Cyber Insurance Landscape

Trends by Industry

White paper 2022
Tokio Marine HCC International Cyber team

TOKIO MARINE HCC

tmhcc.com

Executive Summary

About this White Paper

In this white paper, we focus on three industries: Financial Institutions, Manufacturing and Transportation. In the last three years, these industries have featured among the top 10 targeted by cyber threat actors. Put together, they represented 72% of our book of business at Tokio Marine HCC (TMHCC) International at the end of 2021. Needless to say, we have a deep understanding of these industries, their different segments (revenue size) and how they need to operate in different locations.

Understanding that every industry sector is different – be it due to its purpose, features, approach, or process – is key. Within an industry sector there are several sub-industry sectors and each company within that is different, and therefore, should be assessed on its own merit. That said, for the purpose of this white paper, we have generalised and conflated some information where it helped outline concepts, making this an easier read.

Throughout the paper, we give our readers a quick description of the most common business model used in each industry, along with some indications about how it has evolved in the past or will evolve in the near future. To be pragmatic, we have developed an easy-to-grasp traffic light system that highlights both exposure and readiness "at a glance", and we provide concrete examples where possible.

Also, as brokers and insureds often ask us how we make the link between an "industry business model" and our "underwriting questions", we have included an overview of some of our underwriting considerations; and pushing that connection even further, we highlight some potentially useful coverages.

Lastly, we have added more detail on technical information in a concise roundup at the end of each section of this paper in an "interesting reading" section.

Our Data:

The examples and details we share and describe in this paper are based on the data and results of our close industry monitoring approach, which began in 2016 when the TMHCC International Cyber team was formed. We have always believed that underwriting should be detailed, tailor-made and company-specific.

Over the years, from the many cyber opportunities we see worldwide, we have fed our database with information and categorised it by industry sector. In fact, our international operations have a unique set-up that lends itself to this, as the TMHCC International Cyber team is supervised and mainly run out of our Barcelona (Spain) office, where all this information is centralised and compiled. We have also developed an in-house Cyber threat intelligence tool that assists with this reporting.

All in all, this exercise allows us to extract trends per industry, proactively discuss technical topics with our clients and, ultimately, to make more accurate and tailored underwriting decisions.

Authors

This white paper is a collaborative effort, produced and written by the TMHCC International Cyber Security Leader, Isaac Guasch, with the help of all our International Cyber underwriters, our Cyber Industry Champions and our multiline industry specialists. We hope you enjoy reading and discovering what our group of experts have put together for you.

Cyber Threat Intelligence (CTI)

CTI is a cybersecurity field focused on the usage of information related to threats, vulnerabilities, events, actors that can help in mitigating harmful events. CTI sources might include open-source intelligence (OSINT), social media and human intelligence, technical information from corporate assets (SIEM, IDS, etc), and more.

Cyber threats are evolving fast, and companies are finding it hard to keep up in their efforts to protect their assets. So, the only way to close this gap is by creating the concept of a cyber community and promoting information sharing, so we can all learn from each other.

At TMHCC International, we have created a Cyber Threat Intelligence (CTI) tool that allows our underwriters to maintain direct access to live cyber information such as threats, vulnerabilities, and techniques, in order to ensure that they assess cyber risks efficiently. With this tool they will be able to build and maintain proactive communications with their clients about cyber trends, while speaking the same language as the CISOs.

Industry overview

Manufacturing is where raw materials are transformed into finished products. The 19th century industrial revolution led to the mechanisation of the manufacturing process, which has been changing and evolving continuously ever since.

Previously, manufacturing companies were connected within one network with limited internet exposure. However, today, we have a technology-driven sector that relies on the application of advanced technologies and services.

Operational Technology (OT) and the Internet of Things (IoT) are now business essential for manufacturers. Yet, from a risk perspective, the exposure and impact of these technologies are underestimated. This is largely because companies focus more on the Information Technology (IT) risks than on the potential vulnerabilities of their business-critical systems, of which OT and IoT represent a significant proportion.

With a high number of interconnected systems in a manufacturing company, the attack surface and risk of a potential cyber incident is also high. So, to avoid production collapsing, special OT security should be made a priority. The same OT is usually used for many years in this industry, making it challenging for companies to keep up with the changing attack surface and secure their systems in line with the attack environment of that time.

Contrary to what was thought in the past and at a time when the amount of information at the disposal of attackers was only really taken into account when large corporations were hit hard, the manufacturing industry is attractive to threat actors.

In fact, current activity shows that the usual Information Security measures taken are not enough to protect a manufacturer from a cyber-attack. Incidents at companies such as Norsk Hydro, Nissan and Merck show that a cyber-attack can have a huge impact on this industry.

According to research by ENISA, 33% of confirmed supply chain attacks were reported in 2020 and 66% were reported from January 2021 to early July 2021. Based on this data, the trend forecasts that 2021 may have four times more supply chain attacks than 2020.

Industry evolution/challenges

We have witnessed and worked through Industry 1.0, 2.0, 3.0 and are currently heading towards Industry 4.0. When talking about Industry 4.0, many people see huge potential for companies, including the manufacturing sector. Besides increasing efficiency, flexibility, distribution and quality, there will be new products, services and data-based business models that are created along the value chain. But the usage of new technologies and the increased interconnection in factories, buildings, sites and products also bring new risks that must be managed in new ways.

Industry 4.0 stands for digitalisation and interconnection of the industrial value creation. The real and virtual worlds are merging as technology continues to advance. The vision of self-controlled and adaptive factories is becoming more and more attractive, with a 45% increase in efficiency in smart factories. This is the dawn of the fourth industrial revolution. In the context of global competition, this revolution comes with higher service levels, increased quality, increasing productivity and decreasing maintenance and logistics costs, as well as shorter and more efficient development processes.

Industry exposure & readiness

Exposure

The manufacturing industry is often more exposed to failures in availability than to failures to do with information confidentiality. However, this does not exempt companies from suffering a security breach, since intellectual property (manufacturing processes, designs, etc.) is also a risk factor.

The fact that, historically, it is a less regulated sector and that, in recent years, it has adopted technology as an added-value factor makes it one of the sectors with the lowest level of maturity in terms of cyber management.

From a technical point of view, the large number of obsolete systems and OT systems predicts there will be great complexity in managing updates and patching. In the IoT environment, the limited resources that some devices have (memory, disk space, computing, etc), are pushing companies to use cloud-computing solutions to gather and process all the data coming from beacons and sensors, exposing them to new threats.

At a business-continuity level, the relocation of manufacturing plants makes it more difficult to test continuity and disaster recovery plans.

> "Due to the limited resources of some IoT devices, the usage of cloud-computing solutions has increased drastically in the manufacturing industry."
>
> Isaac's corner

	DB* Exposure	BI* Exposure
Manufacturing	🟢	🔴

Readiness

Due to the low maturity of the sector and the fact that operations are usually spread across multiple locations, the governance of information security is one of the weakest points of many companies in this sector, as is the commonly limited detection capacity in the different IT, OT and IoT environments.

An example is the still few Security Operation Centres (SOCs) that have full visibility of industrial environments and the same intervention capabilities in the event of an incident.

	Identify	Protect	Detect	Respond	Recover
Manufacturing	🔴	🟡	🔴	🟡	🟡

* DB - Data Breach / BI - Business Interruption

Industry incidents/claims

Unfortunately, the manufacturing industry has several examples of cyber incidents. Here are two that clearly represent this growing trend in the sector.

The first one comes from the motorcycle manufacturer Honda, which suffered a ransomware attack in mid-2020. This attack stands out as it was performed by a variant called Snake Ransomware, also known as EKANS or Snakehorse. This snake ransomware is written in a specific programming language called Golang, containing a type of obfuscation not typically seen in this type of malware.

The programme removes shadow copies and kills the processes related to SCADA and industrial control devices, which are the main systems in the OT environment – essential in the manufacturing sector. In addition, the malware also kills processes related to machines, remote management tools, network management software and more. After this, the software encrypts the files on the devices but skips the Windows system folders and files, making it very difficult to detect. This incident shows that ransomware can be tailored to attack specific industries.

The second example involves the airplane manufacturer Bombardier. In February 2021, data from the company was posted on a ransomware leak site. The company confirmed that the attacker had revealed personal and other confidential information relating to employees, customers and suppliers, as well as some confidential design documents for various airplanes and plane parts. In this case, the forensic analysis concluded that a breach was produced by exploiting a vulnerability affecting a third-party file transfer application.

This incident illustrates that the manufacturing industry is not only susceptible to business interruption exposure but also to data breaches.

Insurance benefits/response

The insurance industry should focus on determining if the following aspects are well covered by companies:

- Management and government model: Check whether, despite multiple locations, a global security model is available and how its implementation is ensured at a local level.
- Segmentation of the different environments and networks - IT, OT and IoT: Each of these environments should be totally isolated from the rest and each environment, in turn, should have a level of segregation that allows compartmentalisation to prevent a possible spread of ransomware or any attack.
- The ability to detect anomalies in OT environments: Although the level of monitoring of IT systems is usually high, there is still a large gap in EDR, SIEM, SCADA, etc. systems that allow real-time information on events and threats in industrial systems.
- Updating systems and vulnerability management: Check how companies manage the replacement of their legacy systems and what compensatory measures they implement during the transition.
- Testing the business continuity plan: Check how companies test the plans of the different factories and their ability to transfer their production between different locations.

Other sources / Interesting reading

In February 2022, the Cloud Security Alliance (CSA) published the "Cybersecurity Best Practices for the Manufacturing Industry". The document contains a historical background of the evolution from Industry 1.0 through to Industry 4.0, a compilation of available frameworks that can be adopted to secure the manufacturing sector, and a top 10 list of practical steps that can be taken to secure manufacturing systems from cyber threats as well as a look to the future.

https://cloudsecurityalliance.org/artifacts/manufacturing-industry-cybersecurity-challenges/

In May 2015, the U.S. National Institute of Standards and Technology (NIST) released Special Publication 800-82 Revision 2, "Guide to Industrial Control Systems (ICS) Security". It provides specific guidance for establishing secure industrial control systems (Stouffer, et al. 2015). Included are references to other NIST Special Publication documents that provide guidance and resources to the ICS industry.

https://www.nist.gov/publications/guide-industrial-control-systems-ics-security?pub_id=918368

In addition, NIST is set to release the third review of SP 800-82 "Guide to Operational Technology (OT) Security" which will provide an overview of OT and typical system topologies, identify typical threats to organisational mission and business functions supported by OT, describe typical vulnerabilities in OT, and recommend security safeguards and countermeasures to manage the associated risks.

https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft

In October 2020, NIST announced the publication of NISTIR 8183 Revision 1, "Cybersecurity Framework Manufacturing Profile". The framework is a roadmap for reducing cybersecurity risk for manufacturers. It is aligned with best practices, and intended to enhance current cybersecurity standards (Stouffer et al. 2020). The profile uses the five functions of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover) as a starting point for defining the risk levels of Low, Moderate, and High (NIST, 2020).

https://www.nist.gov/publications/cybersecurity-framework-version-11-manufacturing-profile

In May 2019, the European Union Agency for Cybersecurity (ENISA) published its "Industry 4.0 – Cybersecurity challenges and Recommendations" paper. ENISA lists high-level recommendations to different stakeholder groups to promote Industry 4.0 cybersecurity and facilitate wider take-up of relevant innovations in a secure manner.

https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

Industry overview

The financial sector has a highly mature cybersecurity position mainly due to the large number of regulations and compliance requirements that must be followed.

However, the ongoing digitalisation of supply chains and ecosystems is creating new cyber risks for the sector.

Although it usually commits large amounts of monetary resources to cybersecurity, the financial services sector faces significant challenges such as GDPR fines, a constant threat from State actors, potential compliance violations, M&A activities and system migrations, and contingent business interruption due to the interconnected nature of its operations.

The business model, and the cyber risks inherent in the financial sector, make cross-sector collaboration at a global level a key requirement.

There are several initiatives within the financial sector that are specifically geared towards fighting cybercrime. For instance, there is the Financial Services Information Sharing and Analysis Centre (FS-ISAC), which promotes information sharing about cyber threats across the financial sector to minimise the risk and impact of active threats. In addition, there is the European Financial Services Roundtable (EFR), which brings together executives from leading European banks and insurance companies to fight against cybercrime.

Threat intelligence tools, dark web monitoring and threat actor tracking will also help the industry to prevent and actively anticipate potential attacks. Furthermore, sophisticated tools for underwriting processes such as critical vulnerabilities detection, data breach exposures on the dark web, open ports or expired certificates are also new services that insurance companies are offering to clients.

The average cost of a data breach in the financial sector in 2021 was $5.72 million, according to IBM Data Breach report.

In 2020, the average time it took until identification was 117 days and the average time to contain a breach in this industry was 56 days; that is 233 days in total.

Industry evolution/challenges

Many financial institutions and FinTech firms are now offering new services and technologies such as open banking, blockchain, cryptocurrencies and payments using telephone number information only (e.g. European Bizum transfers), to name a few.

Open banking aims to give consumers more control over their financial data and creates new opportunities for those in the financial industry to innovate and provide new services for their customers.

However, cyber-attacks on open banking and APIs (Application Programming Interfaces) are also on the rise due to the complexity of the network architecture and an increase in vulnerabilities.

Supply chain attacks are probably one of the biggest risks for retail and commercial banks. Therefore, it is very important to be able to clearly trace all Outsourced Service Providers (OSPs) and to test the resilience of the supply chain. Network architectures are increasingly complex, so it is important to identify single points of failure and high dependency links.

Ransomware protocols must be linked to the readiness and responsiveness of the bank, where business continuity plans should be continuously reviewed and monitored.

Cyber risk awareness and training should be provided not only to all employees but also to internal and external users, providers, and clients.

There are systemic and extreme risks which require collaboration within the sector if the challenges of cyber are to be adequately met. The full ecosystem - including suppliers, governments, regulators, and insurers - has to work together to provide strong monitoring and a robust response to the systemic risk.

"More M&A activities in the banking sector are expected in the upcoming years, which will imply more systemic risks."

Isaac's corner

Industry exposure & readiness

Exposure

The financial sector, in general, is highly exposed to cybersecurity risks. The large volume of sensitive data that it processes, its high activity in M&A processes, and the large migrations of information systems and databases that these processes entail, contribute to the high potential risk. In addition, in the banking sector, the large volume of transactions executed by their systems and the high levels of availability of the systems needed for this, mean that the likelihood of business interruption (BI) is comparable to that of a data breach (DB).

	DB Exposure	BI Exposure
Banking	🔴	🔴
Insurance	🔴	🟡
Other	🟡	🟢

Readiness

Despite the high exposure, or perhaps due to it, companies in the financial industry have a highly mature approach to cybersecurity.

The high monitoring and response capabilities of the banking sector make it stand out from other sectors of financial services. Although insurance companies have dedicated equipment and solutions to detect and contain cyber-attacks, they have a smaller proportion of employees dedicated to preventing a cyber-attack compared to a bank. This gap is even larger if we look at private equity firms, FinTechs, or other small companies in this sector.

	Identify	Protect	Detect	Respond	Recover
Banking	🟢	🟢	🟢	🟢	🟢
Insurance	🟢	🟢	🟡	🟡	🟡
Other	🔴	🟡	🟡	🟡	🟡

Industry incidents/claims

While cyber-attacks often originate from outside the organisation, malicious employees can also pose a significant risk.

In one case, a member of a bank's staff extracted very sensitive data from the datacentre – millions of records of members and former members. This individual did not have authorised access to the data himself – he had persuaded three other employees with the relevant rights to access it. The data was downloaded from his computer to USBs on several occasions over the course of a year, and the rogue employee subsequently distributed the data to third parties in return for a relatively small sum of money.

This incident is not an isolated case, but it could have been avoided, not only by having a stricter USB policy with limitations on downloads, but also by incorporating behavioural detection capabilities, to analyse the behaviour of the employees.

These behavioural alerts in the monitoring systems are essential to mitigate not only the threats of a discontented employee but also external threats. Indicators such as the amount of data being transferred, location and time zone of the user, as well as user experience are becoming critical to detect and block these threats.

Insurance benefits/response

There are several factors that must be considered when analysing the risk of a company in the financial sector. Some of the most common ones are:

- Data segmentation and segmentation of OT (ATM) networks: With data breach being one of the greatest exposures, knowing if data is compartmentalised in different instances can help mitigate the risk of data leakage. Likewise, an ATM environment that is totally isolated from the rest of the environments will facilitate containment in the event of an incident.
- Third-party management: This is another fundamental element. Understanding whether there is governance of the different suppliers, an approval process and dependency analysis is very important.
- M&A procedure: Make sure a defined M&A procedure that includes security requirements in all phases of the technological migration process and the new security risk management model is in place.
- Monitoring and response: Determine the scope and capacity of incident monitoring and response that the company's teams can offer, especially those in the "other" sub-sector.
- Interconnectivity with third parties: Understand the processes of interconnection with third parties such as FinTech, IT providers, etc, from a regulatory (PSD2, GDPR, PCI, etc) and technological point of view.

Specific coverages for the industry

The payment card industry has attracted fines of up to $500,000 per incident for security breaches where merchants are not PCI compliant. So, it is vital that the PCI regulatory framework is followed in order to satisfy any of the four levels of compliance.

Affirmative and non-affirmative cyber risk exposures (also called silent cyber) are a hot topic. The difficulty of quantifying and assessing some specific risks is a challenge for the industry. The interaction of the cyber policy with other policies such as the crime policy, professional indemnity, D&O, or property damage policies is not always clear when a cyber incident occurs. Therefore, it is very important for insurers to be as transparent as possible, by having clear coverage and explicit exclusions in their policies. It is the industry's role to provide this clarity and align expectations on cyber insurance coverage, so as to avoid the potential for coverage disputes and costly litigation.

Additionally, it is also possible to offer policies that combine different lines of business, such as cyber plus crime, with separate or combined limits. Other policies such as tech/PI are also on the rise for companies where technology is involved.

Other sources / Interesting reading

In December 2012, the International Organization for Standardization (ISO) published the ISO/IEC TR 27015:2012 "Information technology — Security techniques — Information security management guidelines for financial services". The standard provides information security guidance in addition to information security controls defined in ISO/IEC 27002:2005 for initiating, implementing, maintaining, and improving information security within organisations providing financial services.

https://www.iso.org/standard/43755.html

In March 2021, the European Union Agency for Cybersecurity (ENISA) released "EU Cybersecurity Initiatives in the Finance Sector", as a brief document to outline European cybersecurity initiatives in the sector and a first depiction of the complex landscape of initiatives relating to cybersecurity at an EU level.

https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector

In January 2017, ENISA published a paper named "Distributed Ledger Technology & Cybersecurity – Improving information security in the financial sector". This paper aims to provide financial professionals in both business and technology roles with an assessment of the various benefits and challenges that their institutions may encounter when implementing a distributed ledger.

https://www.enisa.europa.eu/publications/blockchain-security

Industry overview

The Transport and Logistics (T&L) industry consists of three main components: hard infrastructure (including network infrastructure and components), vehicles and operation components. The sector is usually defined by four primary types of transportation infrastructure:

- **Aviation:** aircraft, air-traffic control systems, commercial airports, and additional air transportation facilities for movement of people and cargo.
- **Rail and transit (usually only local and national):** buses, subways, trolleys, systems that support passenger and cargo transport, and telematics for improved maintenance of railroads.
- **Marine:** ports, ships and control systems, mobile connectivity for package tracking.
- **Roads:** technologies collecting and transmitting data, satellite navigation information, connected traffic systems to optimise traffic flows, plate recognition systems, status of road transport, autonomous vehicles, e-scooters, drones, etc.

The T&L industry is exposed to cyber risks as it depends on information systems to manage the flow of vehicles and goods and to control traffic. These systems are also vital to the management, identification and tracking of passengers and cargo.

As cyber technology becomes more sophisticated, the threats from attacks are moving from data breaches to interrupting critical infrastructure and exposing transport operators to economic and reputational damage. Beyond critical infrastructure and essential services, T&L is one of the core elements of our society and economy. Many of the infrastructures (sea, air, road, ports and traffic management) are public companies managed by states.

Transport networks have become increasingly digital, with a wide range of data flowing across systems, tracking and monitoring both digital and physical networks. As more devices and control systems are connected online, more vulnerabilities will appear, increasing the potential for disruption to physical assets. This emphasises the absolute necessity of patches - including patching boarding systems and sending software updates Over the Air (OTA) - and firmware agility. However, ensuring human involvement is also crucial in managing the complexity of infrastructures and outdated systems.

Data indicates that the annual number of cyber incidents and associated costs are on the rise for the T&L industry. The most common incidents involve data breach, while incidents involving unintentional data disclosure have the highest average loss per incident.

Between 2019 and 2020, there was a 530% increase in cyber-attacks reported to Eurocontrol. There were 775 cyber-attacks on airlines in 2020 and 150 at airports.

Industry evolution/challenges

The T&L industry has been through an important digitalisation process, a process that continues to this day, including warehouse robotisation, high speed rail, last mile optimisation, predictive maintenance, and drone supervision, to name a few.

In the **aviation** industry, technical advances in navigation systems and airframe design have reduced the chances of an accident. However, the increasing reliance on computers also creates new kinds of threats. As aircrafts are becoming more digitalised, e-enabled, and automation increases, pilot practices and training will need to adapt in the event of system failure or security breach.

As well as being at risk of theft of customer or company data, **airlines** are also at risk of having their communications and connectivity systems compromised. This includes airlines, manufacturers, maintenance providers, air-traffic controllers, airports and third-party suppliers.

The **marine** transportation industry is at risk of compromises to navigation systems, cargo control and other industrial processes, which threaten lives, the environment and property, as well as disrupt trade activity.

Cyber-attacks on this sub-sector can affect seaport operations, control of temperature for refrigerated containers and emergency systems, port operations, such as raising a drawbridge, controlling traffic lights, scheduling trucks, and controlling pumps, valves and pipelines for delivery of fuel and liquid cargo to ships.

The **rail** industry provides critical national infrastructure and, as such, may be targeted by political groups intending to cause disruption, in addition to amateur hackers and organised criminals. As the rail industry adapts and becomes increasingly dependent on electronic sensors and network technologies, new vulnerabilities to physical networks are increasing.

Within the **rail** industry there is the risk of compromises to signalling controls, network power supply, signalling infrastructure, report on the condition of the rolling stock and associated infrastructure, support operational planning and timetabling.

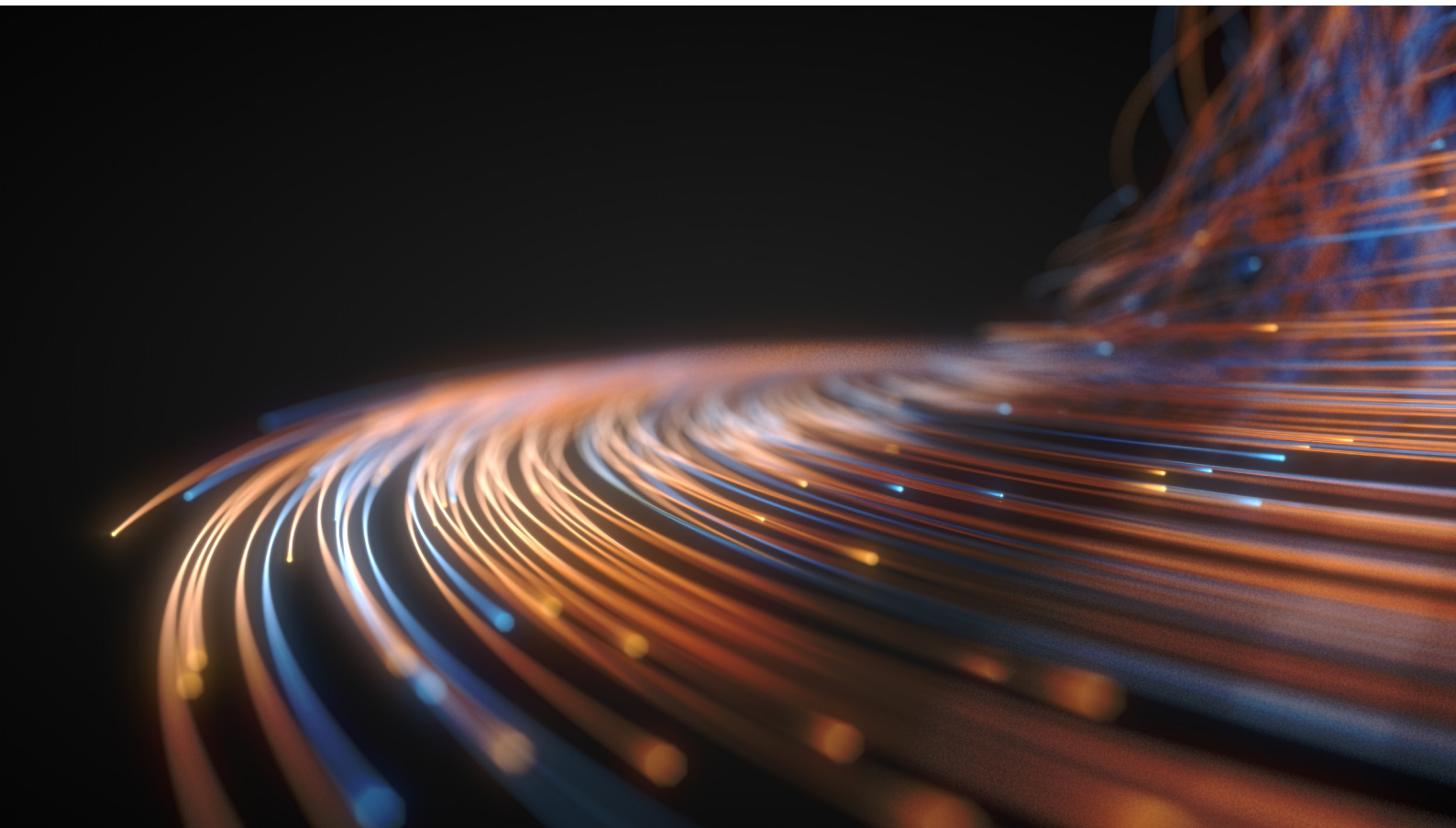
There are two factors that increase T&L cyber risk: the increasing control of computer systems and the increasing networking of computers with each other and the internet. By connecting traditional IT systems with unconnected OT systems and expanding connected endpoints via IoT, the level of security risk that the industry is facing increases exponentially.

The traditional IT perimeter has changed to IT + OT + smart products + services across supply chains.

The problem is that security products are mainly focused on traditional IT and not on OT. The dangerous combination of new, poorly secured IoT devices, and old, poorly updated OT systems that exist in many companies is that they present a good opportunity for hackers to carry out attacks.

"One of the main risks is that safety does not integrate security, and cyber security is generally not well integrated in transportation operations."

Isaac's corner



Industry exposure & readiness

Exposure

The transport sector, especially where passengers are involved, is regulated. Although it does not reach the levels of the financial sector, there are many regulations and safety standards. In recent years, there have been several cybersecurity guides and standards made available too.

The main risk vector for this industry is business interruption (BI). However, it is also an industry that processes large volumes of data, leaving it exposed to data breaches (DB).

In line with the manufacturing sector, transportation has a high component of OT and obsolete systems, and great difficulties in updating them.

Due to the nature of the type of transport undertaken in the marine sector, it is challenging to detect and monitor cyber threats in real time. Finally, the high dependence on the human factor due to semi-manual processes exposes the industry to this type of risk.

	DB Exposure	BI Exposure
Aviation		
Marine		
Rail		
Road		

Readiness

The preparedness of this industry is usually medium to high. People security has always been high on the agenda, which has resulted in a high level of training over the years, not only for the protection of people but also for the protection of information systems that support their operations.

In the case of the maritime sector, a notable drop in the capacity, detection and response to incidents has been observed. The road sub-sector, in general, has a lower capacity level than the other sub-sectors, although it is true that it is less exposed to business interruption (BI) and data breach (DB) risks.

	Identify	Protect	Detect	Respond	Recover
Aviation					
Marine					
Rail					
Road					

Industry incidents/claims

One of the biggest supply chain incidents we have recently in the transportation industry took place in March 2021, affecting a company called SITA.

SITA is one of the largest aviation IT companies providing IT and telecoms services to around 2500+ clients and it is present in 1000+ airports, claiming to serve around 90% of international destinations.

They suffered a data security incident involving passenger data stored on SITA's Passenger Service System servers. These systems are used by airlines for passenger processing purposes, such as boarding, as well as for passenger flow management at airports.

Consequently, multiple airlines were affected simultaneously, and customer data was exposed. Although SITA did not confirm the volume of the data leak, according to their website, one billion passengers per year use SITA boarding services, so the potential impact is extremely high.

Another relevant incident from late 2020 was a global phishing campaign targeting the Covid-19 vaccine cold chain. The cold chain is a component of the vaccine supply chain that ensures the safe preservation of vaccines in temperature-controlled environments during their storage and transportation.

In this case, the phishing emails contained malicious HTML attachments that open locally, prompting recipients to enter their credentials to view the file. This phishing technique helps attackers avoid setting up phishing pages online that can be discovered and taken down by security research teams and law enforcement.

IBM assessed that the purpose of this campaign may have been to harvest credentials to gain future unauthorised access. From there, the adversary could gain insight into internal communications, as well as the process, methods and plans to distribute a Covid-19 vaccine.

Insurance benefits/response

When analysing a company in the transportation industry, some points of special relevance can be identified:

- Segmentation of IT/OT networks: Especially between companies, the public infrastructure they use (airports, ports, stations, etc.) and their means of transport (planes, trains, ships, etc.) is critical.
- Data segmentation: In a sector with high volumes of data, this is also a determining factor.
- The update and management of vulnerabilities: Check how companies manage the replacement of their legacy systems and what compensatory measures they implement during the transition.
- Training and education: The assessment of training and education for all employees and third parties is critical given the importance of the human factor in cyber risks.
- Scenarios: Having several business continuity scenarios, and especially scenarios that consider cybersecurity risk and its relationship with safety, as well as scenarios that assess dependency and third-party risks, is of vital importance.

Other sources / Interesting reading

In December 2021, the International Air Transport Association (IATA) released the 3rd edition of their "Compilation of Cyber Security Regulations, Standards & Guidance Applicable to Civil Aviation" paper.

https://www.iata.org/en/programs/security/cyber-security/

In November 2021, the European Union Agency for Cybersecurity (ENISA) published the "Railway Cybersecurity – Good Practices in Cyber Risk Management" whitepaper. It offers a guide for railway undertakings and infrastructure managers to select, combine or adjust cyber risk management methods to the needs of their organisation. It builds upon the 2020 ENISA report on cybersecurity in the railway sector (ENISA, 2020), which assessed the level of implementation of cybersecurity measures in the railway sector.

https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management

In December 2016, ENISA created the "Securing Smart Airports" whitepaper. The objective of this study is to improve the security and resilience of smart airports, including air-traffic management for what is relevant to the functioning of smart airports. This is to prevent disruption to smart components that could have an impact on the service to, and safety of, passengers, while also promoting cost benefits and protecting the environment.

https://www.enisa.europa.eu/publications/securing-smart-airports

In December 2017, ENISA released their report "Mapping of OES Security Requirements to Specific Sectors". The aim of the report is to provide a substantial and comprehensive mapping between the security measures for Operators of Essential Services (OES) described in the NIS Directive, and sector-specific information-security standards. The analysed sectors include air transportation, rail transportation, water transportation and road transportation among others.

https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors

In May 2016, the U.S. National Institute of Standards and Technology (NIST) published the paper "Performance Evaluation of Secure Industrial Control System Design: A Railway Control System Case Study". This case study focuses on Railway Control Systems (RCS), an important and potentially vulnerable class of Industrial Control System (ICS), and presents a simulation integration platform that enables (a) Modelling and simulation including realistic models of cyber and physical components and their interactions, as well as operational scenarios that can be used for evaluations of cybersecurity risks and mitigation measures and (b) Evaluation of performance impact and security assessment of mitigation mechanisms focusing on authentication mechanisms and firewalls.

https://csrc.nist.gov/publications/detail/conference-paper/2016/04/05/performance-eval-of-secure-ics-design-railway-control-system

Sources

National Cyber Security Agencies (websites):

- European Union Agency for Cybersecurity - ENISA [online] [accessed: 01 February 2021]
  Available at: https://www.enisa.europa.eu/
- Cybersecurity and Infrastructure Security Agency - CISA [online] [accessed: 01 February 2021]
  Available at: https://www.cisa.gov/
- National Cyber Security Centre - NCSC [online] [accessed: 01 February 2021]
  Available at: https://www.ncsc.gov.uk/
- Instituto Nacional de Ciberseguridad - INCIBE [online] [accessed: 01 February 2021]
  Available at: https://www.incibe.es/en
- CSIRT Italia [online] [accessed: 01 February 2021]
  Available at: https://csirt.gov.it/
- Agence Nationale de la Sécurité des Systèmes d'Information - ANSSI [online] [accessed: 01 February 2021]
  Available at: https://www.ssi.gouv.fr/en/

Technical Advisory/Research companies (websites):

- Gartner [online] [accessed: 01 February 2021] Available at: https://www.gartner.com/en
- Forrester [online] [accessed: 01 February 2021] Available at: https://go.forrester.com/
- ISACA [online] [accessed: 01 February 2021] Available at: https://www.isaca.org/
- IBM Research [online] [accessed: 01 February 2021] Available at: https://www.research.ibm.com/

Technical Journals:

- 1 Cost of a Data Breach Report 2020. Traverse City, USA: Ponemon Institute and IBM Security. 2020.
- 2 X-Force Threat Intelligence Index 2020. Armonk, USA: IBM Security. 2020.
- 3 Sectoral/thematic threat analysis. Attiki, Greece: ENISA. 2020-ISBN 978-92-9204-354-4

Financial Industry (web sites):

- European Banking Authority [online] [accessed: 01 February 2021]
  Available at: https://www.eba.europa.eu/
- European Insurance and Occupational Pensions Authority [online] [accessed: 01 February 2021]
  Available at: https://www.eiopa.europa.eu/
- Association of British Insurers [online] [accessed: 01 February 2021]
  Available at: https://www.abi.org.uk/
- National Association of Insurance Commissioners [online] [accessed: 01 February 2021]
  Available at: https://content.naic.org/

Transportation Industry:

- Cyber Startup Observatory [online] [accessed: May 2022]
  Available at: https://cyberstartupobservatory.com/aviation-cyber-threats/
- International Air Transport Association (IATA) [online] [accessed: May 2022]
  Available at: https://www.iata.org/en/programs/security/cyber-security/

Manufacturer Industry:

- Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, Revision 2. U.S. Department of Commerce. 2015.
- Cloud Security Alliance [online] [accessed: May 2022]
  Available at: https://cloudsecurityalliance.org/artifacts/manufacturing-industry-cybersecurity-challenges/

Author and collaborators

Isaac Guasch

Cyber Security Leader
International

iguasch@tmhcc.com

Isaac Guasch is Cyber Security Leader – International

Before joining Tokio Marine HCC, Isaac developed his career as an IT Risk and Cyber Security Manager. Since joining the company, he has spoken at various industry events, released several white papers and is well-known for his timely advice to brokers and clients on pertinent cyber security topics.

Isaac is a qualified Telecommunications Engineer, with a MSc in IT Management and a MSc in Emotional Intelligence and Executive Coaching, among other certifications. He speaks Spanish, Catalan, and English; and, in addition to his role at Tokio Marine HCC, Isaac teaches cyber security to university students.

Xavier Marguinaud

Head of Cyber
International

xmarguinaud@tmhcc.com

Gülsah Dagdelen

Cyber Underwriting Manager
EMEA & LatAm

gdagdelen@tmhcc.com

Arnaud Lapillonne

Cyber Senior Underwriter
Northern EMEA & Asia

alapillonne@tmhcc.com

Eduard Blanxart

Senior Underwriter
Financial Lines

eblanxart@tmhcc.com

Cyber at Tokio Marine HCC

We know... Cyber

Tokio Marine HCC has been innovating in Cyber Liability Insurance worldwide, for over 20 years. Our dedicated global team is made up of cyber insurance and in-house claims experts with deep industry knowledge and a wealth of cyber security experience. We promote active knowledge exchange, making us a global leader when it comes to cyber risk, while keeping you at the forefront of emerging threats on the ever-evolving Cyber landscape.

From offices in the U.S., our cyber team insures US-domiciled businesses, with a focus on the small- to mid-sized segment, as well as individuals concerned with protecting their family, home and privacy from cyber threats. From Europe and the U.K., our team concentrates on mid- to large-sized businesses domiciled anywhere outside of the U.S. In addition, we leverage our in-house Cyber expertise to enhance other Tokio Marine HCC insurance coverages, letting you take on risk with confidence.

Learn more about Cyber at Tokio Marine HCC by visiting tmhcc.com

Follow us on LinkedIn: #TMHCC_Cyber

Find out more about the Tokio Marine HCC International Cyber Security Insurance:

TMHCC Cyber Insurance

Email our Cyber Security Team

Contact Us

Barcelona
Tokio Marine Europe - Spanish Branch
Torre Diagonal Mar
Josep Pla 2, Planta 10
08019 Barcelona, Spain
Tel: +34 93 530 7300
Fax: +34 93 530 7301

London
HCC International
Fitzwilliam House, 10 St. Mary Axe
London EC3A 8BF, United Kingdom
Tel: +44 (0)20 7648 1300
Fax: +44 (0)20 7648 1301

Munich
Tokio Marine Europe - German Branch
Rindermarkt,16
80331 Munich
Germany
Tel: +49 89 3803 4640

#TMHCC_Cyber

A member of the Tokio Marine HCC group of companies

Tokio Marine HCC is a trading name of HCC International Insurance Company plc (HCCII), Tokio Marine Europe S.A. (TME) and HCC Underwriting Agency Ltd (HCCUA), members of the Tokio Marine HCC Group of Companies.

HCCII is authorised by the UK Prudential Regulation Authority and regulated by the UK Financial Conduct Authority and Prudential Regulation Authority (No. 202655). Registered with Companies House of England and Wales No. 01575839. Registered office at 1 Aldgate, London EC3N 1 RE, UK. TME is authorised by the Luxembourg Minister of Finance and regulated by the Commissariat aux Assurances (CAA); registered with the Registre de commerce et des sociétés, Luxembourg No. B221975 at 33, Rue Sainte Zithe, L-2763, Luxembourg; Operating through its Spanish Branch, domiciled at Torre Diagonal Mar, Josep Pla 2, planta 10, 08019 Barcelona, Spain, registered with the Registro de Entidades Aseguradoras de la Dirección General de Seguros y Fondos de Pensiones under the code E0236, VAT number in Spain ("N.I.F") W0186736-E, registered with the Registro Mercantil de Barcelona, at volume 46.667, page 30, sheet number B-527127, registration entry 1; and through its German Branch, domiciled at Berliner Allee 26, 40212 Düsseldorf, Germany, registered with the Handelsregister beim Amtsgericht Düsseldorf under the number HRB 84822, authorised by the Bundesanstalt für Finanzdienstleistungsaufsicht (Ba-Fin) under the number 5217. VAT ID No: DE320932530. We have authority to enter into contracts of insurance on behalf of the Lloyd's underwriting members of Lloyd's Syndicate 4141 which is managed by HCCUA.

The policyholder will always be informed of which insurer in our group will underwrite the policy according to jurisdiction.

Not all coverages or products may be available in all jurisdictions. The description of coverage in these pages is for information purposes only. Actual coverages will vary based on local law requirements and the terms and conditions of the policy issued. The information described herein does not amend, or otherwise affect, the terms and conditions of any insurance policy issued by Tokio Marine HCC Group of Companies. In the event that a policy is inconsistent with the information described herein, the language of the policy will take precedence.

Outside the EEA, the Policyholder is also able to enter into contracts of insurance through the Lloyd's underwriting members of Lloyd's Syndicate 4141, managed by HCC Underwriting Agency Ltd. As such, the policyholder will always be informed of which insurer in our group will underwrite the policy in these jurisdictions..