Disaster Risk Management

Cyber Events in the Maritime Industry

HudsonAnalytix
Complexity Made Simple™

Disaster Risk Management

Cyber systems at Ports & Terminals can be grouped into two main categories:

Exchange Data Systems of Port Community

- Vessel, fishing or freight related services, especially used as central point for data exchange with shipping companies, also called “single window”;

Port Management Information Systems

- Maritime traffic control systems, corporate systems (emails, ERP, etc.), security and safety systems as well as Terminal Operation Management Systems, often owned by private companies.

Cargo handling equipment at the port/railway interface

Commercial Long-Haul Trucks

Port Security and Access Controls (physical, CCTV, gates, TWIC, ID cards)

Container Cranes (or liquid cargo handling systems at oil, chemical and LNG terminals) at vessel/port interface

Automated cargo handling equipment, vehicles and similar conveyances

Shore-based systems that directly support safe vessel operation and navigation:

- GPS
- Lock operation
- Communications
- Maintenance and management
- Systems aboard USCG vessels, tugs, fire boats, port police
- Pollution response systems

Automated Cargo Container Tracking Systems

Terminal Operating Center (financial, communications, customs, security and other back office functions)

Data Flows

Port systems interact with a wide range of systems daily:

- **Mandatory declarations** which includes information that shipping companies and stakeholders must report to the Port Authority and or other governing maritime authorities;
- **Control and authorization** given by the authorities to the commercial stakeholders (e.g. authorization to access to the port, authorization to unload the goods);
- **Operational data** related to the port services and processes (e.g. needs for ship refueling, scheduling of cargo operations);
- **Financial data** (e.g. invoicing from the port to its client, payment); and
- **Navigation data** (e.g. GPS position of a ship in the port area, AIS data).

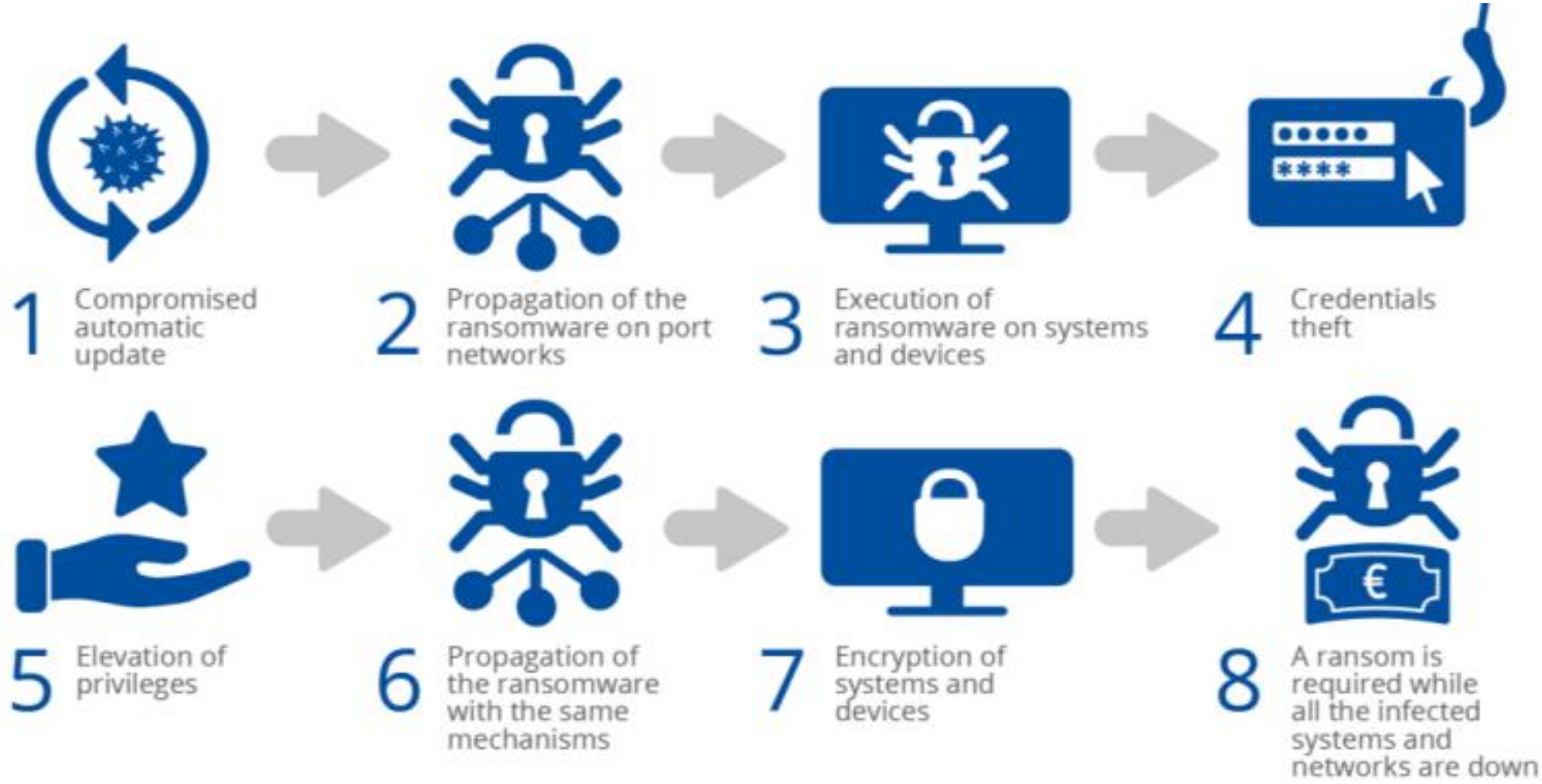
Types of Cyber Threats Facing Ports & Terminals

Threat	Capabilities	Delivery Method
Malware	Any program or code that is created with the intent to do harm to a computer, network or server. Encompasses ransomware, trojans, spyware, viruses, worms, etc.	• Social Engineering: get people to click links, download attachments, or provide access over the phone.
Denial-of-Service (DoS) Attacks	Attackers flood a network with false requests in order to disrupt business operations.	• Multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.
Phishing	Attackers deceive people into revealing sensitive information or installing malware such as ransomware.	• Email, SMS, phone and social media • Social engineering
Spoofing	Attackers disguise themselves as known or trusted sources.	• Email Spoofing: targets businesses by using emails with forged sender addresses

Disaster Risk Management

Cyber Threat: Ransomware

Malware that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return



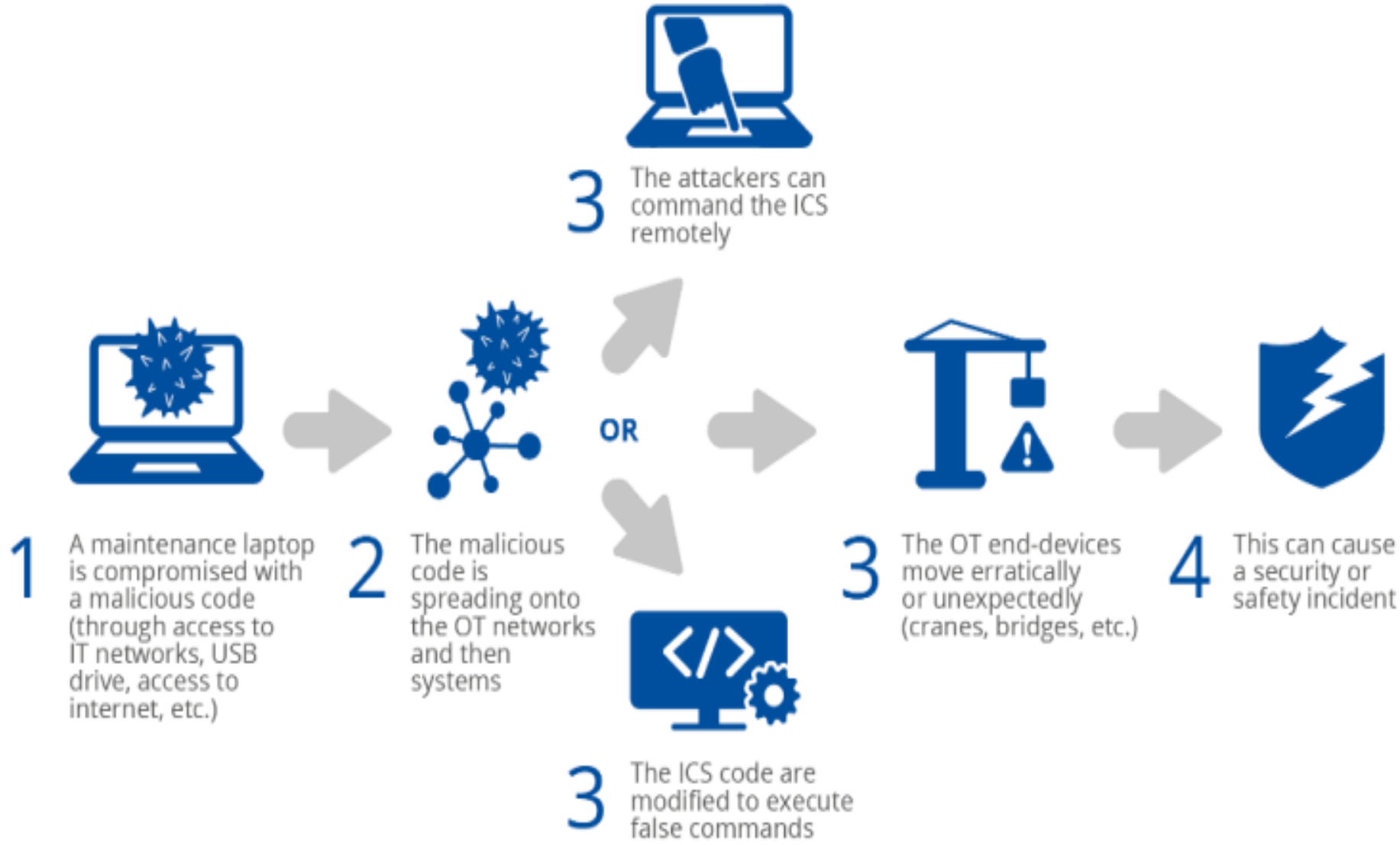
HudsonAnalytix
Complexity Made Simple™

Disaster Risk Management

Cyber Threat: Malware

Malicious code executes unauthorized actions on the victim's system.

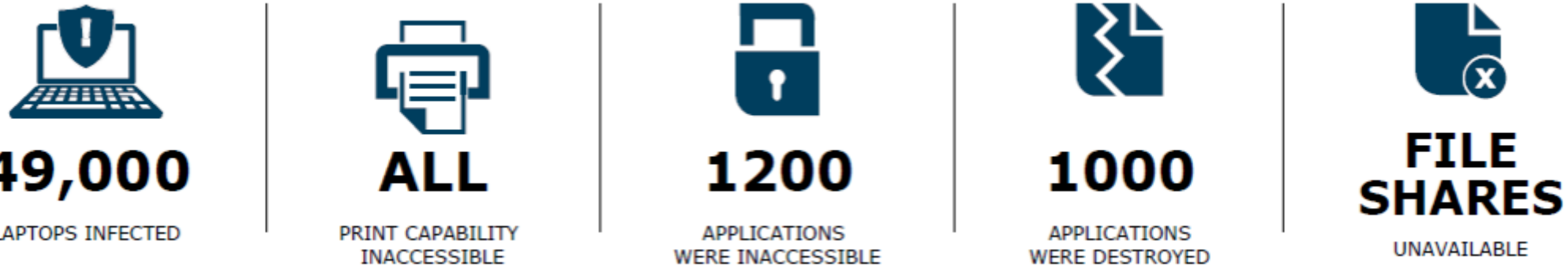
Can include Industrial Control Systems – where the attack can reach physical assets that interact with people.



HudsonAnalytix
Complexity Made Simple™

Disaster Risk Management

On June 27th 2017 Maersk, among many other global companies, were hit by the malware NOTPETYA. This attack led a total paralysis of the Maersk terminal in Rotterdam, with high risks of security and safety incidents, and port terminal operations were managed manually for more than two weeks.



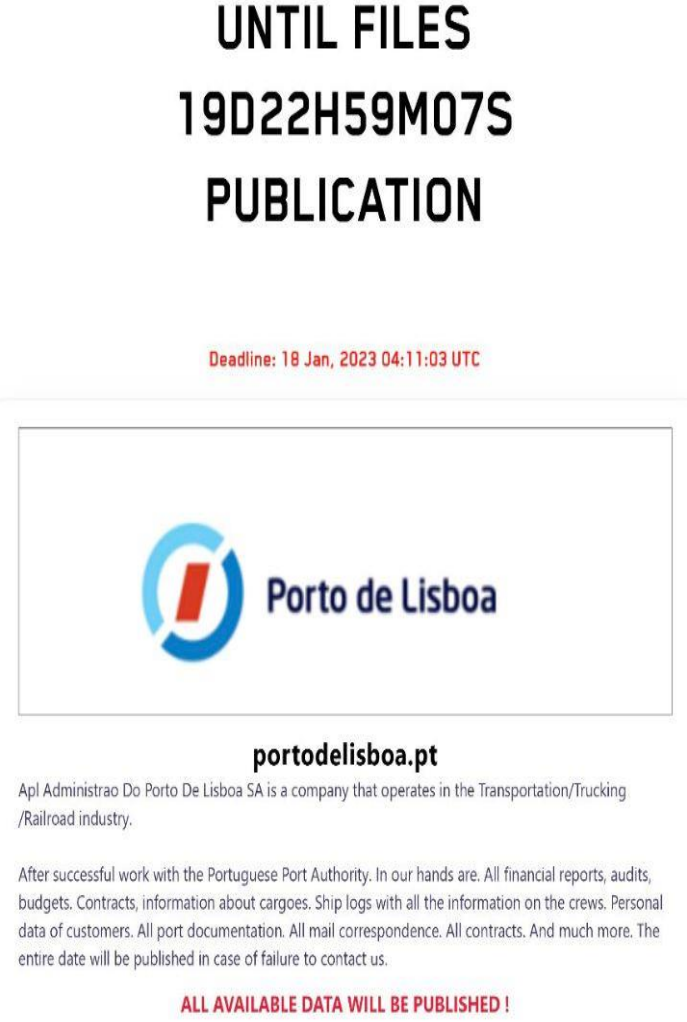
76 port terminals closed around the world, costing Maersk a total of over $300m in damages.

HudsonAnalytix
Complexity Made Simple™

Disaster Risk Management

On January 18th 2022, Port of Lisbon was targeted by ransomware that took down their main website. The hackers threatened to publish all files they stole during the computer intrusion if their payment demands weren't met. The ransom was set at $1.5m. Although PoL managed to get their systems back online, it costed irreparable harm to their global reputation.

According to US DHS, ransomware incidents have become increasingly prevalent among the U.S. state, local, tribal, and territorial (SLTT) government entities, and critical infrastructure organizations, with ransom demands in 2020 exceeding $1.4 billion just in the US.



HudsonAnalytix
Complexity Made Simple™

Disaster Risk Management

On April 12th of this year, Marinette Marine Shipyard fell victim to a ransomware attack. Large swathes of data on their network servers were rendered unusable, this including their manufacturing machines that were connected to the network. The company had their email and some network operations offline for days following the attack.

This shipyard builds military class maritime assets; thus, this attack costed an estimated $5m in damages – not to mention irreparable reputational losses.

HudsonAnalytix
Complexity Made Simple™

Creating Cyber Resilience

- Firewall
- Training
- Create employee usage policy and monitor usage
- Update software per manufacturer’s recommendations
- Decide who has decision making authority
- Pre-planned responses

Continued…

Cyber Risk Assessments:

A cybersecurity risk assessment is an assessment of an organization's ability to protect its information and information systems from cyber threats. The purpose of a cybersecurity risk assessment is to identify, assess, and prioritize risks to information and information systems.

Have YOU completed a cyber risk assessment lately?