DEVELOPING A DIGITALLY RESILIENT SUPPLY CHAIN

Adam Gostling, Managing Consultant, QinetiQ, London, UK

The maritime industry is deeply rooted in the movement of physical goods, but this does not make it immune from digital disruption. Increasingly, operation technology (OT) is highly connected to information technology (IT). Modern ports and vessels have myriad systems performing many functions; tracking goods through loading and transit, navigation systems optimizing docking and shipping routes, and sensors monitoring and adjusting engines to optimise fuel consumption. These digital innovations are brought from, and managed by, an increasingly complex supply chain.

Most suppliers take security seriously, but the very nature of having many suppliers accessing customer networks creates entry points, which could be exploited by criminals or activists. Supply chain breaches have already struck many industries; the biggest of recent times (Target, and TalkTalk) were at least partly due to supplier lapses.

Supply chain security is not unique to maritime, but the industry is behind others such as finance and technology, when it comes to understanding digital risks, and can be viewed as an easier target compared to other sectors. This needs to be addressed to ensure maritime becomes resilient against ever advancing digital threats.

WHO WANTS TO HURT MARITIME?

The maritime industry faces many similar digital risks to other industries, as well some unique challenges due to its international nature. As with any industry with a connected presence, maritime is a target for blackmailers and financial fraudsters, for example via Ransomware attacks, or 'killdisk' software designed to cause customer disruption. It is also a tempting target for activists or terrorists. Ports and shipping are critical national infrastructure, and attacking them would be a coup for those wanting to cause disruption, or to make a political statement. Shipping companies include big businesses operating in industry sectors such as oil and gas, whom activists may wish to harm, for example through a distributed denial of service (DDOS) attack.

More coordinated threats may come from organised criminals, who have long exploited shipping to smuggle contraband and people. As cargo is increasingly managed and tracked by technology, we shouldn't underestimate the ingenuity and resources of organised criminals to surreptitiously infiltrate that technology.

DIGITAL DISRUPTION, DIGITAL SUPPLIERS, DIGITAL RISK

Suppliers are relied upon, by ports and ships, to integrate, run, and maintain connected technology. These include monitoring tools for industrial machinery and propulsion, 4G and satellite connections, navigation systems, cargo management, handling and loading software, and integrated platform management systems. Many such devices have IT interfaces which control or manage OT, increasing the potential 'attack surface' of the system. Many OT systems were designed before the modern connected world. Growing OT connectivity needs to be closely managed, with a continued drive for IT and OT integration.

The result is a very complex supply chain. This presents opportunities to breach digital defences by infecting supplier technology or compromising suppliers' individual employees. Social media, for example, provides a rich platform for criminal gangs intent on compromising or blackmailing people to gain access to their business operations. Once inside, there is opportunity for considerable disruption. The 2015 Ukraine power grid attack targeted a popular website where engineering manuals were downloaded, creating an infection route which compromised engineers' laptops. When a laptop was connected to the target system, the attack would be launched. If a similar virus found its way into ports' critical systems and supply chains, it could cause large-scale financial impact.

The overarching problems, however, are often a lack of detailed awareness and understanding of the digital risks the supply chain presents to operations, and to what extent essential suppliers are embedded in operational networks. Discussions around controlling access for suppliers, or including security responsibilities in contracts, are often less comprehensive than they should be. The maritime industry needs to better understand these risks before it can make informed decisions about mitigating them.

WHAT SHOULD YOU ASK OF YOUR SUPPLY CHAIN?

The starting point is to map out the supply chain, establishing who is involved and what they do. Few companies can do this with the level of detail needed, but it is critical to understanding and mitigating operational risk. Then, there is a need to ask and answer important questions about how they operate, the controls they have in place, and their relationships with their own suppliers. The key questions are as follows:

WHO HAS ACCESS?

Companies should know what suppliers are doing in port or on vessels. Suppliers visit sites to work with technology, and access it via remote logins. They need freedom to do their job, but autonomy creates risk. A clear view of who has access, and when, enables better security decisions. For example, login details for individuals, rather than per supplier, make it easier to quickly identify the source of a problem, as well as deterring abuse.

WHAT SAFEGUARDS DO YOU WANT?

A simple safeguard is a 'sheep-dip' computer, which is used to check the contents of an engineer's USB prior to connecting to any system and to perform updates. Another is tighter access control: can suppliers remotely login whenever they want, or is access granted only in response to a helpdesk ticket which opens a dedicated network port? Is access limited to IP addresses at the supplier's physical premises, or can their employees login from home via personal laptops? In each case there is a balance of security versus convenience.

WHAT IS THE CONTRACTUAL RELATIONSHIP?

Ports and ship operators need to contractually define responsibilities between them. An essential element is who 'owns' what data, and what their responsibilities are for safeguarding it.

ARE SUPPLIERS COMPLIANT?

Good security practice includes ensuring you and your suppliers are compliant with necessary regulations. For example, owners and operators involved in shipping oil and gas must comply with TMSA3, which now includes digital security requirements in Element 13. The International Ship and Port Facility Security (ISPS) Code, covers minimum security arrangements for ships and ports. As of 6th July 2016, the European Union published directive 2016/1148, the Network and Information Systems Directive (NIS-D), which places a number of requirements upon 'Operators of Essential Services'.

IS SOMEONE IN CHARGE OF SECURITY?

Finally, there must be someone responsible and accountable for digital security. Industries like finance have long recognised this, appointing Chief Information Security Officers. Minimising digital risk from complex supply chains means having someone managing the digital relationship with suppliers, and understanding the nature and extent of these digital interactions.

ENSURING DIGITAL RESILIENCE IN THE MARITIME SUPPLY CHAIN

Supply chain resilience starts by asking these questions. This is primarily a human task, involving workshops and questionnaires to benchmark business operations, which can then be mapped against industry best practices, standards and regulations. Once these are clearly defined, more technical and business solutions can be deployed to manage and understand risk in complex, extensive supply chains.

All decisions bring trade-offs between security, usability and cost. There are times when significant new infrastructure will be required and others where digital risk can be mitigated by adjusting contractual relationships or changing process. Correct training of personnel to empower them with digital security knowledge at a basic level enables management of risk to extend throughout the company.

There is no single right answer, but organisations should start by understanding the specific digital risks they face from the way their supply chain accesses their operational systems, and the nature and extent of these digital interactions. There are many legitimate options when it comes to digital security, but those decisions can only be made if they are entered into and based upon evidence and rigorous understanding of how, when and why the supply chain is accessing their IT and OT systems.

ABOUT THE AUTHOR

Adam has worked in the QinetiQ cyber practice since 2002, and as a managing consultant provides cyber advice to clients both in the commercial and government sectors. He has worked extensively overseas, and has performed a number of CISO roles on behalf of customers in support of enhancing their cyber capability. Prior to joining QinetiQ he previously worked in the police within specialist operations based in London, and in the banking and finance sector.

ABOUT THE ORGANIZATION

QinetiQ is a leading science and engineering company operating primarily in the defence, security and critical infrastructure markets. It works in partnership with customers to solve real world problems through innovative solutions, delivering operational and competitive advantage.

ENQUIRIES

https://www.qinetiq.com/