In discussions about digital transformation, artificial intelligence is often referred to as the key to a new era. Little understood by policymakers and top managers, it widely seems to be over- or underestimated. But only those who understand and use its real potential will be among the winners of the transformation. It's now up to every company to apply A.I. in the creation of new business value and competitive advantages.

Join the Maritime Future Summit to learn more about this key to the future.

In cooperation with

secure your early bird ticket before 30 November and save 25%

smm-hamburg.com/ticket

click on the digital route

smm-hamburg.com/digital-route

be connected

1 Feb 2021
Hamburg

Aye aye, A.I.

In discussions about digital transformation, artificial intelligence is often referred to as the key to a new era. Little understood by policymakers and top managers, it widely seems to be over- or underestimated. But only those who understand and use its real potential will be among the winners of the transformation. It's now up to every company to apply A.I. in the creation of new business value and competitive advantages.

Join the Maritime Future Summit to learn more about this key to the future.
»Risk assessment is not a one-time exercise«

It may have been a while since the last big cyber attack in shipping has become public. But behind the scenes shipping companies are working towards compliance with a new IMO resolution, Rachael Bardoe, Director of Operations and Cyber Center of Excellence at Digital Container Shipping Association (DCSA) tells HANSA

The IMO Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems, set to take effect in January 2021. What does it mean for the industry?
Rachael Bardoe: The resolution is a critical turning point for the shipping industry. As the pace of digitalisation increases, the opportunities for malicious actors to compromise vessels increases. Systems that were once standalone are increasingly integrated, which means any cyber attack could have an immediate and widespread impact on the ship and safety of the crew. The IMO Resolution is driving carriers and shippers alike to understand the risks onboard vessels today and to be prepared to apply appropriate control measures to ensure not only data security, but more importantly, crew safety.

Will compliance be enough to make the industry a little more cyber-safe?
Bardoe: Cyber security is a constant journey. The threat landscape is dynamic and cyber adversaries are becoming increasingly sophisticated in their approaches to compromise systems. What is important to understand is that the risk assessment process, a fundamental aspect of compliance, is not a one-time exercise. As organisations move towards a risk-based approach to manage their cyber security, the application of appropriate controls will move from a reactive stance to a more proactive one. This behaviour will undoubtedly increase cyber safety, as will a more vigilant cyber security culture within shipping organisations.

What is DCSA’s advice, what should shipping companies do with regard to the resolution?
Bardoe: Organisations should start their efforts to address the resolution with a risk assessment. The identification of their most critical risks enables an organisation to target their investments correctly and thereby derive the biggest return on that investment. Cyber security risk is really a matter for the Board Room and should be considered as integral to the business as any other type of business risk. Whilst technical and procedural controls are being implemented, there will be a period of change, so clear ownership from the top down is necessary to instil cyber security into the culture of the business.

However, cyber security is not just about firewalls, network segmentation, boundary devices and monitoring solutions. Staff must undergo training and awareness exercises. The majority of successful cyber attacks happen due to human error. Phishing tactics are becoming increasingly sophisticated and are often the first step to a threat actor maintaining persistence in your environment.

Where are DCSA’s members in the compliance process?
Bardoe: One of the main reasons DCSA published the Cyber Security Implementation Guideline was because our carrier members were focused on meeting the IMO mandate and asked DCSA to provide guidelines for a standardised yet adaptable approach to achieving compliance. We know that our members have been engaging in risk assessments and working on their own security roadmaps and implementations. However, we are not in a position to comment on the status of their internal security compliance efforts.

What does cooperation between DCSA members on cyber security look like?
Bardoe: DCSA works closely with all of our members on cyber security. We see engaged, passionate contributions from our members and a willingness to work together to do the best for our industry. Naturally, cyber security is a sensitive topic, especially when there are incidents that could cause significant disruption to the carrier’s business as well as reputational damage. However, recently we have seen a number of maritime organisations, including ocean carriers, publicly share information about cyber security incidents and take definitive actions to remediate. This builds an environment of trust within the industry and with customers, which is key to fostering collaboration.

Do you also talk to other stakeholders like terminals, ports, forwarders etc.?
Bardoe: Yes, DCSA is very keen on cross-industry collaboration. We are stronger together. To drive meaningful change and innovation, we need everyone to embrace digitalisation and adopt a standardised approach to make container transportation services transparent, reliable, easy to use, secure and environmentally friendly. Our engagement with the industry stakeholders is broad, including shippers/BCOs; logistics chain participants such as terminals, ports and freight forwarders; government authorities and regulators; other standards bodies and alliances; financial institutions involved in shipment transactions and solution providers. We welcome feedback from all parties to validate our roadmap and improve our standards. Once published, our standards are free for all to use.

Interview: Felix Selzer