Navigating Rising Cyber Risks in Transportation and Logistics

By Sugar Chan, Eitan Yehuda, Russell Schaefer, Alain Schneuwly, Sharon Zicherman, Stefan Deutscher, and Or Klier

Digitization has become prevalent among transportation and logistics (T&L) companies, improving all upstream and downstream facets of the industry. This process has created unprecedented efficiencies targeted at expanding revenue streams.

That's the good news. The downside is that digitization has exposed a series of shortcomings among T&L companies that have made them extremely vulnerable to cyber attacks. Every sector of the industry—including maritime, rail, trucking, logistics providers, and package deliverers—is affected. The impact is costly, disruptive to operations, and has the potential to create further liability, particularly when sensitive customer data is breached.

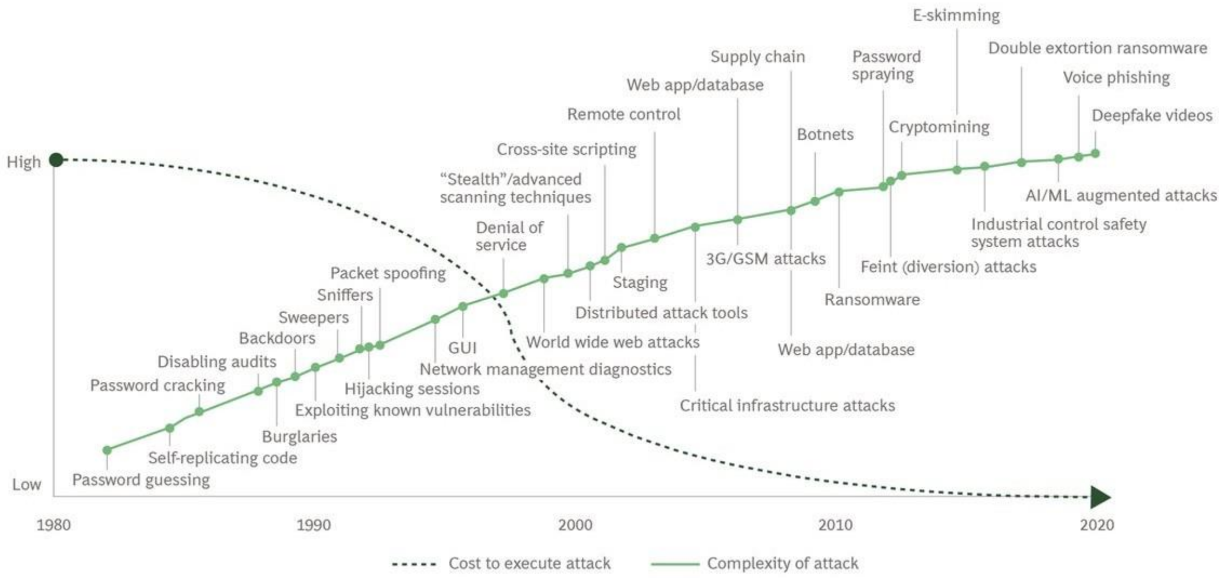
There are multiple reasons for the increased threat. For one, the expanded use of operational technology (OT), which opens new communications and wireless channels that are connected directly to T&L companies' digital ecosystems, is a soft target for hackers. In addition, the T&L industry suffers from lagging cyber regulations and standards, inadequate cybersecurity awareness, and a shortage of cyber-defense talent.

Cyber attacks used to occur every few years in the T&L sector. Now, there seems to be one or two each month. Some are prominent. For example, a cyber attack in May 2021 effectively shut down the Colonial Pipeline, which provides gasoline to almost half of the east coast of the United States, for about a week. The company said that the cost of the ransom and the disruption to business could run upwards of $50 million. Other cyber attacks, even those aimed at major shippers that have been repeat targets, receive less press attention but often involve disrupting email and logistics systems.

Moreover, hackers are increasingly attempting to steal data stored in networks that are critical to the T&L industry's modernization and growth because they provide a more efficient and compelling customer experience. These networks enable digital improvements like automated ordering, shipment tracking, and access to account information. While extremely valuable, such customer initiatives require warehouses of sensitive information collected via online platforms, phone apps, and other mobile devices, which, because they lack strict cyber-protection protocols, are among the most insecure channels.

And, as the potential cyber-attack surface in the T&L sector expands and the nature of risk continues to widen, the cost of break-in has dropped significantly. (See Exhibit 1.)

Exhibit 1 - Cyber Attack Complexity Increases as Difficulties and Cost to Break-In Decreases



Sources: Information Security Incorporated; BCG analysis.

Note: GUI = graphical user interface; GSM = Global System for Mobile Communications.

Considering the amplified urgency, BCG has examined why the industry is so vulnerable to cyber attacks today. We have come up with a set of integrated solutions that companies can deploy to mitigate these risks and create realistic, dependable safeguards against them.

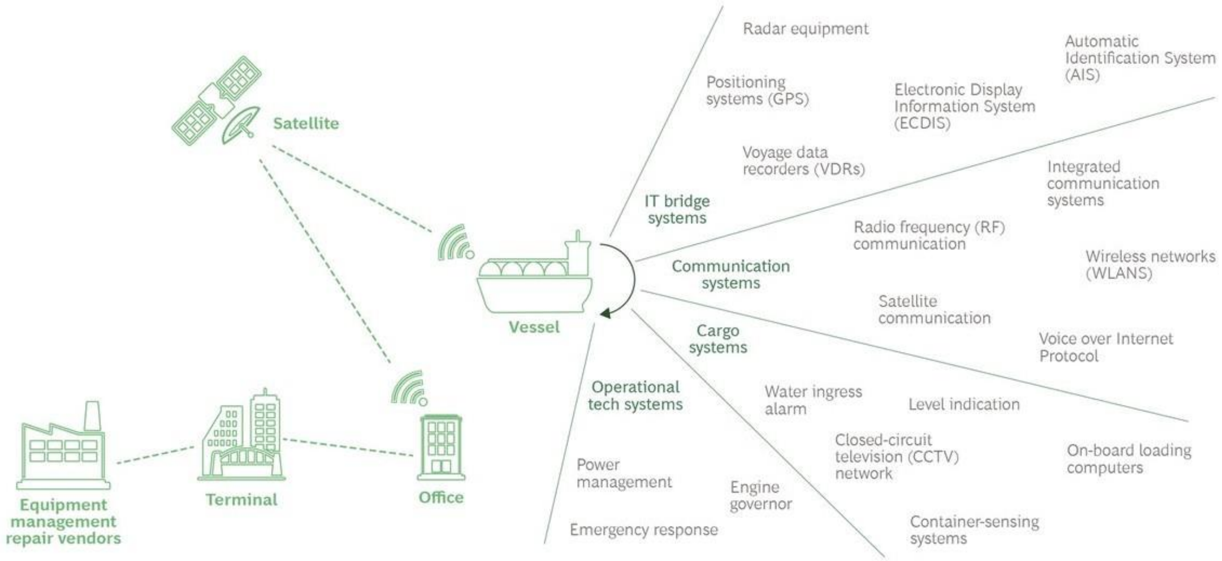
WHERE THE WEAKNESSES ARE

The easiest way to look at the dilemma facing T&L companies is to separate their cyber vulnerabilities into three categories: technology, regulation, and people and processes. Each of these categories needs to be considered carefully to address the emerging threats impacting the broader industry.

Technology. In every segment of the T&L industry, the widened cyber-attack surface is evident. For instance, among maritime companies, relatively simple distress-and-safety systems have been replaced by full-fledged, cloud-based, local area networks, like the International Maritime

Organization’s (IMO) e-navigation program. These networks are a tempting target for hackers because they collect, integrate, and analyze on-board information continuously to track ships’ locations, cargo details, maintenance issues, and a host of oceanic environmental considerations. (See Exhibit 2.)

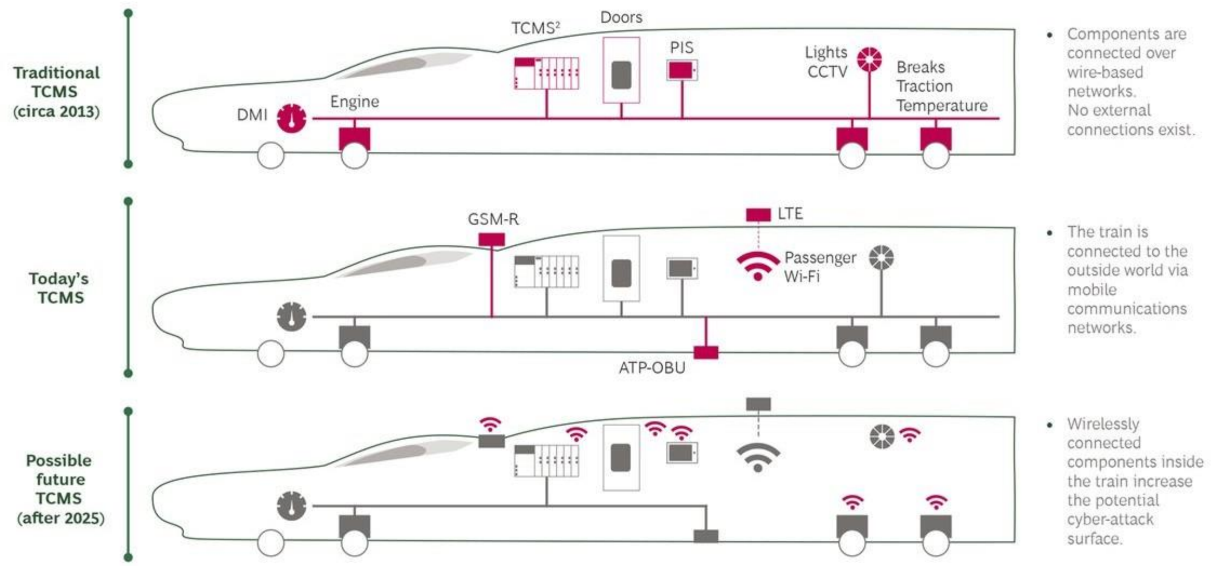
Exhibit 2 - Cargo Ships Are Increasingly Connected To Communications Systems That Leave Them Vulnerable


Satellite
Vessel
Equipment management repair vendors
Terminal
Office
IT bridge systems
Radar equipment
Positioning systems (GPS)
Voyage data recorders (VDRs)
Electronic Display Information System (ECDIS)
Automatic Identification System (AIS)
Communication systems
Integrated communication systems
Radio frequency (RF) communication
Wireless networks (WLANS)
Satellite communication
Voice over Internet Protocol
Cargo systems
Water ingress alarm
Level indication
Closed-circuit television (CCTV) network
On-board loading computers
Container-sensing systems
Operational tech systems
Power management
Engine governor
Emergency response

Source: BCG analysis.

Similarly, in the rail industry, traditional wire-based train control and management systems (TCMS), had only limited communication with external systems are giving way to wireless standards like GSM-Railway, a relatively broad network linking trains to railway regulation control centers. (See Exhibit 3.) As is the case for all mobility providers these days, T&L companies use vehicle infotainment services and other equipment that add another layer of internet-connected communications.

Exhibit 3 - Wireless Network Connectivity Is Making Railroads Easy Targets for Hackers



- Components are connected over wire-based networks. No external connections exist.

- The train is connected to the outside world via mobile communications networks.

- Wirelessly connected components inside the train increase the potential cyber-attack surface.

Source: BCG analysis.

Note: DMI = driver machine interface; TCMS = train control and management system; PIS = passenger information system; GSM-R = Global System of Mobile Communications-Railway; LTE = Long-Term Evolution; ATP = automatic train protection; OBU = on-board unit

While these proliferating networks—which essentially link OT systems with internal IT equipment, such as servers, PCs, and mobile devices—are by default new pathways for hackers, they are sometimes made even more vulnerable by the lack of urgency shown toward cyber attacks by OT vendors and T&L companies alike. In some cases, OT vendors require potentially vulnerable management interfaces to be built into their equipment for remote access, control, and troubleshooting. Further, computing landscapes at T&L companies are rarely modernized to be compatible with strict security protocols.

Equally alarming, beyond their relationships with individual OT vendors, T&L companies are establishing more efficient and technologically driven partnerships with their suppliers and distributors, which are increasingly dependent on network links. Cybersecurity protocols maintained by these partners are generally not policed, leaving T&L companies in the dark about whether their integrated ecosystems are a growing risk.

Regulation. Although the commercial and operational aspects of the transportation and logistics industry are regulated in many regions, there are a relatively small number of rules covering cybersecurity. Despite the sector's global operations—or perhaps because of them—regulators have had a hard time agreeing or focusing on a set of cybersecurity standards that T&L companies should follow wherever they operate. Given this vacuum, cybersecurity investments are not optimized to reduce organizations' overall risk exposure.

However, mindful of the possible perilous impact on global trade and economic stability of a widespread cyber attack on the T&L industry, regulators are beginning to take a more proactive stance in demanding better security protections for company networks. Among the regulations proposed or already established are the EU's Network and Information Security (NIS) directive and the soon-to-be-implemented CLC/TS 50701 and EN 50126 standards for railroads, as well as a series of rules for ships promulgated by the International Maritime Organization. By varying degrees, these regulations attempt to enforce minimum standards to protect companies' most sensitive data and operations, in particular customer records and shipping information.

People and Processes. Cyber threats continuously evolve, but the common thread for some of the most vulnerable areas is people. For example, employees who are unable to identify a phishing email could allow for easy initial exploitation for hackers. Indeed, self-inflicted openings are usually the first step of an attack chain, given that well over half of cyber breaches can be traced directly to flaws in organizational processes and employee capabilities or their lack of knowledge about cyber attacks.

Making matters worse is a large and growing global talent deficit of cyber protection specialists. As many as 4 million cyber specialist jobs were unfilled in 2020, according to the information security trade group ISC2. The shortfall in highly trained cyber staffers stems, in part, from the fact that academic cybersecurity degrees are a relatively new phenomenon that have been in existence only for the past ten years or so.

In our experience, this shortage is acutely felt in the industry—particularly in the Asia-Pacific region—as students graduating with cybersecurity credentials and experienced experts already in the workforce generally do not consider travel and logistics to be a primary career option. Perception is part of the problem. Most job candidates do not view T&L companies as innovative workplaces where technologically minded people can spread their creative wings in areas such as robotics and automation, data analytics, blockchain, autonomous vehicles, and the like. Rather than make a cybersecurity job more attractive—perhaps by offering better wages and benefits as well as encouraging innovation—many T&L companies treat cybersecurity as a cost center that must meet stringent resource budgets.

HOW TO ADDRESS CYBERSECURITY RISKS

T&L companies should begin to drive a cybersecurity agenda by assessing the level of cyber protections in their OT and IT equipment and programs. From there, they can set up safeguards in the most critical and vulnerable applications and networks. Mapping exposure to cyber attacks and identifying a portfolio of protective initiatives can be facilitated using models and tools, such as a cyber risk management and quantification program. Companies should sort their vulnerabilities via a risk-based approach that gives priority to the probability and impact of security threats on critical assets. They can then rank projects based on each's ability to improve resiliency relative to its cost, and, in doing so, effectively optimize their cybersecurity investment budgets.

After taking these precautionary measures, T&L companies should focus on adopting more complex cyber protection concepts, such as zero-trust architecture. This methodology assumes that every device, user, or application attempting to interact with the network is a potential threat. A zero-trust strategy can be implemented by segmenting and segregating networks using DMZ (demilitarized zone) technology, which provides a tightly controlled environment that monitors connections in and out of the organization. The same principle should also be adopted to tighten internal processes where possible, including verifying the identity of users, programs, and endpoint devices before allowing access to information or assets.

T&L companies can take three steps to improve their internal cyber-protection skills.

First, transform the company culture from one that downplays cybersecurity to one that recognizes the urgent need to fight threats. In every department, the notion of reinforcing cybersecurity across the organization should be an open and critical subject. Frequent cybersecurity-awareness training sessions can be a huge help in establishing a risk-aware workforce. Actions that individuals can take to protect against hackers, such as safeguarding passwords and being alert to suspicious activity on the company's networks, must be emphasized.

Second, use this strengthened focus on cyber-risk management to recruit cybersecurity professionals from universities and the private sector. Publicize that the organization's goal is to be a proactive leader in the cybersecurity arena. Companies can attract the best cybersecurity professionals by letting them know they will have the opportunity to build cyber-protection programs from the ground up, using the latest technology and replacing old legacy systems. Similarly, organizations can consider seeking advisory services from unbiased vendors that are not looking to pitch a technology.

Finally, identify the people in the company's technology workforce who are eager to become involved in cybersecurity initiatives and who have demonstrated basic abilities that indicate they are good candidates. Upskilling these workers—and offering them compensation- and title-based incentives for mastering the required capabilities—could enable T&L companies to quickly fill at least a portion of their cybersecurity-workforce needs.

For many T&L companies, the activities required to address cybersecurity risks may seem overwhelming, but one practical solution to increase the transparency and awareness of IT and OT networks and their vulnerabilities would be to create a cyber fusion center. This center would monitor, manage, and oversee cybersecurity governance, operations, analytics, processes, and technology, ensuring that data and intelligence are shared among key players to detect and thwart cyber threats.

In addition, a cyber fusion center would streamline operations by integrating the currently segregated IT and OT cyber management and controls under one roof. The center should meld the expertise of both IT and OT professionals to monitor for any anomalous activities either on the internet or internally—or, importantly, at the convergence of the two functions—which could be early warnings of a cyberattack.

To effectively manage risk, T&L companies should build layers of cyber resilience that uphold stringent standards, protect partner supply chains, and adopt risk-based approaches when designing security controls. Companies need the tools to ensure their organizations develop and maintain appropriate cyber-resilience measures that span dimensions—from technology to regulations and from processes to people.

--

For many T&L companies, proactive cybersecurity policies have not been a priority. But the rapidly growing number of cyber attacks and new regulations are beginning to convince firms that they cannot maintain a relatively hands-off approach for much longer. Hackers are getting more aggressive and keenly aware of which companies are giving cybersecurity short shrift. That’s a list that T&L companies should not aspire to be on.