Cyber Security & Ships

Do we understand | Are we preparing | Can we sustain

Capt Ruchin C Dayal
Master Mariner-MMI, India
AMS-SAMS(USA), FIIMS-UK, AFNI-London, MAIMS-Australia

eDOT Solutions

ISO/IEC 27001:2013

ISO 9001:2015 Certified

ClassNK Certificate of MET

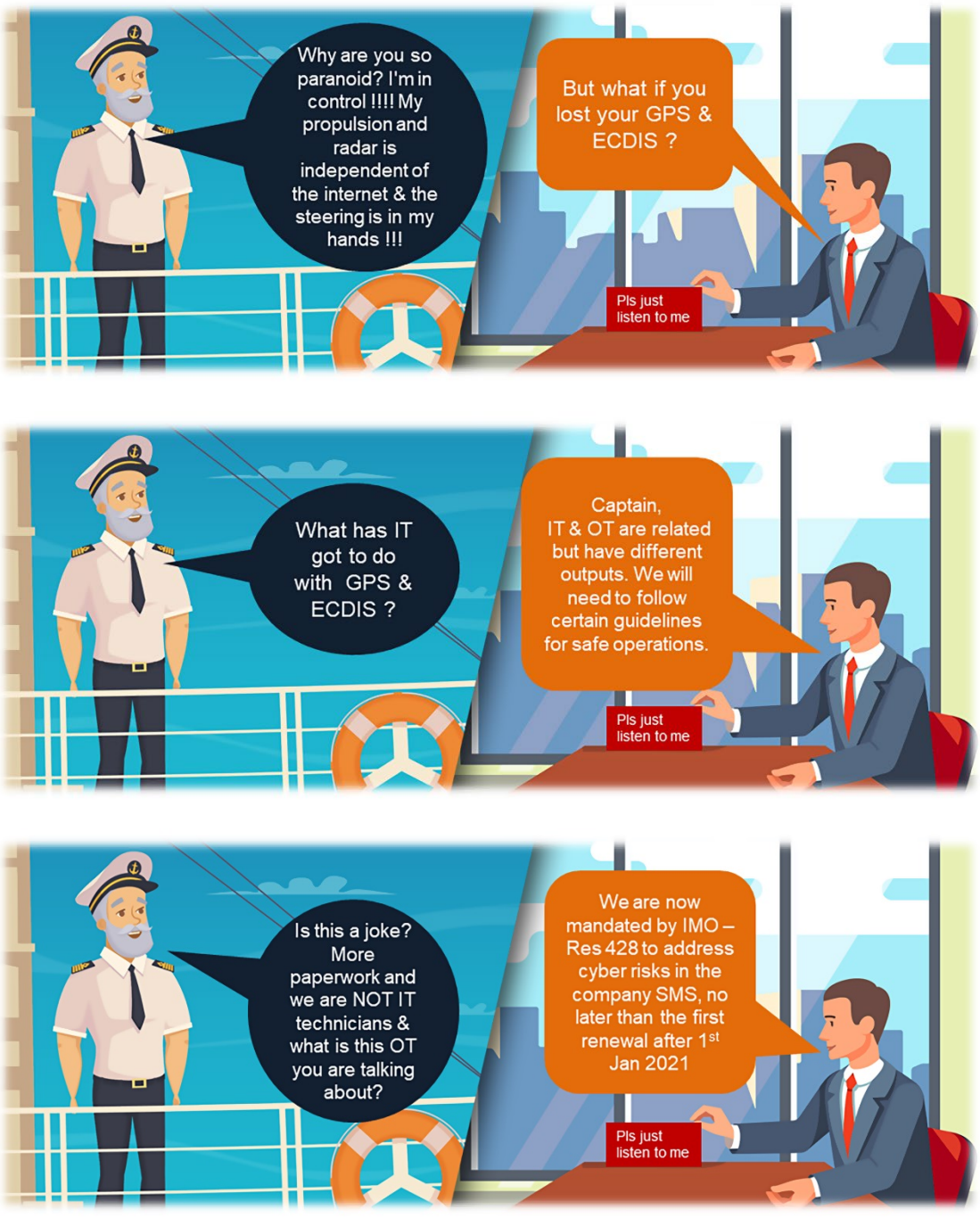
ClassNK eDOT are working for NK-CSMS's consultation services

BIMCO MEMBER

The maritime industry has been overtaken by technology, & while we are struggling to come to terms with it, cyber-attacks on maritime infrastructure are gaining critical momentum. In this article, I have tried to identify some of the vulnerabilities existing onboard merchant ships, analyse them and look at the road ahead.

The Challenges

The Mind-Set



Geographical isolation exposes mariners to a set of unique challenges such as navigating through rough waters, onboard multi-tasking, liaising with authorities & even evading pirate

attacks. Technology on ships plays a significant role to help maneuvering through these conditions and it enables communication in situations of emergency and distress.

Unfortunately, any type of technology has the potential to be used for malicious purposes. Cyber security awareness and culture is relatively new on the agenda of the maritime community, but it must be taken seriously to avoid catastrophic consequences. Cyber risks can be managed by applying procedural & technical controls, unfortunately changing the mindset of an already tired ship crew is often the biggest challenge.

Ship Managing & Budgets

Almost all the merchant navy fleet comprises of a multi-vendor IT, OT & ICS environment; each vendor using hardware and software to accomplish assigned scope, with no bearing on scalability, overall compatibility or the existing and future security. With passage of time, vessels tend to significantly start looking different in networks and cabling to when they were delivered. Seldom are network plans updated, nor is there an inventory of the physical network paraphernalia nor of the software being used onboard. In a few ships where managers have been careful to implement some sort of order for the onboard IT, the control and integrity of maintained data is grossly erroneous and is often devoid of any OT & ICS elements.

Expecting the office IT team to understand the onboard cyber environment is a BAD IDEA. As recommended by BIMCO, it may be essential to have an experienced third party to assess cyber security risks onboard ships.

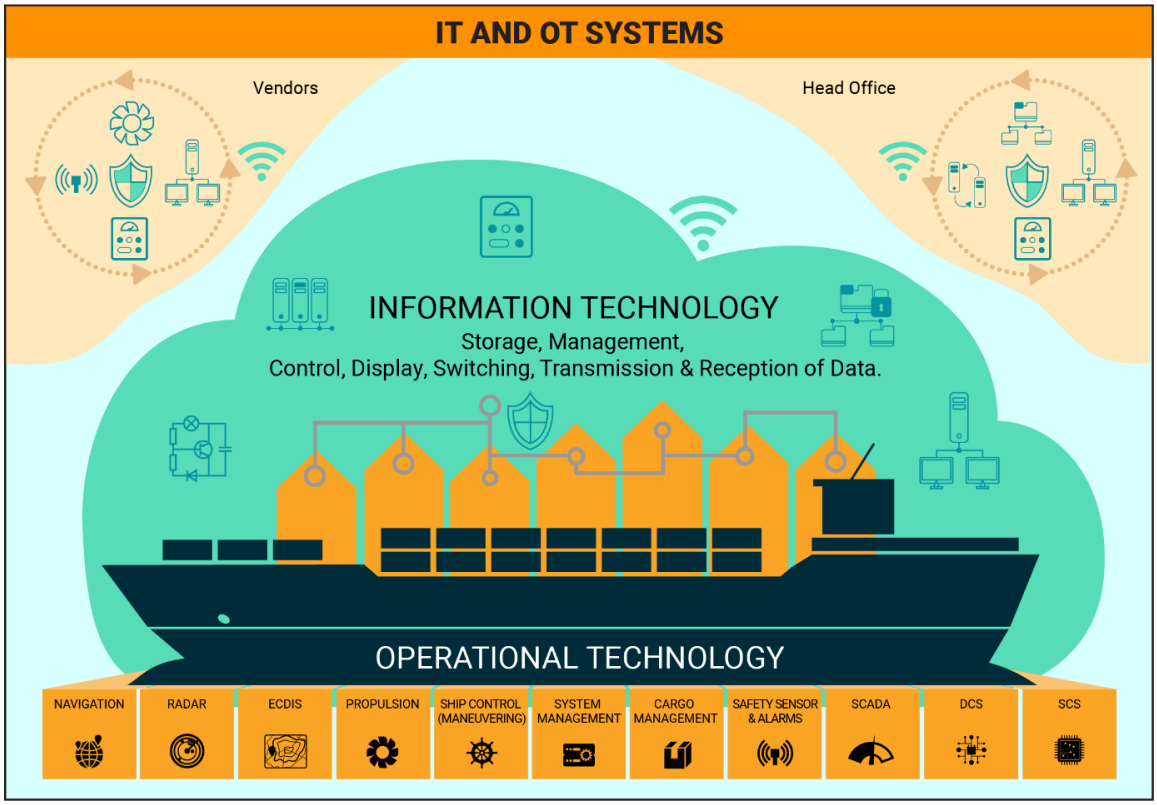
The Ship Staff

How many readers have been receiving seemingly unrelated mails in their accounts? Mails declaring winners and asking for addresses of bank accounts to make deposits are not uncommon, however, casual social-media behavior is making targeted phishing relatively easy. With the internet available to the crew all the time, fresh challenges have emerged in the already crowded security landscape – personalized mails, often quoting very private information are finding their way into individual mailboxes. Hardworking but poorly informed crew are finding their minds getting overwhelmed by these mails. The combination of hard-work and a disturbed mind can be lethal – for the crew as well as for the safety of the ship. Many companies have adopted a "responsible social media policy", within the existing SMS documentation, which is a great idea, but hard to implement.

Let's start at the beginning!

First things first – what is IT & what is OT?

To put it simply – software & hardware, where the output is data, such as communication by way of speech, text (email, records, accounts, etc) can be termed as Information Technology or IT. Onboard examples include onboard computers & accessories, emailing systems, calling systems, accounting systems, etc.



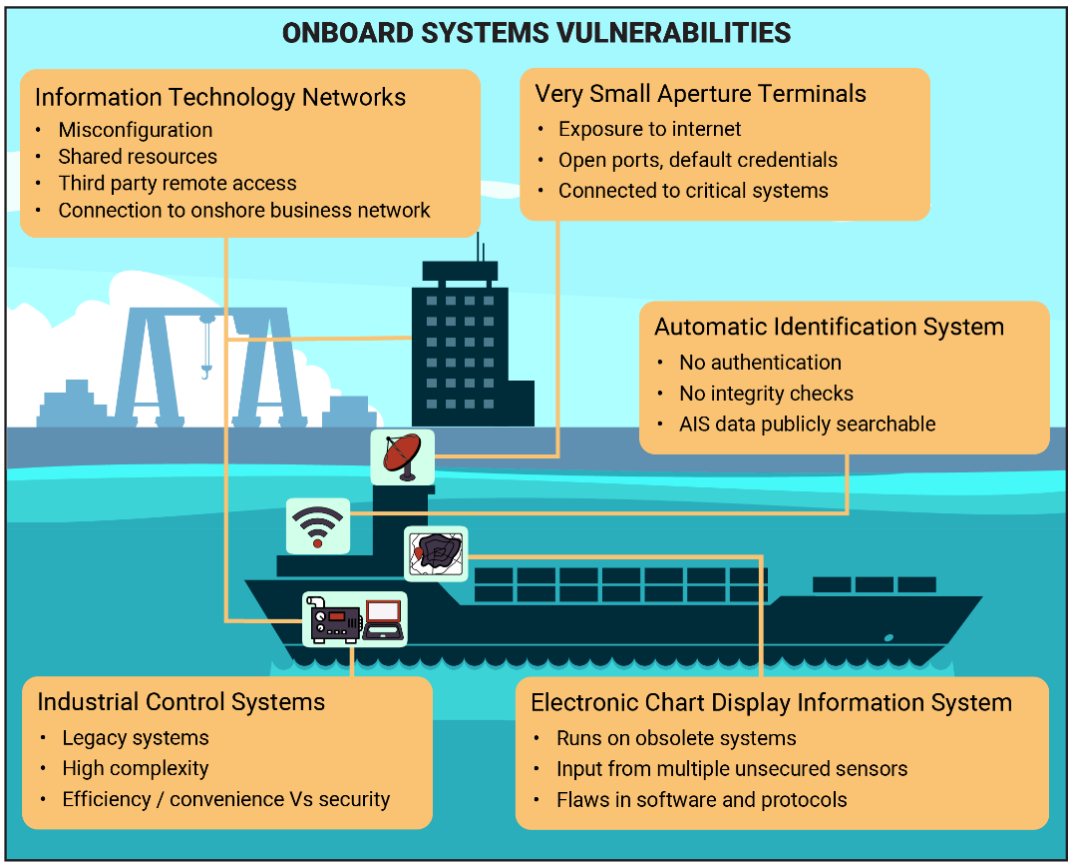
On the other hand, software & hardware, where the output is action (closing of valves, alarms, balancing power loads, etc.) can be termed as Operational Technology or OT. Onboard examples include ECDIS, Power Management, Integrated Automation System of engine (SCADA). Consider an air-conditioner, the thermocouple sensing the temperature of input air will regulate the start and stop of the compressor. Simple PLC (programmable logic controller) operation – code or firmware enabling this action is OT. Or take the example of a washing machine, where a sequence of events is controlled for the cycle selected – stop water, open soap, start rinsing and so on – all controlled by PLC code.

OT systems in the engine room are often referred to as ICS – Industrial Control Systems & are critical to shipboard operations.

While both IT & OT are using code (software), their outputs are different. What do we do when our laptop hangs? Most often than not we restart the machine, with windows autosaving our work, we can retrieve most of the data we are working on, however, OT systems are online and critical to the safety of the vessel. Can we simply restart the ECDIS or the steering gear, especially when in enclosed waters? Of course not, and hence the criticality of ensuring that these systems perform seamlessly each time & every time, ALWAYS.

Let us try and list out some of the common OT systems onboard & understand their vulnerability

Vulnerabilities are inherent weaknesses or flaws in a system that have the potential to be exploited by malicious parties, in the form of a threat.



The Global Positioning System (GPS) or the Global Navigational Satellite System (GNSS)

Many critical systems on board rely on the Global Navigation Satellite System (GNSS) for safe navigation, communication, emergency response, and traffic control. However, disrupting or manipulating GPS signals is fairly simple. INTERTANKO has recognised this risk & published an advisory document in 2019, where there is extensive information on jamming and spoofing of the GPS signals. It may be noted that Jamming of a GPS signal, where the GPS is unable to show a position is fairly easy to detect but it is difficult to detect a spoofing attack, where the position may only be marginally in error, nonetheless slowly but surely misleading every instrument connected to the set.

Manipulated Global Positioning System (GPS) signals have caused collisions, groundings, and environmental disasters. Hence imperative that while technology has eased up the position fixing environment on the bridge, we understand its limitations and do not replace the good old radar bearing and distance fixes or the parallel indexing techniques.

As a best practice, compare the position on the GPS set itself and that on the ECDIS or Radar – should be done at-least once a watch in open sea conditions and every hour when coasting.

ECDIS – Electronic Chart Display Information System

The Electronic Chart Display Information System (ECDIS) has revolutionised modern day navigation & is mandated by the IMO for all commercial vessels. The challenge with the system is that it uses electronic charts which need to be up to date; while the corrections/corrected charts can be received over the internet, the exposure this creates can have a debilitating effect on the vessels primary element – Navigation. Most companies are aware of this glaring vulnerability & have established adequate SOP's for handling the process.

However, ships continue to experience ECDIS failures attributed to this vulnerability. Additionally, more often than not, ECDIS software is run on legacy operating systems like Windows XP, which are no longer supported; with sensory feeds coming in from a multitude of other onboard systems such as Radar, Navtex, AIS, etc, each operating within their own OS, a wide surface for a compromise is created.

ICS – Industrial Control Systems OR OT systems in the Engine Room

Onboard Industrial Control Systems (ICS) form the basis for automation in modern day shipping. ICS controls and monitors key parameters onboard, including temperature, pressure, level, viscosity, flow control, speed, torque, voltage, current, etc. However, the process of inter-connecting many of these systems, without much concern for any cyber security elements, ends up producing a highly automated albeit vulnerable environment.

Furthermore, most of these ICS are based on outdated operating systems like Windows XP & Windows Server 2000.

Much of the onboard ICS network is connected to the vessels ethernet network for onward transmission of data to vendors, office, etc. While many of the standard makers have their own firewalls or VPNs as a standard accessory, there are many who have neglected basic security precautions to make way for crisper budgets. More often than not, an array of devices and protocols from different vendors and technological eras are often "bolted together" to produce an integrated automation system. It is crucial for integrators, implementers, and operators of ICS to understand the system's limitations and the vulnerabilities of its components and protocols.

A major concern is that operators and engineers routinely bypass security for convenience and efficiency, which could have a very serious effect on the entire organisation. This

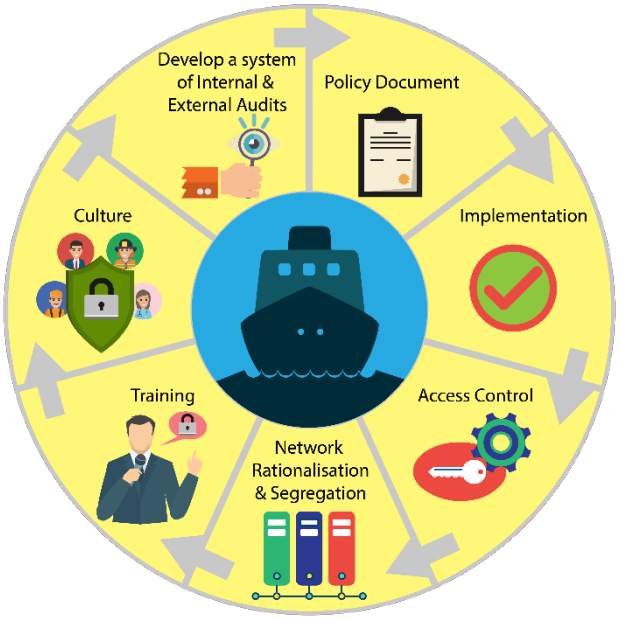
behaviour is mostly attributed to the lack of awareness and competence, the commercial pressures (time and money) & unfortunately to plain non-adherence to security policies (unforgivable).

COUNTER-MEASURES

The concept of cyber security is novel to many maritime stake holders, and it is timely to raise awareness about the existing countermeasures. IMO Res 428 mandates that cyber security elements need to be addressed and integrated with the company safety management system no later than the first renewal verification for DOC after 1st Jan 2021. Industry guidelines from BIMCO, complemented by the BIMCO onboard guide and workbook provide perspective to the compliance requirements of Res 428/MSC-FAL.1/Circ. 3.

It is essential for companies to earmark commensurate budgets for engaging professionals to work with the inhouse ship managers as well as with the office IT team.

Defence-in-depth

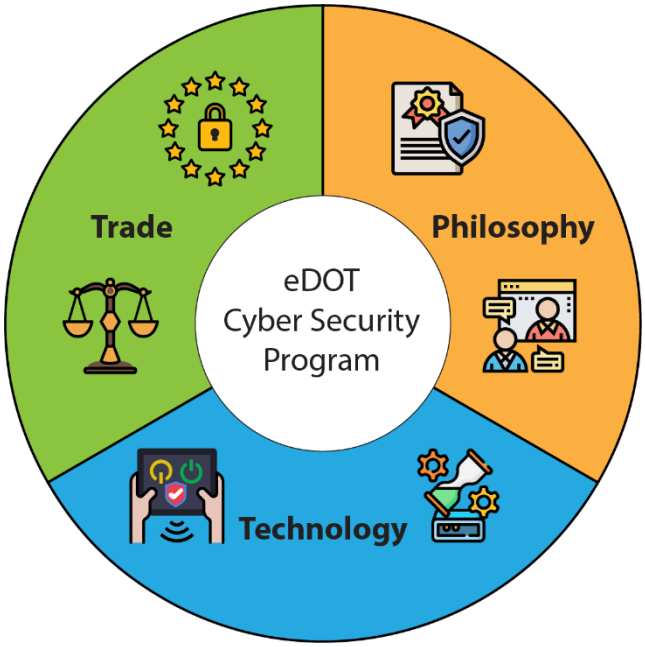


Cyber Security is a long-term management commitment with commensurate budgets. Every organisation must adopt custom made cyber processes which can be integrated with their present-day safety management systems.

The notion that a cyber Security Solution can be bought off the shelf is a myth, & nor can a single solution work for every organisation. It is important to understand that securing the maritime cyber environment "in depth" creates an all-encompassing protection mantle and builds resilience to external and internal threats. This layered approach is depicted in the adjoining figure and includes procedural and technical countermeasures on each layer.

1. *The Policy Document:* Defence begins with the organisation's leadership, where strategies are formed, and policies are made. These policy statements must be exhaustive, covering anti-malware software, information classification, OT firmware patching, remote access protocols, application patching amongst a host of others.
2. *The Implementation:* Policies must be backed up by the plan for implementation, which will include Role Development, Procedures & records.
3. *Access Control:* Physical measures to prevent unauthorised personnel from gaining access into a vessel & to IT & OT onboard elements.
4. *Network Rationalisation & Segregation:* Establish the physical layout and condition of the shipboard network – produce logical & physical network plans. Segregate IT & OT networks by establishing an IDMZ. Establish relevant redundancies.
5. *Training*: None of the above will work if the Master and crew don't have basic knowledge for correctly using of technology & equipment (IT & OT), understand the existing vulnerabilities & appreciate the threat and risk in the current landscape.
6. *Culture:* Imperative that the management stays committed to establishing, implementing and sustaining a cyber hygiene culture. This must be a long-term initiative and the process of change is often sluggish and slow.
7. *Develop a system of Internal & External Audits:* A necessity for any system, dynamic analysis of audit data will help in modifying processes, addressing gaps and assist in continually improving the system.

Recommendations & Deliberations



A. The need of the hour is a Cyber Security Program integrating the following:

1. **Philosophy**

The basis of the framework: IMO Res 428/MSC-FAL Circ. 3, The ISO 27001 standard, NIST, BIMCO/Industry Guidelines, Class guidelines, etc; pragmatically combining elements to culminate in policy making, establishing scope, purpose & objectives, risk assessment and application of controls.

2. **Technology**

Hands-on knowhow of shipboard & office networks (IT & OT) within relevant context | adequate experience in integrating shipboard processes with technology | Development & deployment of a cyber security management tool.

3. **Trade**

Integrating the Philosophy & Technology with the nuances of ship operation & management, in a pragmatic, practical & sustainable manner, with the appropriate cost to benefit to risk ratio.

B. Management team for cyber security

Many companies who may have designed and implemented their safety management systems in the past & have a fairly decent sized IT cell, are in the process of establishing a cyber security management system entirely in-house. While this may seem like a logical solution, it really is not the ideal one, for several reasons; let me list out a couple.

1. *Barring a few, IT professionals are, by and large, concerned with hardware and software relating to solving day to day information processing challenges. Writing code for custom software, maintenance of code, setting up remote sharing and meeting systems, sifting thru software products, etc. is usually their forte. They are not*

seafarers and seldom appreciate the nuances of the day to day ship life. Furthermore, it's just not fair to expect them to understand the working of onboard ICS.
From an organisational environment point of view, it is rather difficult to accept vulnerabilities within systems and processes designed by ourselves, isn't it?

2. *A management system must comprise of policies, roles, procedures and records as a minimum, and has to be auditable for compliance via objective evidences, however, the balance between actual compliance & evidence of compliance must be established in a bold, pragmatic and sustainable manner. With enough on the plate of the ship-staff, adding additional duties and records by way of checklists, forms, entrees, etc, will not go down well with them & the process will falter at the very start. The design of the system should be such that it works for the ship-staff rather than the ship-staff working for the system. The cyber security program must be inculcated in the seafarer's culture. IT professionals cannot be expected to understand this culture, let alone designing something to integrate with it.*

Hence, Establishing, Implementing and sustenance of an efficient & effective cyber security system must be entrusted to an independent dedicated team with commensurate marine and technological professional qualifications. One of the prime requirements of engaging with a professional vendor should be certification under ISO 9001 & 27001.

C. Customised Training of Ship Staff

Develop custom training material, relating to onboard equipment. I strongly recommend a one-day networking training program for deck officers & engineers, which includes practical training – making contact with shore support and following instructions on remote sessions, understanding network designs and basic trouble shooting.
Establish a system of onboard drills & exercises along with digitised training, in line with company's competence management systems.

Conclusion

I would like to conclude with a request to the men in-charge, the decision makers – the Company Chairmen, Presidents, General Managers, Technical Superintendents, DPAs, CySO's, involved in ship management – Please recognise the risk landscape of today, when shipboard connectivity is relatively slow and appreciate the situation in the future when the connection speeds pick up. Ships satellite terminals will become sitting ducks for cybercrime. Furthermore, technology & information overload is an overwhelming experience for the seafarer; a co-mingling of professional roles and social expectations are draining the emotionally fragile sailing men and women. Urgently addressing their training needs and responsible self-regulation of social media behaviour by knowledge empowerment is the need of the day. *Do not adopt a system for complying with statutes, rather develop a culture, wherein statutes are complied with naturally and organically*. Please Act today. Act now!!!

The writer is the CEO of eDOT Solutions, which designs, implements & manages Cyber Security Solutions for ship owners & managers.
eDOT are approved Consultants for ClassNK for establishing, implementing & certifying the NK-CSMC
www.edot-solutions.com | www.marisafe.net | contact@edot-solutions.com | +91 832 2501715