LLOYD'S

Cyber risk

The emerging cyber threat to industrial control systems

CyberCube | GUY CARPENTER

Lloyd’s disclaimer

This report has been co-produced by Lloyd's, CyberCube and Guy Carpenter for general information purposes only. While care has been taken in gathering the data and preparing the report Lloyd's does not make any representations or warranties as to its accuracy or completeness and expressly excludes to the maximum extent permitted by law all those that might otherwise be implied.

Lloyd's accepts no responsibility or liability for any loss or damage of any nature occasioned to any person as a result of acting or refraining from acting as a result of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this report. This report does not constitute advice of any kind.

About Lloyd’s

Lloyd's is the world's specialist insurance and reinsurance market. Under our globally trusted name, we act as the market's custodian. Backed by diverse global capital and excellent financial ratings, Lloyd's works with a global network to grow the insured world –building resilience of local communities and strengthening global economic growth.

With expertise earned over centuries, Lloyd's is the foundation of the insurance industry and the future of it. Led by expert underwriters and brokers who cover more than 200 territories, the Lloyd’s market develops the essential, complex and critical insurance needed to underwrite human progress.

About CyberCube

CyberCube delivers the world’s leading cyber risk analytics for the insurance industry. With best-in-class data access and advanced multi-disciplinary analytics, the company’s cloud-based platform helps insurance organizations make better decisions when placing insurance, underwriting cyber risk and managing cyber risk aggregation. CyberCube’s enterprise intelligence layer provides insights on millions of companies globally and includes modelling on thousands of points of technology failure.

The CyberCube platform was established in 2015 within Symantec and now operates as a standalone company exclusively focused on the insurance industry, with access to an unparalleled ecosystem of data partners and backing from ForgePoint Capital, HSCM Bermuda, MTech Capital and individuals from Stone Point Capital. For more information, please visit www.cybcube.com or email info@cybcube.com.

About Guy Carpenter

Guy Carpenter & Company, LLC is a leading global risk and reinsurance specialist with more than 3,100 professionals in over 60 offices around the world. Guy Carpenter delivers a powerful combination of broking expertise, trusted strategic advisory services and industry-leading analytics to help clients adapt to emerging opportunities and achieve profitable growth. Guy Carpenter is a business of Marsh & McLennan (NYSE: MMC), the world’s leading professional services firm in the areas of risk, strategy and people. The company’s 76,000 colleagues advise clients in over 130 countries. With annual revenue of $17 billion, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses including Marsh, Mercer and Oliver Wyman. For more information, visit www.guycarp.com and follow Guy Carpenter on LinkedIn and Twitter @GuyCarpenter.

Acknowledgements

CyberCube, Guy Carpenter and Lloyd's Underwriting and Exposure Management worked closely with the Lloyd's Market Association (LMA) to gain early feedback on the ICS scenario. The assistance of the individuals involved and the support of their respective organisations is greatly appreciated.

CyberCube

- John Anderson, Principal Client Product Advisor
- William Altman, Cyber Security Consultant
- Charlotte Anderson, Cyber Risk Analyst
- Jenna McGrath, Economist
- Darren Thomson, Head of Cyber Security Strategy
- Yvette Essen, Head of Content & Communications
- Nick Beecroft, Strategic Partnership Lead

Guy Carpenter

- Jamie Pocock, Head of GC Cyber Analytics – International
- Neil Sharma, Actuary, Cyber Analytics
- Siobhan O'Brien, Leader, Guy Carpenter Cyber Centre of Excellence, International and Global Specialties

Lloyd's project team

- Kirsten Mitchell-Wallace, Head of Portfolio Risk Management
- Emma Watkins, Head of Exposure Management
- Charlie Melly, Exposure Management Manager
- Nicola Beckles, Marketing Manager

Contents

Executive summary 5
1. Introduction 8
2. Overview of the proposed scenario 11
3. Impacts on the insurance market 13
Classes of business 13
Cyber Clauses and Exclusions 14
4. Examining different scenario pathways 16
Developing attack pathways 16
Pathways originating with nation-state affiliates 17
Pathway 1: Targeted supply chain malware attack 18
Pathway 2: Targeted IoT vulnerability attack 19
Pathway 3: Infiltration of IT networks to cross the OT “air-gap” 20
Pathways originating from non-malicious sources 21
5. Target industries considered 23
Manufacturing 23
Energy 24
Transportation 24
Shipping 25
6. Trends and scalability of the current threat 27
IoT proliferation and the convergence of IT/OT 28
Increased cloud adoption in industrial operations 28
7. Conclusions 30
8. Glossary of terms 32
References 33

Executive summary

A Lloyd's, Guy Carpenter and CyberCube Analytics collaboration provides an original analysis of potential cyber attack pathways to an industrial target.

Synopsis

Cyber risk is continually evolving, meaning insurers should understand emerging risks in order to keep pace with their clients' exposures.

Lloyd's, CyberCube and Guy Carpenter have conducted an analysis detailing three scenarios which represent the most plausible routes by which a cyber attack against industrial control systems (ICS) could generate major insured losses. All three scenarios have historical precedents. The report describes how more severe events could unfold.

This report considers four key industries dependent upon ICS (Manufacturing, Shipping, Energy and Transportation) and assesses precedents and the potential impact on each.

The potential for physical perils represents a major turning point for the broader cyber (re)insurance ecosystem. This risk has previously been considered unlikely to materially impact the market, with cyber perils traditionally emerging in the form of non-physical losses.

However, crossing the divide between information technology (IT) and operational technology (OT), along with increases in automation and the sophistication of threat actors, means it is paramount that (re)insurers carefully consider how major losses may occur and the potential impacts.

What is the study?

Lloyd's, CyberCube Analytics and Guy Carpenter collaborated to develop a view of cyber industry insured loss from a range of different cyber scenarios. These proposed scenarios are based on attacks against cyber-physical ICS.

Using a schematic, the report illustrates the "plausible" and "preferred" attack pathways that form the backbone of what was originally a quest to develop a realistic disaster scenario (RDS). Several illustrative scenarios that can be used by Lloyd's syndicates for understanding and measuring emerging operational cyber risks are included.

The study sheds light on an environment where, to date, the overwhelming majority of instances have been based on IT, and not physical processes. We believe we are at an inflection point where the potential for cyber threats to bridge the gap between IT and OT is growing increasingly apparent.

The report concludes by making a number of recommendations and suggesting potential areas of focus for the Lloyd's market but also for anyone with an interest in cyber exposure management or underwriting.

Key takeaways:

- The risk of a cyber-physical ICS incident is increasing, especially for individual entities.
- Only a nation-state or nation-state affiliated actor is likely to possess the resources and level of technical sophistication necessary for a malicious ICS-oriented attack.
- Three plausible scenarios consider: (1) a targeted supply-chain malware attack, in which malicious actors breach a device manufacturer and compromise that manufacturer's products before distribution; (2) a targeted Internet of Things (IoT) vulnerability attack, in which attackers exploit a vulnerability in widely used IoT devices found in industrial settings; and (3) the infiltration of industrial IT networks to cross the OT "air-gap".
- An OT event could conceivably trigger a loss that leads to property damage and loss of life in one entity, and lead to extensive forensics, remediation, and product recall as necessary to limit further damage. However, an event leading to widespread property damage, business interruption, and human costs across multiple sites is currently less likely to occur.
- A targeted attack against an industrial site in an industry with outsized strategic, economic or societal importance (or any combination of those factors) would be hugely significant. The key industries considered include manufacturing, energy, transportation and shipping.
- Continued trends of increased cloud adoption in industrial operations, the convergence of IT and OT, and the proliferation of IoT and "smart manufacturing" can exacerbate security concerns and increase exposure profiles.

We recommend continued research and focus on developing and improving exposure management and underwriting standards in an emerging area of cyber risk whose boundaries are yet to be defined.

Furthermore, we recommend continued diligence around the increasing aggregation potential that could transition the groundwork laid for a threat specific to individual portfolios to one that may aggregate across the market.

The insurance market has a rich legacy of adapting to emerging risks and changing trends. As the risk of cyber-physical losses grows, it is essential that the market develops products and expertise to service this.

1. Introduction

1. Introduction

Cyber attacks and incidents that affect the confidentiality, availability, and integrity of data and information systems have become increasingly ingrained into society. The fast-paced evolution of today's cybersecurity threat landscape, combined with increased reliance on Internet-connected technologies in critical industrial operations, has the potential to give rise to an increased number of cyber incidents. In response to this, the standalone cyber insurance market has grown significantly, to a point where it will soon move beyond a $10 billion market threshold. The (re)insurance sector needs to proactively consider dynamics that are likely to affect the way that businesses should manage cyber risk. Building a robust forward-looking view of risk to manage cyber risk portfolios and set risk tolerance thresholds is a complex and resource-intensive task.

To date, the overwhelming majority of cyber incidents have related to IT rather than being based on physical processes. However, we now find ourselves at an inflection point where the potential for cyber threats arising from the prolific use of digital systems to control physical processes will bring IT and OT risks closer together.

The potential for physical perils represents a major turning point for the broader cyber (re)insurance ecosystem. This risk has previously been considered unlikely to generate insured losses with cyber perils traditionally emerging in the form of non-physical losses. However, as bridges are being built between IT and OT and there is increased automation and greater sophistication of threat actors seeking new avenues to create disruption, incidents are increasingly likely.

For large industrial risks transferred into the insurance market, threats to OT could be associated with significant claims. This report has, therefore, been designed to aid individual syndicates' understanding of the impact of an emerging cyber risk on their portfolio.

This research identifies scenarios exploring a range of attacks impacting IT and OT that cause physical damage to major industrial organisation(s). It offers a blueprint for developing a unique cyber-physical ICS scenario that syndicates and managing agents can apply to risks within their own portfolios.

The proposed scenarios are based on attacks against cyber-physical ICS. We illustrate "plausible" and "preferred" attack pathways. Several scenarios have been identified that can be used to understand emerging operational cyber risk.

The resources and level of technical sophistication necessary for such an attack would most likely come from a nation-state or nation-state *affiliated* actor. Today there are many uncertainties surrounding policy exclusions that relate to nation-states and acts of war in cyberspace. In this analysis, we explore threats for the proposed scenario to be perpetrated by affiliates of nation-states, noting that these are less likely to trigger any exclusions related to acts of war or cyber terrorism.

This analysis also underscores the importance of considering non-malicious pathways in a cyber-scenario. To this end, we discuss an upstream programming error within a third-party's OT that results in multiple impacted entities.

Three specific attack pathways representing the most plausible set of attacks given today's pertinent threats, historical precedents, and broader technological trends are included. Attack pathways include a targeted software supply chain (SSC) malware attack, a targeted attack on an IoT vulnerability, and a discussion of infiltrating IT networks to cross into an air-gapped OT network. We include precedents for all of these.

The importance of considering a targeted attack against an industrial site in an industry with outsized strategic economic and societal importance is also highlighted. Critical industrial operations for which an attack could result in cascading impacts across other industries are also considered. These include: manufacturing, energy, shipping and ports, and transportation. These four industries exhibit particular opportunities and potential targets for attackers.

This report includes a discussion of the classes of business exposed as well as coverage and exclusion considerations. We also consider current impediments that affect the scalability of this type of scenario, whilst noting the trends that make this an increasing concern for the insurance industry.

Finally we conclude with a call to action for the Lloyd's market, and wider (re)insurance industry outlining how to respond proactively and effectively to the growing threat.

2. Overview of the proposed scenario

2. Overview of the proposed scenario

The foundation for researching this threat was to assess its relevance as a scenario that could result in market-wide physical loss on an aggregated basis. Following careful consideration of the most relevant current threats and those on the horizon for Lloyd's, Lloyd's decided to investigate development of a scenario based on an IoT supply chain event impacting the industrial/manufacturing industries. To meet the criteria for Lloyd's-wide scenario development, it would need to be measured as an aggregable and insurable event affecting a significant number of syndicates.

Upon initial reflection on the premise for this scenario, we examined the potential for the following characteristics:

(1) exploitation of an IoT vulnerability
(2) impact on supply chains
(3) targeting of industrial/manufacturing industries
(4) resulting physical damage from the incident

Through researching the idea of this being an IoT scenario, we determined that a common understanding of what is meant by "IoT" was needed, differentiating the wider technological phenomenon from its common association with wearables or even ICS.[1] The defined scope included networks of devices and machines - "things" - embedded with sensors and software that enable those things to exchange data over the Internet, as well as various administrative systems and associated instrumentation such as devices, networks, and more which are used to operate and automate industrial processes.

As is true with all scenario development, one of the first steps in designing this scenario was to find and understand any precedents. As this report will uncover, each one of these incidents is part of the foundation for building a cyber scenario, however, a critical part of scenario development is to take these learnings from past precedents and introduce scalability beyond isolated incidents.

3. Impacts on the insurance market

3. Impacts on the insurance market

Classes of business

The crossing of the IT/OT divide means that many lines of business are potentially exposed beyond the standalone cyber insurance market. The types of costs that could conceivably arise are as follows:

- Material damage costs
  - Property destruction
  - Loss of life and bodily injury
- Non-material damage costs
  - Business interruption
  - Contingent business interruption
  - Loss of shareholder value
  - Loss of data
  - Bricking of machines

The kinds of targets that could be contemplated in such an event would be large and have a wide range of relevant insurance coverages. These are broadly grouped as follows:

Lloyd's Class of Business	Potential Scalability to Core Classes
Accident & Health	Potential impacts to A&H, Medical Expenses, and PA for any locations that suffer property damage and fires or explosions. Product Recall could be a significantly exposed class, particularly if a defective component is the point of failure.
Aviation	Limited, in the context of the scenarios explored.
Casualty Treaty	Significant potential impacts, particularly around contributing classes such as Employer's Liability and Product Liability.
FinPro Casualty	Significant potential exposure to Cyber, D&O, and Professional Indemnity.
Other Casualty	Some possible exposure for other classes such as General Liability.
Energy	Depending on the target industries, Energy Property and Liability could be significantly impacted by such a scenario.
Marine	Limited, in the context of the scenarios explored.
Other Specialty	Engineering could be significantly exposed. Other bespoke products that could conceivably be triggered include Extended Warranty, Legal Expenses, and Terrorism.
Property (D&F)	Significant potential exposure to large risks, with conceivable impacts to binder business with proximity to those impacted sites.
Property Treaty	Significant potential exposure to large risks, with conceivable impacts to binder business with proximity to those impacted sites.

These would all be subject to both the scenario synopsis in question as well as the specifics of the coverage offered in respect to cyber-triggered occurrences.

Cyber Clauses and Exclusions

‘Silent Cyber’ refers to cyber-related exposure found within many all-risk general insurance products, where there is no explicit contract language to either include or exclude coverage. This ‘silent’ exposure has the potential to aggregate significantly, a major issue concerning the (re)insurance industry. Policies with no explicit exclusion, an implicit coverage grant, or where language was ambiguous could be triggered by losses. The 2017 NotPetya and WannaCry cyber events demonstrated the very real existence of this Silent Cyber exposure, with economic losses exceeding $8 billion and insured losses estimated at $3.6 billion on both affirmative and non-affirmative (silent) covers globally.

Lloyd’s and global regulators are therefore aligned in their goal to safeguard the sustainability of the insurance market by requiring contract certainty for clients and driving innovation of new cyber products to fill the evolving needs of clients.

One of the challenges is in the lack of a globally-agreed definition of what constitutes “cyber”. Across various classes of insurance, the differences become apparent as some clauses refer to “cyber events” while others refer to the use of “software”. Certain clauses deal only with “malicious” cyber events, some refer to “systemic” risk, and others impose conditions related to an insured’s ability to demonstrate the adequacy of their cybersecurity.

This lack of consistency presents considerable challenges, though underwriters are actively taking steps to address the issue. Following a series of mandates issued by Lloyd’s to seek clarity of coverage and contract certainty, there has been increased activity to address this in policy language on both direct and reinsurance policies. In response to these mandates and other regulatory discussions, the Lloyd’s Market Association (LMA) has produced various cyber clauses to facilitate this clarity of intent under policies.

While still gaining traction in Casualty lines, the direct and reinsurance Property markets have been deploying these exclusions widely, with four options available to clients:

- Affirmation of coverage by direct coverage grant
- Affirmation with a sublimit
- Absolute exclusion, excluding all cyber exposures
- An exclusion but with write-backs for specific areas of coverage

The implementation of these clauses is important in eradicating the uncertainty of Silent Cyber and this new language will likely impact the loss outcomes associated with the scenarios discussed in this paper.

4. Examining different scenario pathways

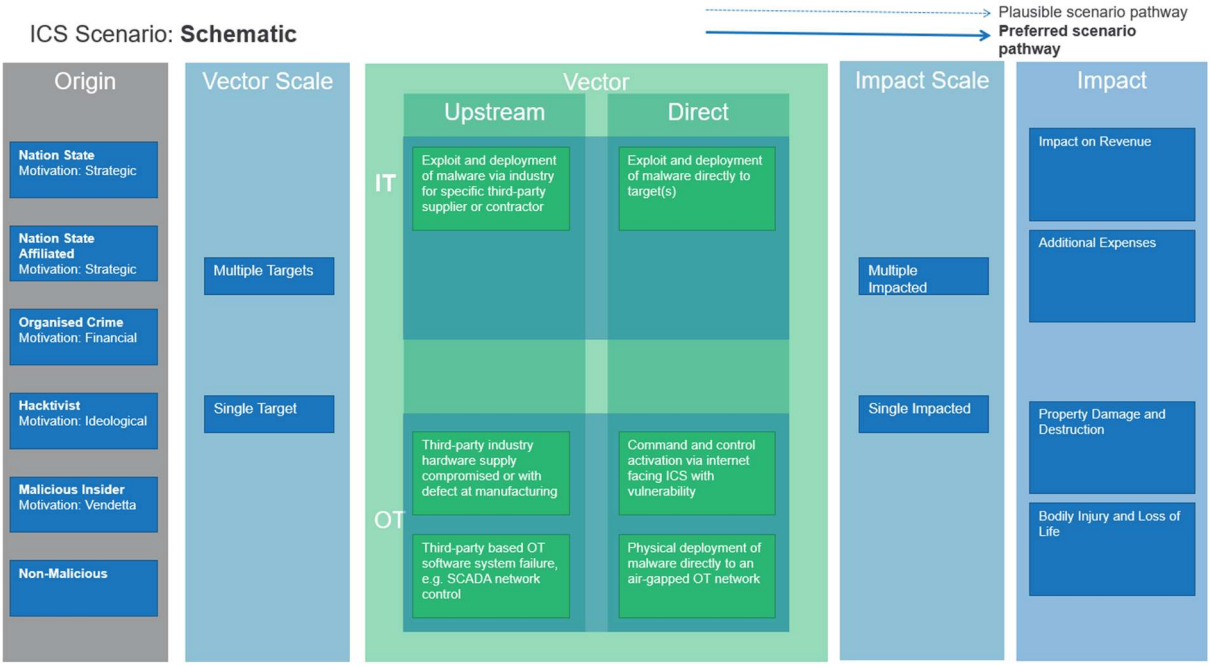
4. Examining different scenario pathways

Developing attack pathways

Schematics for probable attack pathways help to inform the creation of aggregation scenarios. There are five factors which can be considered to develop a credible cyber scenario. These are:

1) **Origin** which may correspond to malicious or non-malicious actors and forces. This could include nation-states, organised criminal groups, hacktivists, and malicious insiders.
2) **Vector scale** which differentiates an occurrence of one or multiple initial targets involved.
3) **Vector** which describes the systems directly impacted (IT vs. OT) and whether the original impact is direct or upstream in the supply chain.
4) **Impact scale** which sets out whether it is one or multiple large entities that are being impacted and incurring costs.
5) **Impact** describes the specific types of loss that may occur. These consider both financial and physical consequences such as lost revenue and additional expenses, property damage and destruction, and bodily injury or loss of life.

The schematics later in this report illustrate “plausible” and “preferred” attack pathways, which correspond to the different likelihoods of occurrence. Plausible attack pathways help to illustrate the multitude of realistic ways an attack could unfold. Preferred attack pathways reflect the pathways judged to be most likely given the risk landscape. The base schematic is illustrated below:

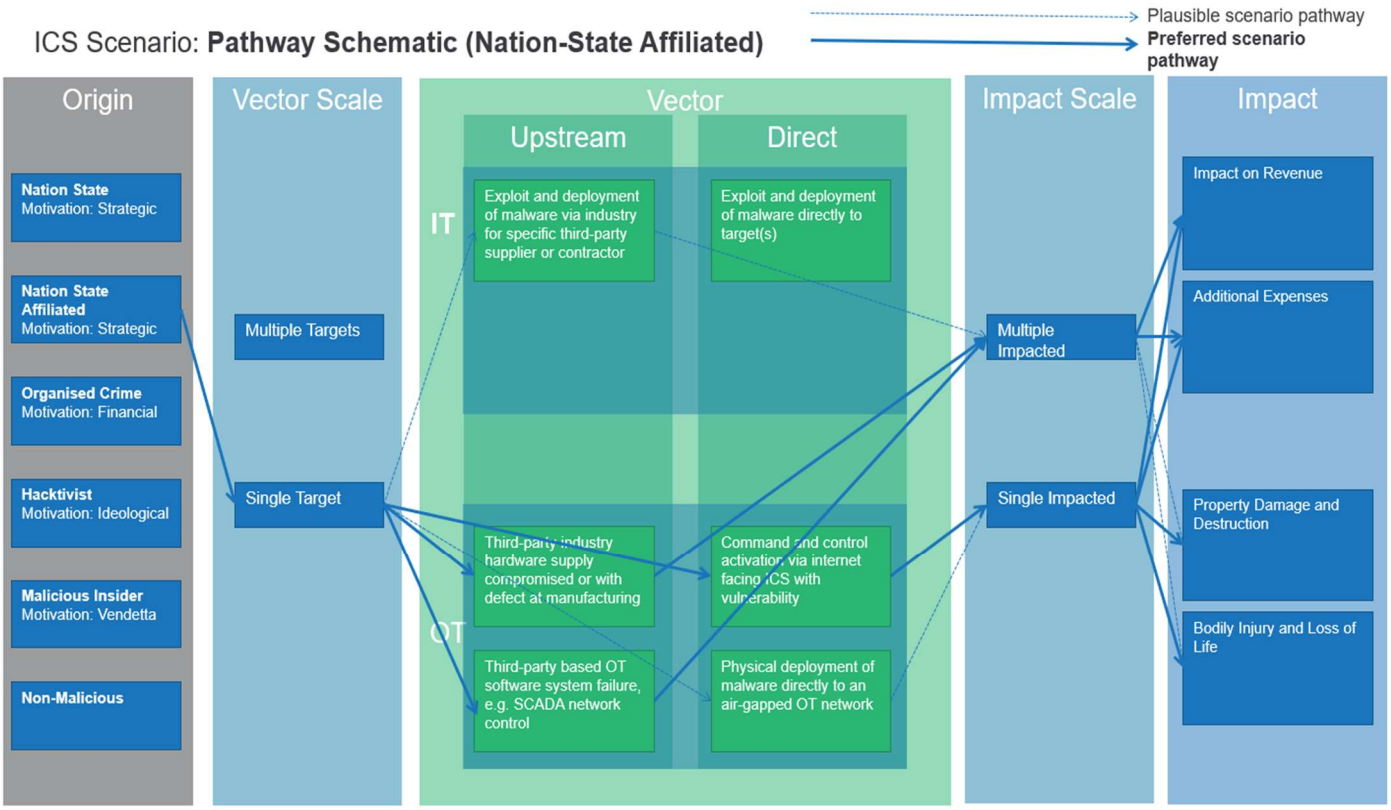


Pathways originating with nation-state affiliates

We concluded that a nation-state or nation-state *affiliated* actor is most likely to possess the resources and level of technical sophistication necessary for a malicious ICS-oriented attack.

Several nations have been known to house cybercriminal hacking groups operating within their borders. There is the potential for activity to be unofficially condoned with uncertain links to the state. One example of this is Advanced Persistent Threat (APT) APT41[2], a very active group with attacks across critical industries, that the US Department of Justice claims is "loosely" associated with Chinese state security.

Below, we illustrate a preferred scenario in which a strategically-motivated nation-state affiliated threat actor attacks a single target via an OT threat vector. The attacker either uses upstream methods or establishes direct command and control activation via an Internet-facing ICS with a vulnerability.



In the case of an OT upstream attack, multiple entities would likely be impacted. In the case of an OT direct attack a single entity would likely be impacted. A single entity impacted in this attack pathway could conceivably see lost revenue, additional expenses, property damage and destruction, as well as bodily injury and loss of life.

For an event impacting multiple entities, there is the potential for significant costs, many of which may be from the same sources. However, differences in the nature of supply chains could lead to different impacts for different parties. An OT event might trigger a loss that leads to property damage and loss of life in one entity, and lead to extensive forensics, remediation, and product recall to limit further damage, which then impacts additional entities. As such, there may be first and second order effects that scale separately for different impacted organisations.

The following pathways are specific representations from the schematic above, representing the most plausible set of attacks given today's pertinent threats and precedents and taking into account broader technological trends.

Pathway 1: Targeted supply chain malware attack

A recent KPMG survey confirmed that 15% of cyber incidents affecting ICS occurred due to “hardware or software infected with malware ‘off-the-shelf’.”[3] These kinds of supply chain attacks are not often reported publicly. Nevertheless, there is growing concern around threat actors targeting the supply chains of industrial sites in an upstream malware attack.

The MITRE ATT&CK Framework for ICS states that: “Supply chain compromise can occur at all stages of the supply chain, from manipulation of development tools and environments to manipulation of developed products and tools distribution mechanisms”.[4] Keeping this range of supply chain compromises in mind, there are three plausible steps to consider.

- **Step 1:** An attacker infiltrates the supply chain manufacturer of an IoT device used widely in industrial operations. The attacker either plants malware into the device before it is shipped, or injects malicious code into software update cycles.
- **Step 2:** Malware is introduced into the industrial site via software updates and/or installation of new (infected) devices. A logic bomb in the malware might delay the activation with specified conditions that can be programmed for maximal impact.
- **Step 3:** Activated malware causes physical damage and potential bodily injury or loss of life when infected control systems cause machine failures and explosions. The potential for the failure of industrial emergency response systems or employee communication systems could exacerbate adverse impacts.

Notable precedents include the following:

- The FBI warned in February 2020 of increasing software supply chain attacks specifically targeting ICS in the energy sector with malware such as the Kwampirs RAT, and a Shamoon analogue.[5]
- The 2020 SolarWinds attack is an example of a targeted supply chain malware attack using malicious software updates.[6]
- The LemonDuck attacks in 2020 included attempts to target supply chain providers by installing self-spreading malware on IoT devices and impacted more than 50 industrial sites in the Middle East, North America, and Latin America.[7]
- Groups such as DragonFly 2.0 and Havex have trojanised legitimate software such as standard Windows applications and even software available for download on ICS/SCADA manufacturer websites to deliver malware to energy sector targets.[8]

Pathway 2: Targeted IoT vulnerability attack

In this pathway, attackers exploit a widespread vulnerability in a popular IoT product to coordinate an attack that impacts multiple industrial entities at the same time. It is not assumed that they infiltrate industrial supply chain software vendors; rather that they take advantage of vulnerabilities in those vendors' products to directly conduct simultaneous attacks on targeted industrial sites.

There is potential for this pathway to originate with coordinated malicious insiders or external groups such as nation-states or nation-state affiliated actors. Free and easily accessible tools, enabling attackers to scan the Internet for exposed IoT devices that can serve as attack entry points into industrial sites, exist online.[9]

The plausibility of this attack pathway is underpinned by the fact that industrial operations often have difficulty applying timely and widespread software patches to prevent the exploitation of vulnerabilities. These environments can contain outdated legacy systems (including embedded Windows and Linux systems vulnerable to a wider variety of malware) due to the cost of upgrading equipment and the specialised and costly nature of such equipment. Moreover, halting ICS for patches or upgrades can cause significant downtime.

- **Step 1:** A critical software vulnerability goes overlooked by supply chain software manufacturers and becomes present in IoT devices that are then used in a variety of industrial settings.
- **Step 2:** Attackers (external or coordinated internal) discover the vulnerability and develop a sophisticated exploit, then target all industrial networks that are exposed.
- **Step 3:** Successful exploitation of the vulnerability enables infiltration into multiple industrial OT networks. Targeted malware or the ability to alter configuration settings, network, and device failures could then result in physical damage.

Notable precedents include the following:

- The Ripple20 vulnerabilities are an excellent example here; discovered in 2020, Ripple20 represents a series of critical vulnerabilities affecting the Treck TCP/IP communication stack used in hundreds of millions of IoT devices across a wide variety of industries, including industrial, power grids, medical devices, oil and gas, aviation, transportation, and retail.[10]
- Additionally, the Israeli water facilities attacks in April 2020 were reportedly due to SCADA control systems that were outdated with weak access configurations and/or exposed to the Internet.[11]

Pathway 3: Infiltration of IT networks to cross the OT “air-gap”

The process of “air-gapping” describes the separation of OT machines onto a specific network so that those machines do not connect to the Internet. Inadequate air-gapping can occur with employees operating in IT environments on Internet-facing networks that do not have adequate safeguards in place between the two systems. This could arise in relation to phishing, connecting malicious USB devices, or otherwise facilitating malware movement to the IT to OT network leading to a destructive impact.

A recent KPMG study revealed that 14% of respondents had critical industrial equipment such as programmable logic controllers (PLCs) remotely accessible from the business IT network. This suggests that whilst air-gapping is a core security defense requirement for industrial sites, it does not operate as intended everywhere it is deployed.[12]

The attack could unfold as follows:

- **Step 1:** Attackers successfully spear-phish IT administrators or other employees and gain persistent high level IT network access within the target industrial site.
- **Step 2:** With administrator-level access to the IT network, attackers can move laterally to find and exploit insecure devices that will serve as a bridge into the OT environment.
- **Step 3:** Once inside the OT environment, attackers are able to deploy self-spreading malware or ransomware. This could be used to escalate privileges in order to alter system controllers or safety configurations, or cause sudden unplanned outages.

Notable precedents include the following:

- NotPetya and Stuxnet involved destructive self-spreading malware strains that crossed over from corporate IT to manufacturing OT networks when network segmentation was not properly implemented. These attacks disabled OT devices and disrupted industrial operations at sites for major companies such as Merck.[13]
- Conficker and W32 Ramnit malware that spread to a German nuclear plant in 2016, triggering a cautionary shutdown.[14]
- Ransomware infected the aluminium producer Norsk Hydro’s plants causing operators to resort to manual processes while systems were out.[15]
- Attackers in the Shamoon[16], BlackEnergy 3[17], German steel mill[18], and Triton/Trisis[19] incidents all infiltrated OT networks via targeted phishing emails sent to employees that gained them initial corporate network access.
- 2009 NightDragon attacks against companies in the energy sector[20], and attacks on US gas pipelines.[21]

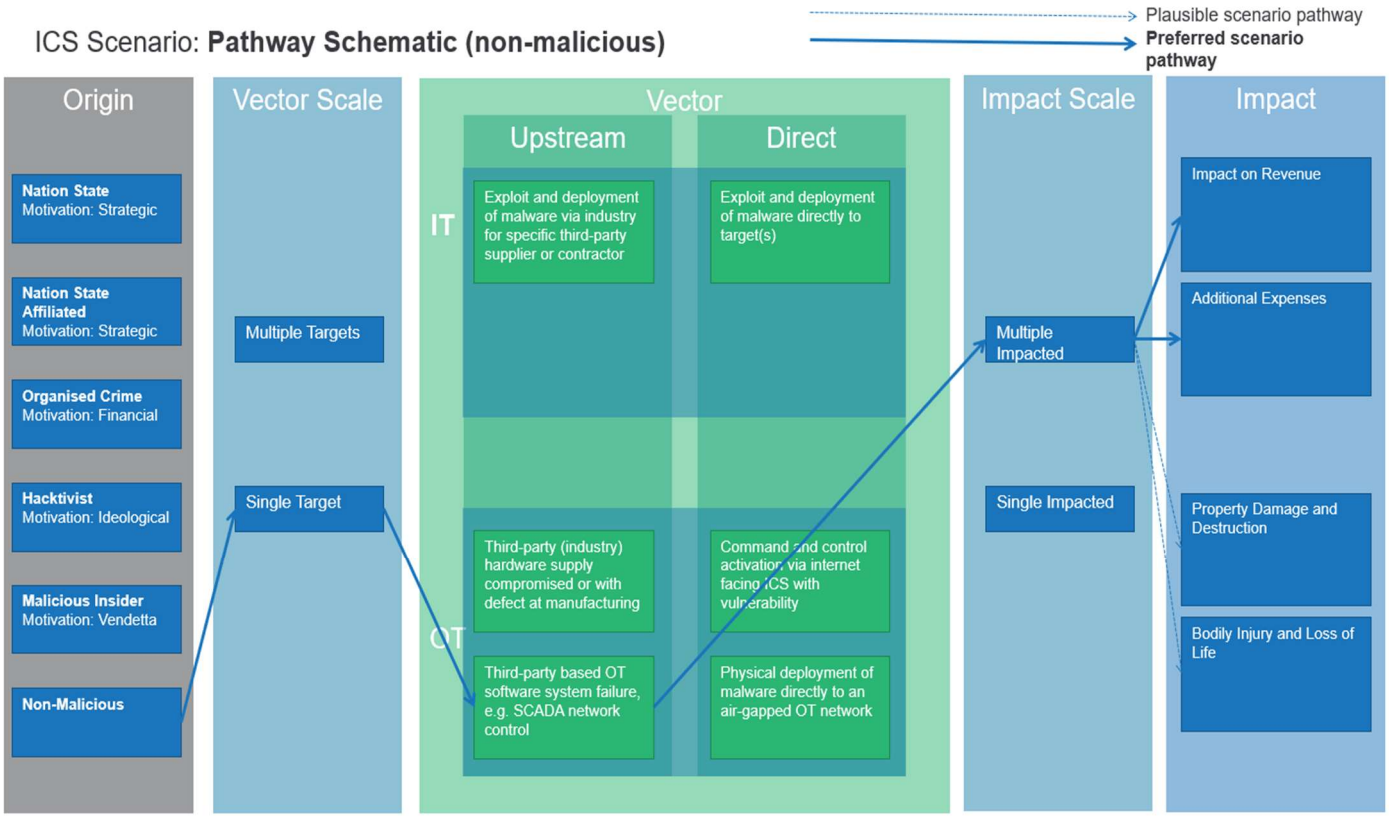
Pathways originating from non-malicious sources

In addition to malicious drivers, consideration of non-malicious pathways is also important. Non-malicious pathways could arise from an upstream programming error within a third-party's OT software. This origin could, therefore, also affect the scale and result in multiple-impacted entities.

The rise of industrial automation technologies and practices, including automated and over-the-air updates for software and machines, in turn exacerbates the potential adverse impacts of a software bug. The increased complexity of OT software and hardware development environments also adds to the potential for a non-malicious pathway to arise from a design error.

However, a non-malicious case would likely *not* result in the same scale of impact as a malicious attack. For example, we can consider a strategic nation-state or nation-state affiliated actor planting well-crafted malware into underlying software; well-crafted malware is not easy to detect or stop once it has infected a system. The sophisticated Stuxnet malware that destroyed Iranian nuclear centrifuges in 2010 was designed to obfuscate itself in real-time to avoid detection by system administrators for an extended period, whereas an OT software programming error would not benefit from intentional obfuscation to prevent detection. Administrators would have a better chance of finding the software bug, and would likely be empowered to take action to limit damages after the bug is discovered.

In the example below, we set out the non-malicious pathway in which such a software bug is present that is critical to the functioning of industrial operations.



5. Targeted industries considered

5. Target industries considered

A targeted attack against an industrial site in an industry with major strategic, economic or societal importance (or any combination of those factors) would be hugely significant. This includes industrial sites such as manufacturers, water and energy utilities, shipping facilities and ports, transportation infrastructure, as well as other critical industrial operations for which an attack results in cascading impacts across other industries.

The potential attack steps and the corresponding impacts can vary widely depending on the industry and the strategic value of the industrial site targeted. Additionally, it is important to consider attackers' motivations in targeting each respective industry and industrial site to best forecast impacts and measure risk.

Manufacturing

Security firm CrowdStrike reported in 2020: "The manufacturing industry has experienced a dramatic increase in interactive intrusion activity compared to past years."[22]

Manufacturing production processes increasingly incorporate smart devices and embedded intelligence, and the number of IoT devices in manufacturing settings is expected to continue to grow.[23] Increased digitisation and reliance on the IoT creates new security vulnerabilities such as opportunities for hackers to cross from IT to OT networks. Large scale attacks on manufacturing operations could cause large explosions or chemical spills impacting surrounding areas as well as supply chain disruptions.

Notable precedents include the following:

- A number of companies have seen production line outages due to ransomware spreading to OT environments, such as Honda, Fresenius Group, and ENEL targeted by SNAKE/EKANS ransomware. Ryuk malware impacted steel maker EVRAZ in March 2020, shutting down production and leading to the temporary furloughing of more than 1,000 workers for at least four days.[24]
- Garmin's manufacturing was impacted by WastedLocker in July 2020.[25]
- Belgian airplane parts maker ASCO experienced production line outages in 2019 due to ransomware.[26]
- Also in 2019, Norsk Hydro, a multi-national aluminium manufacturer with operations in 40 countries, closed many of its plants and was forced to move others offline due to the LockerGoga ransomware.[27]

Energy

The energy sector and especially oil and gas production operations have a diverse and complex supply chain that can be exploited and is difficult to defend in its entirety. Moreover, these industrial sites are incorporating new technologies including the IoT and the cloud for enabling automation and intelligence. Consequently, oil and gas companies are becoming more exposed to cybersecurity threats.[28]

Throughout the first half of 2020, the amount of computer systems attacked in the oil and gas industry increased significantly compared to the same time period last year.[29] Worst-case-scenario attacks on oil and gas systems could lead to explosions at refineries or offshore drilling units; in a cyber-induced Deepwater Horizon scenario.

Notable precedents include the following:

- The Stuxnet malware targeted centrifuges in a uranium enrichment facility in Iran. Malware called Industroyer has been used to deliver attack payloads that affect ICS used in electric substations and can be used to target other critical infrastructure.[30]
- A recent ransomware attack caused a US natural gas compressor facility to shut for two days.[31]
- Attacks on ICS systems in the energy sector can lead to explosions, as in the attempted Triton/Trisis Saudi Aramco attack in 2017[32], and long-lasting power outages as was the case in the Ukraine BlackEnergy and CrashOverride attacks.[33]

Transportation

Similar to other critical industries explored in this report, advances in IT and interconnectivity have improved efficiency for transportation infrastructure, but they have also created higher risk associated with cyber attacks.[34]

The annual number of transport-related companies affected by cyber incidents and associated costs are on the rise, however, most attacks on transportation infrastructure have not been destructive to date. The most common incidents involve data breaches, while incidents involving privacy violations have the highest average loss per incident.[35]

However, increased threat activity alongside digitisation trends and rising susceptibility to remote cyber attacks, signals that future attacks resulting in physical damage to transportation infrastructure are not unlikely. We can consider a disaster scenario in which attacks on control and navigation systems on passenger trains cause widespread stoppages, or in a worst-case scenario a cyber-induced multi-passenger-train crash.

Notable precedents include the following:

- In 2008, a teenager in Lodz, Poland, altered a television remote control and took over the ICS managing light-rail track points in the city. Four trains were derailed and 12 people injured as a result.[36]
- In November 2016, hackers attacked San Francisco's light-rail system.[37]
- In May 2017, Deutsche Bahn, the German national rail network, suffered an attack on its data systems. The WannaCry virus affected 450 Deutsche Bahn computers, bringing down passenger information systems, ticket machines and CCTV networks. The same attack, which is thought to have originated in North Korea, hit the national railway systems in both Russia and China.[38]

Shipping

Shipping infrastructure and especially maritime assets such as ocean transport vessels and port facilities are at an increased risk of cyber attacks.[39] The maritime cybersecurity firm Naval Dome found a 400% increase in attempted cyber attacks since the start of 2020.[40]

Notably, the attack increase coincides with a period when the maritime industry is turning to more remote enabled technologies due to the Coronavirus pandemic. According to Naval Dome: "OEM technicians are unable to fly out to ships and rigs to upgrade and service critical OT systems, resulting in operators circumventing established security protocols, leaving them open to attack."[41]

According to the Cyber Risk Management (CyRiM) project, the Singapore-based public-private initiative that assesses cyber risks, of which Lloyd's is one of the founding members, losses of up to $110 billion would occur in an extreme scenario in which a computer virus infects 15 ports. Transportation, aviation and aerospace sectors would be the most affected ($28.2 billion total economic losses), followed by manufacturing ($23.6 billion) and retail ($18.5 billion).[42]

With threats to the shipping industry on the rise, a plausible attack could arise against a large shipping vessel's ballast pump control system. This could lead to capsizing or crashing in a major port, with major supply chain disruptions and physical damage.

Notable precedents include the following:

- In mid-2017, Maersk, the world's largest container shipping company, was taken down for weeks by the NotPetya ransomware and wiper malware.[43]
- In 2018, the Port of Barcelona reported a cyber attack that affected only internal IT systems[44], and shortly after the US Port of San Diego experienced a serious IT system disruption.[45]
- In 2018, COSCO Shipping Lines was brought down for weeks by ransomware.[46]
- In 2020, Mediterranean Shipping Company was hit by an unnamed malware strain that brought down its data centre for days,[47] and CMA CGM took down its worldwide shipping container booking system after its Chinese branches in Shanghai, Shenzhen, and Guangzhou were hit by the Ragnar Locker ransomware.[48]

6. Trends and scalability of the current threat

6. Trends and scalability of the current threat

A traditional aggregation scenario might consider the accumulation of losses across multiple organisations and sectors. This could be represented as the result of a targeted attack on multiple unconnected ICS systems in parallel. Such a scenario would create significant accumulation.

However, an event leading to widespread property damage, business interruption, and human costs across multiple sites is, at present, unlikely to occur for the following reasons:

1. The successful breaching of a critical air-gapped ICS system is challenging.

For example, it is estimated that the Stuxnet attack took multiple engineers three years to prepare. It consisted of a significant and costly reconnaissance phase, and could have involved malicious insiders as well as advanced bespoke malware. To scale such an attack to more than one entity might require resources and motivations that stretch the capabilities of one criminal or nation-state affiliated entity at present.

2. Given the difficulty of a targeted, simultaneous breach of multiple critical air-gapped ICS, the event might rely on a supply chain software attack targeting multiple ICS systems with similar design features.

Based on research into update processes used by the major ICS manufacturers, this would appear difficult to execute. Nevertheless, the recent SolarWinds cyber attack suggests that sophisticated adversaries are increasingly targeting critical equipment and software inside ICS supply chains, which suggests there is a trend towards this becoming more relevant that should be carefully monitored.[49]

3. As a consequence, it is bespoke rather than generic malware that is likely to have more of an impact.

Each ICS/SCADA system is configured very specifically to carry out tasks that are unique to the entity that makes use of them. Previous attacks on these systems have involved advanced and very specific malicious instructions that have impacted the targeted system. An example of this is the Stuxnet malware which began to spread in the wild due to its aggressive nature, however, it did little damage to outside computers because they did not match the criteria that the malicious code was written to disrupt.

However, the threat landscape is constantly changing and the insurance market should look to the information presented in this report as a foundation for beginning to conceptualize the creation of scenarios for ICS environments.

Future ICS scenario research should consider the following ongoing trends and considerations:

IoT proliferation and the convergence of IT/OT

Throughout this report, we highlight that IT and OT environments are converging as industries adopt the IoT. The increased amount of remotely connected devices in industrial environments offers attackers more opportunities to bridge an air-gapped system to infect OT environments.

The (re)insurance industry needs to continue to monitor the increased use of IoT devices and other "smart manufacturing" trends that can further exacerbate security issues. In particular, attack vectors that include IoT devices will become more important as long as security is considered a characteristic rather than a design principle in IoT systems. IoT regulations are emerging as attack volumes and published vulnerabilities increase.

Increased cloud adoption in industrial operations[50]

Critical infrastructure and industrial site operators are starting to take advantage of cloud computing. Industries such as communications, energy, financial services, IT and transportation are increasingly virtualising their on-premises computing resources and pushing them into the cloud. Driving this trend is the fact that the cloud offers scalability, high availability, and decreased ownership cost.

However, cloud service environments are riddled with many of the same potential cybersecurity vulnerabilities as internally hosted environments, as well as unique exploits that affect virtual systems and networks. It seems apparent that widespread cloud outages could in turn have devastating consequences on industrial sites in the future.

Hosting critical industrial operations in the cloud is an emerging practice. In fact, evidence for new "SCADA in the Cloud" solutions were starting to appear at the time of this study. Keeping an eye on the development of industrial cloud security standards and best practices will be key to assessing cyber risk in these environments going forward.

7. Conclusions for the Market

7. Conclusions

There are a number of key takeaways that we would strongly recommend the (re)insurance market considers:

Although the affirmative cyber insurance product is well established, there is a comparative lack of understanding and awareness of cyber-physical risks. Cyber has been traditionally viewed as a non-physical peril, but this is demonstrably no longer the case. Use of the CZ risk code in the Lloyd's market acts to help focus attention on cyber-physical risk, but it is very important that the market builds a foundation of expertise and experience in this emerging area of risk.

Syndicates should monitor product coverages carefully across classes for relevance to the cyber-physical peril. This requires an active strategy to consider different potential cyber-physical scenarios, and where the losses may fall from these. As part of this, attaining coverage clarity across traditional classes is key. The findings of this report can be used to aid the development of bespoke cyber-physical scenarios for different classes of business for stress testing purposes.

Whilst an imminent mass-scale cyber-physical attack may be unlikely, the threat is evolving very rapidly. Precedents strongly point to continual targeting of strategic industrial sectors, as described in this report. Currently technology implementation and vulnerabilities can be fairly bespoke in many cases, but attackers are aided in this respect by the increasing interconnection of systems and the homogenisation of technology. This will act to heighten the risk significantly over time which requires a comprehensive response.

As part of a risk mitigation strategy, syndicates need to monitor the correlation potential for risks stemming from attacks bridging the IT/OT gap. This is particularly a concern for portfolios with concentrations of comparable large industrial risks. Insurers should consider commonalities of exposure within industry segments, and identify the increasing uniformity of components in supply chains. In practice, syndicates can improve awareness by building a technology inventory for their insureds. This might include identifying leading PLC components, and investigating the use of common industrial OT and IoT assets.

It is very important for syndicates to focus on procedures as well as components. Among other aspects, this should encompass the extent of air-gapping between IT and OT systems, the nature of risk management protocols such as automated patch updates, and the presence of known industrial component vulnerabilities. In addition to technological safeguards, information should be gathered to ascertain from insureds in relation to business-critical system dependence and operational resilience should an incident occur.

Beyond understanding exposure, syndicates should monitor the threat landscape carefully. Attack incidents, precedents, and near-misses can all be cross-examined to understand active risks and how they might be aligned to portfolios. Malicious actors routinely target specific sectors or institutions, and these evolving trends can be examined in real-time to help inform the view of the risk.

Finally, it is crucial that syndicates recognise that cyber-physical risks are growing and require considered and committed action. The question of a significant event occurring is one of "when", and not "if". The response required from the market is to build a comprehensive and sustainable base across underwriting, product development, pricing, and exposure management. Resources like this report should form part of the start of that journey.

8. Glossary of terms

8. Glossary of terms

- **Advanced Persistent Threat (APT):** a nation state or state-sponsored group with the resources and skills to stage long-term attacks with specific goals to gain unauthorized access to a computer network and remain undetected for an extended period.
- **Air-Gapped Network:** a computer network that is physically isolated from unsecured networks, such as the public-facing Internet or an unsecured local area network (LAN).
- **Industrial Control Systems (ICS):** Various administrative systems and associated instrumentation such as devices, networks, and more used to operate and automate industrial processes.
- **Information Technology (IT):** Hardware and software built to store, retrieve, transmit, and manipulate data or digital information, often via the Internet.
- **Internet of Things (IoT):** Networks of devices and machines - "things" - embedded with sensors and software that enable those things to exchange data over the Internet.
- **Malware:** Any software that is malicious by design. Malware takes many forms and includes software for establishing command and control, delivering ransomware, etc.
- **Operational Technology (OT):** Hardware and software built to detect and monitor as well as control and alter physical industrial equipment, assets, processes, and events.
- **Original Equipment Manufacturer (OEM):** A company that manufactures and sells products or components of a product with the intention of selling to other companies who then resell the original products or parts under their town branding.
- **Programmable Logic Controller (PLC):** An industrial digital computer which has been ruggedized and adapted specifically for the control and automation of manufacturing processes.
- **Ransomware:** A specific type of malware that is designed to encrypt a victim's critical data. Once encrypted, attackers demand payment in exchange for decrypting the data.
- **Realistic Disaster Scenario (RDS)**: A plausible and severe real world event with measurable and aggregatable insurance loss potential.
- **Software Supply Chain Attack (SSC):** Adversaries gain a foothold inside of larger and more secure organizations by first infiltrating an organization's software vendors.
- **Stuxnet:** A highly-sophisticated and malicious computer worm, allegedly used by the US and Israel to destroy the PLC and SCADA systems running Iran's nuclear program.
- **Supervisory Control and Data Acquisition (SCADA):** A control system architecture comprising computers, networked data communications, and graphical user interfaces for high-level monitoring and management of processes within industrial environments.
- **Threat Vectors:** The multitude of attack routes that malicious actors may take to get past your defenses and inside your network. For example, social engineering attacks known as phishing are one of the most common cyber security threat vectors today.

References

[1] SCADA systems are one such example of Industrial Control System

[2] https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

[3] https://www.cs2ai.org/reports

[4] https://collaborate.mitre.org/attackics/index.php/Technique/T0862

[5] https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies

[6] https://us-cert.cisa.gov/ncas/alerts/aa20-352a

[7] https://www.securityweek.com/iot-devices-major-manufacturers-infected-malware-supply-chain-attack

[8] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

[9] https://www.shodan.io/

[10] https://www.bleepingcomputer.com/news/security/ripple20-vulnerabilities-affect-iot-devices-across-all-industries/

[11] https://securityaffairs.co/wordpress/102361/hacking/israeli-water-facilities-attacked.html

[12] https://www.cs2ai.org/reports

[13] https://www.forescout.com/company/blog/malware-keynotes-4-ics-cybersecurity-lessons-learned-from-20

[14] https://www.securityweek.com/concerns-raised-over-malware-infecting-german-nuclear-plant

[15] https://www.bbc.com/news/business-48661152

[16] https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/

[17] https://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security/

[18] https://www.rt.com/news/216379-germany-steel-plant-hack/

[19] https://arstechnica.com/information-technology/2020/10/us-sanctions-russian-hackers-who-hit-chemical-maker-with-dangerous-malware/

[20] https://www.zdnet.com/article/night-dragon-attacks-another-reason-to-care-about-consumer-malware/

[21] https://www.csmonitor.com/USA/2012/0505/Alert-Major-cyber-attack-aimed-at-natural-gas-pipeline-companies

[22] https://www.governing.com/security/Cyberattacks-on-Manufacturing-Industry-Increase-During-COVID.html

[23] https://global.hitachi-solutions.com/blog/top-manufacturing-trends

[24] https://www.darkreading.com/attacks-breaches/manufacturing-sees-rising-ransomware-threat/d/d-id/1339

[25] https://www.wired.com/story/garmin-ransomware-hack-warning/

[26] https://www.computerweekly.com/news/252465178/Asco-breaks-silence-on-ransomware-attack

[27] https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

[28] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry

[29] https://ics-cert.kaspersky.com/reports/2020/09/24/threat-landscape-for-industrial-automation-systems-h1-2020/

[30] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry

[31] https://www.worldoil.com/news/2020/2/20/cyberattack-targets-oil-infrastructure-shuttering-facility-for-two-days

[32] https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known/d/d-id/1333661

[33] https://www.threathunting.se/2020/05/13/black-out-in-ukraine-blackenergy-in-power-grid-cyberattack/

[34] https://www.sciencedirect.com/science/article/abs/pii/S0967070X18307248

[35] https://www.sciencedirect.com/science/article/abs/pii/S0967070X18307248

[36] https://www.wired.com/2008/01/polish-teen-hac/

[37] https://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomware-cybersecurity-muni

[38] https://www.masstransitmag.com/safety-security/article/21116419/securing-the-railroads-from-cyberattacks

[39] https://www.cybersecurity-insiders.com/shipping-companies-are-extremely-vulnerable-to-cyber-attacks/

[40] https://www.offshore-energy.biz/naval-dome-400-increase-in-attempted-hacks-since-february-2020/

[41] https://www.offshore-energy.biz/naval-dome-400-increase-in-attempted-hacks-since-february-2020/

[42] https://www.hstoday.us/channels/global/a-maritime-cyber-attack-could-cost-110-billion-and-cripple-global-supply-chains/

[43] https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/

[44] https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/

[45] https://www.zdnet.com/article/port-of-san-diego-suffers-cyber-attack-second-port-in-a-week-after-barcelona/

[46] https://www.cybersecurity-insiders.com/cyber-attack-on-cosco/

[47] https://www.msc.com/che/news/2020-april/network-outage-resolved

[48] https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack

[49] https://www.cyberscoop.com/solarwinds-hack-dragos-ics-breach/

[50] https://scadahacker.com/library/Documents/ICS_Vulnerabilities/DHS-OCIA%20-%20Risks%20to%20Critical%20Infrastructure%20that%20use%20Cloud%20Services.pdf