Embarking on IMO 2021 – A Journey Towards New Horizons

By **Anu Khurmi**, Managing Director, Global Services, Templar Executives

Anu Khurmi is a skilled and experienced business leader who works across all the Templar Business divisions in the development and delivery of strategic global business. She is also leading on the Maritime Cyber Response Team (MCERT), an international collaborative industry initiative and the Templar Cyber Academy for Maritime (T-CAM), focused on providing Cyber resilience and awareness for the Maritime sector.

“IMO 2021 is not just a destination or tick box for Cyber compliance – it is an opportunity to embark on a journey to create a safe, resilient and digitally enabled future for the Maritime industry,”

Safety and security management practices have always been the cornerstone of the maritime industry and intrinsic to the safety of vessel and crew. As the world evolves and digitalisation and automation become fundamental to the efficiency and productivity of the industry, there has been a dawning acceptance of the increasing threats from Cyber attacks and data breaches – a realisation accelerated by the COVID-19 pandemic. Yet, despite unprecedented adversity, the sector continues to live up to centuries of tradition and demonstrates remarkable resilience as it comes together to resolve the current challenges on how to operate effectively in the ‘new normal’.

For the shipping industry, a key part of this ‘new norm’ includes responding to the series of IMO guidelines and Resolution MSC.428(98), encouraging administrations to ensure that Cyber risks are assessed and mitigated in vessel Safety Management Systems effective from January 2021. However, in an environment where hybrid working, operational technologies (OT) and cloud services are increasingly underpinning business operations onshore and offshore, the IMO 2021 agenda should not be viewed merely as a compliance exercise.

Rather, the approach should reflect informed decision-making at the leadership level and provide a perspective on how making the right investments on Cyber initiatives now, can enable businesses for the future.

Understanding the evolving Cyber threat landscape and its impact on the business and operational resilience is fundamental to identifying, prioritising and mitigating the risks. This, in turn, will help to determine which solutions will be most cost effective and sustainable to implement – thus justifying current expenditure and further investment going forward.

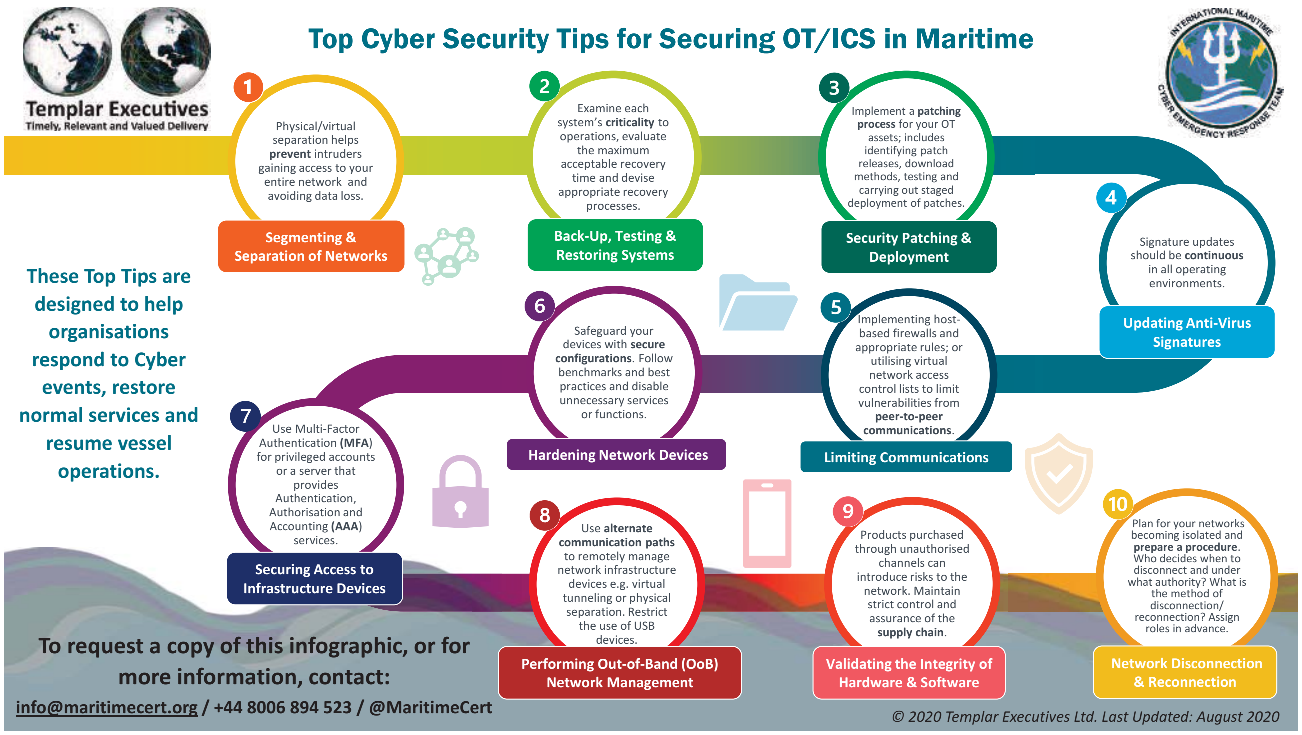
A recent publication by the Digital Container Shipping Association (DCSA) states maritime, as part of the critical transportation sector, is now estimated to be the second most targeted sector. The Maritime Cyber Emergency Response Team (MCERT)   saw a 3000% spike in the activities and interests of low-skilled but nonetheless disruptive hackers; not seasoned Cyber criminals but so-called ‘script-kiddies’, simply bored with nothing better to do during lockdown. International government edicts continue to warn of increasingly sophisticated scams and there has been an escalation in malicious activity targeting not only large organisations, but also small and medium businesses and individuals. MCERT analysis, which monitors Cyber attacks on the maritime ecosystem highlights that to date in 2020, ransomware and phishing, triggered by the exploitation of individuals, continue to be the most frequent and easily enacted types of attacks in the sector. State sponsored attacks and Cyber espionage activities are also prominent headlines.

[1] https://dcsa.org/how-to-prepare-for-a-maritime-cyber-attack/
[2] https://www.maritimecert.org/

With less than five months to go, IMO 2021 provides a great impetus for the industry to address the maritime imperative on Cyber and the goal of supporting safe, secure and efficient shipping.

The human element continues to be a major cause of maritime industry breaches and it is therefore no surprise that the ISM code requires organisations to "raise awareness on the Cyber risk", and "embed a culture of Cyber risk awareness". Relevant education and training are fundamental to making employees the 'first line of defence' and preventing seafarers and onshore employees from opening emails containing malware or inserting infected USB sticks into company computers. Another major element is the integration of technologies and the specialist skillsets required. However, very few companies have experience of the complexities of their offshore and onshore IT and OT environments; segmenting and separation of networks, hardening network devices, security patching and deployment are just some aspects of implementing best practices.

With less than five months to go, IMO 2021 provides a great impetus for the industry to address the maritime imperative on Cyber and the goal of supporting safe, secure and efficient shipping. For many organisations there is still much to do; but with time running out, budgets under pressure and finite skilled IT resources, the danger is that businesses will take a tick box approach to compliance. This does not need to be the case; there is excellent best practice from other sectors to refer to as well as the guidance being developed by industry stakeholders. Innovative, off the shelf solutions such as the MCERT collaborative platform, Templar Executives' risk assessment tools and certified education and training, offer a holistic portfolio of pragmatic services addressing IMO 2021 and beyond. As shipping looks to new horizons, viewing Cyber as a business opportunity can deliver tangible benefits and enable a safer and more resilient maritime industry fit for the digital era.



Templar Executives
Timely, Relevant and Valued Delivery
INTERNATIONAL MARITIME CYBER EMERGENCY RESPONSE TEAM

Top Cyber Security Tips for Securing OT/ICS in Maritime

1 Physical/virtual separation helps **prevent** intruders gaining access to your entire network and avoiding data loss.
Segmenting & Separation of Networks

2 Examine each system's **criticality** to operations, evaluate the maximum acceptable recovery time and devise appropriate recovery processes.
Back-Up, Testing & Restoring Systems

3 Implement a **patching process** for your OT assets; includes identifying patch releases, download methods, testing and carrying out staged deployment of patches.
Security Patching & Deployment

4 Signature updates should be **continuous** in all operating environments.
Updating Anti-Virus Signatures

5 Implementing host-based firewalls and appropriate rules; or utilising virtual network access control lists to limit vulnerabilities from **peer-to-peer communications**.
Limiting Communications

6 Safeguard your devices with **secure configurations**. Follow benchmarks and best practices and disable unnecessary services or functions.
Hardening Network Devices

7 Use Multi-Factor Authentication **(MFA)** for privileged accounts or a server that provides Authentication, Authorisation and Accounting **(AAA)** services.
Securing Access to Infrastructure Devices

8 Use **alternate communication paths** to remotely manage network infrastructure devices e.g. virtual tunneling or physical separation. Restrict the use of USB devices.
Performing Out-of-Band (OoB) Network Management

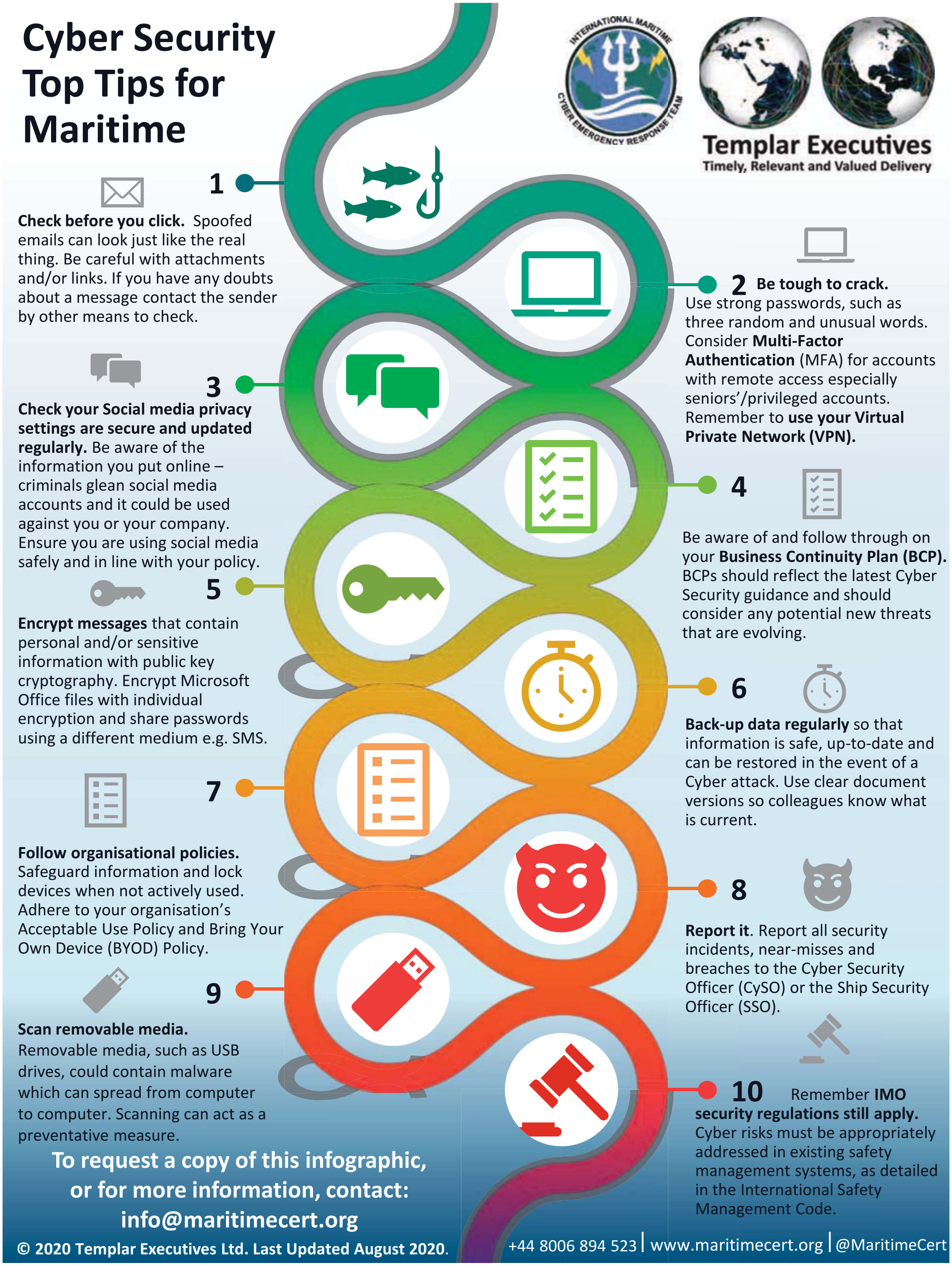
9 Products purchased through unauthorised channels can introduce risks to the network. Maintain strict control and assurance of the **supply chain**.
Validating the Integrity of Hardware & Software

10 Plan for your networks becoming isolated and **prepare a procedure**. Who decides when to disconnect and under what authority? What is the method of disconnection/reconnection? Assign roles in advance.
Network Disconnection & Reconnection

These Top Tips are designed to help organisations respond to Cyber events, restore normal services and resume vessel operations.

To request a copy of this infographic, or for more information, contact:
info@maritimecert.org / +44 8006 894 523 / @MaritimeCert

© 2020 Templar Executives Ltd. Last Updated: August 2020



Cyber Security Top Tips for Maritime

Templar Executives
Timely, Relevant and Valued Delivery

1

Check before you click. Spoofed emails can look just like the real thing. Be careful with attachments and/or links. If you have any doubts about a message contact the sender by other means to check.

2 Be tough to crack. Use strong passwords, such as three random and unusual words. Consider **Multi-Factor Authentication** (MFA) for accounts with remote access especially seniors'/privileged accounts. Remember to **use your Virtual Private Network (VPN).**

3

Check your Social media privacy settings are secure and updated regularly. Be aware of the information you put online – criminals glean social media accounts and it could be used against you or your company. Ensure you are using social media safely and in line with your policy.

4

Be aware of and follow through on your **Business Continuity Plan (BCP).** BCPs should reflect the latest Cyber Security guidance and should consider any potential new threats that are evolving.

5

Encrypt messages that contain personal and/or sensitive information with public key cryptography. Encrypt Microsoft Office files with individual encryption and share passwords using a different medium e.g. SMS.

6

Back-up data regularly so that information is safe, up-to-date and can be restored in the event of a Cyber attack. Use clear document versions so colleagues know what is current.

7

Follow organisational policies. Safeguard information and lock devices when not actively used. Adhere to your organisation's Acceptable Use Policy and Bring Your Own Device (BYOD) Policy.

8

Report it. Report all security incidents, near-misses and breaches to the Cyber Security Officer (CySO) or the Ship Security Officer (SSO).

9

Scan removable media. Removable media, such as USB drives, could contain malware which can spread from computer to computer. Scanning can act as a preventative measure.

10 Remember **IMO security regulations still apply.** Cyber risks must be appropriately addressed in existing safety management systems, as detailed in the International Safety Management Code.

To request a copy of this infographic, or for more information, contact: info@maritimecert.org

+44 8006 894 523 | www.maritimecert.org | @MaritimeCert