subject or their company does not have extensive in-house resources. Any assessment of risk is a subjective assessment. If the assessment is faulty, efforts at mitigation are likely to be misdirected. Assessing the risk of a cyber attack is the first and most fundamental step towards devising and providing the most appropriate defences. Appropriate in this case means effective and representing good value for money.

The procedures which are hopefully already employed within the company for safety or financial risk assessment will be sufficient to assess cyber risk, but there are two important differences in which cyber risk assessment differs from other, more conventional risks. Firstly, there is no claims history to rely upon, no catalogue of incidents that might inform the vigilant as to where and how the security system might fail. Secondly, there is at present a culture of non-reporting by companies who have suffered from a security breach. The reasons for such secrecy are obvious; the company feels that the reputational damage of a security breach would be too damaging.

A risk assessment should also examine the likely consequences, and attaching a cost to these consequences is often used as a ranking or prioritising method.

In a recent case, an ingenious piece of malware, dubbed "The Phantom Menace", was injected into the computer systems of oil brokers across Europe by a seemingly innocuous email attachment using a PDF, previously felt to be safe. The aim of the malware was to identify and obtain legitimate documentation used to buy and sell Bonny Light Crude on the commodities market. This documentation would be used to initiate a sale of oil which did not in fact exist. In a strange twist, although the likely perpetrator has been identified the lack of a complaint from anyone who may have been swindled means that the authorities are powerless to act.

Assessing marine cyber security risks requires a return to first principles, because there is not enough shared experience in shipping upon which to base any further reasoning. The most likely outcome is disruption to the business and loss of time and thus money.

Any use of computers to store, process or share information is vulnerable to attack which could cause loss of data, theft of data, denial of service or disruption of service. Any of these outcomes will have financial and reputational consequences either directly or indirectly.

The Variety of Threats

The assessment of hazard must also recognise the particular threat facing particular enterprises or activities. The motivation of the attacker is a useful indicator of the particular threat, and to an extent the type of attack that might be employed. Activities involving assets of significant value, be they physical or otherwise, will attract the attention of thieves. Activities that are linked to high profile and controversial enterprises, such as Arctic or deep water drilling, may attract the attention of hacktivists. Activities furthering the particular aims of a state or other political entity may attract the attention of hacktivists or state "sponsored" organised criminals taking up a cause. Enterprises new to a particular activity may attract the attention of criminals employed for anti-competitive reasons. The list is longer, but the key skill for the responsible manager is to see the enterprise as others see it.

The style of the attack can be inferred by motivation. Would success for the criminal be theft, disruption or destruction? Accordingly, would the attack be long term, sophisticated and covert or a crude denial of service?

Threat assessment and analytics is another area where a large number of products and providers have come to market, with some being more effective than others. It is important to carry out threat intelligence assessments, but even more important to use those assessments effectively.

Cybercrime differs from conventional crime in a particular respect. Because the target is usually data of some kind, and data is shared between organisations, the effects of a cyberattack can cascade across a sector, supply chain or a trade. Any risk assessment must therefore examine the way in which the ship, and the company, interacts with key suppliers, providers or partners. In practical terms that might mean a bunker supplier, a terminal operator or a partner in a vessel sharing agreement.

The presence of computers or computerised systems on board does not automatically trigger the risk of physical loss or damage to a ship. The computer systems need to be accessible, and they need to be linked, to provide a pathway for an attack that might lead to the kind of denial or disruption of service that would be causative of damage.

Figure 2: Supply chain assessment – where to look for potential threats and vulnerabilities

Five Common Assumptions Examined

Assumption 1: A cyber attack is increasingly likely.

It is wise to assume that the risk of a cyber attack is likely, but that likelihood should be positioned properly by a considered risk assessment to determine the realistic effects on a shipping company or its vessels.

Cyberattacks are perpetrated in the expectation of gain, criminally or for social reasons. It is in our nature to feel more vulnerable to a hazard if it is widely discussed, as opposed to a hazard that is seldom mentioned and that seems remote. Any enterprise that has market value, or has custody of data, funds or property could be a target for criminals, and cyber can be considered as another means by which criminals can threaten the security and profitability of that enterprise.

The opportunities offered to the criminal by a particular ship, fleet, company or activities are varied. The operator of large high profile passenger ships will therefore form a different threat assessment than the owner/master of a small cargo vessel trading in Northwest Europe. Similarly, operators of ships directly owned by or visibly aligned with oil majors, either in transportation, exploration or exploitation, will see the threat differently to the operator of a small fleet of harbour tugs. The threat is specific to the potential victim. Whilst it is difficult to identify a case or a claim where physical loss or damage has been caused to a ship as a direct result of a cyberattack, the probability of such a loss is increasing.

Another factor that might affect the assessment of likelihood is the position of that ship or operation within a larger, more visible, supply chain or activity. The ship could be reasonably inconspicuous, until it is berthed at a terminal operated by an oil major suffering from unwelcome media attention.

Assumption 2: The effects could be catastrophic.

The commercial and physical consequences of an attack are inversely proportional to the effectiveness of defences, security measures and business continuity plans in place. The well prepared enterprise is much more resilient.

However, it would be unwise to underestimate the potential effects of a cyberattack. At the moment, the consequences of such attacks have been financial (theft), or reputational (business disruption).

"Catastrophic" means different things to different people, and ships and marine operations are variably vulnerable. Disablement of the navigating systems will not automatically result in a grounding or sinking. A ship being rendered powerless in one of the world's major canals, for example, would be disruptive, but resolvable. However, any well run commercial enterprise should already be considering issues like resilience, business continuity and security. Provided these issues have been addressed in a way that is proportionate to the hazard, losses of any kind could be controlled, and the procuring of an effective insurance policy will provide some redress if the exercise of reasonable due diligence proves insufficient. Conversely, maritime enterprises that are not resilient or hardened could suffer badly, to the extent that they may not survive the commercial consequences of an attack.

Within a supply chain, there could be varying degrees of hardening. The consequences of an attack could either start with, or engulf a smaller ship or operation and give rise to physical or financial loss. An example might be an attack directed at a large energy ship owned by an oil

major, but directed through the weaker defences of the smaller, independent bunkers supplier. One of the particular qualities of a cyberattack is its potential to cascade into related activities and organisations, because of the nature of a world connected by the internet.

Assumption 3: Defences are technically complex, difficult to understand, limit functionality and are expensive.

Provided that a mature risk assessment is in place, care is taken in the procurement of expert advice and procedural measures are simple and proportionate, a well-managed ship or company should find that setting up good defences against attack is simple and straightforward. The essential factor is leadership.

The defences against attack fall into two broad categories; people based and design based. The first is provided by people and procedures, and the second by the construction and configuration of equipment.

People based defences are simpler, but can be difficult to implement because they depend upon changes in behaviour that may go against human nature, or custom and practice. The speed and success of implementation is therefore dependent upon intangibles like workforce engagement and leadership. The nature of ship operations is normally fast-paced, with some trades being much more demanding than others. Masters and crews have a great deal of regulation to comply with, and a strong commercial imperative to service. It is only natural that the imposition of more rules and governance will not be welcomed anywhere in the management chain. Seafarers are vulnerable to social and commercial pressure exerted by strangers on board, such as technicians or agents. Cybercriminals are largely dependent upon procedural lapses to gain access to data or systems. However these threats can be diluted by strong leadership.

Technical defences are dependent upon the design of the equipment, the way that different components are organised into a system and the use and control of the right software. It is not easy for the lay person to decode what is actually on offer, and the value for money proposition. Expert advice is available in the market, but difficulties can arise when the expert advice is either less expert than it purports to be, or the expert and the customer do not have a shared view of the actual requirement, and the way that the ship or enterprise operates. From the ship owner's perspective, a clear articulation of the user requirement is essential.

Assumption 4: A lone hacker in a remote location can cause huge and spectacular damage.

There is an enduring perception that a cyberattack perpetrated from afar is certainly possible and even likely. One of the attractions of cybercrime to the criminal is the physical distance between the perpetrator and the victim. These attacks are usually attempts to steal data, plant malware or take control of websites or social media accounts. It should be emphasised that a lone hacker taking control of a ship or platform, or a system on board a ship or platform is, at least for the moment, unlikely.

Two factors need to combine to increase the risk of damage caused by or to a ship or platform under attack. The first is that on board technology advances further to place the ship or platform and its control systems into a real time cyber environment, with little or no latency and a reasonable amount of available bandwidth. The second is that ships or platforms are less likely to be targeted outside of media reach.

Assumption 5: The internet is a dangerous place.

The internet affords an opportunity for reconnaissance not previously enjoyed by criminals. A clear analogy for the risks of internet use lies between internet activity and shore leave in a risky port; provided that users obtain security advice, stay away from unknown areas and suspicious looking people, all should be well. If there is trouble on the internet, there is no law or policing to rely upon for protection or redress.

Many shipboard operations, principally related to commercial activity, operations management and crew social activity, rely upon the internet. The activity of the company, ship and crew on line (on and off duty) casts a digital shadow.

That shadow is a rich source of information for anyone planning an attack. It is difficult for most users to understand how information that they place on line can be accessed by others, and how persistent it is. Generally speaking, information put into cyberspace is very persistent as demonstrated by the problems of taking down personal photographs which have then been widely shared on the internet without authorisation. Unless the security settings on social media are used, it is easy for hackers to construct a detailed picture of individuals, their life and movements by using the information which social media shares, stores and leaves open to all.

The ability of criminals to obtain information which individuals may otherwise consider to be private gives rise to the perception that the internet is dark and dangerous and teeming with predators. The ability of malicious users to conceal their identity, or impersonate others, amplifies this sense of unease.

The reality is that the internet is unregulated and extra jurisdictional and holds a truly vast amount of data. The sheer volume of that data provides some measure of concealment. The ubiquity of the internet, and the extent to which it can ease or enable commercial activity, has over the past decade caused users to lose sight of the risks. Whilst the internet may not be an inherently dangerous place, it is certainly not a safe place for the unprepared.

Areas of Vulnerability – Current and Potential

Connections

The two areas of examination must be the connection, and the way in which the connection might lead to a critical system.

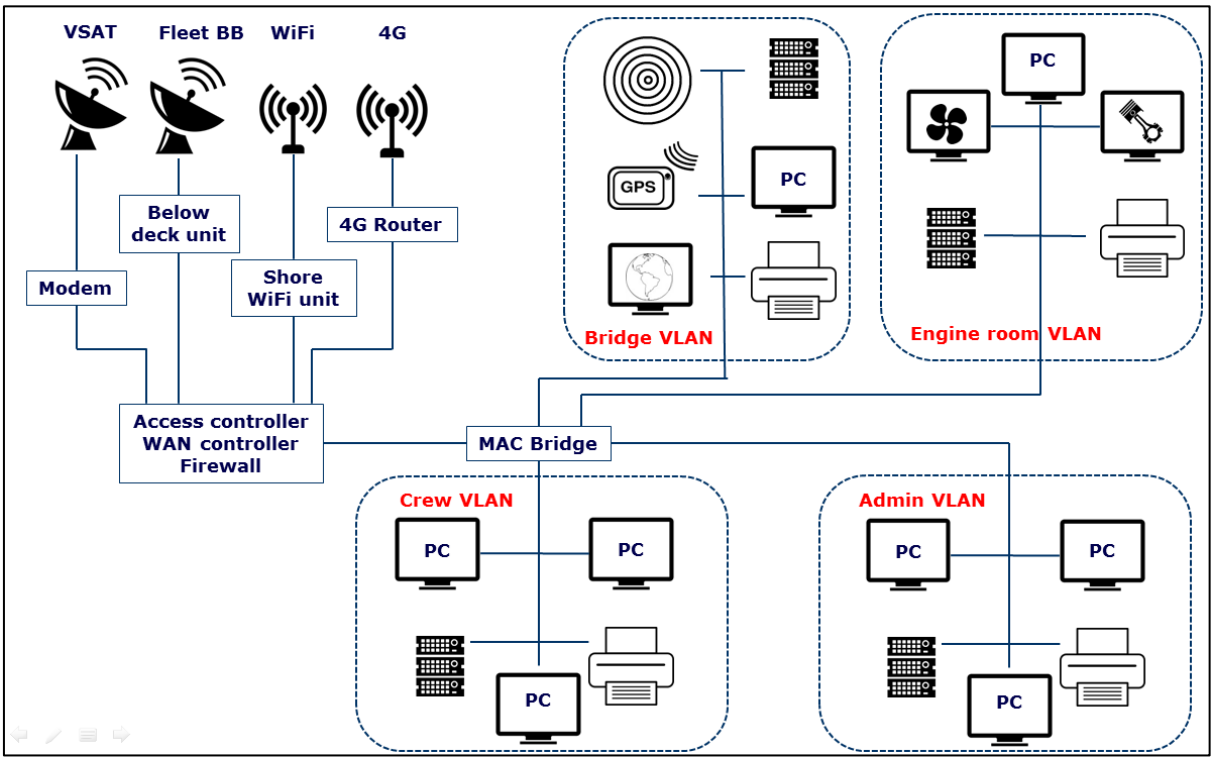

Figure 3: Modern typical shipboard IT system configuration

The connections via satellite, 4G or Wi-Fi are vulnerable to varying degrees, with the satellite connection probably being the most robust and Wi-Fi the least. The attacker would need specialist knowledge and equipment to breach the security perimeter of satellite providers, which although difficult is not impossible. It would be costly, and the attacker might look for a better return on effort.

4G and Wi-Fi are much more promising prospects. Both use relatively straightforward security protocols, and both are widely understood by hackers.

The architecture of on board systems is critical to both risk and mitigation. Although more and more individual systems on the typical ship rely upon computers and/or microchips to operate, they are not normally interconnected. Integrated bridges do share information between systems such as AIS, radar and GPS, but these remain essentially stand alone.

The typical modern ship has computers connected to the internet that send commercial and social traffic, autonomous condition monitoring information and asset tracking information to and from the shore. The systems that control and monitor the average ship are a mix of computer driven and electromechanical systems that are interconnected to varying degrees. Additionally, these systems have backups relying heavily upon the human element.

This makes the likelihood of an attack that deprives the crew of control of navigational or propulsion and steering systems to the extent that a loss occurs very unlikely. At present, such ships are probably only vulnerable to accidental loss of data or service by malware infection

caused by poor housekeeping and access controls. Ship's computers are often heavily contaminated through the misuse of unauthorised physical media, typically USB memory sticks. However, this misuse can only give rise to data loss or corruption, or the temporary loss of a single system i.e. it is of a lower order.

More sophisticated and specialist ships may be more vulnerable if they are more heavily reliant upon computerised, interconnected systems. Ships used for exploration and exploitation are required to maintain their position very precisely using Dynamic Positioning, a computer enabled system. Additionally, equipment can be controlled from the ship using supervisory control and data acquisition, or SCADA. SCADA is a remote control system using coded signals over conventional radio communication channels. The number of successful SCADA attacks is unknown, as they are usually not reported, but industry monitors view SCADA as vulnerable and a tempting target.

Asset tracking systems

One of the applications of GPS is to track the movement of high value assets. GPS technology has been available for the past 10 years in its current form, as small devices or even printed cards incorporated into other devices. It has two uses; as a reliable time base and as a position fixing device.

A simple GPS device allied to a transmitter will pass the position, course and speed of anything it is attached to over any communications means. The increasingly low cost of satellite communications, the vast area of coverage and the brevity of the data bursts (and thus their cost) allows for cost effective asset tracking from everything to buses, parcel vans, prestige cars and shipping containers.

In the latter case, the more sophisticated container lines track their high value containers, typically refrigerated containers and ally the tracking to a simple condition monitoring system. This allows the line to monitor the health of a refrigerated unit, send repair technicians to the right location if required and to advise customers almost to the minute when their perishable goods will be delivered.

This presents, at present, two security risks. In the case of high value goods such as prestige cars, asset tracking devices are often foiled by thieves using a simple denial of service jammer. This jamming has the effect of knocking out GPS signals over a 250 metre radius. There are already well documented cases of ships having their GPS services denied by a jammer attached to a stolen prestige car in a container on board. The modern ship is heavily dependent upon GPS for safe navigation. These incidents prompted the UK General Lighthouse Authority, Trinity House, to conduct simulated GPS denial of service attacks on ships to assess the risk. In their view the modern ship is over reliant on GPS for safe navigation.

The second risk is that container tracking devices, although not currently configured to control the container, will tell the hacker where the cargo is, and thus where the ship is at any moment. This may be used as intelligence to plan a cyber attack.

Cloud Computing

Cloud computing is a term that loosely describes the movement of data and software away from a physical presence on a hard drive into a virtual presence that can be accessed on demand. Cloud computing describes a world where the only equipment required to use software and create, collect, analyse or store data is a web browser. The actual equipment that hosts the browser could be a PC, a tablet or a smart phone.

Cloud computing means that there is only ever one version of a data set in existence, removing the possibility of out of date copies of files lurking on a particular PC. It offers software as a service, ensuring that users have access to the latest versions of office tools. It offers efficiency of storage. Data storage in the Cloud is vastly superior and cheaper to that available conventionally.

Working in the Cloud requires an always-on internet connection of sufficient speed and with virtually no latency. Cloud computing is already facing security challenges. There may be a possibility that information belonging to different customers resides on the same data server. Information leakage may arise by mistake when information for one customer is given to another. Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack, a process called "hyperjacking".

The risk to shipping presented by Cloud computing is almost identical to the current and likely risks ashore. The Cloud is not in itself a risk driver because it can only be used at sea with the right type of connection. However, as E-navigation will probably provide that connection, it seems inevitable that owners and operators would seek to put their ships into the Cloud. As such the use of the Cloud is not a risk in itself, but it does magnify the likelihood of risks already identified.

Machinery and Condition Monitoring

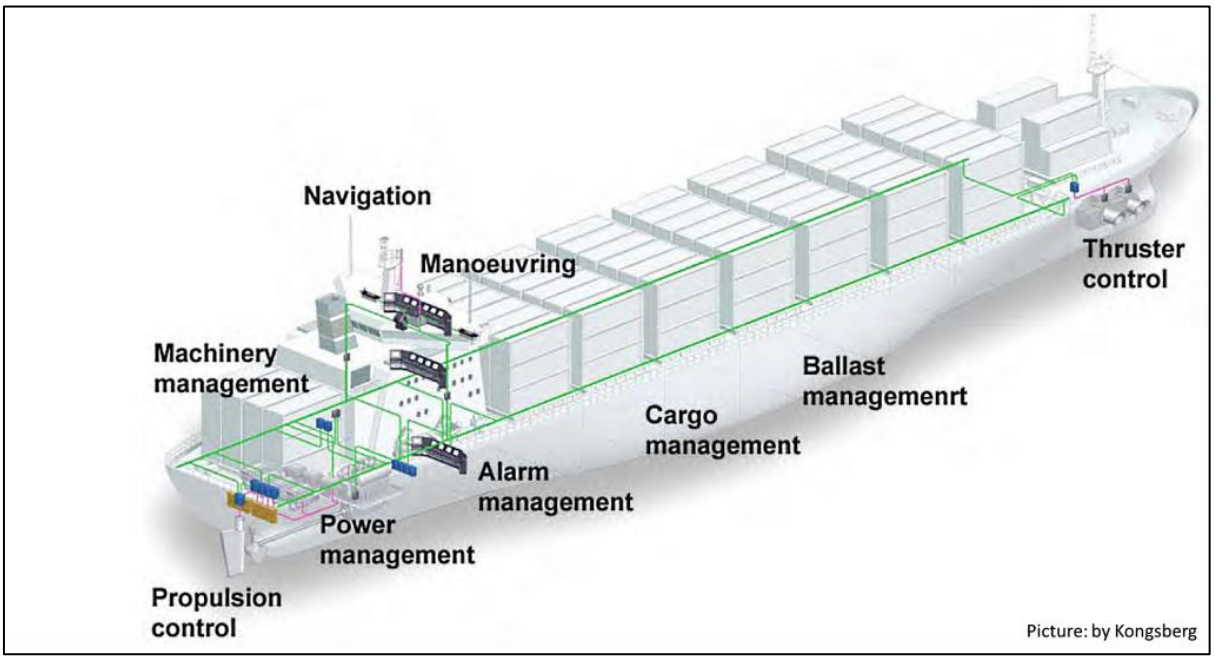

Figure 4: Ship systems capable of remote monitoring or operation

Modern ships are technically complex in terms of their machinery. This complexity and sophistication is driven by:

- The need for fuel efficiency with finite fuel resources
- The adaption to new fuels such as methanol or LNG
- Environmental requirements such as emissions control, ballast water treatment

- Increasingly stringent standards for noise and vibrations
- The specialist role of a particular ship, such as dynamic positioning.

Increased sophistication leads to increased capital cost and means that machinery failure, or increased rates of wear, are in turn increasingly costly. To improve the performance and longevity of modern machinery, continuous and autonomous monitoring systems measure and test, amongst other things, temperatures, pressures, flow rates and fuel and lubricating oil quality. These systems record the measurements taken, log them and make reports and send alerts to the shore via the ships communication system. These messages are sent autonomously, through a connection that is always on.

It may be that condition monitoring systems are designed to shut down systems automatically if they stray out of acceptable operating parameters.

This also offers a potential pathway to the hacker, particularly if the condition monitoring equipment has not been properly installed and configured. It might be working as intended, but it might also be opening a back door into other critical systems such as machinery or ballast control.

A properly designed and integrated on board system will zone, and isolate, systems that use an always-on connection so that they do not present a vulnerability to attack. Any ability to operate a system remotely will need to be carefully considered and the right technical safeguards put in place.

The Internet of Things

The Internet of Things is a phrase recently coined to describe the way in which devices interact with each other over the internet, usually wirelessly. The devices that can join the Internet of Things need to be "smart", which means that they have to have the right electronics, software, sensors and connectivity to be able to exchange data with other, similar, devices.

At the moment, the Internet of Things is in its infancy. Some additional work will need to be done to devise access protocols and other software related issues to allow for the huge number of devices expected to appear on the internet. The appetite for this connectivity is considerable and high growth is forecast.

The opportunities presented by the Internet of Things are the sharing of information of all types across devices in real time, and the remote control of these devices. Small scale examples already exist; on the market now is a user installable gadget that allows the monitoring and control of home heating through a smart phone from anywhere in the world. It is likely that most of the applications for the Internet of Things have not been thought of yet. A quick examination of the technical rate of change over the past decade would indicate that the next five years will see an explosion in new products and solutions, many of which could be of use on board.

There are three significant risks presented by the Internet of Things. Firstly, security issues have not been properly dealt with by regulators, and so enthusiasts and hackers will be ahead of the market when issues like exploitation of weaknesses are considered. Secondly, the potential for remote control will probably supersede SCADA in many applications, increasing the number of remotely controlled shipboard systems with no gain (or the reverse) in operational security. Thirdly, the amount of data collectable by enabled devices will massively increase the store of data available. Today's Big Data may very soon come to look quite small.

The Internet of Things, allied with E-navigation, will move shipping and ships firmly into the realm of the cybercriminal.

E-navigation

E-navigation is an IMO led initiative intended to keep ships and shipping included in the benefits of the technological advances currently being made in the field of telecommunications.

E-navigation is defined as the harmonized collection, integration, exchange, presentation and analysis of marine information on board and ashore by electronic means to enhance berth to berth navigation and related services for safety and security at sea and protection of the marine environment.

In practical terms that means the sharing of information relating to navigation, routing, weather, tides, cargo loading, carriage and stowage in real time between ships and between the ship and the shore. E-navigation is therefore split into a number of development projects intended to provide the shipping industry with clear guidelines for technical development and equipment standards.

The E-Navigation Strategy Implementation Plan contains a list of tasks required to be conducted in order to address 5 prioritized E-Navigation solutions, namely:

- Improved, harmonized and user-friendly bridge design
- Means for standardized and automated reporting
- Improved reliability, resilience and integrity of bridge equipment and navigation information
- Integration and presentation of available information in graphical displays received via communication equipment
- Improved Communication of VTS Service Portfolio (not limited to VTS stations).

These tasks should be complete by the end of 2019, and it is likely that implementation at least in part will be commenced by early adopters by the end of this decade. The communications systems and protocols required by E-navigation will move shipping technology significantly toward the point where a hull and machinery loss caused by a cyber attack is possible. One analysis of the progress of E-navigation is that the insurance market has less than 5 years to prepare itself for the risk of a cyber-attack at sea materialising into a hull and machinery loss.

Appendix

Background and information

Shipping is characterised by its global nature, the high values associated with the goods and commodities it moves, and the low costs of doing so. Society depends on shipping. Ship design and technology has not until recently moved that far forward from the ships built in the 1970s.

The breath-taking pace of technical innovation, particularly in data storage, retrieval and transmission, and telecommunications, has done much for the development of shipping. Increasingly, the technical sophistication of ship systems, previously restricted to specialised vessels, is becoming the norm. Ships are getting larger and more expensive and insured values are on the rise.

A brief history of cyber

Cyberspace, cybercrime, hackers, code and other such terms first entered the mainstream through the fictional works of the author William Gibson, and more recently through films such as Johnny Mnemonic and The Matrix, both heavily based on Gibson's work. These books, first published in the early 1980's, and the films made in the mid to late 1990's, postulated a dark and mysterious electronic universe populated by strange and terrifying heroes and villains.

Figure 5: The iconic representation of The Matrix, inspired by Gibson

In the real world, the Internet was first described by Tim Berners-Lee in the early 1980's and became a part of the lives of many people a decade later. The breathtakingly rapid pace of development in information technology now means that computers, computing and the internet permeates every part of the lives of most of the world's citizens, and to an extent that is beyond the capacity of many people to fully understand or engage with.

Most people's perception of cyber related issues, and current technical capability, comes from Hollywood and media rather than from education or experience. This disconnection can make conversations about risks related to cyber issues difficult, as there may be no shared understanding of the capabilities of information technology between the participants. Additionally, there is both a desire for, and a higher expectation of, information technology as it facilitates our daily lives at work and socially.

In the shipping industry, most people in influential positions are not of the "internet generation" and have assimilated the new technology and its language to varying degrees.

The Risk of Attack: Perception and Reality

The concept of cybercrime has been discussed in industry and commerce for at least 30 years but, it is only relatively recently that the well reported attacks on Home Depot and Sony in the United States, together with similar stories originating from within the European banking system, have raised the issue of cybercrime and cybersecurity within shipping. This is almost certainly because in the past decade, ships and shipping have become increasingly technically enabled, and the shipping industry now expects information technology to facilitate business instantly regardless of time or distance.

Connectivity Methods and Characteristics

VSAT (Very Small Aperture Satellite Dishes) are in widespread use at sea. The different commercial providers offer shipboard users narrow and broadband data at rates approaching 4Mbit/second, which is respectable but not as fast as modern terrestrial provision where speeds of up to 20Mbit/second are common. Specific and purpose built VSAT units have achieved 16 Mbit/second.

VSAT works well below latitudes of about 70 degrees, because it relies upon a network of geosynchronous satellites. These data transfer rates are sufficient to enable point of sale transactions, polling, radio frequency identification devices, broadband data such as VoIP or streaming video and SCADA (Supervisory Control And Data Acquisition). VSAT does tend to suffer in heavy rain, where the static charge of precipitation can degrade the incoming signal.

Figure 6: Typical VSAT above deck equipment

Satellite communications are also used to support telephony and data at lower rates to support statutory communications means called for by the Global Maritime Distress and Safety System, and for commercial use where bandwidth is less critical. Such applications include condition monitoring and asset tracking. These systems are more robust because they use a different and more reliable part of the radio spectrum to VSAT. These different connections present different risks.

VSAT providers, and conventional satellite providers, offer their services from within a secure perimeter protected by robust defences. The high levels of security they offer are essential to

their ability to operate, and to offer services to commercial and governmental clients. Satellite signals can be encrypted for additional security. This level of security is an obvious deterrent to the criminal, who will look for an easier way in. However, these systems are not invulnerable; they are just harder to crack.

4G transmits and receives broadband data from the ship to terrestrial mobile telephone networks using equipment which is simply a larger version of the common smartphone. The ship must be a subscriber, and 4G will support voice and data in the way that users of smartphones will be very familiar with.

4G allows for significant improvements on data rates because it is based upon the TCP/IP (Transmission Control Protocol/Internet Protocol) commonly employed by other systems intended to send and receive data over the internet. These protocols are well understood by hackers and are vulnerable to exploitation, using the same type of malware that might be used to attack a computer based system. 4G is also vulnerable to denial of service attacks by jamming or scrambling signals. 4G allows the criminal to locate the target system because 4G devices tell the network where they are, or to use the moment the device is handed over from one radio cell to another to enter the system.

Wi-Fi is a local area network using wireless technology, allowing access to the internet by wireless connection. In marine applications it works in exactly the same way that it works ashore, and is a service offered by modern ports and terminals. Wi-Fi can be set up as a local network within the ship to allow portable devices access to the ship intranet. The responsibility for security lies away from the ship or company, as Wi-Fi is usually provided by the terminal. This is a good example of vulnerability in the supply chain.

Wi-Fi is potentially extremely vulnerable to attack, monitoring or unauthorised use. It uses well understood technology and protocols. Even security keys are weak, and can be easily unlocked with off the shelf equipment and software.

4G and Wi-Fi are used in port and coastal areas, with Wi-Fi only being available alongside. Satellite means tend to struggle alongside where cranes and shore structures can disturb or interrupt the signal. An integrated on board system will use all three types of connection, and the system can be configured to switch to the "least cost" data bearer without the knowledge or approval of the operator.

Who and why? Hackers, Crackers and Script Kiddies

The motivation for cyber crime of any type commonly has psychological and social roots. Cybercriminals typically display a kind of cognitive dissonance which enables them to wilfully minimise or even misunderstand the effects of their actions upon others. This degree of disassociation with the consequences is assisted by their physical remoteness from the crime, and the general sense of unreality engendered by using computers as a tool. It feels like a game. Ships and shipping will not be exempt from this game.

Most publicised cyberattacks are perpetrated by nuisance hackers, or "script kiddies". They are typically young white males between 12 and 30. They are usually caught because they like to brag about their exploits. They tend to be socially inept, with limited educational achievement and a low boredom threshold. Their usual aim is to disrupt or vandalise systems. They tend to use exploitation kits purchased on line, but some may have the skills to write sophisticated code. The targets selected by Script Kiddies are within sight of their everyday lives, such as large corporates, banks or retailers. A high profile media event involving shipping might bring ships into view.

Professional criminals, or "crackers", are more mature and make a living breaking into systems and selling the information they find, typically username and password files. This information is sold on for use in identity theft or other fraud. They might be retained for corporate or government espionage where a specific target is contemplated. They will have ties to criminal groups. They do not brag about their exploits and use more sophisticated tools and techniques. Some crackers work from within loose federations or associations. Probably the most notorious is the Russian Business Network (commonly abbreviated as RBN). RBN is a diverse cybercrime organisation, involved in everything from data theft to pornography. RBN has a commercial structure, and an eye catching corporate logo. As with other similar organisations in other states (North Korea, China and Iran), RBN members are revered at home and will align their criminal activities to the political aims of their host state. This kudos is an undoubted source of motivation.

Highly skilled but individualistic technicians, or "hacktivists", are motivated by ethical imperatives that include a distrust of the establishment, a belief in the complete and free sharing of information, and the virtues of cyberspace as a place for human intellectual development. Hacktivists may be highly qualified academically, and be retained by governments or organisations to design and test defences. Hacktivists are also prone to engaging in criminal activity to further social or political causes. The case of the security "researcher" Chris Roberts, who claims to have hacked airliners in flight and the International Space Station, is a good example of severe nuisance caused by an individual claiming to be altruistically motivated. The recent activities of the Lizard Squad, and Anonymous, are good examples of nuisance crime such as distributed denial of service, aimed at large enterprises for allegedly altruistic or noble reasons.

State sponsored cyber attacks are a form of warfare, and it is possible that an enterprise, including one involved in shipping, could be the victim of an attack from such a source. State sponsored attacks are characterised by the sophistication of the personnel involved and the tools that they use.

References

International Ship and Port Security Code, International Maritime Organisation, 2002

International Safety Management Code and Guidelines on Implementation, International Maritime Organisation, 2014

Safety of Life Sat Sea Convention 1974 as amended, Chapter XI

Standards for the Training and Certification of Watchkeepers Convention, International Maritime Organisation, 2010

Safety and Shipping Review 2015: An annual review of trends and developments in shipping losses and safety, Allianz

The Risk of Cyber-Attack to the Maritime Sector, Marsh, 2014

The Phantom Menace, Panda Labs, 2015

Threat Intelligence - Collecting, Analysing, Evaluating, Council for the Protection of National Infrastructure, MWR InfoSecurity, CERT-UK 2015

Mobile devices, Centre for the Protection of National Infrastructure (CPNI) and MWR InfoSecurity, 2013

Online Reconnaissance, Centre for the Protection of National Infrastructure (CPNI), 2015

The Critical Security Controls for Effective Cyber Defense Version 5.0, Centre for the Protection of National Infrastructure (CPNI), Council on Cybersecurity

The Masked Avengers - How Anonymous incited online vigilantism from Tunisia to Ferguson. The New Yorker, September 2014

The U.S. e-Navigation Strategic Action Plan, U.S. Committee on the Marine Transportation System, 2011

Common Cyber Attacks: Reducing The Impact, CESG (The Information Security Arm of GCHQ) with CERT-UK, 2015

ISO 27001, International Organization for Standardization

Emerging technologies, Qinetiq, 2015

With grateful thanks to

Christopher Turberville, Head of Marine Hull and Liabilities, Allianz UK

Mark Edmonson, Marine Class Underwriter, Chubb Managing Agent, Joint Hull Committee

Neil Roberts, Manager, Marine, Lloyds Market Association

The membership of the Joint Hull Committee

David Walker, Managing Director, Live Wire Communications

Alex Davis, Partner, Stephenson Harwood LLP

Mike Pullen, Partner, Stephenson Harwood LLP

And other old friends and former colleagues who must remain nameless.

About the author

Rod Johnson, Marine Manager, Stephenson Harwood LLP

Rod investigates marine casualties as a member of Stephenson Harwood's Marine Insurance Casualty Response Team and provides marine technical expertise and advice across a broad spectrum.

He is a Master Mariner, and a former head of Her Majesty's Coastguard, with nearly 40 years of experience in the maritime sector. His experience encompasses marine operations, safety and risk management, regulatory compliance, marine spatial management, maritime surveillance and security, emergency planning and response, and environmental protection.

He is also a registered ship surveyor, with extensive experience of casualty investigation, audit, survey and inspection, sale and purchase, due diligence assessments, managing regulatory compliance, and advising on special and novel projects.

Rod is a member of Stephenson Harwood’s industry leading cybercrime investigative and legal advice team, offering a response and intervention service to major multinational corporations, primarily in the critical infrastructure, financial and blue-chip insurance and retail sectors.

STEPHENSON HARWOOD

Joint Hull committee