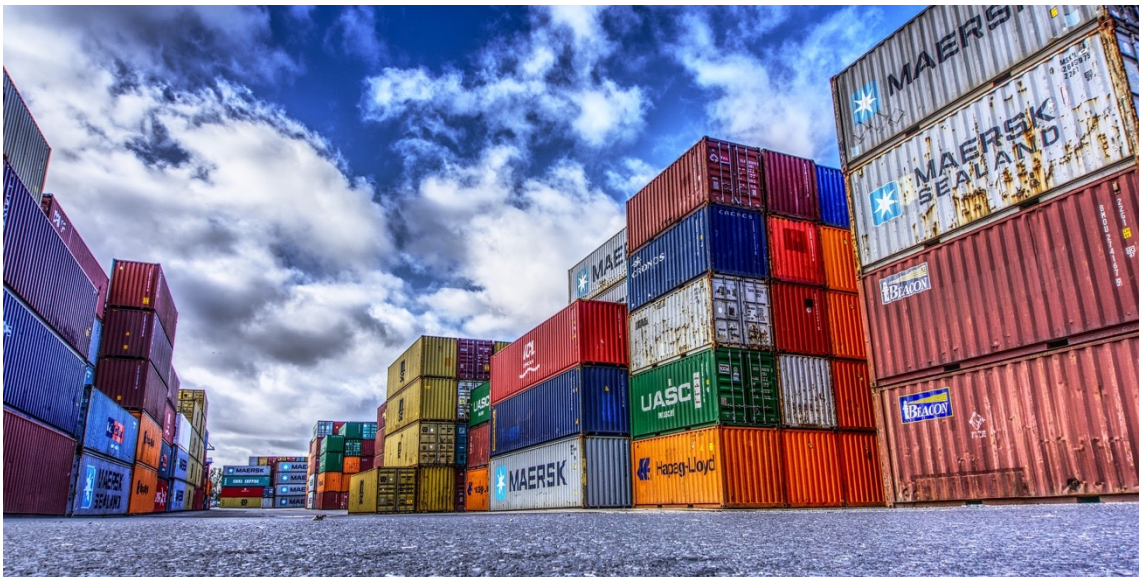
WHITEPAPER

Cyber-attacks: An increasing danger for ocean carriers

Flowfox

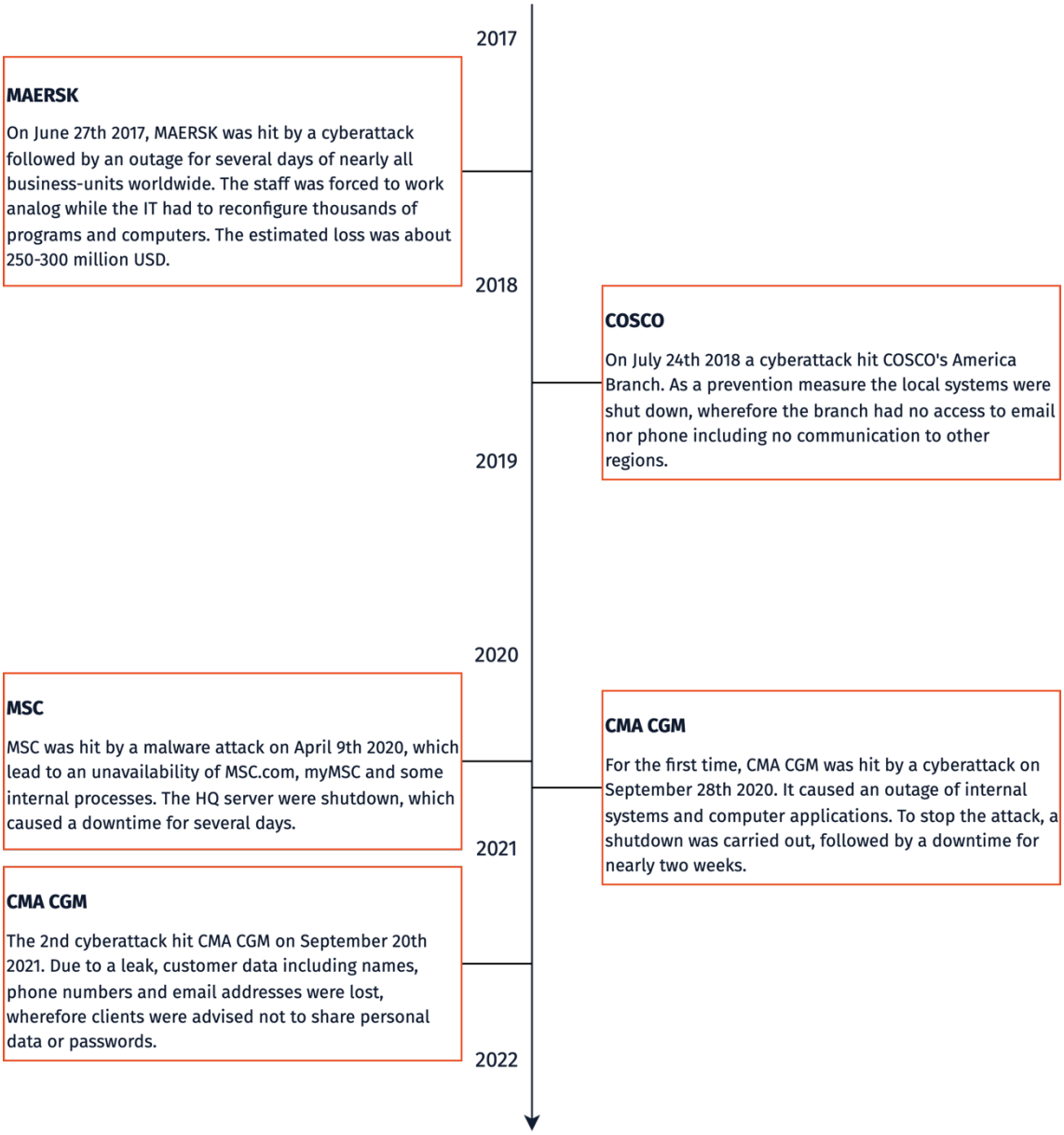
An increasing danger for ocean carriers: being hit by cyber-attacks

In today's environment the supply chain can no longer function without technology that enables fast processing and enhanced efficiency. Producers, ocean carriers, importing parties and buyers all have one thing in common: requiring digital connections and services.
This leads to networks consisting of an increasing number of processes and systems. An associated phenomenon of this development is the increase in criminal activities in the form of cyber-attacks. Cyber-security, data-safety as well as protection and prevention are topics of utmost importance in today's high value global container shipping trade. 8.4 trillion USD of goods are shipped in containers annually, involving a vast number of parties constantly exchanging information. Therefore, the global container shipping industry is at a high risk of cyber-attacks.



Lack of cyber-security: A massive danger

Ransomware, malware, phishing as well as blackmailing aren't new to the shipping industry but present a major threat due to their unpredictability and complexity. They not only cause losses and damages to the affected party but also to partners and customers, due to shutdowns, outages, and leaks. Furthermore, the subsequent recovery usually requires intense actions, which cause high monetary and workforce expenses. Some incidents that have affected ocean carriers in recent years can be seen in the following timeline:



These harmful events are possible due to different attack vectors that are either technical or process-related.

Technical attack vectors

Technical attack vectors are visible in the area of data security, such as antivirus-programs, data defenders, firewalls and the like. Missing patches and updates can lead to outdated systems being left vulnerable to the outside. In combination with discontinuous control instances, which could theoretically notify users about incoming or ongoing threats, this vector is very vulnerable. Usually, a complete and total shutdown is one of the last options to prevent the cyber-attack from spreading to other systems. These shutdowns are frequently followed by a heavy downtime with a huge impact on the ocean carriers, their customers, and other parties involved. During the downtime they have no access to services, systems, communication, and data, which is necessary to perform a smooth and cost-efficient workflow. Downtimes therefore lead to an excessive additional workload for all parties involved, directly or indirectly.

Process-related attack vectors

Process-related attack vectors focus on the weakness of identification and authentication processes. Through daily communication via email or phone, email addresses, phone numbers or the signature are typically used to identify the counterpart. This leads to an increased risk for mistakes and fraud *(Example case: Criminals Used AI To Clone Company Director's Voice And Steal $35 Million (screenrant.com))*. Additionally, high value data, such as PINs for full-container releases and invoices with sea freight conditions are still being transferred via email attachments, often to non-verified customers. Power of attorneys are exchanged in PDF files, which could contain harmful content. These reasons lead to a growing demand for secure communication for identified and authenticated partners. Furthermore, blackmailing of staff with access to PINs for the container release is a concern. In numerous ports and for many ocean carriers blackmailing is an ongoing threat, as they have custody over the container and its value from the very beginning of the transport until the import to the destination country, often also including the delivery to the receiving party. Since the ocean carrier has the authorization to release the container from their custody, its staff can be a target of blackmailing and other fraudulent intents by criminal groups.

Improving cyber-security

Unfortunately, there is no panacea to close all vulnerabilities and cyber-security must therefore be seen as a continuous process of improving protection and making it more and more difficult for attackers. In that context, all stated vulnerabilities show the need for a holistic solution with fundamental strategies, starting with the identification of the vulnerable gateways, followed by encryption of sensitive data, secured processes and elimination of attack vectors. To return to the import process as an illustrative example, we at Flowfox developed a platform with latest security technologies and all necessary preventive measures to support a safe and reliable import process for all users, partners, and their clients. A “know-your-customer (KYC) approach” within the registration process to ensure to only communicate with trusted and registered parties is only the beginning. With Flowfox’ completely email free import processes sensitive data like PINs are no longer transferred via unencrypted emails and the attack vectors of infected PDF files are closed. The data transfer via the encrypted Flowfox system hereby enables massive security gains. In that regard, particularly proven procedures are, for example, AES-256-Standard and TDE (Transparent Data Encryption, a method to encrypt data), which makes data only processable to the holder of a decryption key. Especially for the container release security is key. Handling the sensitive PIN can be a risk as the PIN easily enables everybody to pick-up the full container at the terminal. So whenever possible it is highly recommended to implement sophisticated secure terminal release solutions, like the SCR from T-Mining, allowing to transfer the pick-up rights from party to party while disposing of the unsecure PIN. For ports still using the PIN process, we at Flowfox have developed a secure PIN release solution, where PINs are generated and encrypted within the Flowfox system, so the ocean carrier has no responsibility and access to the PIN protecting ocean carrier’s employees from blackmailing. In the worst case, which is not to be wished on anyone, it is absolutely crucial to be prepared and have a mature and functional disaster recovery plan that can take effect immediately to be operational again as soon as possible.