PLAYING IT SAFE IN THE DIGITAL REALM

WITH THE MISSION OF SAFEGUARDING THE DIGITAL INFRASTRUCTURE OF THE MARITIME INDUSTRY, CYBERSTAR HAS BEEN EMPOWERING ORGANISATIONS TO ACHIEVE CYBER RESILIENCE

The Covid-19 pandemic has accelerated digitalisation globally. It has now become an essential part of most industries, including logistics and maritime. While the transition has ensured greater efficiency, the use of sophisticated technology and intelligent devices has also made shipping companies vulnerable to cyber-attacks. A report from cybersecurity consultancy Naval Dome suggests that since February 2020 cyber-attacks on maritime vessels shot up by 400 per cent. This dramatic surge has shocked and alerted businesses in the industry, prompting them to find effective solutions to tackle this. Cyberstar CEO Mr. Ronen Meroz speaks to The Zone about cybersecurity concerns in the maritime sector and the significance of digital safety.

What is the biggest cybersecurity threat currently faced by the industry?

The nature of the supply chain is that it is tightly knit. In our experience, the biggest threat for a maritime or logistics company is to lose access to core operational and commercial systems, and to be "cut off" from the supply chain by business partners due to a cyber-attack.

What happens when a company is under a cyber-attack?

An unprepared maritime organisation that is under attack would have huge challenges shaking off the attack's impact on its information and operating systems and as a result, on its critical business processes. In such a case, the compromised company may not be able to communicate with vessels, terminals, its alliance partners, customers, and vendors. A logistics company will lose the ability to plan its operations and communicate with its vendors and customers. Moreover, once its supply chain partners find out that the company has been compromised, they will most likely refuse to collaborate with it digitally until the problem is fully resolved. Such a scenario will aggravate the already-critical operational and commercial condition of a compromised company, leading it to suffer from major financial, and reputational losses almost overnight.

MR. RONEN MEROZ
CEO, CYBERSTAR

> WE MUST SHIFT THE FOCUS FROM PREVENTING TO PREVAILING, AND THE MINDSET FROM BEING REACTIVE TO BEING PROACTIVE, WHILE INVESTING IN PROPORTIONAL BUDGETS AND PAYING ATTENTION TO MONITORING AND RESILIENCE.

How does a cyber-attack occur?

Cyber security has three layers: Protection (mitigating the attacks), monitoring (identifying the attack/breach) and resilience/readiness (how to manage and rebound from a cyber crisis after the protection has failed and a breach has occurred).

Hands down, most of the attention and budgets today are directed at prevention. Fewer companies perform adequate levels of monitoring, but almost no one fully embraces the concept of being resilient and ready, i.e. establishing a tangible and realistic plan to manage a severe cyber crisis not to mention rehearsing it.

What are the challenges on the road to overcoming cyber threats in the sector?

The number one challenge is to change the current mindset. While statistics show that companies have a very real chance of suffering a major attack, many executive teams are either overconfident or feel that they have ticked the box by having the IT or CISO "take care of it". In reality, however, this mindset is failing companies one after the other.

How does Cyberstar make maritime companies resilient?

Our services focus on programmes that elevate a company's cybersecurity capabilities, gaps and resilience levels. Meaning, we can very efficiently evaluate current capabilities, and develop the necessary plans, processes, and practical cyber-drills to start building the company's ability to withstand a cyber-attack and continue operating under such circumstances even without its core systems.

With the rapid increase in digitalisation, maritime companies will be more prone to cyberattacks. How can this be avoided?

Cybersecurity should be a priority for every organisation. Organisations need to understand the risks and have the necessary solutions and controls. Cybersecurity professionals - either in-house or 3rd party must be brought in to perform cybersecurity jobs. Additionally, companies must invest in at least one cybersecurity drill for the management team. The ROI of such exercise in spreading awareness, exposing the capabilities and gaps and building "muscle memory" towards such an event - is extremely high.

> IN OUR EXPERIENCE, THE BIGGEST THREAT FOR A MARITIME OR LOGISTICS COMPANY IS TO LOSE ACCESS TO CORE OPERATIONAL AND COMMERCIAL SYSTEMS, AND TO BE "CUT OFF" FROM THE SUPPLY CHAIN BY BUSINESS PARTNERS DUE TO A CYBER-ATTACK.

IN 2020 CYBER-ATTACKS ON MARITIME VESSELS SHOT UP **BY 400%**