Photo: Alex Andrews/Pexels

Navigating in an Online World

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

The world remains in the grip of a global pandemic and alongside essential frontline sectors, our dependency on the maritime industry and seafaring community has never been greater. The International Maritime Organisation (IMO) Secretary-General Kitack Lim has noted: "In these difficult times, the ability for shipping services and seafarers to deliver vital goods, including medical supplies and foodstuffs, will be central to responding to, and eventually overcoming, this pandemic."

Anu Khurmi is an experienced business leader, working across all of Templar Business divisions in the development and delivery of strategic global business. This involves engaging with Governments, regulators and private sector organisations across key industries, including maritime, to promote and provide Cyber Security and Information Assurance Advisory services and solutions. Anu is also leading on the Maritime Cyber Response Team (MCERT), an international industry initiative aimed at helping achieve the IMO 2021 requirements, and the Templar Cyber Academy for Maritime (T-CAM), focused on developing Cyber resilience and awareness within the Maritime sector.
For more information please contact: enquiries@templarexecs.com, or phone: +44 (0)844 443 6243 or visit: www.templarexecs.com

As the response to COVID-19 dominates political and national agendas, the global lockdown is having major impacts on the critical issues of crew changeovers, repatriation of personnel and port entry for vessels. There are growing calls from industry leaders to urgently address these challenges and support the key workers who are making the flow of goods, services and trade possible. However, these are not the only issues facing maritime stakeholders at a time when safety, security and stability are paramount.

The maritime sector has long been combatting threats posed by state and non-state actors, pirates, organised criminal gangs and in recent times, growing Cyber Security risks. Almost overnight the requirements for social distancing, travel restrictions, curfews, port closures and lockdowns, have thrown into sharp focus the ruthlessness and digital prowess of these threat actors, who are unhampered by any rules. The COVID-19 pandemic has highlighted their ability to exploit vulnerabilities and we are seeing a proliferation of Cyber attacks and scams being reported on an unprecedented scale.

This month, the International Chamber of Commerce (ICC) warned of scammers exploiting the spread of the COVID-19 pandemic to carry out fraudulent activities and Cyber threats. The US Navy is not alone in advising that, "… the COVID-19 pandemic presents an opportunity for malicious actors to conduct spear-phishing campaigns, financial scams, and disinformation campaigns via social media to collect sensitive information, steal money via fake donation websites, spread false information and deliver malware to victims." A joint alert from the United States Department of Homeland Security (DHS), Cyber Security and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) notes the various methods that Advanced Persistent Threat (APT) groups and Cyber criminals are using to target individuals, small and medium enterprises, and large organisations with COVID-19 related malicious Cyber activity. These Cyber exploits are also more likely to

Photos: Templar Executives

succeed as businesses rapidly deploy and ramp up remote working for employees.

Yet the current situation is also serving as a wakeup call and opportunity for individuals and businesses who are having to adjust en masse to different ways of working. The maritime sector like many other industries, has been automating and digitalising at pace to create greater operational efficiencies and productivity, but it has been notoriously slow in addressing the accompanying Cyber Security issues. Flag states, regulatory bodies and maritime associations have been advocating the need for better 'Cyber hygiene' to enable the safety and security of all those working in the sector and to ensure its future resilience. The International Maritime Organisation's Resolution on 'Maritime Cyber Risk Management in Safety Management Systems', due to be implemented in January 2021, mandates that shipping firms properly address Cyber risks within existing safety management systems. These regulations require stakeholders to "raise awareness on the Cyber risk", "embed a culture of Cyber risk awareness", "respond quickly to a Cyber incident" and "notify other parties quickly".

The Digital Container Shipping Association this month unveiled its 'DCSA Implementation Guide for Cyber Security on Vessels', a document intended to support cargo ships as they prepare for the IMO Resolution. In addition, national data protection laws and requirements, such as the General Data Protection Regulation (GDPR), are forcing compliance and accountability at Board-level for reporting data breaches of sensitive and personal information. In all of these instances, common recommendations include the need for greater Cyber Security awareness amongst employees and for organisations to have effective business continuity plans.

The same guidance also applies for those who have been catapulted into a world of working and socialising online. Education and training are key to creating a vigilant workforce and embedding a culture of "Cyber risk awareness" and best practices. A proactive approach to organisational resilience includes implementing measures such as regular patching, equipping all devices with up-to-date antivirus software, threat monitoring and email services with protective features. International industry initiatives such as the Maritime Cyber Emergency Response Team (MCERT)[1], offer a platform for sector collaboration and Cyber emergency response services, invaluable when IT skills and resources are finite and budgets stretched.

Today business leaders face a complex and uncharted landscape; as they navigate how their organisations survive the present, they also have an opportunity to consider how they can thrive in the future. For the maritime sector and its significant seafaring community, this is a time for acknowledging that effective Cyber Security is integral to business resilience and enablement. Proactive and defensive measures usually left to the ICT Department should be part of an informed business process, delivering quantifiable benefits and reflecting upon the level of risk the Board is willing to take and justify. Investment in education and Cyber best practices should create a sustainable culture to keep employees safe and productive, and businesses protected and operational. This is critical in a sector responsible for carrying over 90% of the world's trade by sea and essential for future prosperity . ■

[1] *https://www.maritimecert.org/*