THE IMPLICATIONS AND THREATS

OF CYBER SECURITY FOR PORTS



Norbert Kouwenhoven, IBM EU solutions leader customs & borders, Amsterdam, the Netherlands, Martin Borrett, director of the IBM Institute for Advanced Security Europe, Hursley, Hants, UK, and Milind Wakankar, IBM safety & security consultant, travel & transportation CoC, New Delhi, India

Ports are critical infrastructures. Unavailability of a large port could present a major economic incident for a state or country, and could bring 'just in time' supply chains to a grinding halt in a number of days. Due to their interconnections and dependency on information and communications technology (ICT) systems and the internet, ports are increasingly vulnerable to cyber attacks. A solid cyber security plan is a must in any modern port. How ready are you?

PORTS ARE CRITICAL INFRASTRUCTURES

Critical infrastructure in any country's context can be defined as physical facilities, supply chains, intangible assets, communication networks etc. whose destruction or unavailability for an extended period would seriously impact the health, safety, security or economic wellbeing of that country, its citizens and expats, or could cause a large scale loss of life, major social disturbance or mass casualties. Ports are such critical infrastructures.

They are a key facilitator in international trade and logistics, and they play a unique role in global supply chain activities. The key function of a seaport as a connection point between sea and inland transportation substantiates its importance to a regional economy.

In the EU, sea ports play an important role facilitating the European Union's external trade (90 percent of the total, in terms of weight) and internal market exchanges (43 percent of the total). Industries and services belonging to the maritime sector contribute between three and five percent of EU gross domestic product (GDP), and maritime regions produce more than 40 percent of Europe's GDP.[i] Ports are nodal points of inter-modal logistic chains. They are key for the sustainable growth of transport in Europe.

THE IMPACT OF DISRUPTION ON PORT OPERATIONS

Maritime activities are so crucial that their unavailability or major delays in their supply chain would present a serious economic incident. The zero-inventory, 'just-in-time' delivery system that sustains the flow of global commerce would come to a grinding halt; in a matter of days shelves at grocery stores and gas tanks at service stations would run empty. In certain ports, a disruption affecting energy supplies would likely send shock-waves through the global economy. The impact of the closed sea and airports after 9-11, where the automotive industry had to close factories within 48 hours after port closing, clearly demonstrated the vulnerability of the 'just-in-time' based economy.

RISKS AND VULNERABILITIES

Ports are susceptible to various kinds of operational risks: accidents; equipment failure; mishandling of dangerous goods; congestion; labour strikes; inadequacy of labour skills and security breaches including sabotage, thefts and direct attacks.

The maritime sector is characterised by an extremely diverse international labour force, thousands of intermediaries and vessel registration practices where some vessel owners can easily hide their true identity. It has already displayed vulnerabilities in the past (illegal smuggling of drugs, etc). Surprisingly, until now the threat of cyber security has not been discussed. Cyber security threats should be an important consideration in the maritime sector, considering the dependency of many of its operational aspects on Information and communications technology (ICT).

CYBER SECURITY THREATS

DEPENDENCE OF PORTS ON ICT

The maritime industry has evolved from the 'paper and fax' culture and adopted process automation through ICT, the use of the internet, and integrated IT systems. This has helped to achieve reduced cargo delays, faster processing times, better asset control, decreased payroll, fewer losses due to theft, and decreased insurance costs.

While large ports have benefited from increased productivity due to IT improvements in their supply chain, other stakeholders and trading parties – small shippers, forwarders, land and sea carriers, customs authorities, port and terminal operators have equally achieved tremendous savings and process improvements. Vessel turn-around times have been shortened, customs clearing accelerated, costs associated with redundant data entry eliminated and cargo handling costs slashed.

This has led to an increased dependency on e-processes, electronic information exchange, networked computers and control systems. The flip side of these operational benefits is that ports and maritime operations are now vulnerable to cyber threats. Digitisation and automation have given networks a key role in communications, and ports are increasingly dependent on the nerve systems of our societies.

TARGETED SYSTEM COMPONENTS

System components that are potential targets are multiple: the terminal operating system contains the location of containers and destination directions for unmanned vehicles. It has been deemed entirely feasible that pirates could hack a ship's system and redirect it.

The location system of the vessels could be used to misdirect vessels with terrible consequences. Malfunctioning of the port community system could prevent clearance and disrupt logistic flows. Failing radar systems would prevent proper vessel traffic management. Failing communication networks could cause various types of accidents, and endanger emergency response. On board vessels there is a growing reliance on electronic systems. There is a longstanding fear that terrorists may hack into systems and cause, at best, chaos and, at worst, a real disaster.

CYBER ATTACKS

Looking back at 2013, it is clear that successful tactics implemented by attackers continue to challenge enterprises to keep up with security basics. At IBM we continue to see operationally sophisticated attacks as the primary point of entry. Some of these were attacks of opportunity, where unpatched and untested web applications were vulnerable to basic SQL injection (SQLi)

or cross site scripting (XSS) exploitation. Other attacks were successful because they violated the basic trust between end user and sites or social media personalities thought to be safe and legitimate. Many of the breaches reported in 2013 were a result of poorly applied security fundamentals and policies and could have been mitigated by putting some basic security hygiene into practice. For a variety of reasons, companies seem to be struggling with a commitment to apply basic security fundamentals.

Watering hole attacks, which have continued, are a great example of how operational sophistication is being used to reach targets not previously susceptible. By compromising a targeted central site and using it to serve malware, attackers are able to reach more technically savvy victims who may not be fooled in phishing attempts, but who do not suspect that the sites they trust could be malicious. Several high tech companies, as well as government agencies have been successfully breached in past months. Often satellite sites, like franchises or local language sites, are not secured with the same standard as the home office. By going after a weaker point of entry into larger enterprises, attackers were able to reach and tarnish well-known brands. This can damage a brand's reputation and create legal issues if sensitive customer data is leaked. These types of leaks affect the food industry, consumer electronics, automotive, and entertainment industries in particular.

Attackers have demonstrated enhanced technical sophistication in the area of distributed denial of service (DDoS) attacks. DDoS methods per se are not advanced, but the method for increasing the amounts of capable bandwidth is a new and powerful way to halt business by interrupting online service. The banking industry was hit particularly hard in the first half of 2013. DDoS attacks are being used as a distraction; allowing attackers to breach other systems in the enterprise while IT staff are forced to make difficult risk-based decisions, possibly without visibility of the full scope of what is occurring.

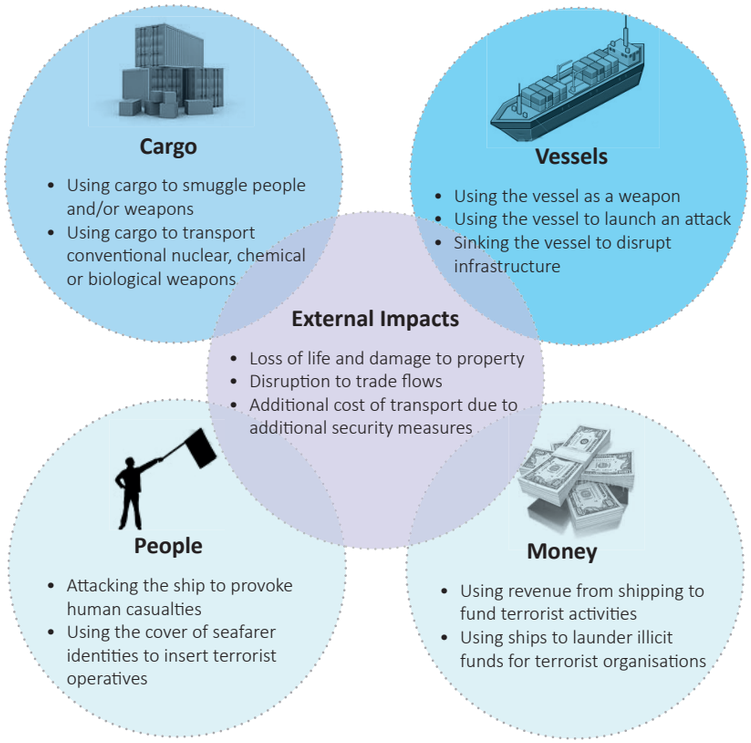

Figure 1: Risks associated with ports and the maritime sector.[ii]

PORTS, ARE YOU READY?

Security intelligence relies on data and the analytics, tools, and people who use them. These days most enterprises, including ports, are generating more data about what's going on inside their businesses than they can put to good use. You're likely to find that the complexity of your environment is making it difficult to understand and analyse all available data in a way that will help you make smarter decisions about cyber security.

At IBM, we are constantly striving to find the balance between improving the way to do business and the need to control and mitigate risk.[iii] Our approach includes technology, process and policy measures. It involves 10 essential practices:[iv]

1. **Build a risk-aware culture:** Build a risk-aware culture where there's zero tolerance at a company level to colleagues being careless about security. Management needs to push this change relentlessly from the top down, while also implementing tools to track progress.
2. **Manage incidents and respond:** A company-wide effort to implement intelligent analytics and automated response capabilities is essential. Creating an automated and unified system will enable an enterprise to monitor its operations and respond quickly.
3. **Defend the workplace:** Each work station, laptop or smart phone provides a potential opening for malicious attacks. The settings on each device must all be subject to centralised management and enforcement. And the streams of data within an enterprise have to be classified and routed solely to authorised users.
4. **Security by design:** One of the biggest vulnerabilities in information systems comes from implementing services first, and then adding security on afterwards. The only solution is to build in security from beginning, and to carry out regular tests to track compliance.
5. **Keep it clean:** Managing updates on a hodgepodge of software can be next to impossible. In a secure system, administrators can keep track of every program that's running, be confident that it's current, and have a system in place to install updates and patches as they're released.
6. **Control network access:** Organisations that channel registered data through monitored access points will have a far easier time spotting and isolating malware.
7. **Security in the cloud:** If an organisation is migrating certain IT services to a cloud environment, it will be in close quarters with lots of others possibly including scam artists. So it's important to have the tools and procedures to isolate yourself from the others, and to monitor possible threats.
8. **Patrol the neighbourhood:** An enterprise's culture of security must extend beyond company walls, and establish best practices among its contractors and suppliers. This is a similar process to the drive for quality control a generation ago.
9. **Protect the company jewels:** Each enterprise should carry out an inventory of its critical assets- whether it's scientific or technical data, confidential documents or clients' private information and ensure it gets special treatment. Each priority item should be guarded, tracked, and encrypted as if the company's survival hinged on it.
10. **Track who's who:** Organisations that mismanage the 'identity lifecycle' are operating in the dark and could be vulnerable to intrusions. You can address this risk by implementing meticulous systems to identify people, manage their permissions, and revoke those permissions as soon as they depart.

FORWARD THINKING

Ask yourself and your colleagues how well your organisation is currently following the 10 essential practices outlined above. But don't stop there. The complexity involved in making sound security decisions in today's environment means you'd probably benefit from talking to a specialist security expert from outside your company. A solid Port Cyber Security Plan is a must for any port in today's interconnected world.

REFERENCES

[i]ENISA Workshop on Cyber Security Aspects in the Maritime Sector
[ii]Report on security in maritime transport: Maritime Transport Committee of OECD
[iii]link to the 10 Essentials- www.ibm.co/EssentialPractices
[iv]link to Cyber Security Intelligence Index- www-935.ibm.com/services/us/en/security/infographic/cybersecurityindex.html

ABOUT THE AUTHOR

Norbert Kouwenhoven has over 20 years of international experience in various areas of the public sector. In his current role as sales executive at IBM, Norbert Kouwenhoven is focusing on IBM EU solutions in the area of customs and borders. These cover solutions like the eCustomsFramework, Maritime Single Window, Risk Management, and Security. During his work in customs he found that security is a major theme in almost all links of the supply chain. Cyber security in ports, being a relatively new factor, deserves special attention, hence the article.

Martin Borrett is the director of the IBM institute of advanced security in Europe. He leads the Institute and advises at the most senior level in clients on policy, business, technical and architectural issues associated with security. Martin leads IBM's security blueprint work and is co-author of the IBM Redbooks "Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security" and "Understanding SOA Security". He is chairman of the European IBM Security User Group community and a member of the board of EOS, the European Organisation for Security. He is a fellow of the British Computer Society, and a Chartered Engineer (CEng) and member of the IET. Martin has a passion for sailing and has represented Great Britain; he is also a keen tennis player.

Milind Wakankar is an industry consultant for IBM's travel and transportation sector, and member of the Global Centre of Competence. He is based in New Delhi, India, and specialises in safety and security. He has worked with many clients in the travel and transport area across the world on topics of safety and security.

ABOUT THE ORGANISATION

IBM is the world's leading IT company, with over 400.000 employees spread around the globe. IBM offers a wide range of services and products, including strategy consulting, industry consulting and IT services. IBM's X Force is famous for monitoring and protecting IT networks against cyber threats, and the IBM software product stack recently has been extended with a unique portfolio of secure middleware and analytic products. After beating the world's best chess player Kasparov with 'Deep Blue', and beating the world's best Jeopardy player with 'Watson', IBM's research department recently made the headlines with its ability to manipulate individual atoms, producing a movie 'A boy and his atom', featuring walking atoms.

ENQUIRIES

Email: norbert.kouwenhoven@nl.ibm.com

PREPARE FOR THE NEXT ATTACK

2016 UPDATE

Since the article ´Cybersecurity in Ports´ was written in 2014, the use of information technology in ports and in cyberspace has evolved. Ports have become nodal points of intermodal logistic chains. With even more use of information technology, sharing of data and optimised processes, their increased interconnectivity makes them as vulnerable as ever to disruption.

The Internet of Things (IoT) has taken off: Sensors connected to a network, in combination with code where specific sensor signals trigger automated execution of predesigned processes. Sometimes signal data are used to trigger physical follow-up actions, like the movement of a crane, or the opening of a locked door. Other times sensor data are used to improve operational and situational awareness. A new trend is to store signal data in block chains if they represent evidence of key events. Key events that could trigger invoicing, mandate specific payments, or transfer ownership from one party to another.

The Self Driving Car is rapidly gaining traction in the automotive industry. We all know the Google car, the Tesla cars and other electric vehicles. The IoT allows for the use of autonomous vehicles in ports as well. It was a no brainer for the designers that the two recently opened terminals in the Port of Rotterdam (APM Terminal, Rotterdam World Group Terminal) are using an IoT network plus IoT enabled autonomous transport vehicles. The next step could be the use of cognitive techniques where vehicles, cranes and other assets get smarter every day. Cognitive IT capabilities allow them to collect, interpret and actually understand structured and unstructured data. Based on these insights they will apply learning techniques to autonomously improve their efficiency and effectiveness. They will remodel their behaviour accordingly.

All this sophistication makes ports very vulnerable to disruption. Manipulating sensor data or software algorithms can lead to physical and financial damage. Experiences of the last few years show that cyberattacks increase in number and get more sophisticated every year.

The public awareness of cyber vulnerability fortunately is growing. Governments are wide awake now. The EU is building a construct of legal and policy measures that enforce proper protection of European organisations against cyberattacks. Already the new European General Data Protection Regulation (GDPR) has been adopted, forcing organisations to take measures to protect the data in their custody and report data breaches. The EU Member States have until 2018 to implement the required measures, ports will certainly be affected. The NIS Directive is another EU initiative- in force since 2016. It aims to bring cybersecurity capabilities at the same level of development in all the EU Member States, and has specific rules for critical public services. Ports will definitely be identified as such. Subsequently it will be mandatory for ports to implement specific cybersecurity measures, aimed to ensure resilience as an operating port.

Besides cybersecuring the ´in house´ information systems, ports have to be aware of their cloud security. Service providers such as IBM, Amazon, and Soget these days offer solutions ´on cloud´ (Supply Chain Visibility Platform, analytic applications). This is a very attractive model for a port or a trade lane community, since it reduces cost and the need for extensive in-house IT capabilities. Security and privacy concerns are similar across cloud services and traditional non-cloud services. These concerns are amplified by the existence of external control over the cloud. Information as well as system components that were previously under the ports direct control now are under external control (cloud provider). There is a risk of cyberattacks in the cloud and the cloud-based solutions/assets. Ports will need to take responsibility for the security of the used cloud computing services. The port needs to ensure that the cloud contract has appropriate provisions for security and privacy. The contract e.g. needs to help maintain legal obligations to protect privacy of data stored and processed on the provider's systems (GDPR). The port must also ensure appropriate integration of cloud computing services with the ports own systems for managing security and privacy.

Do you make use of autonomous transport vehicles, do you use the IoT, sensor data, do you have a data sharing platform or a Port Community System? Your port is at risk!

You run a critical economic service, increasingly vulnerable for cyberattacks. Legislative measures NIS, GDPR will demand you to focus on cybersecurity, so will your shareholders and your clients. Did you apply the ten essential practices from the original article? They are valid, and more important than ever!