Our reliance on Information & Communications Technology (ICT) is stemmed deep in our everyday lives in the modern world and the Maritime and Offshore Oil & Gas industries are no different at all. Whether it’s the Internet (for business or pleasure), dynamic positioning, navigation, GPS or crew welfare terminals, all these come with vulnerabilities that can be exploited by cyber criminal’s intent on causing operational disruption, financial loss, reputational damage or worse still potentially loss of life.

Over the past few years we have seen many incidents of cyber-attacks in the maritime and offshore oil and gas sectors including the lifting of oil rigs, malware riddled platforms and even port facilities industrial controls systems being hacked. Despite these incidents there seems to be a distinct lack of awareness throughout organisations. From the research JWC have conducted over the last 12 months for a study with the Company Security Officers (CSO) Alliance and Coventry University, entitled ‘Cyber Security: The Unknown Threat at Sea’, we had the pleasure of speaking to security and risk professionals from across the maritime and offshore industries. The purpose of the investigations, which were part of an overall assessment of offshore risk management were to identify how shipping companies and major offshore oil and gas producers managed the cyber threat and how well they understood the risks associated with a cyber-attack.

The findings were somewhat surprising for me as I made the mistake of assuming that most HSSE managers would be taking an orthodox risk based approach to managing the cyber threat (and many were) but more than 50% of the personnel questioned did not believe cyber was a security or safety issue and referred me directly to their IT departments for further discussion and investigation. Many organisations I visited did not implement cyber or ICT usage policies or procedures, although this was more prevalent in the shipping industry and less so in the offshore oil and gas sectors, the findings were still significant.

It occurred to me that the maritime and offshore sectors are playing a dangerous game and the stakes are extremely high. In a world of globalisation and interconnectivity, cyber security is a threat that needs to be taken more seriously and management need to take responsibility sooner rather than later. At a recent conference I attended in London, it was highlighted that more than 80% of identified cyber security and information security breaches and related incidents offshore, are as a direct result of human error, this tells us we need to start getting the basics right before we invest on advanced (and expensive) technical mitigation measures. Training and awareness for personnel is one of the biggest vulnerabilities right now and with the clear deficiencies that do not necessarily require significant investments, the offshore oil and gas sectors are high profile, lucrative and attractive targets for criminals and 'hack-tivists'.

When you combine the absence of training for personnel, the lack of clear and understood policy, with the current economic climate and add some fierce competition for business, it creates a natural increase in the risk appetite that security and safety managers may not not be fully aware of. We are seeing many energy firms combining Industrial Control Systems (ICS) with much wider networks for the purpose of quicker information exchanges across the operational environment. Although this may be more cost effective and offer speed and efficiency, it also creates more vulnerable junctions within the system, that can leave operations significantly exposed to the outside world. If systems are attacked or compromised this could quickly lead to operational shut down, which would be catastrophic for all stakeholders concerned.

As more companies continue to increase internet access offshore for operational and also welfare purposes, it comes with an increased risk of suffering a cyber-attack at sea. The Offshore Sector and International Shipping and Logistics environments, including port facilities too are becoming more complex with less dependency on manual systems by advancing to more automated technology. For a multitude of reasons and as highlighted earlier, we are beginning to see an increase in Information Technology (I.T.) and Operational Technology (O.T.) networks being connected together at sea which are also connected to the Internet. It is no secret that many ships and nearly all offshore oil and gas process plants are online 24/7 these days and protecting vital digital infrastructure against cyber-threats is paramount in ensuring a safe and secure operational workplace and also optimal productivity at all times.

It is often said that complacency is simply a lack of awareness and training and the offshore and maritime industries need to do more to ensure they are not the next victims on the cyber battlefield!

www.jwcinternational.com