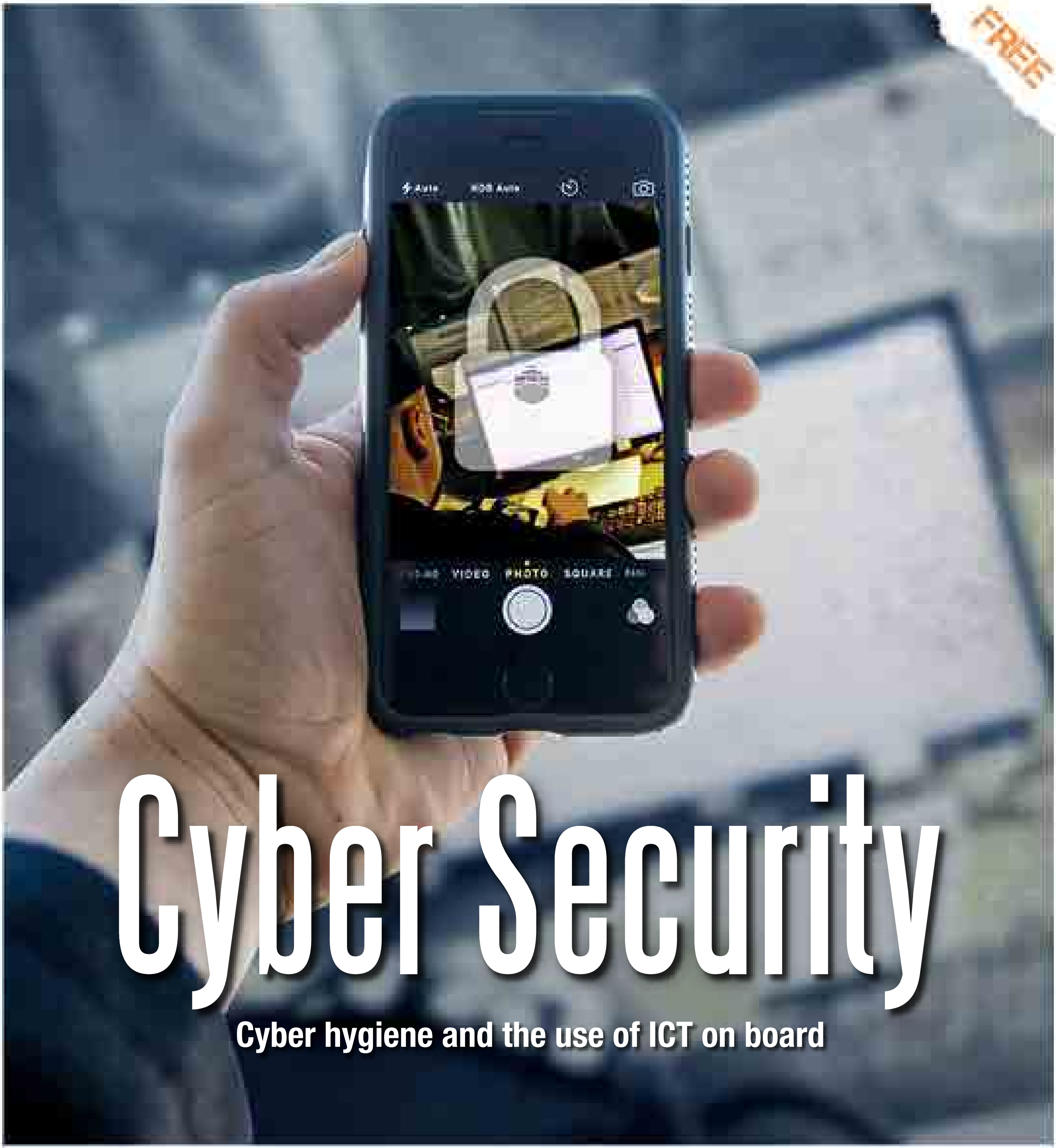
June 2016 Issue no. 12

THE NAVIGATOR

Inspiring professionalism in marine navigators



Cyber Security

Cyber hygiene and the use of ICT on board

A free publication by The Nautical Institute in association with the Royal Institute of Navigation

NAV BRIEF

David Patraiko FNI
Director of Projects, The Nautical Institute

Making sense of cyber security

Modern shipping relies on modern Information and Communication Technology (ICT) to compete and thrive in the global transport industry. We rely on it for cargo documents, port arrangements, crew management and all the other services that ships need to operate efficiently and competitively. ICT is also widely used onboard in engineering systems and cargo control and monitoring.

The bridge bristles with technology too. Not just for commercial effectiveness, but for the safety of those onboard, the wider society and the environment. Can you imagine driving large ships through busy waters surrounded by navigation hazards at speeds exceeding 20 knots without Radar, GPS or ECDIS? Or worse yet, conning that same ship and suddenly having those systems fail? It can be done, of course, but not comfortably and certainly not without increased risk.

Electronic systems can fail for many reasons. Professional navigators must take all reasonable effort to ensure that they don't, train and drill for the possibility that they might, and have a recovery plan for the worst case. It will not escape you that cyber security is a world-wide issue. On a personal level, you probably keep virus protection on your personal devices and are wary about opening attachments that look dodgy. It is important to take equivalent precautions for shipboard systems, too. Managing risks is a natural role for a navigator, and you will probably find that most of the common sense processes of good cyber hygiene are already in place, but awareness and preparedness are essential.

Ships are vulnerable to cyber threats, both intentional and unintentional. An unintentional incident could include somebody mistakenly jamming the GPS signal while working on a different system, or a crew member unknowingly bringing a virus onboard via a USB memory stick that they keep their navigation notes on. An intentional attack might include tampering with cargo records to hide contraband, or a malicious attack on the ship's control system to gain commercial advantage.

Cyber attacks have been the theme of Hollywood movies, but in reality major attacks are unlikely and minor attacks are largely preventable. For most companies, the greatest threat comes from the naivety of their own employees, on ship and shore. Awareness and good procedures can dramatically reduce the risk. This is often referred to as good 'cyber hygiene'.

There is a lot of good advice available for cyber hygiene and the use of ICT. Shipping companies should incorporate this into their treatment of ISM, ISPS and the ship's Safety Management System.

INSIDE THIS ISSUE

A Nautical Institute project sponsored by IFAN

202 Lambeth Road, London SE1 7LQ, UK
Tel:+44 (0)20 7928 1351 Fax:+44 (0)20 7401 2817
navigator@nautinst.org www.nautinst.org

With support from: 1 Kensington Gore, London, SW7 2AT, UK
Tel: +44 (0)20 7591 3134 Fax: +44 (0)20 7591 3131
www.rin.org.uk

Editorial committee:
Editor Emma Ward
Design Phil McAllister
For The Nautical Institute
Bridget Hogan, Lucy Budd,
David Patraiko FNI, Theresa Nelson MNI
For the RIN Dr Andy Norris FRIN FNI

Published by
The Nautical Institute
The Navigator (Print) – ISSN 2058-6043
The Navigator (Online) – ISSN 2058-6051
Printed in the UK by
Frontier Digital Innovation Ltd.,
Milton Keynes, Buckinghamshire

ALL AT SEA

Emma Ward

If you would like to get in touch with us, please contact the editor, Emma Ward at navigator@nautinst.org. You can find out more about fellow *Navigator* readers and what they are doing on our Facebook page. We look forward to hearing from you.

Get the app

Join the debate on LinkedIn
http://www.linkedin.com/groups/Nautical-Institute-1107227

Follow us on Twitter
https://twitter.com/NauticalInst

We are active on Facebook
https://www.facebook.com/thenauticalinstitute

Watch our videos on You Tube
http://www.youtube.com/TheNauticalInstitute

You can read a digital version of *The Navigator*, or download it in PDF format at
http://www.nautinst.org/publications

We welcome your news, comments and opinions on the topics covered in *The Navigator*. We reserve the right to edit letters for space reasons if necessary. Views expressed by letter contributors do not necessarily reflect those held by The Nautical Institute

Cyber Security

What's changed recently that prompted all this discussion and advice coming from left, right and centre? Probably not much, except that having internet onboard vessels is becoming more common, bringing with it all the associated issues. Until very recently, we were immune to hacking because… there was nothing to hack and no means to get into our ships. This is slowly changing, and hence I would like all of us to start thinking about whether we are indeed immune? Is there anything you can do to improve the cyber security situation onboard your vessel? Can you be more 'street-wise' when it comes to your smartphone, laptop and tablet?

Read this issue of *The Navigator* and think critically – start thinking about cyber security and… stay calm. There is no need to panic (yet?).

Capt. Kuba Szymanski FNI, Secretary General, InterManager

My officers, cadets and crew are enjoying reading *The Navigator*. The content is very open and inspiring. Our thanks must go to the AMSA PSC Inspector, who brought us these magazines when he came up in Townsville last call.

Capt. Jo Juson, *Kwangsi*

I am a deck cadet onboard the vessel *Glovis Composer*. I am learning so much from *The Navigator* – especially the CPD issue and Take 10. I shared some of the topics with the crew onboard our vessel. We don't have a hard copy onboard but I shared the app with the crew to show them this informative magazine.

Ernest Alfred Burgos

Greeting to all my brothers in this profession! I am a die-hard fan of this magazine, but since I shifted to the offshore industry, it is very seldom or not at all that I can see *The Navigator* magazines on board. I was happy to finally receive a copy of the magazine here in Dubai. Long live Navigators!

Alvin Belleza Renomeron

I was lucky to be introduced to *The Navigator* magazine at a training workshop with Capt Yashwant Chhabra at the Maritime Academy of Asia and the Pacific in Bataan, Philippines, where I am currently enrolled in the Marine Transportation BSc degree. It can be used as a reference for professionalism in maritime navigators. Moreover, it serves as an eye opener for us to be really cautious in the maritime industry. Thank you, and we'll enjoy reading it!

In the long run, I am endeavouring to work in pilotage in Singapore. During my cadetship I became deeply fascinated with the pilotage whenever we went to our home port, Singapore. At that time, I was already thinking of working in that profession, commanding the vessel safely. The maritime profession is a never ending process of learning, and I will continue my endeavours to work in this different field in the maritime industry. I know this will take time, but just by dreaming about it, I am already starting to see how I can realistically bring it about.

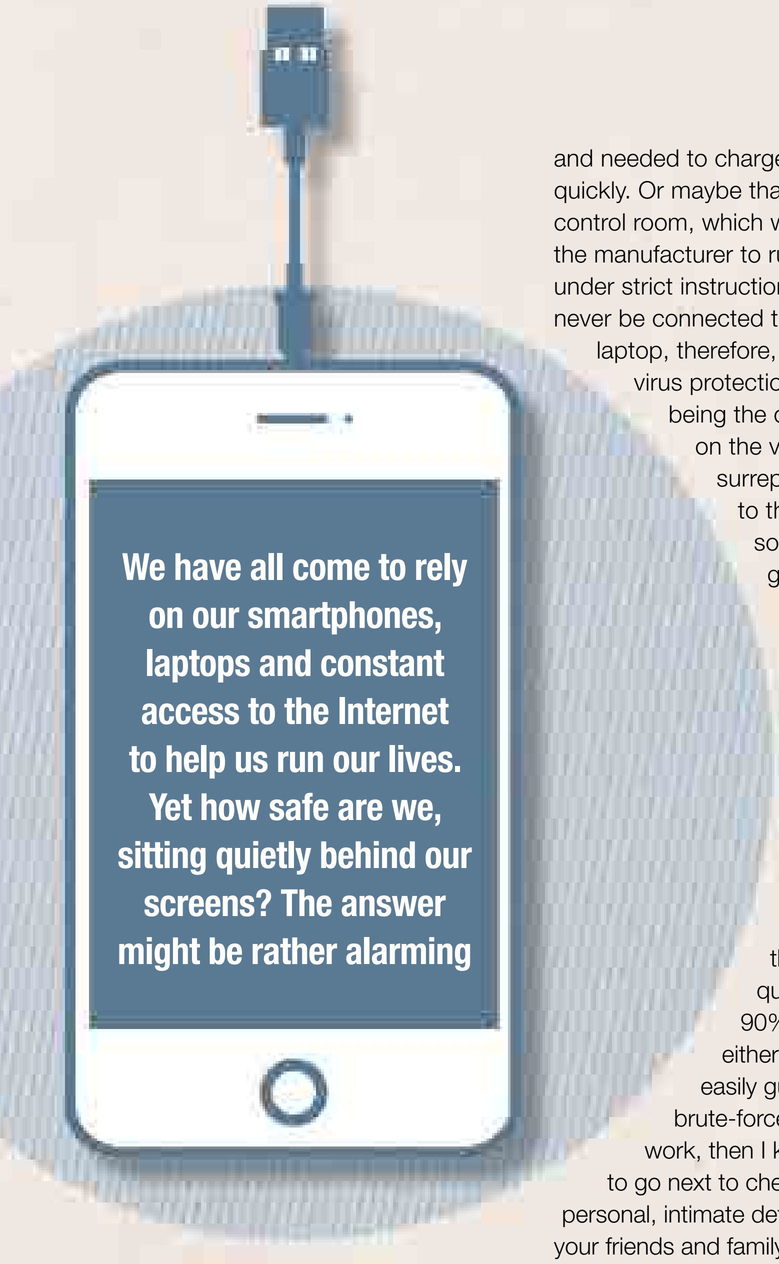
Niel Borja

Just wanted to share my thoughts. The issue dated February 2016 was really a great help for me. I'm in my second contract in this position, and the thoughts I gathered from that issue building on competence were indeed helpful for guiding my development. Thank you.

Loid Anthony Cadungog
Third officer, *Orient Centaur*

Be a distributor! To sign up for a copy of *The Navigator* for your vessel, visit http://www.nautinst.org/navonboard

Knowledge is Power



We have all come to rely on our smartphones, laptops and constant access to the Internet to help us run our lives. Yet how safe are we, sitting quietly behind our screens? The answer might be rather alarming

Most of you reading this will have a smartphone onboard with you at the moment. I know this because, each year since 2012, Futurenautics has run the Crew Connectivity Survey, which asks around 3,000 seafarers about their access to, and usage of, devices and connectivity onboard. 2015 was the year in which smartphones overtook other devices to become the most common piece of equipment seafarers have on ships. For the record, the others are laptops, hard drives and other types of mobile phones. Oh, and one guitar. Yeah, I know. I don't think he understood the question.

There is something else I know about your smartphone. If it is running Android software and apps then there is a 90% likelihood that it is carrying malware – malicious software which should not be there. If it is an iPhone running iOS then that's up to an 80% likelihood. That's malware of which you will be entirely unaware, and unlikely to affect your usage of the device at all. It is sitting there quietly, waiting until the phone is plugged into something else, when it will execute and infect whatever machine it has been offered.

That machine might be a laptop, or desktop PC, or perhaps the ECDIS, because someone was low on battery and needed to charge up their phone quickly. Or maybe that laptop in the engine control room, which was delivered by the manufacturer to run the main engine under strict instructions that it must never be connected to the Internet. A laptop, therefore, with absolutely no virus protection or firewall that, being the only open computer on the vessel, has been surreptitiously hooked-up to the FleetBroadband so that the crew can get online.

Password-protected?

I also know that there's a 60-70% likelihood that the password you use both for your personal devices and the corporate network onboard will be the same, and that the password in question has an 80-90% likelihood of being either weak, default or quite easily guessable. If a little brute-force cracking doesn't work, then I know exactly where to go next to check out the kind of personal, intimate details about you and your friends and family that will allow me to fashion a very plausible email.

Where do I go for that? Facebook, which I know is the number one social media site for seafarers accessed by around 79% of you while you're at sea. The email, when it arrives, won't come from me. It might come from someone in your IT support unit ashore telling you that they think that someone has been trying to use your login to access

43%
OF YOU REPORTED THAT YOU HAD SAILED ON A VESSEL WHICH HAD BECOME INFECTED WITH A VIRUS OR MALWARE

PROPERLY TRAINED AND RESOURCED, YOU ARE A LINE OF DEFENCE STRONGER THAN ALL THE FIREWALLS AND PRIVILEGES YOUR IT DEPARTMENT CAN MUSTER

the network, but they know it can't be you because HR say you're at sea. It might correctly identify the name of the vessel and its next port of call, and ask for your login credentials in order to investigate. And I know that there is a 70%+ likelihood that you will supply them.

But you might not. On the off-chance that you're one of the 30% who decides to dig a little further, recognises a spelling mistake in the company name in the email address or just gets a little suspicious, that's still not a problem for our hacker. Financially motivated cyber crime is a US$1 trillion+ per year industry and it can be very random. Not always, though. Sometimes, individuals are carefully targeted because they have access to systems or privileges which others don't.

Navigation officers onboard ship have access to systems which could be crippled — or not — in return for a ransom. The good news, or bad news depending upon your perspective, is that according to our survey, seafarers have above average technology skills and competence — you guys are pretty savvy. So you're likely to make the hacker's job harder. But not that much harder.

Risky recruiting

For the first time in 2015, LinkedIn appeared as a favourite job search site for deck officers, according to our data. Even if you're happy where you are, there's no harm in connecting with a recruiter on LinkedIn who is advertising the kind of jobs you might be interested in, paying a bit more money. When that recruiter asks you to contact him directly by email to discuss opportunities, you will. Then, when he sends you a positions-listing sheet encouraging you to take a look and let him know whether you're interested in being put forward, you will click on the attached document, download it, and read it. There's no harm in that, right? Other than the fact that the recruiter is me, and contained within the document is malware which, when opened will begin beaconing to an external IP address that will allow me to install a PHP reverse shell on your system, search, collect, change or remove sensitive data or access systems at will.

Sound unlikely? I've been reliably informed by one connectivity provider that the volume of unauthorised traffic over its network — that is malware beaconing IP addresses from ship's networks all over the world — is so great that it's beginning to cause network issues. To the extent that the provider is contacting its customers and trying to help them root out the malware in their systems.

This would tend to bear out our survey findings, because 43% of you reported that you had sailed on a vessel which had become infected with a virus or malware. Yet 88% of you claim never to have received any advice or training around cyber security or hygiene.

There are a lot of numbers here. For most cyber criminals, it's a numbers game. Every single one of the scenarios I have outlined above has taken place on a ship or shore-based office. The guy who plugged his phone into the ECDIS was responsible for malware wiping every single electronic chart on the vessel.

Unlike the majority of seafarers, people who run shipping companies, and particularly shipping associations, are often far from technology-savvy. They have failed to understand that technology dependence leads to cyber risk and have not adequately addressed the issue at board level in the same way they would address any other type of risk. It is a risk to you because their networks and their vessels are your home and hold a wide range of data about you. For example, the data on your phone alone right now is worth around $14,000 to a cyber criminal.

The truth is that attackers no longer target infrastructure, they target people. So if you are one of the thousands of seafarers who have been given no cyber hygiene support, training or advice then I suggest you ask for it – or seek it out.

There's one other thing I know about you. Properly trained and resourced, you are a line of defence more solid and impregnable than all the firewalls and privileges your IT department can muster.

I know that. The cyber criminals know that. Now you know it too.

Author: K. D. Adamson, Futurenautics

Futurenautics' Crew Connectivity Survey can be viewed as a PDF online at **www.futurenautics.com/crewconn15**

The lowdown on cyber security

More and more ships are being digitalised and connected to the worldwide web. That means cyber security should concern everybody on board – even if they are not computer experts. All seafarers can make a difference – here's how

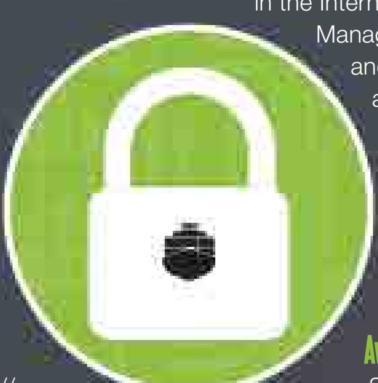
Protecting a ship's computers can be compared to protecting your home. A fence keeps strangers out, just as a computer is protected by a firewall. If your fence breaks, you must mend it. Your firewall must be kept up to date to prevent malware from getting in.

On the other hand, there need to be gaps in the fence to allow wanted visitors in. We must be able to welcome friends and family while assessing the risk of inviting in a stranger. Some guests are granted access to every room in the house, while the delivery guy might just be allowed into the hallway. But even if you offer your aunt unrestricted access to your home, you may still decide to keep your valuables in a locked safe. In other words, you are in full control.

When it comes to life onboard ship, officers must take control to make sure they know who has access to what data, and who is allowed in rooms containing key technical equipment.

Industry guidelines

In January 2016, a group of industry organisations including BIMCO published new *Guidelines on Cyber Security Onboard Ships*. These can be downloaded for free from www.bimco.org. There is a quick link at http://www.nautinst.org/NavInspire The guidelines are designed to develop understanding and awareness of key aspects of cyber security. They do not focus on the technical aspects of cyber security.



Cyber security should start at the senior management level of the company ashore. You cannot protect a ship 100% against cyber incidents (a cyber incident is anything that may adversely affect an onboard system, network and computer or the information it handles). So it is important to have contingency plans ready for when something goes wrong.

Senior management has the strategic responsibility to decide on how best to protect the ship. For example, a barge trading in inland waters will be protected differently from a 15,000 TEU container ship trading worldwide. Cyber security is related to business processes and crew training, as well as technical systems. It is not just a matter for the IT department.

Cyber security has both safety and security aspects. So all plans and procedures for cyber risk management should be seen as complementary to the existing security and safety risk management requirements contained in the International Safety Management Code (ISM) Code and the International Ship and Port Facility Security (ISPS) Code.

Both information technology (IT) and operational technology (OT) might be vulnerable to cyber threats.

Awareness

Some of the main points from the industry guidelines which may be relevant to you as a seafarer:

> Every ship is different, as is its trade and cargo. Start by identifying the threats and vulnerabilities to develop a response in case anything happens to the IT and/or operational technology (OT) on board.

> Cyber security should be considered at all levels of the company, from senior management ashore to crew on board, as an inherent part of the safety and security culture necessary for the safe and efficient operation of a ship.

Cyber security onboard ships protects:

> operational technology against the unintended consequences of a cyber incident;

> information and communications systems and the information they contain from damage, unauthorised use or modification, or exploitation; and/or

> against interception of information when communicating and using the internet.

Identifying a threat

Firstly, you need to understand the specific threats to which the ship and its operations are exposed. For example, if a container is very valuable, there may be criminals who want to steal the contents. In order to do so, they need to know the location of the container and ship. So this information must be restricted to as few people as possible.

In general, there are two categories of cyber attacks, which might affect companies and ships:

> Untargeted attacks, where a company's or a ship's systems and data are one of many potential targets; or

> Targeted attacks, where a company's or a ship's systems and data are the intended target.

Untargeted attacks are likely to use tools and techniques available on the internet to locate known vulnerabilities in a company and onboard a ship. For example, to try to locate the container, the criminals may check if a valuable container is mentioned on social media. This method is called social engineering.

Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a particular company or ship. To locate a container, for example, they may send a personal email to someone who knows which ship the container has been loaded on. This email may contain malicious software or links that automatically download malicious software. Such software will then send the information to the criminals, thereby enabling them to intercept the container.

Vulnerabilities

There are a number of onboard systems which may be exposed to cyber risks. It is important to identify these systems and their vulnerabilities. They could include:

- Cargo management systems
- Bridge systems. Even bridge systems that are not connected to other networks may be vulnerable, as removable media are often used to update such systems from other onboard networks
- Propulsion and machinery management and power control systems
- Access control systems e.g. for the accommodation and cargo control rooms
- Passenger servicing and management systems
- Public networks for passengers
- Administrative and crew welfare systems. These are particularly vulnerable when they provide internet access and email. They should not be connected to any safety critical systems on board
- Communication systems

Risk assessment

A risk assessment will help find out how vulnerable and how exposed the different systems are. The Industry Guidelines outline two risk assessment methods used by the crew or by a third party. When doing it yourself, elements of a Ship Security Assessment can be used to physically test and assess the IT and OT systems on board.

1. Identify existing technical and procedural controls to protect the onboard IT and OT systems. Is there unused or defective software, or are systems outdated or unpatched?
2. Identify specific vulnerabilities in IT and OT systems, including human factors, and the policies and procedures governing the use of these systems. Do you use passwords, are personal profiles changed regularly, etc?
3. Identify and evaluate key shipboard operations that are vulnerable to cyber attacks. For example, who is allowed access to what systems and what are they allowed to do?
4. Identify possible cyber incidents and their impact on key shipboard operations, and the likelihood of their occurrence. For example, what to do if the communication to the shoreside has been compromised?

Training and awareness

You can reduce the risk of cyber incidents by procedural controls, focusing on how seafarers use the onboard systems. Plans and procedures that contain sensitive information should be kept confidential and handled according to company policies.

In many cases, a cyber incident is started by personnel working in the company. Personnel, even with the best of intentions, can be careless, for example by using removable media to transfer data from one computer to another without taking precautions; and data can be mishandled and files disposed of incorrectly. To limit these risks, training and awareness should be developed for:

- Onboard personnel, including the Master, officers and seafarers; and
- Shoreside personnel who support the management and operation of the ship.

An awareness programme for seafarers should cover:

- **Emails and how to behave in a safe manner;**
- **Internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored;**
- **Use of own devices;**
- **Risks related to installing and maintaining software on company hardware;**
- **Poor software and data security practices where no anti-virus checks or authenticity verifications are performed;**
- **Safeguarding user information, passwords and digital certificates;**
- **The physical presence of non-company personnel, for example where third-party technicians are left to work on equipment without supervision;**
- **Detecting suspicious activity and how to report if a possible cyber incident is in progress;**
- **The consequences or impact of cyber incidents to the safety and operations of the ship;**
- **Understanding how to implement preventative maintenance routines such as anti-virus and anti-malware, patching, backups, and incidence-response planning and testing; and**
- **Procedures for protecting against service providers' removable media before they are connected to the ship's systems.**

Author: Aron Frank Sørensen, Chief Marine Technical Officer at the Baltic and International Maritime Council (BIMCO)

WATCHOUT

In this series, we take a look at maritime accident reports and the lessons that can be learned

Charging your phone on the bridge? Think again!

Usually in this series, we look at a report from an official accident investigation to see what lessons can be learned. The risks with cyber security are so new that there are no official reports available yet – although there is plenty of anecdotal evidence from people who have experienced minor incidents. Here, we look at one of the biggest risk factors – USB ports on the bridge.

What might happen?

It's the middle of the night, your phone is running flat, and there is a handy USB port on the ECDIS. You are not going to download anything, so what's the harm in plugging it in to charge?

More than you might think. If software on the phone is in need of update, that could potentially override the ECDIS display to show the dialogue box. It might not be malware – but it's still in the middle of the screen, obstructing the chart. Or it might cause the display to switch to displaying the underlying Windows or Linux system screen. Again, even if no damage has taken place – you still don't have an ECDIS display!

Worst case scenario?

Captain Richard Madden, writing in the *Maritime Executive*, warns that: 'Anecdotal evidence has shown that difficulties in updating ECDIS charts and licenses ensued [as a result of charging phones or using unauthorised USB]'. Beyond that, 'It can be certain that this is a potential vector for computer viruses or malware,' he says.

What changes could be made?

Capt. Madden suggests: 'Perhaps it's time the bridge officers or Master address where these devices might be charged.'

IT'S ALL FUN AND GAMES UNTIL YOUR ECDIS FAILS AT A CRITICAL JUNCTURE.

If you find our accident reports useful, check out The Nautical Institute's Mariners' Alerting and Reporting Scheme (MARS). A fully searchable database of incident reports and lessons, updated every month. Seen a problem yourself? Email the editor at mars@nautinst.org and help others learn from your experience. All reports are confidential – we will never identify you or your ship.

WHO'S NAVIGATING?

Proud to be a seafarer

Deck Cadet **Jisilda Nguli** loves life at sea and takes enormous pride in her status as a 'seafarer'. She has ambitions to become a Master, and is keen to learn from those around her

What made you interested in a life at sea?

In the beginning, I was just interested in studying, but after two months, I fell in love with the sea and way of life. I identified myself as an officer and loved doing something different from my family and friends. I could not stop dreaming about one day being a captain of a big ship.

Where did you train?

I trained in three separate places. First of all in India at AMET University, where I did my STCW course and studied English (I'm from Angola and not a native English speaker). Then, I did my HND with the first year in Angola at CFMA and my second year at City of Glasgow College in Scotland.

What was your first day at sea like?

My first day at sea was amazing! I joined a very friendly and professional crew on an oil tanker ship from my home town. She was called *Benguela-Angola* and there were seven other Angolan women onboard. The weather was tropical, with a calm sea and light wind. It was the best experience ever.

What do you like best about working at sea?

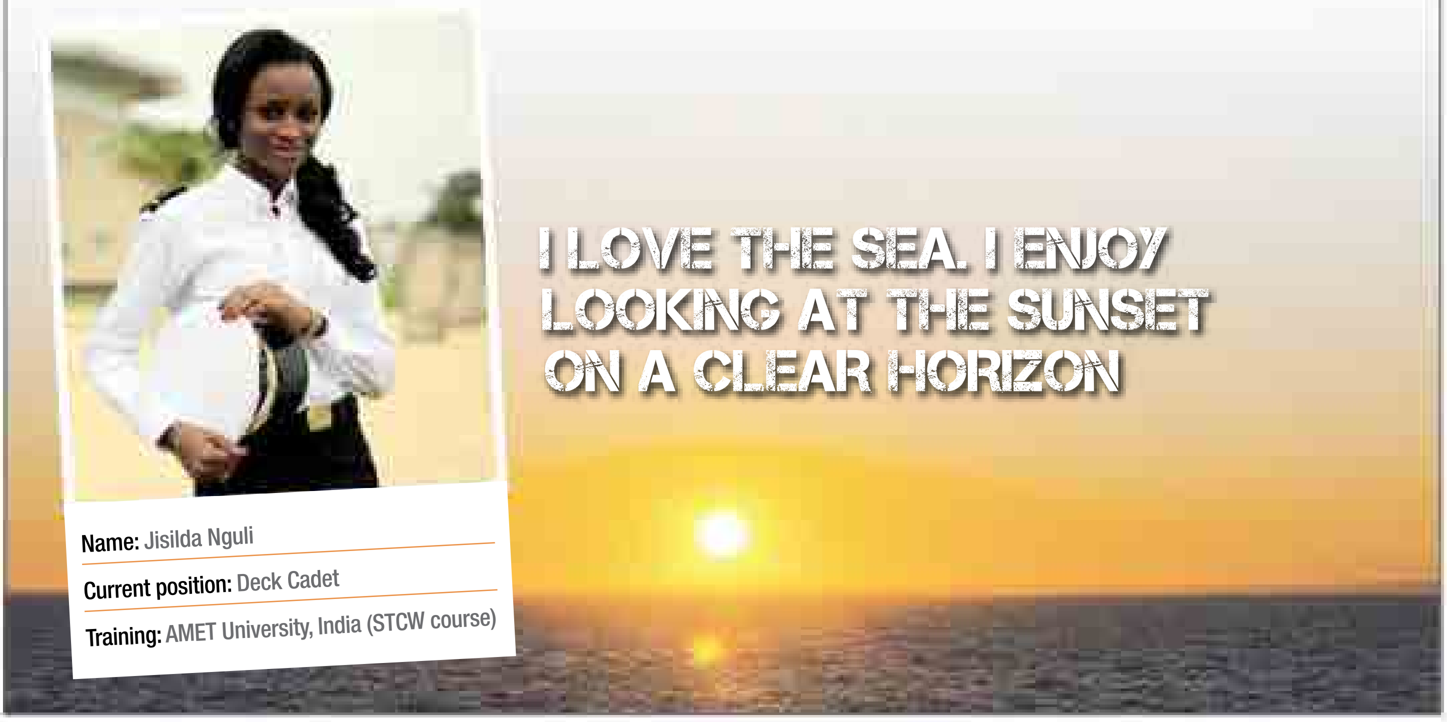
I love the sea. I enjoy looking at the sunset on a clear horizon. I like the idea that my workplace is just three minutes' walk from my bedroom, and that I don't have to face commuter traffic every day. I also like being called a seafarer; it makes me proud of myself.

How can you become a successful bridge officer, in your opinion?

You have to know how to listen – even when you think it is unnecessary. Follow the rules, stay aware of any changes in the situation (a good officer is always alert), remain engaged and work as part of the team. Communication is very important onboard ship. Know that you can learn something from anyone, and most importantly, put the safety of everyone onboard ship first, along with the cargo and environment.

Where do you see yourself in five years' time?

I see myself as a second officer, sharing my experience and travelling all over the world, showing one more time that women can do anything. I want to take part in big conferences with opportunities to speak and encourage others to follow this career. In ten years, maybe I will be a captain, doing the same job of sharing my experience. I will enjoy each stage of my career and try to learn as much as I can. I will do every single course that my company can offer me and keep reading the latest nautical publications. Above all, I will try to always be happy, safe and grateful.



I LOVE THE SEA. I ENJOY LOOKING AT THE SUNSET ON A CLEAR HORIZON

Name: Jisilda Nguli

Current position: Deck Cadet

Training: AMET University, India (STCW course)

Spoofing and hacking – thwarted by competent navigation

Dr Andy Norris, an active Fellow of The Nautical Institute and the Royal Institute of Navigation, dives into the complex world of spoofing and hacking

Minimising risk is central to navigation. Hacking and spoofing contribute to the risks, but by following conventional best practices, we can ensure that any potential problems rapidly become apparent. Of course, we must remain fully aware of the possibilities of hacking and spoofing, not least to help ensure that our own procedures minimise the chances of a successful attack.

Our training and experience shows us that GNSS does not always give a continuous and accurate position. Assuming that it does so is a very dangerous mindset to get into. Any single system, whether for positioning, bearing measurement, depth sounding, speed or target detection, has vulnerabilities.

Our main role is to compare and integrate all the data sources available to us and make our own intelligent decisions. Information sources include ship-borne sensors, human sensors – especially our eyes – and data from electronic or paper sources on the bridge. If anything suggests that some information is unexpectedly out-of-step, we must take appropriate action, such as increasing safety margins by changing course or slowing down.

The spoofing of GNSS signals has been technically feasible for many years but, so far, has fortunately remained very rare. It's also worth bearing in mind that the physical spoofing of a buoy or other navigational marker (e.g. by moving its physical position) has always been feasible – but rare. More likely events that can compromise navigational safety are that a buoy has drifted or a marker has been damaged.

IT IS IMMENSELY DIFFICULT TO SPOOF EVERYTHING AT THE SAME TIME TO CREATE A CONSISTENTLY MISLEADING NAVIGATIONAL PICTURE

Fortunately, it is extremely difficult for those attempting to achieve undetectable malign action to spoof everything at the same time to create a consistently misleading navigational picture. As this includes the radar information and, not least, the view from the bridge windows, it is immensely difficult to pull off successfully.

Knowledgeable human correlation of target Radar and AIS data is a useful way to detect positional errors, whether they are caused by the system itself or are malignly introduced. Keeping a close eye on data from the sonar will alert you to any unexpected changes in well-surveyed areas – including if a spoofer or hacker was attempting to make you go aground.

In principle, the growing use of fully integrated navigation systems (INS) could give a highly sophisticated hacker a potential route for providing a seemingly coherent but misleading picture to the navigator, effectively by spoofing the entire display. However, the problems that must be overcome are huge, and so the probability of this happening today is extremely low. Importantly, when using an INS, a good navigator will still be checking for consistency, taking into account the view from the bridge windows and the individual displays of the primary sensors.

In any waters, you will be falsely confident if you only check whether the vessel is following its planned track, especially when under the control of a track-keeping autopilot. If the GNSS has been spoofed (or is just in error) it will continue to look as if you are consistently on track, however large the error. How good are the track checking and bridge security procedures on your vessel?

In ocean waters, regular consistency checks on the GNSS indicated position are also essential. Of course, the tie-up with the GNSS position will only be approximate, but is it believable? On an ECDIS-fitted vessel, look at using its automated DR/EP facilities to considerably ease this estimation.

Fortunately, maintaining good conventional navigational practice significantly lowers the risks of being dangerously mislead by both miscreant equipment and humans!

Contact RIN at: www.rin.org.uk | 1 Kensington Gore, London, SW7 2AT | Tel: +44 (0)20 7591 3134

TAKE 10

In this issue of *The Navigator*, cyber security has fallen under the spotlight. Here are ten key points to take in

1
Attacks happen

Cyber security should concern everybody, even those who are not computer experts. All seafarers can make a difference.

2
Data protection

Ship's officers must make sure they know who can access what data, and who is allowed in rooms containing key technical equipment.

3
Personal risk

Personal devices (smart phones, laptops, USB sticks) and ship systems (navigation, cargo, control, communication) are susceptible to attacks. Connecting personal devices to ship systems for exchanging data or even for charging is highly risky. Don't do it!

4
Know your weaknesses

Vulnerable systems include cargo, bridge, propulsion, access control, passenger services, public networks, administrative and crew welfare systems, and all external communication systems.

5
Be prepared

Cyber security plans require both safety and security aspects. All procedures for cyber risk management should complement existing requirements contained in the ISM Code and ISPS Codes. Contingency plans must be ready and well rehearsed for when something goes wrong.

6
App awareness

Android software and apps have a 90% likelihood of carrying malware; iOS have an 80% likelihood, of which you will be entirely unaware until it is plugged into something else (Futurenautics Crew Connectivity Survey).

7
Social skills

Social media is a key source of viruses or information for targeting individuals. Be aware of what you post!

8
Jamming and spoofing

Global Navigation Satellite Systems (GNSS – including GPS) are vulnerable to intentional and unintentional jamming and spoofing. By following conventional best practice, such as observing radar and visual references, you can minimise the risks.

9
Risk training

Every ship will have different risks and levels of risk. All crew should be informed and trained about the risks appropriate to their roles, how to manage them and how to react to an incident. Regular onboard updates, drills and mentoring are also key.

10
Want to know more?

Good advice on cyber strategies is widely available online. Specific guidelines for cyber security onboard ships has been published by BIMCO and can be found at www.BIMCO.org

WIN AN IPAD

We want to see who is reading *The Navigator*! Just post a picture of you with your *Navigator* on Twitter, including the hashtag **#NAVsnap**, or send us a message on Facebook with your photo attached (www.facebook.com/thenauticalinstitute) and tell us the name of your ship or your college, if you have one. Or send us the information in an email! One reader per issue will win an iPad mini as a thank you.

AND THE WINNER THIS ISSUE IS...

Congratulations to Gaville Dsouza, winner of our Issue 11 NavSnap competition! Gaville is Chief Officer on board *Spar Capella*. He is a keen photographer and has sent *The Navigator* some of his photographs taken on board.

Gaville Dsouza
NAVIGATOR CHAMPION