RiskIntelligence

The cybersecurity threat to ports: Context, assessment, and looking forward

Whitepaper | May 2021

Risk Intelligence A/S
Strandvejen 100
2900 Hellerup
Denmark

Tel: +45 7026 6230
info@riskintelligence.eu
www.riskintelligence.eu

Contents

About Risk Intelligence

Risk Intelligence is a leading, trusted and reliable partner, providing end-to-end risk assessment and planning. We specialise in analysing threats from the interaction between piracy, organised crime, terrorism, insurgency and military conflicts – since 2001. Our team is dedicated and resourceful, drawing from international experience and a diverse range of backgrounds.

Background

As central hubs to the global supply chain, the physical protection of ports has long been considered important. However, as ports have increasingly digitalised their operations, the safeguarding of their digital networks and assets has often remained underdeveloped, even as the criticality of them has grown. Ports have now reached levels of automation, systems integration, and connectivity wherein interference with digital networks could greatly impact operations and safety. Despite this, the standardisation of port cybersecurity remains far behind that of port physical security. This is all the more concerning as a cybersecurity breach in one port is more able to impact other ports, suppliers, partners, and clients than a traditional security breach could.

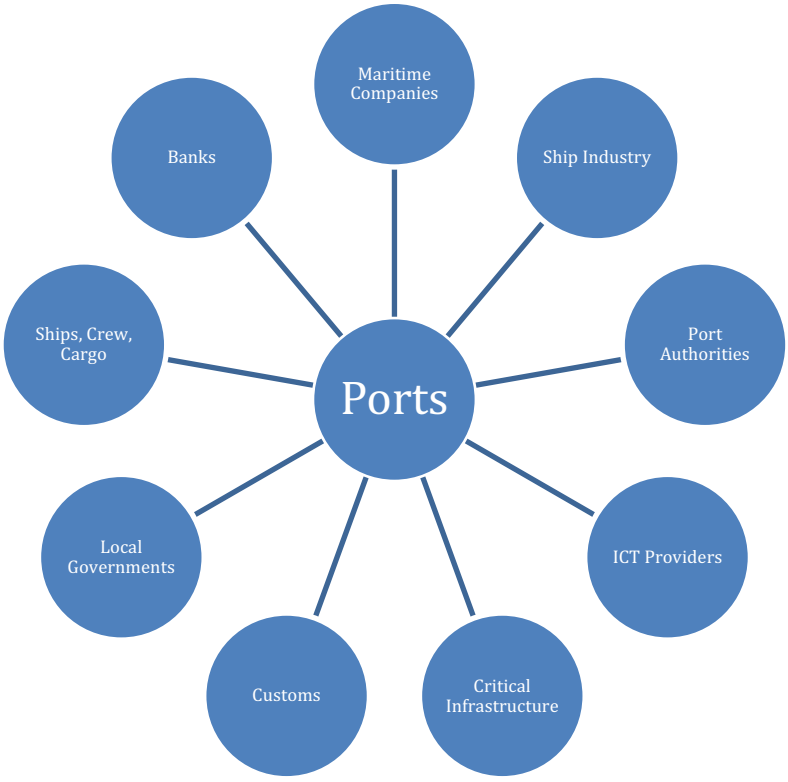

Figure 1: *Port stakeholders*

The increased dependency on information and operational technologies has both attracted new threat actors and provided alternative methods for traditional ones. This is not a phenomenon exclusive to the maritime industry: cyberattacks are increasing in all sectors, but ports have seen a markedly sharp increase in incidents and the potential impacts from them. The digitalisation of processes means cyberattacks can not only steal sensitive data and disrupt corporate systems but also facilitate smuggling, shutdown port operations, or cause physical damage.

Cyberattacks seeking monetary gain are still the most common occurrence. These can often result in disruption of business continuity, damage of reputation, and financial loss. Ports also operate as gateways for trade. They are considered as critical infrastructure by many maritime states as an extensive disruption to a large port could have major economic or security consequences. The bolstering of port cybersecurity requirements is not only in the interest of port authorities, therefore, but also the private and public parties who rely on the maritime supply chain.

Port cybersecurity in context

The digitalisation of ports

Ports have been undergoing a digital revolution in order to remain competitive and more efficiently meet the challenges of modern supply chains. This has been done through the interconnection of Information Technologies (IT), Operational Technologies (OT), Internet of Things (IoT), cloud computing, and the digitisation of data.

The creation of these so-called 'smart ports' has allowed ports to handle larger volumes of cargo faster through better logistic operations, automation, simplified administrative processes, and streamlined information exchanges. This process has not only connected the majority of port assets, including cranes, vehicles, and storage yards, to central digital port systems but has also connected port systems to external networks.

Terms	Definitions
Cyberspace	The interconnected physical and digital networks of information and operational technology systems
Cybersecurity	The protection and risk management of digital systems, devices, software programs, and data from attack, unauthorised access, manipulation, or disruption
Critical Infrastructure	Asset, system, or part which is essential for the maintenance of societal functions or well-being, and the disruption or destruction of which would have a significant impact
Digitisation	The conversion of analog data to digital
Digitalisation	The use of digital technologies and data to transform operational processes
Internet of Things (IoT)	Objects capable of sharing information with other objects or users remotely
Operational Technology (OT)	Technology which monitors or remotely controls physical instruments
Information Technology (IT)	Networks of devices used for storing, retrieving, managing or sharing data

Figure 2: *Port cybersecurity definitions*

The growth of port cybersecurity

The increased connectivity and digitalisation of port systems has heightened security risks and provided vulnerabilities for threat actors to exploit. Cybercriminals have increasingly targeted ports as their cybersecurity sophistication is on average lower than that of other, similarly sized industries. The ports of Barcelona and San Diego, for example, have both experienced significant cyber incidents, leading to bottlenecks in shipping and high business costs. While standard IT security has been widely implemented, holistic cybersecurity covering connected OT and IoT assets and shared external networks is just now starting to become a priority.

Governance of port cybersecurity

The varied structures of ports and the diversity of port operators responsible for processes without common security standards has created substantial cybersecurity vulnerabilities. The port authority/owner typically leases facilities to private terminal operators, who are then in charge of maintaining assets and delivering specific facility operations. Operators are frequently allowed to build infrastructure as required. The larger the port, the less the port authorities often have to do with port operations themselves.

This has created environments where a full understanding of the technologies and infrastructures being used is lacking, complicating the steps to safeguard it. Operators are private companies and there can exist a culture of reluctancy to share information on internal cyber vulnerabilities, even though they may impact other port stakeholders.

International treaties and legislation have created comprehensive physical security requirements and responsibilities for ports. However, when it comes to cybersecurity the legislation remains fragmented and there still lacks integrative requirements to mitigate cybersecurity risks. Practices vary port to port and country to country, with inland ports usually being less regulated.

As many ports share suppliers and operators, the interconnectedness and inter-dependencies across port ecosystems necessitates that all involved operators to maintain similar baselines of cybersecurity to be effective. Many organisations have published guidelines and recommendations; but until the required in-depth industry regulations are created, the impacts and risks of cyberattacks will continue to grow.

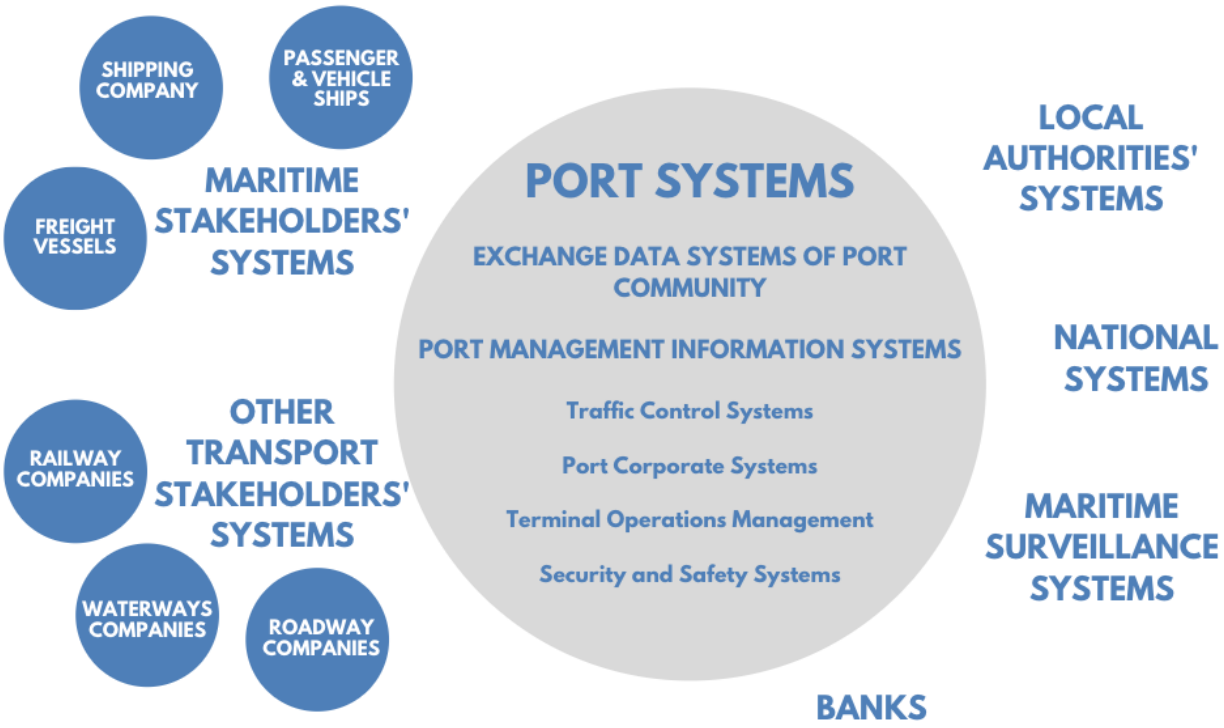

Figure 3: *Port and stakeholder systems*

Port cybersecurity threat environment

Attack surface

As mentioned above, ports operate as a nexus for a multitude of stakeholders that depend on data systems to facilitate the movement of enormous volumes of goods or passengers. A mix of private and public actors work together to facilitate port operations. They are all linked through digital networks either directly or through shared partners. This is makes port systems appealing to malicious cyber actors as after initial ingress there is access to a sizeable amount of sensitive data in connected systems.

The attack surface for malicious cyber interference has steadily grown as automation, digitalisation, and the use of IoT (Internet of Things) have been adopted. Each inherently led to an increase of remotely accessible interfaces that can be used to gain access into networks. The ecosystem of ports requires the linkages of digital systems both within and outside port infrastructure. These systems have often developed independently from each other to meet specific sector needs and standards. Security gaps and vulnerabilities can therefore unknowingly be introduced when connected.

It should be noted that there is a high degree of diversity between different ports' infrastructures and systems. Differing sizes, locations, and services has led to different challenges and ways of implementing technology. Despite this, the majority of commercial ports have digitalised along the same lines, adopting cybersystems that are encompassed within seven layers: physical, network, systems and software, electronic data and information, services, user functions, and processes. These layers involve almost all operations within a port and demonstrates just how much of a reach a cyberattack could have.

Layers of Digitalisation	Examples
1. Physical	Gates, Storage, OT End Devices
2. Network	Internet, Satellites, Wi-Fi
3. Systems and Software	Data Identification, Port Community Systems
4. Electronic Data and Information	Trade Data, Coastal Data
5. Services	Invoicing, Container Management
6. User Functions	Personnel, Port Authorities, Maritime Companies, Ships
7. Processes	Loading, Unloading

Figure 4: *Port digitalisation layers*

Each layer represents possible points of ingress to a malicious cyber actor. The method of infiltration depends on discovered vulnerabilities and which asset the actor is pursuing. In general, there are ten categories of port assets which could be targeted:

1. **Network and communication components** such as radios, servers, and routers
2. **Information and data** such as operational, commercial, and financial data
3. **IT systems** such as Port Community Systems (PCS), Terminal Operations Systems, Cargo Community Systems (CCS), and Berth Management Systems
4. **IT end-devices** such as workstations and mobile devices
5. **OT systems** such as Industrial Control Systems (ICS)
6. **OT end-devices** such as vessels berthing and vessel loading and unloading

7. **Fixed infrastructure** such as hinterland connectivity, port infrastructure, and seaside connectivity
8. **Mobile infrastructure** such as post-service ships and special vehicles
9. **Safety and security systems** such as traffic monitoring systems, detection systems and emergency communication or evacuation systems
10. **People** such as port authority staff, commercial staff, ship personnel, and IT/OT staff

These assets and the automation or integration of them are not universal but they represent common targetable assets of standard large commercial coastal ports. The scope of infrastructures connected to the cyber domain has rapidly grown over recent years. While this has streamlined operations, the increase in remote access capabilities has resulted in diverse port assets being exposed to potential cyber interference.

Port cybersecurity vulnerabilities

Complexity

The scale and diversity of connected stakeholders has made it challenging for ports to implement in-depth cybersecurity procedures. The difficulty in establishing a holistic oversight of connected digital systems has created weaknesses in defences and allowed malicious software to spread rapidly between stakeholders post infiltration. As the maritime industry has fallen behind in cyber defence it has both attracted new malicious actors as well as spurred traditional threat actors to take up new methods.

Increasingly connectivity and remote control

As port infrastructure and operations have digitalised, their interconnectivity, and therefore dependency, has increased. Sensing and control systems such as Supervisory Control and Data Acquisition (SCADA) are increasingly enabling globally networked remote-control functions. While this increases efficiency and data volumes that can be processed, it also exposes the systems to unauthorised persons gaining access. The tendency to integrate systems into one another means wider access for malicious actors.

Poor cybersecurity hygiene

The complexity of port systems has meant cybersecurity measures have often been adopted piecemeal. This can lead to unclear roles over who is responsible for cybersecurity and risk mitigation, as well as fragmented awareness training. Human error is one of the biggest causes of cyber incidents and defined roles and training have been shown to mitigate risks.

Non-Standardised Technology and Procedures

With port operations being global and cross-sectoral, the standardisation of technologies has not been possible. This has led to a mix of off-the-shelf, aging, and heterogenous systems being interlinked. Patches and software updates are often applied asymmetrically, leaving vulnerabilities in networks. A lack of standardised cybersecurity procedures means complex systems without comprehensive oversight.

Potential cybersecurity threats

The impacts of a cybersecurity incident can vary greatly in severity, from a minor inconvenience to a complete shutdown. Ports face numerous cybersecurity threats, some which are industry specific and many which are common across sectors. Increasing interconnectivity, high volume of stakeholders, complicated networks, lack of standardisation, and comparatively belated cybersecurity initiatives have amplified these risks by creating vulnerabilities and attracting threat actors. Some use digital tools to augment traditional maritime threats such as theft or smuggling. Others are professional cybercriminals who target multiple industries with similar attacks in the hopes of increasing success rates.

Financial loss

A cyber incident can impact administrative or operational systems and result in loss of revenue, restart and repair costs, higher insurance premiums, and potential lawsuits.

Reputation or competitiveness loss

A cyber incident can impact not only operations but customers and their trust, especially if sensitive data relating to them is compromised or their networks impacted.

Sensitive or patented data theft

Cyber threat actors often target port systems to gain access to sensitive, commercial, and national security information either for future infiltration, their own benefit, or profit.

Eavesdropping or interception

Malware or hacking of networks can be used to intercept digital emissions in order to gain sensitive information or perform network reconnaissance or manipulation.

Fraud

Financial systems of ports can be compromised to steal money or falsify customs declarations. Email systems can be co-opted wherein a malicious actor pretends to be a legitimate client or participant in order to divert payments or mine for information.

Cargo theft

Threat actors can gain access to digital cargo and container lists to target specific goods to steal.

Trafficking

Gaining access to port systems can facilitate the transportation of illicit goods past customs and security checkpoints

System outages

Cyber incidents, accidental or malicious, can result in outages of power supply or networks, which can impede operations.

Shutdown of port operations

Cyber incidents can shutdown port systems, and therefore operations, for extended periods of time resulting in lost profits and bottlenecks. Ransomware attacks have resulted in several recent port operation shutdowns.

Personnel injury or death

Cyber incidents can impact Operational Technologies (OT), meaning unexpected equipment malfunctions which could endanger industrial environment.

Threat actors

The extensive digitalisation of the maritime industry matched with recognised cybersecurity gaps has led to new threat actors targeting ports. Ports have attracted many cybercriminals due to the sheer amount of saleable, sensitive, or patented data available. Traditional threat actors continue to target ports, but with new digital tools to augment operations such as espionage and cargo theft. It is important to recognize that there is often overlap between the aims, tactics, and tools of cyber threat actors.

Cybercriminals

Cybercrime involves the use of computers and information systems, either as a tool or target, to gain financial benefit. A common method increasingly seen by cyber criminals is the use of ransomware to take control of networks, providing re-access only on receipt of payment. Ports are becoming a popular target for ransomware, which has seen an overall global increase, as the significant impact from stalled operations will theoretically tempt operators to pay the ransom quickly. Cybercriminal operations can also include robbery of cargo, smuggling, trafficking, fraud, forgery or identity theft, and data or information theft.

States

Many states have the capabilities to gather intelligence from digital domains through cyberespionage. It is relatively cheap and low consequence compared to traditional espionage methods. Ports attract state espionage due to the concentration of intellectual capital, importance to national supply chains, and military linkages. If war between cyber developed states was to break out, it is likely attacks will happen in the cyber domain. Ports are relevant from a military perspective and there is the possibility some states may have pre-emptively infiltrated strategic port systems in preparation for possible conflict.

Terrorists

Terrorists are individuals or organised groups seeking to use violence against civilians for ideological reasons. Terrorists have sought to impact critical infrastructure previously, though usually through kinetic means. A large port cyberattack would either significantly disrupt a nation's supply chain or cause widespread physical damage, theoretically possible with operational technology being increasingly remotely controlled.

Hacktivists

Hacktivism is the use of hacking techniques to create pressures on an organisation or draw attention to a specific issue. The target could be the port itself, the operator of a port facility, or a third, connected party.

Threat overview

There was a marked increase in frequency and severity of cybercrimes targeting ports and port stakeholders in the last year. This trend is likely to continue as more malware as a service becomes available. There are cyber criminals who have started specialising in maritime sector attacks due to the potential high payoff and known cybersecurity vulnerabilities.

As such, there is a high possibility that many port stakeholders will experience attempted or successful cybercrime incidents as they have become commonplace. These attacks will likely target business systems or disrupting administrative services; but there is increasing possibility of physical operational systems being impacted.

Cyber espionage is common within port systems and likely to continue occurring, both by criminals and states. Organised criminals target ports due to the large amount of goods and saleable data moving through them. Cyber espionage is frequently used to set up future malicious operations or steal sensitive information. Victims of cyber espionage may face damaged business reputations, lost profits, recovery costs, or an increased risk of a future attack.

Port systems are targets of espionage from states due to their status as critical infrastructure and the maritime technologies used. However, cyberwar, or the use of a physically destructive cyberattack by a state, would be unexpected. Some states have the capability to deploy cyberattacks, which could result in large physical damage or death. However, the likelihood of them launching such a cyberattack against a port is low. It would widely be seen as an act of war and therefore there would need to be considerable cause and reason for a port to be targeted.

Cyberthreats	Actors	Motivations	Objectives
Cybercrime	Individuals, Industrial Spies, Organised Crime	Financial Gain, Information, Egoism	Cargo, Digital Assets, Network Access, Organisational Data
Cyber Espionage	Industrial Spies, Governments, Organised Crime, Individuals	Information, Political, Financial Gain, Ideological	Digital Assets, Knowledge, Organisational Data
Cyber Terrorism	Terrorists, Insurgents, Activists	Ideological, Political, Religious, Social	Disruptions, Damage, National Institutions, Critical Infrastructure
Hacktivism	Hacktivists, Hackers, Individuals	Political, Societal, Egoism, Reputation	Attention, Disruption, Knowledge
Cyberwar	Governments, Terrorists	Political, Social	Military, National Damage,

Figure 5: *Port cyberthreats*

The threat from cyber activism has tapered off in recent years and no recent incidents have been recorded. Individual ports may be targeted due to, for example, an animal welfare or environmental incident. However, as ports often do not publicly disclose cyber incidents, activists may choose other methods to draw attention their cause. Similarly, a cyber terrorist attack targeting a port is difficult to imagine. Known terrorist organisations lack the supposed technical capabilities to trigger a destructive port cyberattack. Traditional methods are more accessible and impactful for their purposes and it is therefore unlikely it is a strategy that will be attempted in the near future.

The most common threat against port cybersecurity systems will continue to be criminals: either exploiting vulnerabilities to facilitate traditional activities such as smuggling or trafficking, or using malware and hacking to steal data or ransom systems. While incidents with more serious consequences have become possible, they are still not probable. However, the continued costs of cyber disruptions to port systems should not be ignored. Malicious cyber actors are continuing to evolve and gain more advanced tools, increasing both the frequency and impact of incidents.

Looking forward

Commercial ports are a key component of supply chain critical infrastructure. The development of integrated smart ports has meant that their operations are now dependent on both physical and cyber systems functioning properly. While efficiency has increased, the accumulative interconnectivity of stakeholders and infrastructure, and the growing amounts of critical data being processed, has opened ports up to new threats. The resulting rise in incidents has caused cybersecurity to become a central concern for maritime ports.

However, the standardisation and strengthening of cybersecurity in ports is still far behind that of physical security. Governments and oversight bodies are starting to realise the hazards of a non-standardised cybersecurity environment and have begun implementing directives. Initiatives, however, have mostly focused on risk assessment, while formulised incident handling procedures remain underdeveloped.

The complexity of port networks means that complete oversight of the infrastructure and software used is difficult. Port digital systems need all participants in the supply chain to realise their criticality in order to become secured. Building cybersecurity awareness across operational levels has been shown to mitigate the likelihood and impact of cyber incidents. Including the shared responsibilities of securing digital infrastructures and ensuring business continuity and disaster recovery in service level agreements helps clarify responsibilities. Auditing and certification systems for port software have been suggested as ways to reduce vulnerabilities and increase accountability.

Overall, these are all methods that have been successfully used in other industries. Ports have now reached a stage where the potential cost of not integrating cybersecurity procedures outweighs that of implementation.