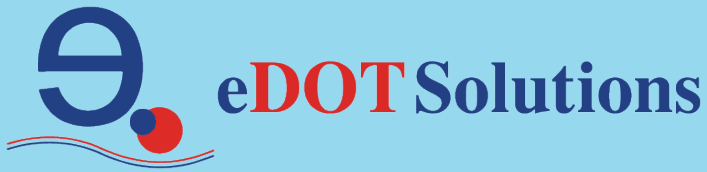


Custom-made Maritime Cyber Security Management Systems



Near Miss

Shipboard Cyber Security – Information Technology

Whitepaper



Rohit Messias

Head – Networks & Security
eDOT Solutions, India
EC Council certified Cyber Security Analyst



rohit@edot-solutions.com

Capt. Ruchin C Dayal

CEO, eDOT Marine, India
Master Mariner (MMI) | FIIMS (UK) | AMS - SAMS (USA)
MAIMS (Australia) | AFNI (London) | ISA



ruchin@edot-solutions.com

Table of Contents

1	Foreword	2
2	First things first – If only for the sake of good order!!!	3
3	What’s the big deal? IT infrastructure is everywhere.	5
4	Definitions	8
4.1	Incidents	8
4.2	Near-Miss	8
4.3	Near Miss Scenarios by Incident Vectors	8
4.4	Incident Vector – Inadvertent Infection	9
5	Effects of infection on a system or network – Recognizing a problem	13
5.1	Frequent mail errors	13
5.2	Sudden & noticeable change in the response time of the system (slowness)	13
5.3	Password errors	13
5.4	System crash / freezing of screen	14
5.5	Network failure	14
5.6	Unexplained change in the browser settings	14
5.7	Camera & Mike	14
6	Recognizing an IT near-miss	15
7	Conclusion	21

Near Miss – IT Incidents (Shipboard Cyber Security) Whitepaper

1 Foreword

With so much focus on understanding of OT (operational technology), and understandably so, it being a new element in the maritime narrative, the significance of IT (information technology) is seemingly undermined. There is a growing need to reiterate, that the digitization revolution started with IT. The terms, IT & OT have now been categorized separately basis the designed output of the software & hardware in question, however, the basis of any automation is software and hardware, running a custom programme to drive related machinery elements; this may be in the form of an HMI (human machine interface – can be a regular computer running a Windows or Linux operating system), PLC (programmable logic controller), or a custom-made machine driven by IT resources, integrated with machinery, to perform critical onboard operations. Furthermore, IT, even in the current sense of the data driven cyber security landscape, is essential for the day-to-day shipboard functions; from emails to accounting, to records, to planning, to checklists, to digital communication, etc. Hence, while IT may not have an immediate or direct impact on critical shipboard operations like Navigation & Propulsion, it remains an extremely important segment in the shipping adventure.



[OT Risk Assessment](#)
Whitepaper



[Near Miss - OT](#)
Whitepaper



[Cyber Security & Ships](#)
Published Article

Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

2 First things first – If only for the sake of good order!!!

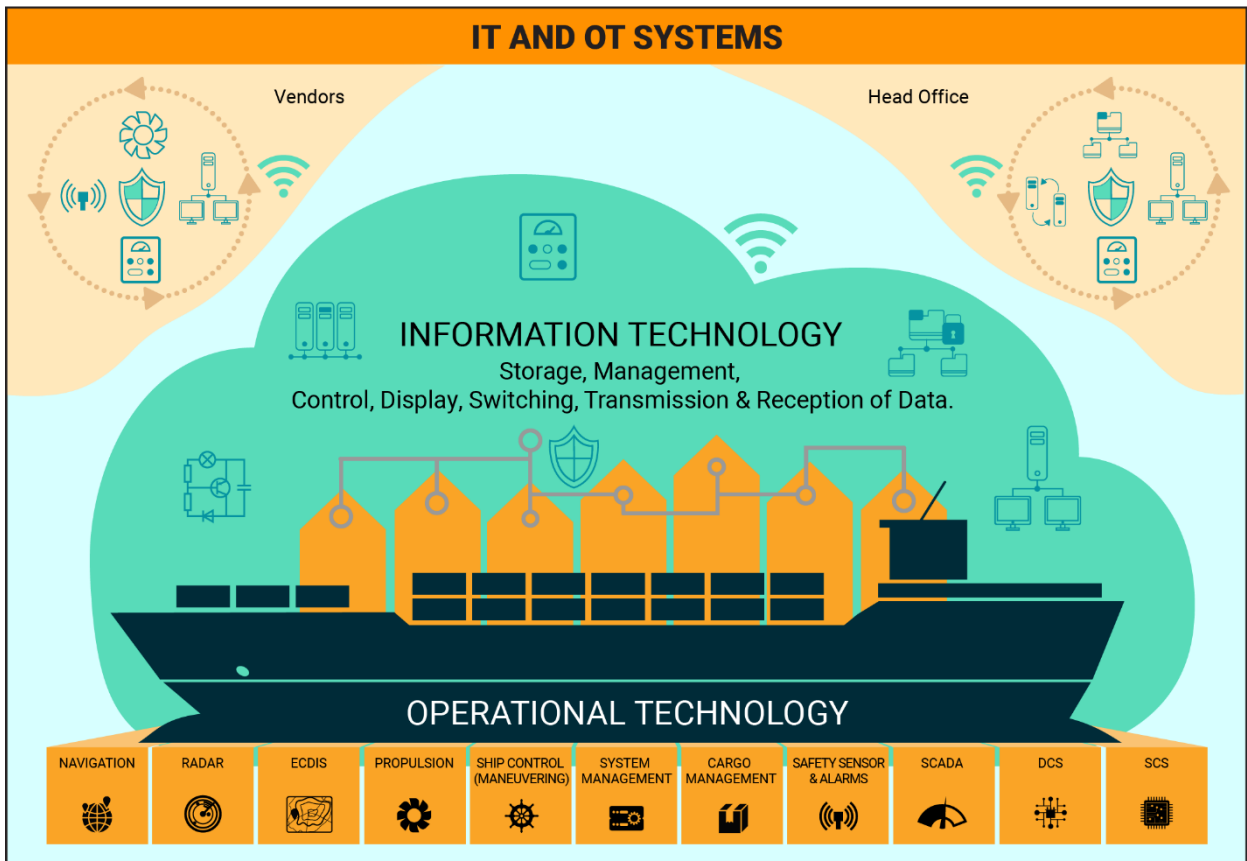
IT Systems	OT Systems
Software & hardware, where the designed output is communication, is termed as IT (information technology).	Software & hardware, where the designed output is action, is termed as OT (operational technology).
Usually pertains to typical computing systems (networked or stand-alone) & their related peripherals, like switches, printers, etc.	Often pertaining to SCADA (supervisory control & data acquisition) systems, such as the power management system of the ship.
Non-critical & offline systems. Can be rebooted without affecting vessel’s operational levels.	Critical & online systems. Cannot be rebooted as will directly affect vessel’s operational levels.
IT systems have a COMMON output. Each system may run different Operating Systems (OS), different versions of office, different anti-virus software, but will have a common output – communication. Can be in the form of accounting/inventory data, email, verbal speech, etc.	Each OT system will have a UNIQUE output – physical change. From closing of valves to starting of motors, from opening drains to dispensing of material, etc. Each OT system usually has its own unique firmware. This may have an ability to use HMI (human-machine interface) using a standard windows operating system.
IT systems are usually standardised – using generic hardware and software, like MS windows, Intel motherboards, etc. These are designed to be patched and maintained by inhouse IT teams or outsourced IT maintenance contracts.	OT systems use customised hardware and proprietary software, which can be patched and maintained only by the makers or their authorized and trained service contractors.
Early signs of malfunction or infection are relatively easy to detect – sluggish speed of the PC, unwarranted pop-ups, or the usual hanging of the machine. Most times, just a simple reboot and running the antivirus scan may resolve the issue.	Most times, infection of an OT system may only be detected when a malfunction affecting the operational integrity of the vessel takes place – power shutdown, non-responsive engines, failure of ECDIS, etc. Rebooting of these systems is not an option.
Risk assessment & treatment (RART) of IT systems is based on standard parameters – OS, AV, software licenses, etc. – Each system/machine will be assessed individually for the status of their standard defined parameters,	The output of OT systems is unique to each system and contributes towards fulfilling diverse onboard operational requirements. Hence, the risk assessment is based on the impact the OT system may have on a particular

Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

based on the deliverability of the common output – communication.	onboard activity, such as Navigation, propulsion, etc.
Makers/OEM inputs are usually not required for RART.	Crucial inputs from makers or integrators or specialist technical service contractors are required for RART.
Integrity & Confidentiality are important. Usually has no bearing on immediate operational safety. IT systems can be considered as offline.	Integrity & Availability are important. Has an immediate and direct bearing on operational safety. OT systems are online systems.

The following illustration encapsulates the categorization of onboard common equipment (systems) into IT & OT, based on their designed outputs.



Having absorbed the difference in the rationale behind categorization of systems into IT & OT, let’s try and focus on the matter at hand – Recognizing & Reporting of Near-Miss with regard the use of IT systems. Oh, but before we do that, there is another small matter we need to address.

3 What’s the big deal? IT infrastructure is everywhere.

Landlubbers often ask, what’s the big deal with onboard IT infrastructure. Aren’t the IT networks in offices and homes looked after and maintained without much fuss? So, what’s the difference? And why should seafarers be expected to be careful in IT infra handling and educated in recognizing irregularities which may affect system functionality. Is a system failure onboard a vessel equivalent to that in the office?

Let’s try and find some reasonable differences.

Shore / Office / Home IT	Shipboard IT
<p>Large to medium size ship management companies, almost always, have their own IT department. Hence, there is in-house competence to resolve the day-to-day issues raised by the office staff.</p> <p>From network cable failure to hard-disk crashes, there is in-house competence for immediate attendance.</p> <p>The smaller companies usually have an AMC in place from a vendor across the street.</p>	<p>Ships do not carry any IT qualified & competent staff. They must depend upon telephonic or email support. Most times they are talking to an IT engineer who has no clue about the nuances of shipboard life or the level of IT literacy of the ship-staff.</p> <p>“Ports” & “switches” ring different bells to the shore IT engineer & the ship-staff.</p> <p>This kind of remote troubleshooting is a cumbersome & time-consuming affair and seldom has long-term benefits.</p>
<p>Maintenance schedules, including back-ups are performed by professionals. There is almost never a problem with upgrading and updating of the operating system, anti-virus definitions, MS office, etc. – as most of the world now is exposed to high speed & affordable internet access.</p>	<p>Maintenance schedules for onboard IT are non-existent. Nobody attends to anything unless something doesn’t work. All back-ups are performed by related onboard personnel, in addition to their respective shipboard duties. Furthermore, onboard internet speeds are very low. We are talking of shared 1-3 Mbps. This makes the updating and upgrading of software a very cumbersome affair. Most times, updates are sent on DVDs or external drives from the office. Really, not the ideal process.</p>

Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

<p>Common spares (RAMS, switches, connectors, cables, SMPS, etc.) are maintained by the IT department or are easily available across the counter.</p>	<p>IT spares are almost never maintained onboard. The very nature of the spares being almost universally compatible, invites misuse of the spares, and even the best of intentions to maintain some kind of an inventory of IT spares onboard, just doesn't work.</p>
<p>The redundancy of systems in an office, coupled with the availability of an IT technician at hand, makes the failure of a system non-critical.</p>	<p>Onboard IT inventory is always maintained just as much as is absolutely necessary. Failure of a system may be critical, especially when the main system for vessel email fails, or when the system for the PMS fails. In addition to the inconvenience of setting up another means of data transmission, it also eats into the schedule of the seafarers, especially when they are hard pressed for time – nearly always!</p>
<p>Office IT infrastructure plays almost no role in statutory surveys or certifications, vettings, or audits. Policies (eg: for password change), software licenses, purchase protocols, etc. are all handled by the IT department.</p>	<p>Shipboard IT infrastructure is under the scrutiny of all onboard inspections. With the IMO Res 428 in place, PSC inspectors look at onboard IT with rejuvenated motivation. Software licensing records are almost never available onboard. Furthermore, purchase of software as well as hardware is seldom regulated, with the technical superintendents making decisions to bide over case by case. In the long term, a multi-vendor, multi maker IT environment becomes established onboard.</p>

Now, having understood the difference between IT & OT, as well as the difference between the IT environments onboard and onshore, it becomes easier to understand the importance of developing a controlled system of handling, maintaining onboard IT equipment, as well as establishing a structure for continual improvement. This is essentially a part of the shipboard CSMS (Cyber Security Management System) as mandated by the IMO res 428 as well as the BIMCO Industry Guidelines.

Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

Recognizing, reporting and recording of IT near-miss & incidents is an integral part of the process, and is expected to go a long way in experiential learning of the seafarers, as well as educating the shore IT support staff about shipboard experiences and how to make the change in vocabulary & instruction-documents for better understanding of the seafarer.

There is also a glaring requirement of basic IT & network training for ships officers. While a few mature companies have embarked on this visionary journey of training, most companies are yet to find the need to do so.

Think before you respond to unknown mails, messages and calls.
Protect yourself from phishing attacks.

Whaling
Scammers target a specific group or profile, for e.g. CEOs. The attacker impersonates an employee or trusted source to acquire account or payroll details.

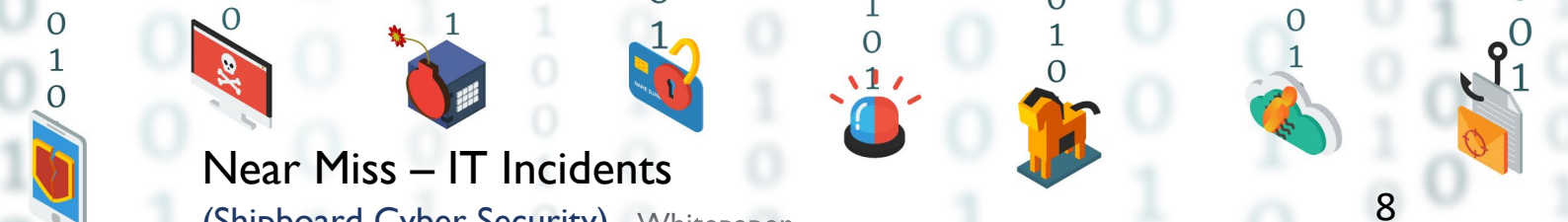
Clone Phishing
E-mails are sent from a familiar email id with malicious software. Scammers also create cloned websites to steal data.

Email Phishing
Scammers use fear tactics or lure the victim with offers. They also demand urgent action or request the victim to confirm personal information.

Pop-up Phishing
Scammers send fraudulent messages which appear as pop-ups that redirect you to fake websites with malicious software.

Email Spoofing
This is an individually targeted email with tampered information.

Spear Phishing
Scammers impersonate friends, relatives, family members to acquire sensitive information.



Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

8

4 Definitions

4.1 Incidents

An Incident may be defined as an occurrence of an undesired event, **adversely impacting**

- the efficiency or integrity of shipboard operations; or
- the safety of the vessel, shipboard staff, cargo; or
- the environment.

Most mature management systems develop categories or levels of “incidents”, each level designated by a code (e.g., I1, I2 or A1, A2, A3), basis the seriousness of the incident, with respect to actual effect and loss to the vessel, crew, cargo, or the environment.

4.2 Near-Miss

‘Near-Miss’ in layman terms is a ‘close shave’ or a ‘close call’ or even a ‘lucky escape’. In the maritime world, it is quite common to be simply defined as:

- a) When a potential risk is identified, and due to corrective action taken in time, an incident is avoided — usually by due diligence; or
- b) When a potential risk is not identified, and hence no corrective action is taken. However, an incident is still avoided — usually by sheer luck.

For recognizing or identifying an IT related near-miss, it is necessary to understand, how an IT system is affected in the first place. Except for dedicated or designated systems like the ship’s email or the VDR or any other system where the confidentiality & integrity of data generated is perhaps paramount, most onboard systems are used by multiple personnel; Many of whom have access to training servers and even the crew internet; some may even have access to the business network of the vessel. An infection of the onboard systems can take place either inadvertently or purposefully with malicious intent, both having similar results on many occasions.

4.3 Near Miss Scenarios by Incident Vectors

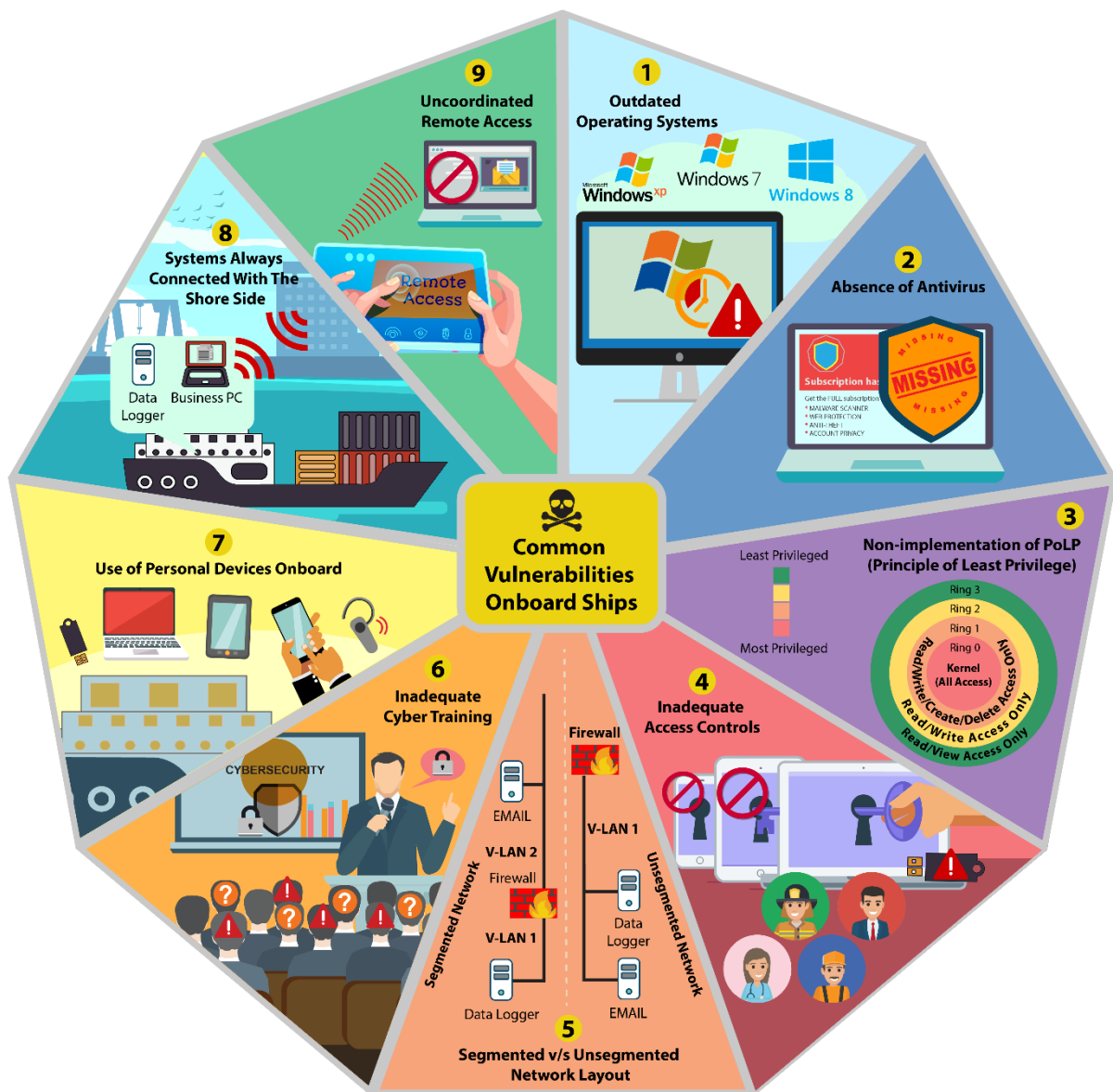
The path or means by which a system/computer or network server is accessed, and infected with malicious code, with an adverse outcome, is called an Incident vector. When the infection is perpetrated deliberately and illegally, exploiting

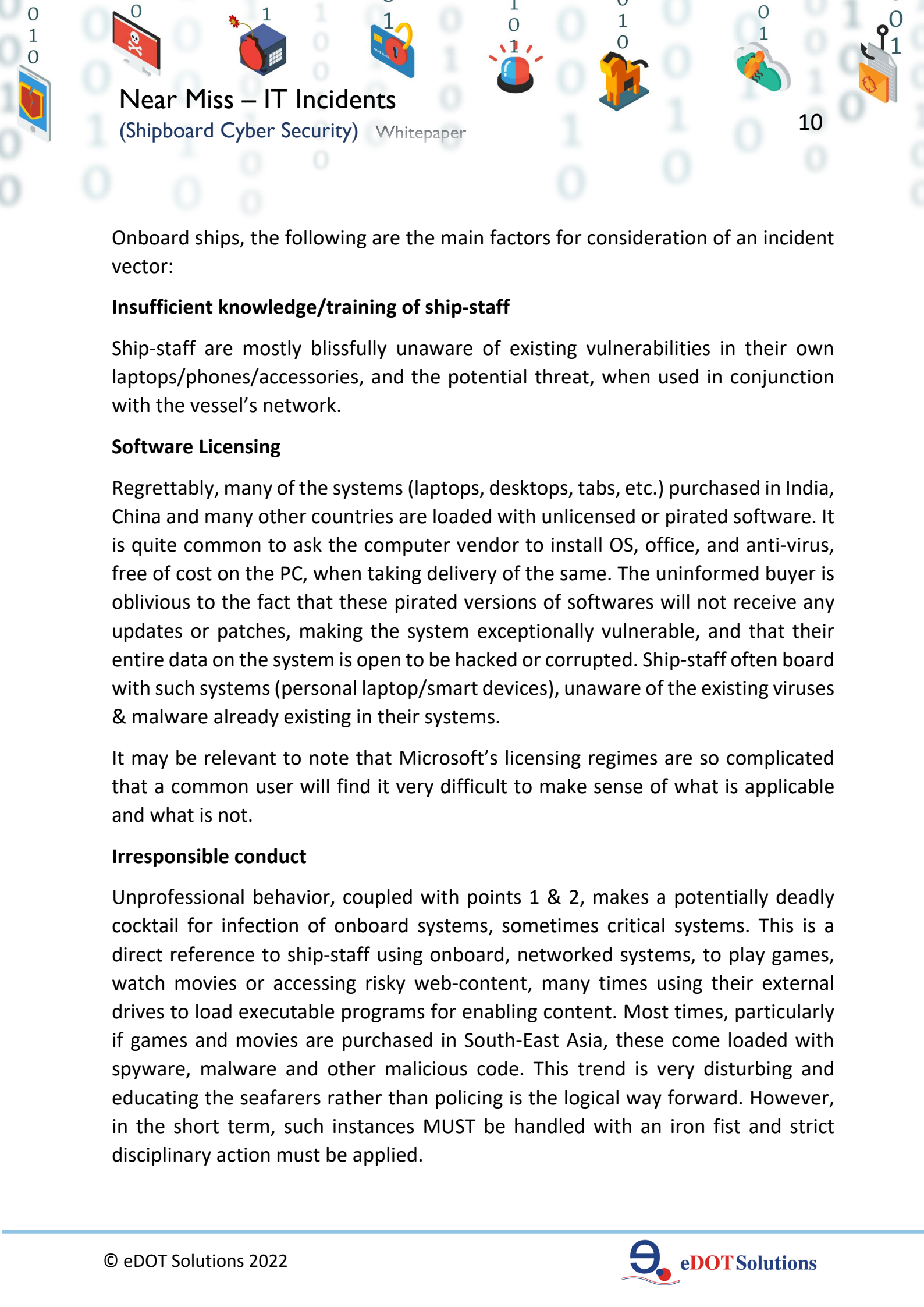
Near Miss – IT Incidents (Shipboard Cyber Security) Whitepaper

system vulnerabilities, with a malicious intent, then the Incident vector may be referred to as an Attack vector.

4.4 Incident Vector – Inadvertent Infection

Perhaps the most common source of system infection, not only onboard ships, but across homes and offices, and around the globe.





Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

10

Onboard ships, the following are the main factors for consideration of an incident vector:

Insufficient knowledge/training of ship-staff

Ship-staff are mostly blissfully unaware of existing vulnerabilities in their own laptops/phones/accessories, and the potential threat, when used in conjunction with the vessel's network.

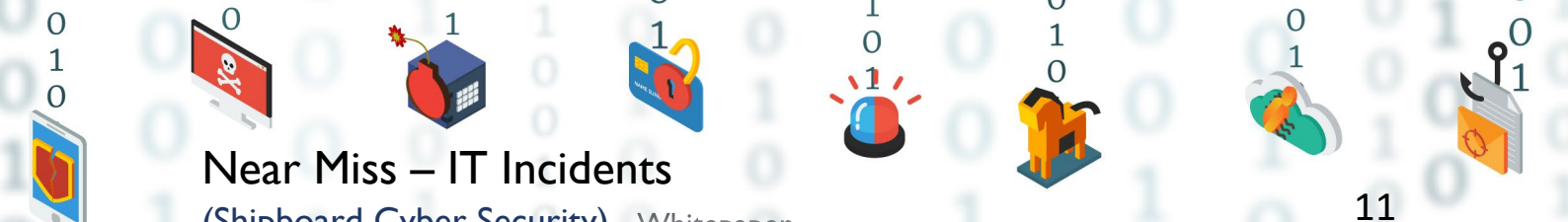
Software Licensing

Regrettably, many of the systems (laptops, desktops, tabs, etc.) purchased in India, China and many other countries are loaded with unlicensed or pirated software. It is quite common to ask the computer vendor to install OS, office, and anti-virus, free of cost on the PC, when taking delivery of the same. The uninformed buyer is oblivious to the fact that these pirated versions of softwares will not receive any updates or patches, making the system exceptionally vulnerable, and that their entire data on the system is open to be hacked or corrupted. Ship-staff often board with such systems (personal laptop/smart devices), unaware of the existing viruses & malware already existing in their systems.

It may be relevant to note that Microsoft's licensing regimes are so complicated that a common user will find it very difficult to make sense of what is applicable and what is not.

Irresponsible conduct

Unprofessional behavior, coupled with points 1 & 2, makes a potentially deadly cocktail for infection of onboard systems, sometimes critical systems. This is a direct reference to ship-staff using onboard, networked systems, to play games, watch movies or accessing risky web-content, many times using their external drives to load executable programs for enabling content. Most times, particularly if games and movies are purchased in South-East Asia, these come loaded with spyware, malware and other malicious code. This trend is very disturbing and educating the seafarers rather than policing is the logical way forward. However, in the short term, such instances MUST be handled with an iron fist and strict disciplinary action must be applied.



Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

11

Attack Vector – Deliberate Infection with malicious intent

Presently rare; with the low internet speeds onboard merchant ships, hacking into a vessels network remotely is not easy. Furthermore, with most of the satellite communication system providers (Inmarsat, VSat, etc.) managing firewalls themselves, the active security level is acceptable. Nonetheless, vulnerabilities exist, and can be exploited.

Let us look at some Common Attack Vectors by which the Cyber Attacks unfold:

External/Removable Media:

An attack executed from removable media (e.g., flash drive, Ext. hard drive, CD) or a peripheral device.

Malicious code is transferred into the vessel's network using a personal device. This may be applicable in the case of the actions of a disgruntled employee with sufficient IT knowledge or when third parties like ship chandlers and technicians board the ship – such individuals may be compromised and may be working towards a hidden and a long-term agenda of gaining control of confidential and critical information communication to and from the vessel. This kind of an attack vector will usually involve systematic planning and a targeted approach – especially when perpetrated by third parties boarding the vessels.

Web:

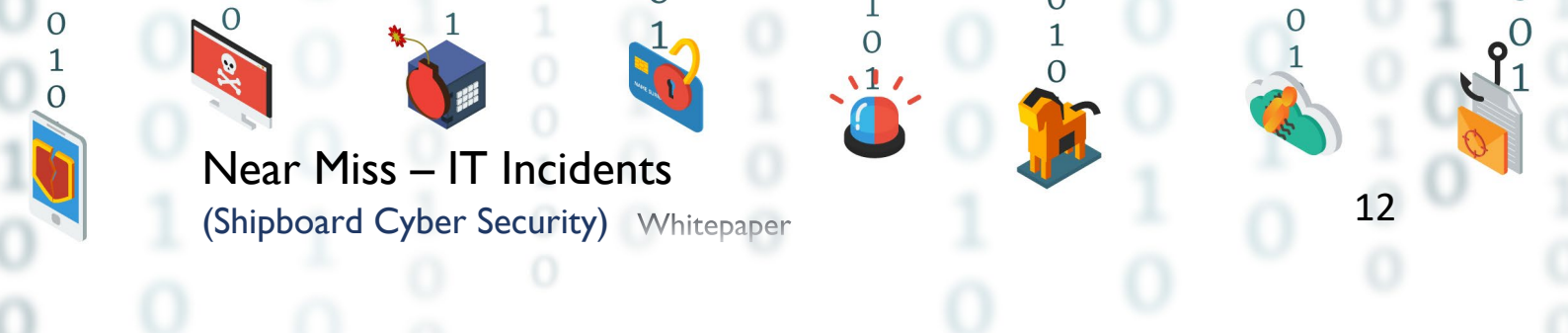
An attack executed from a website or a web-based application (e.g., drive-by download).

This is rare, as the main firewalls of the ships are usually well managed, blocking unsuitable/unsafe websites and downloads. While motivated individuals or organizations may design, develop, and deploy misleading web-content, hoping that gullible browsers may download disguised, malicious code, ships are shielded by reasonably well managed firewall.

Email:

An attack executed via an email message or attachment (e.g. malware infection).

Extremely common method adopted by hackers for delivering malicious code into systems. A visibly harmless email from supposedly a relatively known entity




Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

12

(contact or Amazon or Netflix or from the bank), asking the user to click on a link for confirming “general” information. While awareness is increasing, there are individuals who get roped into clicking such links. Good news for ships is that the download prompted by such clicks is usually disallowed by the main firewall. End-point security on the system may also warn the user of nature of the download.



Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

13

5 Effects of infection on a system or network – Recognizing a problem

IT systems, as well as networks, across makers, follow a relatively standard protocol of hardware and software, and have a common output – data for communication. Hence, irrespective of the incident/attack vector, owing to the commonality of software, hardware and output, most IT systems exhibit very similar symptoms when infected or damaged. Master and ships officers must be aware of these signs. These may be highlighted when systems are being used for mail, accounting, inventories, PMS and any other shipboard activity. Some of the tell-tale signs of system infection are as follows:

5.1 Frequent mail errors


- Inbox not refreshing, Sent mails not showing
- Email addresses not auto-prompting
- Unexplained delivery failure
- Receiving attachments with unrecognizable extensions
- Corruption of outlook folders

5.2 Sudden & noticeable change in the response time of the system (slowness)

- The system doesn't respond as expected or "like before".
- Takes "forever" to perform single tasks like "saving", "printing", "opening" a file.
- Upon accessing "task Manager" (press control+alt+delete), the CPU usage as well the memory is showing close to "100%".

5.3 Password errors

- The system refuses access even after entry of the correct password.
- The system allows access without password, despite being password protected.
- The system prompts for untimely & unplanned password change.
- During changing of password, system doesn't accept the new password despite following the set standard protocols.



Near Miss – IT Incident

(Shipboard Cyber Security) Whitepaper

14

5.4 System crash / freezing of screen

- While software programs do experience “crash” (many times due to insufficient memory), the frequency of such an instance will increase, when a system is infected.
- The system gets into a loop during restart after a crash. Windows doesn’t start.

5.5 Network failure

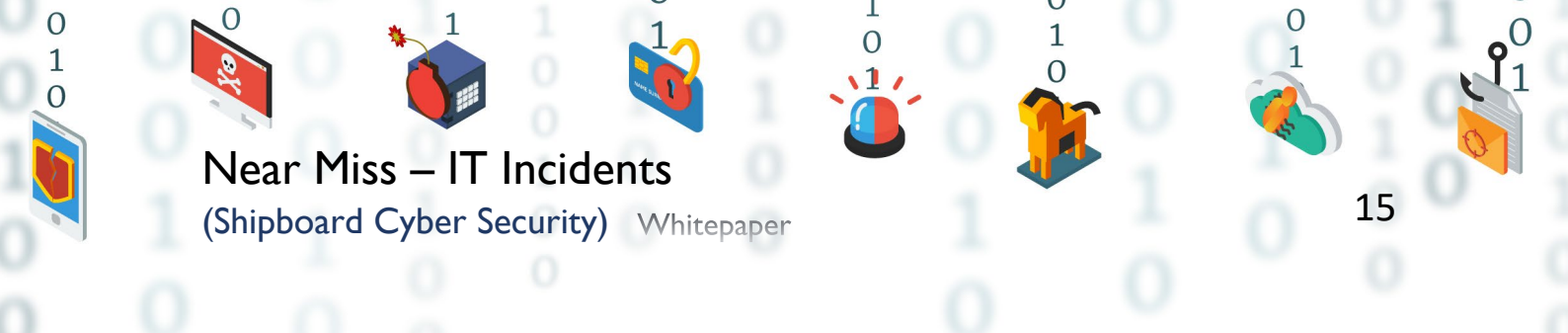
- Unexplained intra-connectivity problems, despite checking the network hardware – switches and cables.
- Unexplained prevention of access to crew internet or training networks.

5.6 Unexplained change in the browser settings

- Frequent and annoying pop-ups.
- Browser observed to have installed unrecognized plugins, involuntarily.
- Browser redirecting the user to unrecognized web pages.
- Browser prompting for frequent updates.
- Unexplained loss of browsing history & stored links.
- Unexplained loss of auto-logins and stored passwords.

5.7 Camera & Mike

- Unexplained change in the settings for camera & microphone.
- Camera observed to be in “on” position involuntarily.



Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

15

6 Recognizing an IT near-miss

While recognizing an OT near-miss is fairly complex, the tell-tail signs of a problem in an IT system are very straight forward and easy to relate to. This can be attributed to the heavy standardization of the equipment. We use the same equipment in homes and offices and are aware of generally acceptable performance standards. It may be relevant to note that unlike OT, the quick fix method for IT related problems is a system reboot. It generally helps most times. However, in the case of an infected system, the experienced malfunctions will reappear sooner than later.

Few IT onboard near-miss scenarios have been produced in the following section. These are not exhaustive but only meant for gathering the thought process of seafarers in the right direction. Hopefully, the same may help for onboard IT near miss reporting.

Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

SCENARIO 1

It's a sunny Monday morning, in the Atlantic, sailing east, due to arrive in Gibraltar for bunkers and stores.

Master is sending mail to agents, serving 5 days' notice of arrival. Upon drafting the notice, Master presses the "send" button and gets busy in other shipboard functions.

After a couple of hours, he notices a "delivery failure" notification in his inbox. He also realises that the usual end-of-the-day message from his superintendent, based in Hong-Kong hasn't arrived... "that's strange", he thinks.

He sees that the satellite connectivity is showing "ok". He decides to reboot his mail computer; goes through the prescribed checks and accesses the mail. No mail!!

ACTION

Master makes a call to his superintendent, explains the situation. Its already late night in Hong-Kong but the superintendent makes a call to their regular IT vendor.

IT Vendor

The IT vendor smells an infection after speaking with the Master – uploads updated virus definitions to the vessel. Vessel downloads the same using their business network on another system.

The IT vendor then guides the Master on how to over-ride the blocked USB ports and run the updated anti-virus on the mail computer.

Antivirus

Upon scanning the mail computer, multiple viruses are detected and deleted. While the mail starts working, an entire backup of the mail folder is taken, and the system is formatted.

Email Backup

The backup of the mail is checked for virus and corruption – found clean. The system is then loaded with the backed-up data.

Other than a few anxious hours, no real incident or inconveniences take place – near-miss.

Near Miss – IT Incidents (Shipboard Cyber Security) Whitepaper

SCENARIO 2

Vessel is loading at the Bitor Single Point Mooring buoy, at Puerto Jose, in Venezuela. The Chief officer is handing over to his reliever and looking forward to a well-earned leave. He was stuck onboard for over a year on account of COVID.

Loadicator Software

The incoming mate is not happy with the loadicator; he used to be on a sister ship earlier and is carrying an updated program on his external drive.

USB Drive

He claims that the new version is far more user friendly than the present version in use. As soon as he takes over, he updates the loadicator software using his external drive.

The program updates but the laptop becomes sluggish.

WHAT!

ACTION

A couple of days later, the Chief Officer connects his external drive to the training computer for uploading his CMS (competence management system) status.

This computer has an updated anti-virus system running; almost immediately a warning of an infected file is displayed on the monitor, and then more warnings show up. The anti-virus software deletes and cleans the drive. The matter is referred to the IT team in the office.

However, no major problems are encountered, and the vessel completes loading and sails to Europe.

It was inferred that the Chief officers drive had been infected by multiple viruses & malware, while he was on leave, at home, when he had used his drive with his domestic systems.

The loadicator did not display any warnings as it was supposed to be a stand-alone system having no internet, an outdated windows XP OS and not loaded with any antivirus.

The IT team had to format the loadicator and reload the stability software using the Class approved back up DVD carried onboard.

CISO

USB Usage Policy

This was a great escape of sorts, by sheer luck. The CISO of the company had a serious look at the USB usage policy and developed a process for blocking the same.

SIGH!!

The Chief officer, the main protagonist, was reprimanded and pushed back in prospects of promotion.

Reloaded Software

**Sheer luck allowed the vessel to complete loading and sail on time.
A big lesson for ship & shore staff – near-miss.**

Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

SCENARIO 3

It's 0800 hrs, in the calm Bay of Bengal, this particular vessel, a VLCC, has just been made fast to a SPM (Single Point Mooring), for discharge at Paradeep, India.

The pilot is onboard and will remain onboard until the vessel completes discharge and is on her way. This is a routine practice in many ports, all over the world.

Master leaves the pilot on his own and proceeds to the office for a meeting with the Ch. Off and the terminal representatives.

Please call me if you need me !!

Meantime, radar technicians board the vessel for a maintenance call and make their way to the bridge. They are accompanied by the 2nd mate, who has hardly got any sleep in the night; once the technicians get to work, he leaves the bridge to catch a nap before he is back on watch at noon.

The pilot in attendance is very senior, in his 60's, and is content listening to music on his cell phone.

At about 1130 hrs, the technicians notice that the pilot has plugged the charging cord of his cell phone into the main mail computer.

They immediately ask him to remove the same; the pilot is unable to understand the fuss – he has left active sailing 15 years back and is not aware of what cyber-security is ???!! The technicians run down to the office and have the Master accompany them on the bridge.

OHH!!

USB Charging Cord

Whats All The Fuss !!!

ACTION

The Master calls the poor 2nd mate back on the bridge. A virus scan is performed on the computer.

No viruses are found; however, the matter is reported to the CISO, who has the office IT team perform a full system check with the latest downloaded virus definitions.

CISO

While everything seems OK. The Pilot's cell phone is checked – its an old NOKIA with hardly any multi-media functionality. Furthermore, there is no connectivity in their present position.

Old Nokia

A more sophisticated phone, handled by a savvy individual may have meant an active load of malwares and viruses on the phone. The pilot, who by his age and nature was not inclined towards active internet and was reconciled to hearing music stored on his device.

Sheer Luck! It was decided to block the USB of the mailing computer. This used to be kept ready for use for the sake of sending scans, logs, etc. to the office.

Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

Some other situations, which may be classed as “near-miss” are produced in the following tabular format:

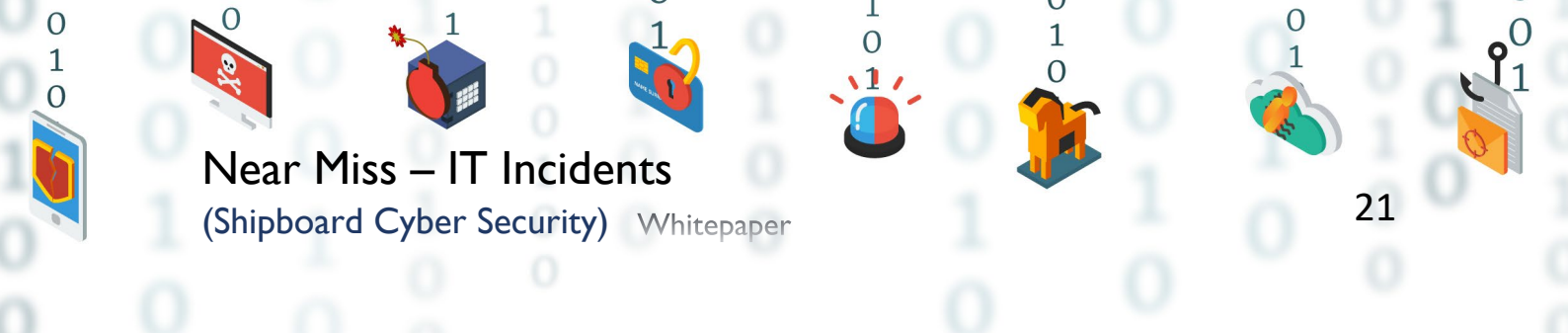
CYBER SEC. INCIDENT VECTORS	NEAR MISS SCENARIOS	
External / Removable Media	1	Ship staff negligently connects a malware infected USB drive to a PC without anti-virus (ex. The Loading computer @CCR), but the malware didn't execute due to outdated OS & no internet on the PC. The same drive was connected to a different PC onboard, but malware was detected and neutralized by the anti-virus Software.
	2	USB blocker missing from Critical OT PC/System. But no unauthorized USB access attempted thus far.
Improper Usage	1	Master of the Vessel unwittingly shares his Windows login creds (with admin access) on request by OT Shore technician without supervision. Shore technician accesses the internet to download a Software update and transfers the downloaded data to Personal USB Pen drive, no foul play involved but Pen drive could have been infected with malware.
	2	Remote access by unauthorized third-party App (ex. Ammy admin) given by Ship staff to remote technician unwittingly to access Ship Network for troubleshooting.
	3	Windows Admin Login Password written down on piece of paper by User and stuck on Bridge Business Computer in plain sight, but no unauthorized login has taken place so far.
Email	1	Ship Staff unwittingly clicks on a link in a phishing email, but the phishing site has been taken down in time, so no damage was done.
	2	Ship staff clicked on phishing email link but the URL re-direct is blocked by VSAT firewall rule preventing malware downloads.
	3	Master reports about random Spoofing/Phishing emails directed to VSL email ID to IT Team. The timely reporting of this info allows IT Team to blacklist the email ids preventing further potential risk of these mails being opened by VSL Staff.

Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

20

Web	1 User downloaded a zipped attachment with Malware, but file could not execute due to WinZip App being uninstalled from Computer.
External Threats Computer / Server system breach (Attempts to gain unauthorized access)	1 Remote user login Password of an online PC/System were duly updated by Admin in compliance with policy; post this unauthorized login attempts (failed login attempts) were found in security logs by Unknown actor in an attempt to gain access with compromised passwords.
	2 Ransomware attack attempted on Ship Business Network PCs but foiled due to timely Patching/Security updates of Windows OS & Antivirus Software by SCyO/IT Team.



Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

21

7 Conclusion

Let's admit it, we are a slave to technology. How would we manage our life, without our laptop, our smart phone, or without a 24x7 high speed internet connection? Not a pleasant thought !! However, how many of us are really gadget savvy? Do we really bother to understand the nuance of how a technology works, or are we just hooked to the conveniences it brings? LAN, WAN, 4G, Cloud, Network sharing, bandwidth, etc, etc; do we really understand what these terms bring to the table? We may scramble to possess the latest iPhone or the latest Galaxy models, but how many of us actually use or even understand all the functionalities which come with the gadget? Very, very few, I would reckon.

So yes, our intellectual capabilities are far less developed than technology itself. We are lagging far behind. What becomes really relevant to this paper is that we carry this baggage of poorly understood technology into our offices and even onboard ships.

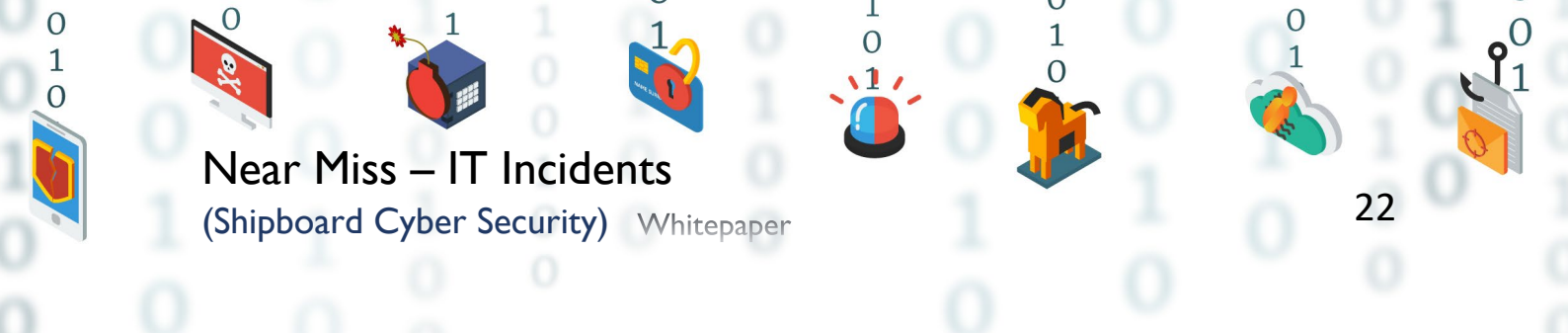
Like it used to be said, in the days gone by, “seafarers boldly venture into uncharted seas”, today we are doing the same with technology, without realizing that we may be putting critical operations at risk, when we boldly handle technology without properly understanding it.

While our offices may be complemented by an IT department, onboard ships seafarers are most often left to the mercy of their own intellect. From firewalls, switches, VLANs, to systems, customized programs, to data instruments, an entire gamut of an IT environment exists onboard, and we are dependent on it for many a daily chore.

The only way forward is getting better informed, and with the IMO Res 428 leading the progress in Maritime Cyber Security, we are left with little or no option. Training is an integral part of any responsible and mature CSMS. Incident & “near-miss” reporting plays a big role in training – contributing in “experiential learning”.

If we can't think of life without our technology, then we will have to come to terms with the efforts we will need to apply, for ensuring a cyber hygienic environment. We will have to pledge to the following:

- Make a conscious effort in understanding our limitations, read the onboard cyber security training manual
- Spend time in reading related topics, upping knowledge quotient
- Use & invest in licensed software ONLY
- Frequently update OS, office & antivirus
- Abide by onboard instructions related to CSMS
- Unless under direct instruction, do not try to “repair” IT hardware or “fix” software
- Adopt a responsible social media behavior
- Follow established best practices related to email, specially phishing related
- Do not buy compromised gaming or pirated movies
- Develop responsible browsing habits



Near Miss – IT Incidents

(Shipboard Cyber Security) Whitepaper

22

The above list is not exhaustive and only indicative of where we need to head. While we most definitely need to follow this prescribed regime onboard, it will help the seafarer immensely to follow the same practices at home, while on leave. This may also rub off on family and friends, only to increase the overall intellect and hence the cyber hygiene culture.

It's a long road ahead and we must remain committed to follow the course.

Custom-made Maritime Cyber Security Management Systems



Email: contact@edot-solutions.com

Website: edot-solutions.com

India. Singapore. Texas. Philadelphia



ISO/IEC 27001:2013



ISO 9001:2015 Certified



ISO 21001:2018

GOA (INDIA)

🏠 FO/2, 4th Floor, Rukmini Towers, Near Tilak Maidan, F.L. Gomes Road, Vasco-Da-Gama, Goa – 403802.

☎ +91 832 2501715

✉ contact@edot-solutions.com

SINGAPORE

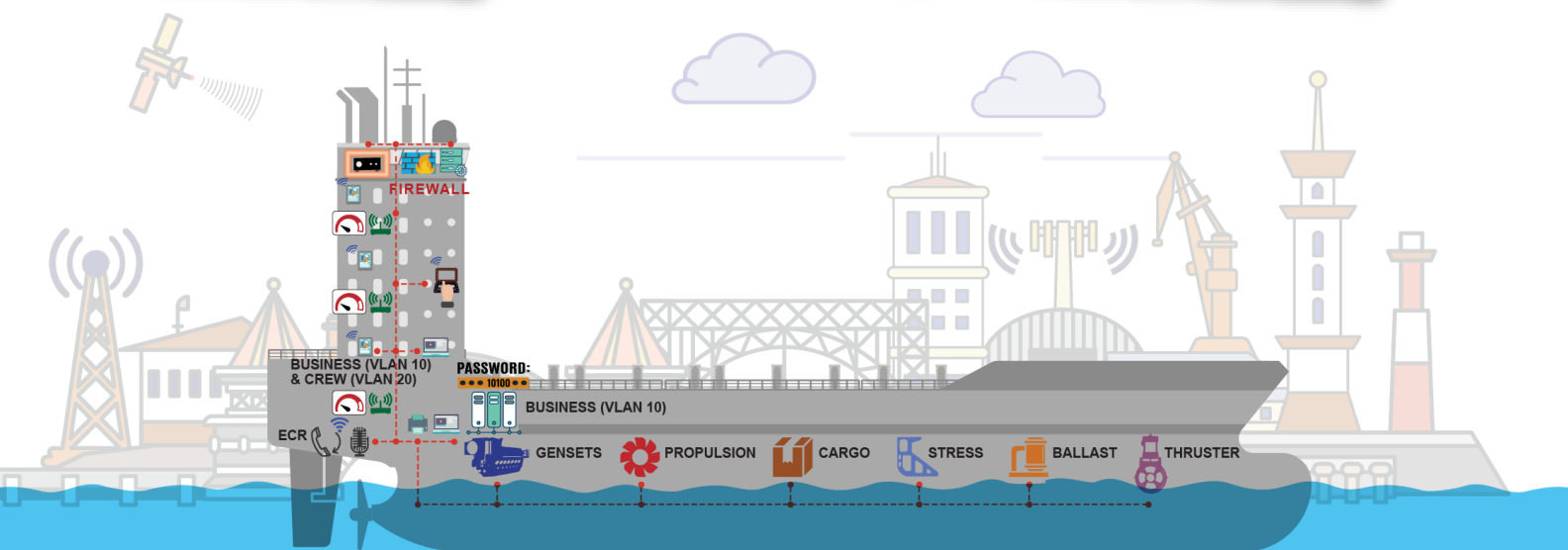
🏠 10, Raeburn Park, #02-15E, Singapore-088702

TEXAS

🏠 7618 Westmoreland Drive, Sugar Land, TX 77479

PHILADELPHIA

🏠 Yorktown CT, Malvern, PA 19355, U.S.A.



© eDOT Solutions. 2022

QUALIFIED

ACCREDITED

EXPERIENCED