2025

OT Cyber Threat Report

Navigating the Future of OT Security

waterfall

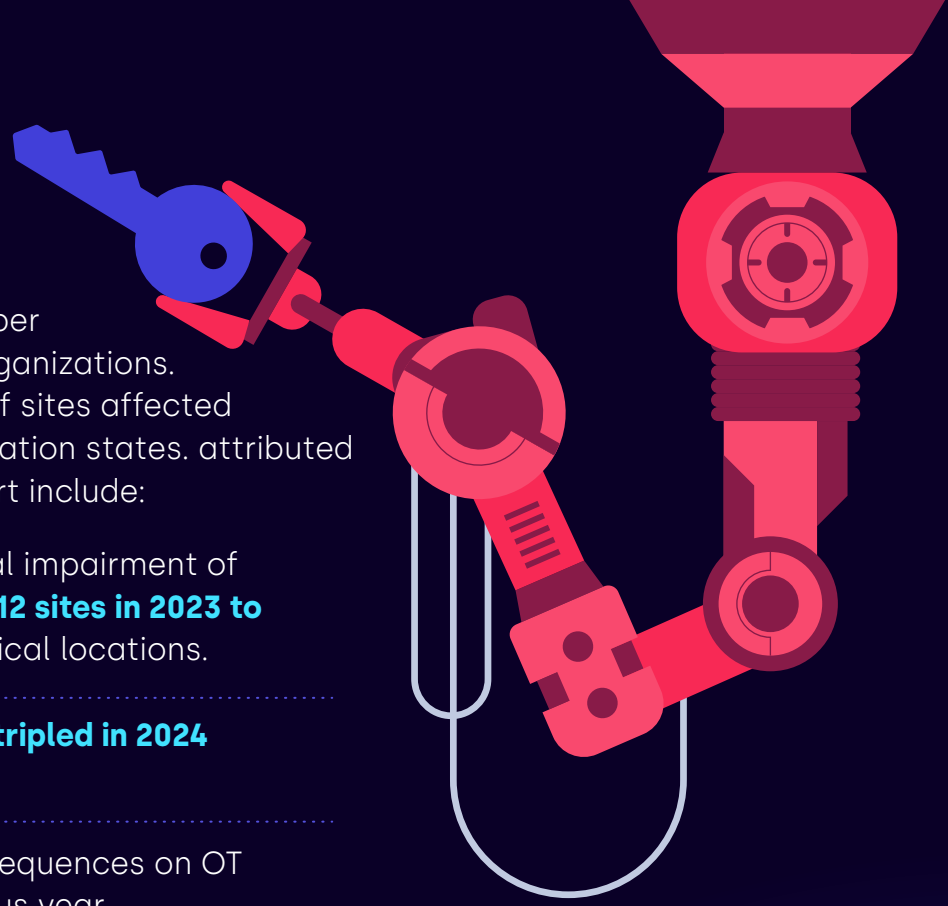
INDUSTRIAL CONTROL SYSTEM
ICS STRIVE
COVERING SECURITY, THREATS, REGULATIONS, INCIDENTS, VULNERABILITIES WITH EXPERTS

2025 OT Cyber Threat Report
Cyber Attacks with Physical Consequences

Contents

Authors:
Rees Machtemes, Director Industrial Security, Waterfall Security Solutions
Gregory Hale, Editor & Founder, Industrial Safety and Security Source, ICS STRIVE
Monique Walhof, Consultant, Industrial Safety and Security Source, ICS STRIVE
Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

Key Takeaways



Compared to 2023, 2024 saw a smaller increase in cyber attacks that caused physical consequences on OT organizations. Nevertheless, there were sharp jumps in the number of sites affected by the hacks, as well as in the number of attacks by nation states. attributed to nation state threat actors. Key findings in this report include:

- 2024 saw a **146%** increase in sites suffering physical impairment of operations because of cyber attacks, rising **from 412 sites in 2023 to 1,015 in 2024.** Most attacks impacted multiple physical locations.
- Nation-state attacks with physical consequences **tripled in 2024** compared to the previous year.
- There were **76 attacks** which caused physical consequences on OT organizations. This is a **5% increase** over the previous year.
- Making up **37%** of all attacks, the **transportation industry** was the single biggest vertical impacted by OT cyber attacks with physical consequences in 2024.
- The **discrete manufacturing and transportation** industries continue to dominate OT attacks with physical consequences.
- New **ICS/OT-designed malware** are increasingly being discovered in the wild.

In short, the OT threat environment and its consequences continues to worsen.

146% increase in sites impacted by cyber attacks with physical consequences.

Introduction & Methodology

This report documents cyber attacks with physical consequences. Security teams seeking funding for cybersecurity initiatives and business decision makers responsible for allocating such funding each need accurate data as to what attacks have occurred in the past and what we should reasonably expect of the attack environment in the future. Planning for the future is especially challenging and important for high-consequence operations where every change can pose a threat to safe and correct operations, which means changes and upgrades to our security programs can be made only at long intervals.

In support of understanding today's threats and projecting tomorrow's, this report documents cyber attacks on physical operations and infrastructure that:

- are deliberate in nature – not errors and omissions, not equipment nor software failures;
- produce physical consequences including production delays and outages, equipment damage, environmental disasters, injuries or casualties – not just data theft or computer system clean-up costs;
- impacted manufacturing, building automation, heavy industry, and critical industrial infrastructures, including transportation of people and goods;
- are found in public – not private – disclosures;
- and which the research team agrees meet the above criteria with a high degree of confidence.

This report's data is a conservative estimate, underreporting actual attack activity. Many incidents were excluded due to disclosure restrictions, insufficient confidence in authenticity, or lack of access to reports in certain languages or regions. Additionally, numerous attacks likely went unreported or were unreliable, particularly in censored or conflict zones. As a result, the actual severity of today's threat environment is certain to be higher than the figures presented.

In 2024, there were 76 attacks that met the strict inclusion criteria for this report.

Any reader wishing to verify the data can consult Appendix A, which contains the full data set of all incidents since 2010 and their public descriptions.

This report also touches on important developments in the threat environment in 2024 in addition to the incident data above, including:

- near misses – important incidents that did not cause physical consequences but are noteworthy for other reasons;
- so-called "living off the land" attacks that are very difficult to detect;
- and three new ICS-capable types of malware discovered in 2024.

We conclude with defensive highlights of 2024 and recent developments in ICS defenses including:

- New advice from multiple agencies that encourages more secure remote access solutions than VPNs, including hardware-enforced remote access protections for OT systems.
- New advice that describes principles of OT security, especially the safety imperative.
- The beginning of a shift of terminology to "credible threats" rather than "attack likelihood" in OT security standards and guidance.

As the threat environment worsens, more kinds of attacks which were previously ignored are becoming credible threats that must be addressed in security programs.

This report is a cooperative effort between Waterfall Security Solutions and the ICS Strive OT incident repository. We hope you find the material useful.

The incident database and numbers in this report regarding attack and outage activity are certain to be an underestimation.

OT Incident Macro Trends

In 2024, there were 76 attacks that met the strict inclusion criteria for this report. Most attacks affected multiple physical sites. This is a 5% increase over the 72 attacks in the data set for 2023.

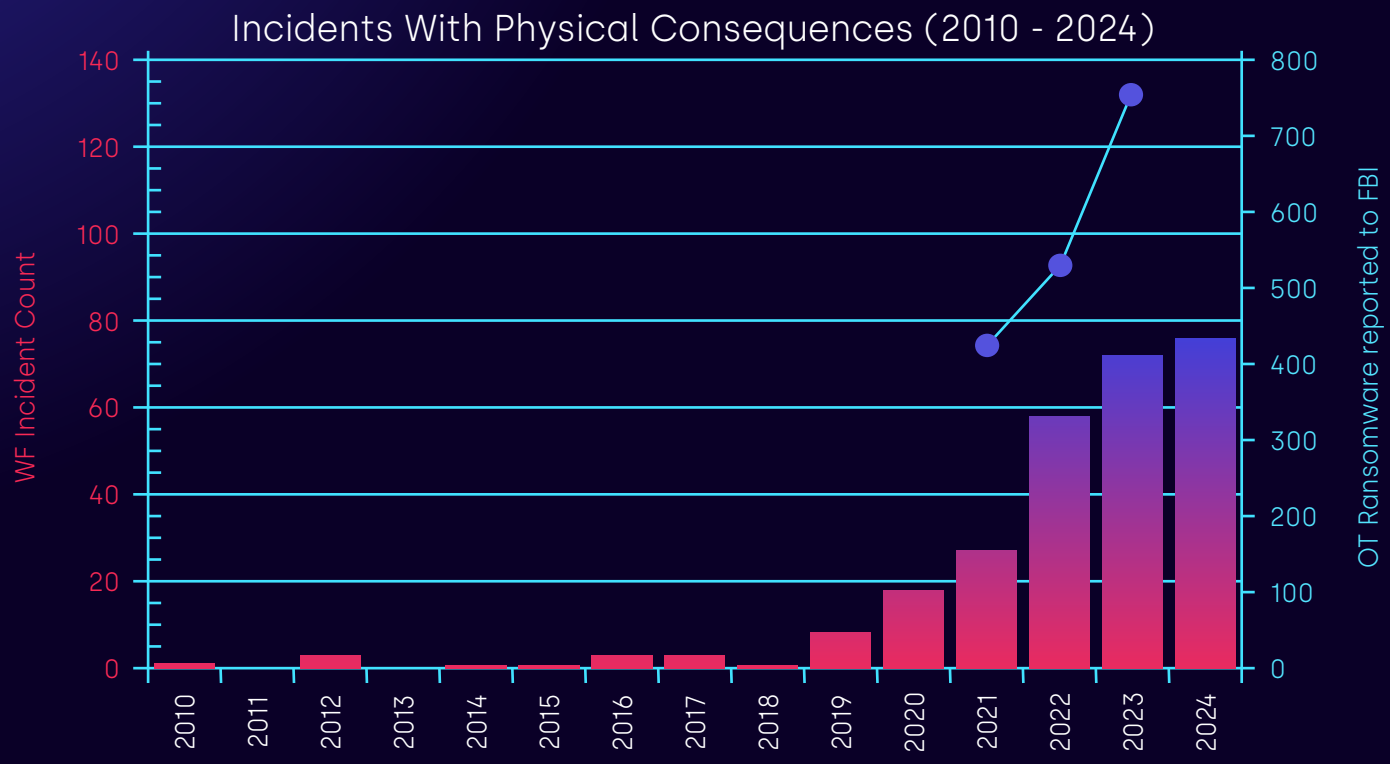


Figure 1: Incidents with physical consequences (2010 - 2024)

The complete count of attacks in the data set since 2010 is illustrated in Figure (1). Most of these attacks were ransomware. Most of the attacks impaired physical operations at multiple sites. For comparison, the line in the chart also indicates the number of OT ransomware incidents reported to the Federal Bureau of Investigation[1] for the years where this data exists[2], not all of which resulted in physical consequences.

In 2024, 87% of identifiable attacks were ransomware.

[1] Note that the scale for incidents with physical consequences is at the left of the chart, and the different scale for FBI-reported incidents is at the right.

[2] The FBI's IC3 group releases their annual report by mid-March, and so 2024 statistics are not available at the time of this report's writing.

For 2024, the ICS STRIVE OT incident repository also reported 390 incidents, not all of which met the inclusion criteria for this report. Readers interested in the broader set of incidents impacting businesses with physical operations should consult ICS Strive.

16hrs: The average time it takes between a ransomware criminal gaining remote control of some machine on a network and encryption activity starting. Half of attacks are even faster than that.

SEC Filings

What is the reason for the slowing rate of increase in OT security incidents? One likely factor is that in late 2023 the US Securities and Exchange Commission (SEC) started enforcing regulations that require publicly traded businesses to disclose "material" cybersecurity incidents; incidents that reasonable investors might use as cause to buy, sell or value shares in the victim company. Similar rules are already in place or are coming soon in many jurisdictions. These new rules for incident disclosures may well affect the number of incidents in the public record.

In December 2023, the SEC reduced somewhat the level of detail needed in these reports out of concern that too much public disclosure might either impede incident response or provide other attackers too much of a road map as to how to attack similar sites. On the other hand, the SEC is prosecuting businesses who fail to disclose cyber incidents adequately. In June 2024, the SEC accepted a $2.1 million civil penalty settlement offer from R. R. Donnelley & Sons in part for disclosure violations from 2021-2022, predating the new, even stronger disclosure rules.

New SEC & other incident disclosure rules may be reducing, rather than increasing, public reports of cyber attacks with physical consequences.

Given these new public disclosure rules in many jurisdictions, one might assume public reports of cyber attacks causing physical consequences would increase sharply during 2024 over 2023. But this was not the case. Why?

New disclosure rules may be prompting legal teams to get involved in cyber incident investigations earlier and requiring a minimal level of public disclosure. Following the prosecution of SolarWinds executives for improper disclosure of details of cybersecurity programs, legal teams may have decided to limit public reporting to only what is legally required to reduce the risk of similar legal consequences. If this is occurring, it would tend to reduce the number of non-material incident disclosures and reduce the level of detail published for potentially material incidents.

Nation States & Hacktivists

Nation state and hacktivist attacks both seek to bring about physical consequences with cyber attacks. This is in contrast with ransomware criminal groups who are financially motivated and generally seek to extort cryptocurrency. In ransomware attacks, physical consequences are most often accidental side effects of extortion attempts. While the numbers involved are still small, Figure (2) shows what appears to be a marked change in the frequency of hacktivist and nation state attacks since 2022 – attacks deliberately targeting physical operations and often critical infrastructures.

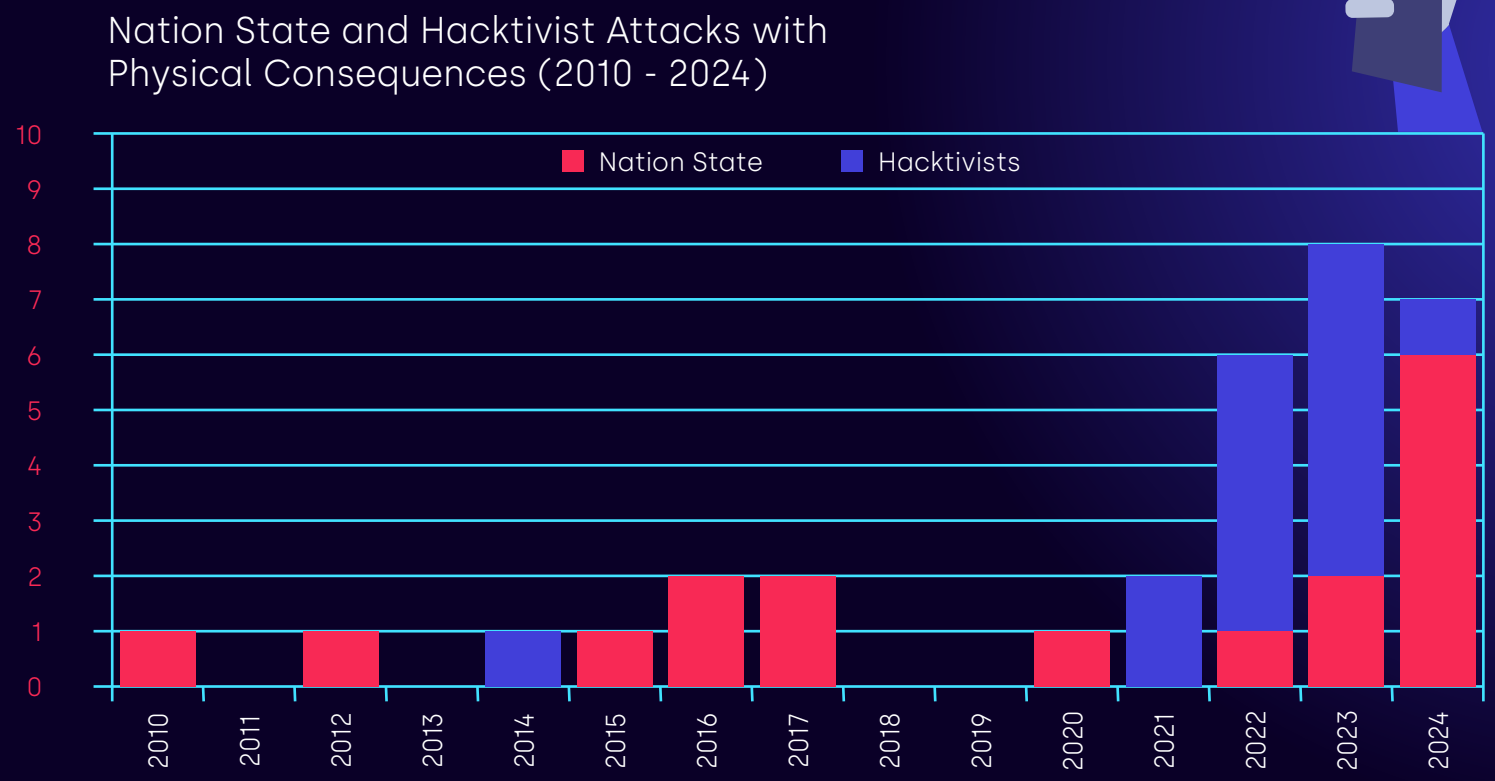


Figure 2: Nation state and hacktivist attacks with physical consequences (2010 – 2024)

Most attacks relate to three ongoing geopolitical conflicts:

1. The Russo – Ukrainian war
2. The Israel – Hamas (Iranian proxy) war
3. The Western Democracy-Chinese Grey Zone Conflict

> *"The greatest long-term threat facing our country, in my view, is represented by the People's Republic of China … which I consider to be the defining threat of our generation." … "[The] Chinese government [is] pre-positioning on American civilian critical infrastructure. To lie in wait on those networks, to be in a position to wreak havoc, can inflict real-world harm at a time and place of their choosing."*
>
> *FBI Director Christopher Wray*
>
> *Source: CBS News*

In 2024, we saw significant incidents and near misses in all three conflicts which are detailed in this report. In addition, sophisticated Russian and Chinese nation-state attacks are targeting a wide array of Western infrastructures, thus far without serious physical consequences. The most important development in 2024 regarding nation state attacks is the near-universal conclusion by Western intelligence agencies and governments that the ongoing threats from China are the most significant and of greatest concern. See the section "Volt Typhoon' and Salt Typhoon" for additional details.

Number Of Sites Impacted

There was a year-over-year increase of 146% in the number of sites impacted by attacks with physical consequences. The number of sites affected per incident is also increasing.

146% increase in sites impacted by cyber attacks with physical consequences.

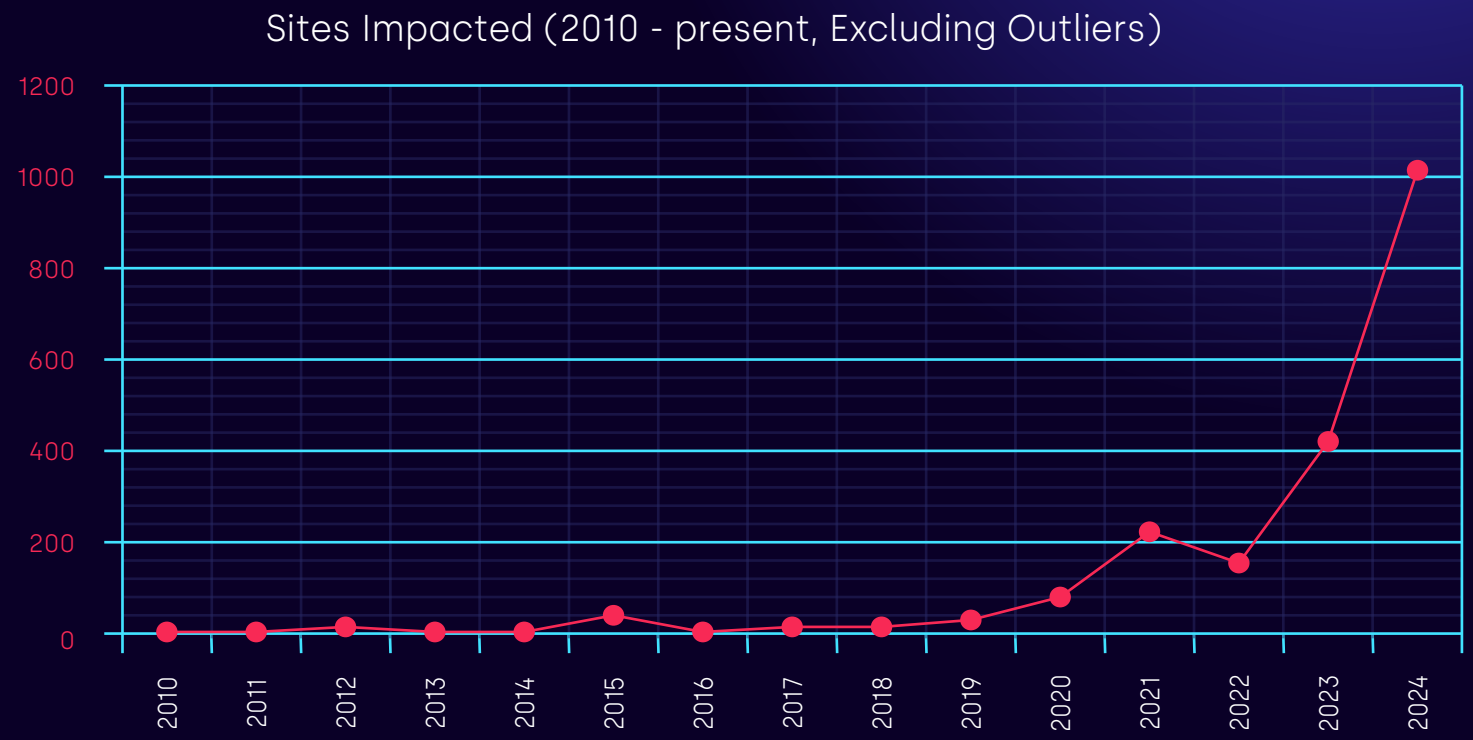


Figure 3: Number of Sites Impacted (2010 – 2024, excluding "outliers")

Figure (3) excludes "outlier" incidents where the concept of "number of affected sites" is unclear. For example, if the Russian military jams or spoofs GPS signals across a large region, how should we count the affected "sites"? Should every cell phone be counted? For a more detailed breakdown of site counts, see Appendix A.

Impacted Industries

Much like in 2023, 2024's cyber attacks with physical consequences, illustrated in Figure 4, continue to disproportionately impact the transportation and discrete manufacturing industries. In 2024, these industries make up 69% of all incidents. While transportation is the single biggest impacted vertical at 37% in 2024, transportation and discrete manufacturing have alternated in "first place" for the last three years.

69% of attacks with physical consequences hit the transportation and discrete manufacturing industries.

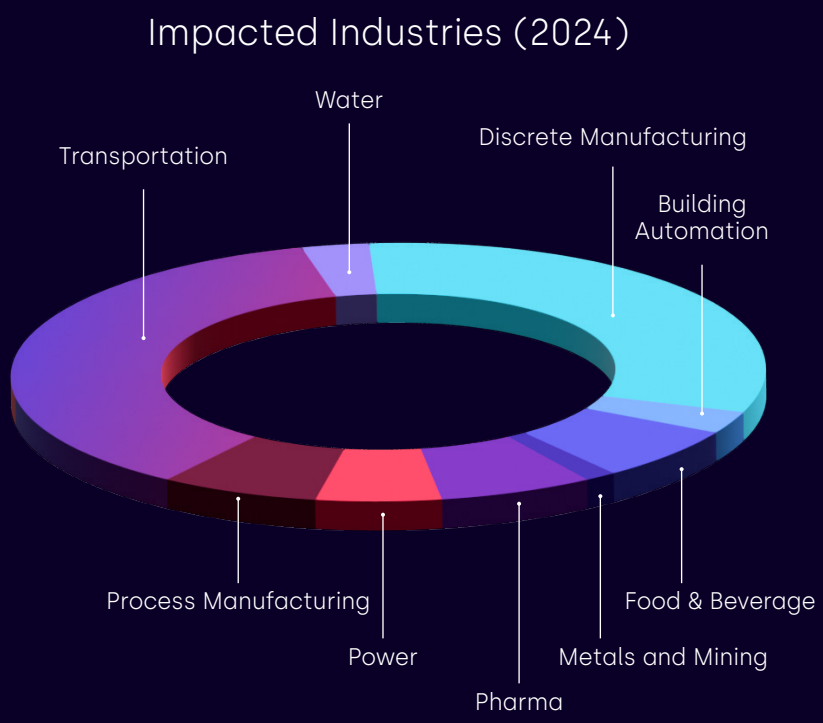


Figure 4: Industries Impacted (2024)

Attacks on North America's water and wastewater sector increased in significance and number in 2024. This report documents seven (7) new consequential attacks and near misses on water utilities. While the number of attacks causing OT impacts remained the same as last year (2 incidents), the overall threat level increased with all but one of the seven attacks attributed as nation-state sponsored. Five of the seven attacks in 2024 were attributed to Russia's Sandworm group, a group notorious for attacks on Ukraine's power grid. These attacks were part of a "grey zone" campaign where Sandworm masqueraded as hacktivists who called themselves the Cyber Army of Russia Reborn (CARR). See the 'Near Misses' section below for more information about attacks on water utilities.

Other industry trends:

- Both the power and metals & mining industries disclosed a small number of incidents this year (5 combined), with similar numbers last recorded in 2022 (6 combined).
- Incident counts remain steady in the process manufacturing, food & beverage, and pharmaceuticals verticals.
- 2024 saw two more incidents in automated "smart" buildings, both on the hospitality industry.
- The oil and gas sectors saw no new disclosed incidents in 2024.

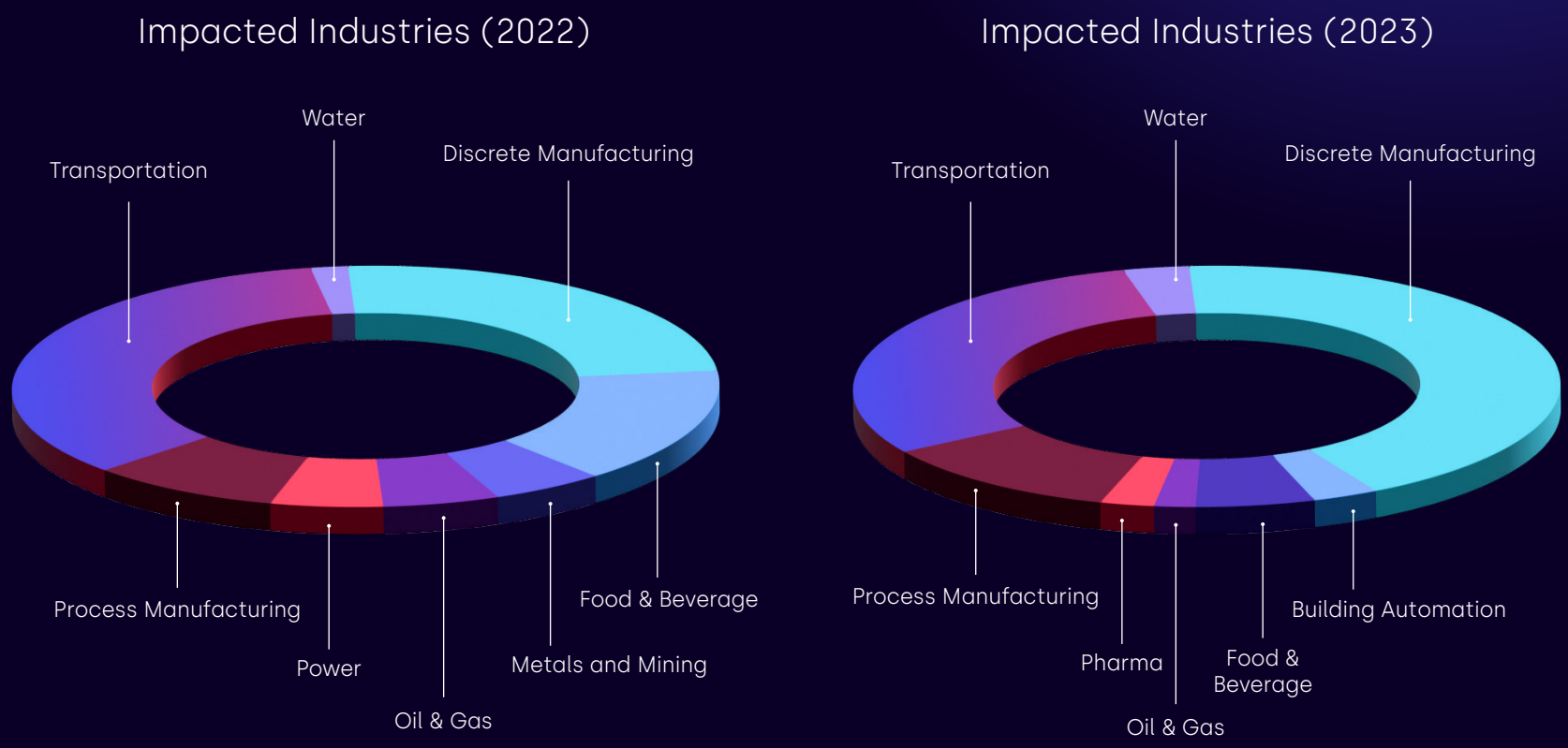


Figure 5: Impacted Industries (2022 & 2023)

Impacted Regions

Regionally, the USA and Germany suffered the largest number of incidents with physical consequences in 2024, in first and second place respectively, followed by Japan, the UK and Canada.

> The USA and Germany suffered the largest number of incidents with physical consequences in 2024.

While the reasons for these regional numbers and trends are unclear, it may be that criminal ransomware is exploring new territories with strong economies and a willingness to pay ransoms, or it may also be that politically supported ransomware criminals and nation state threats are strategically targeting victims in the US, Europe, and Asia-Pacific.

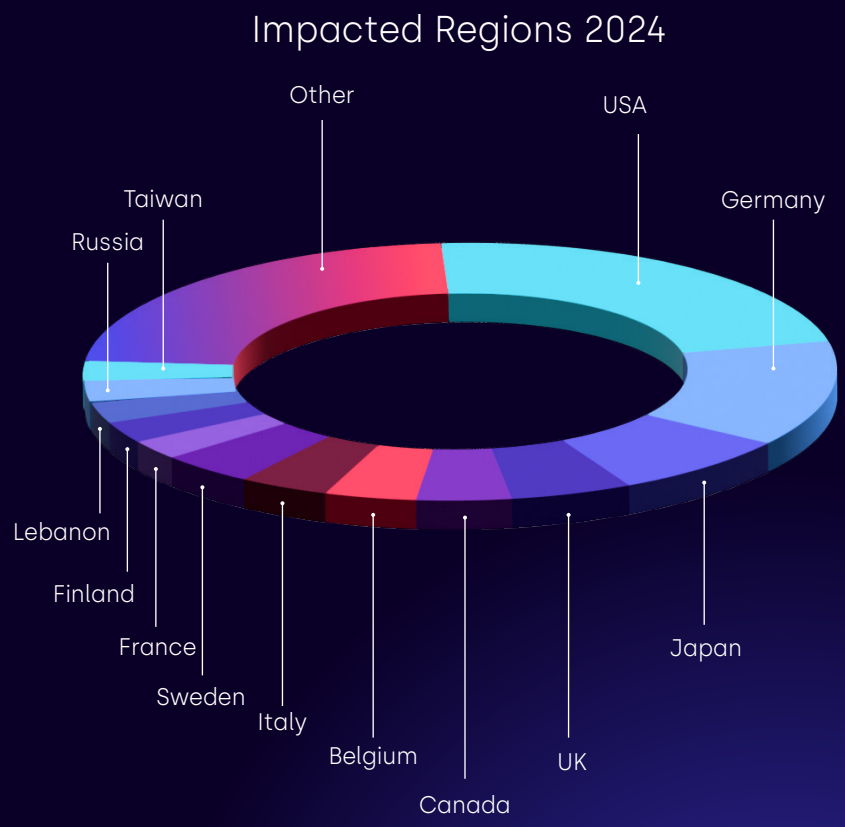
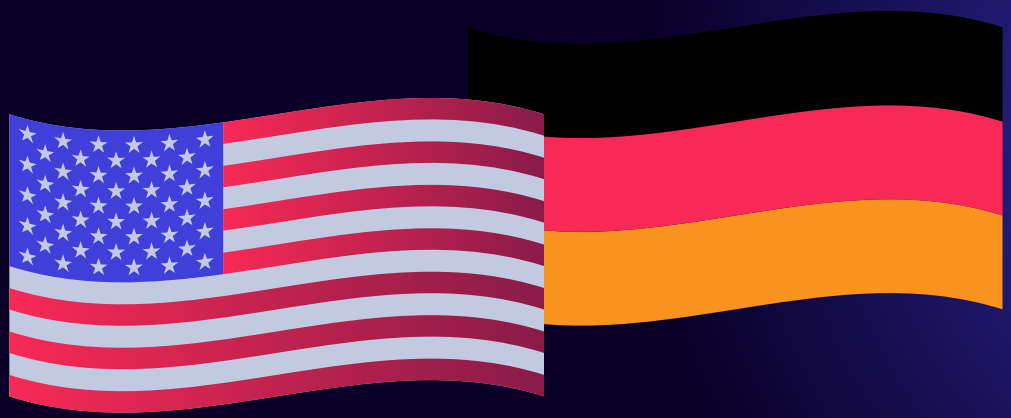


Figure 6: Impacted Regions (2024)



How was OT Impacted?

For attacks where the attack pattern could be determined from public records, 13% of attacks with physical consequences directly impacted OT automation systems. Nearly 90% of attacks caused physical consequences indirectly. This is very similar to data from 2023.

Almost 90% of indirect attacks on OT had physical consequences.

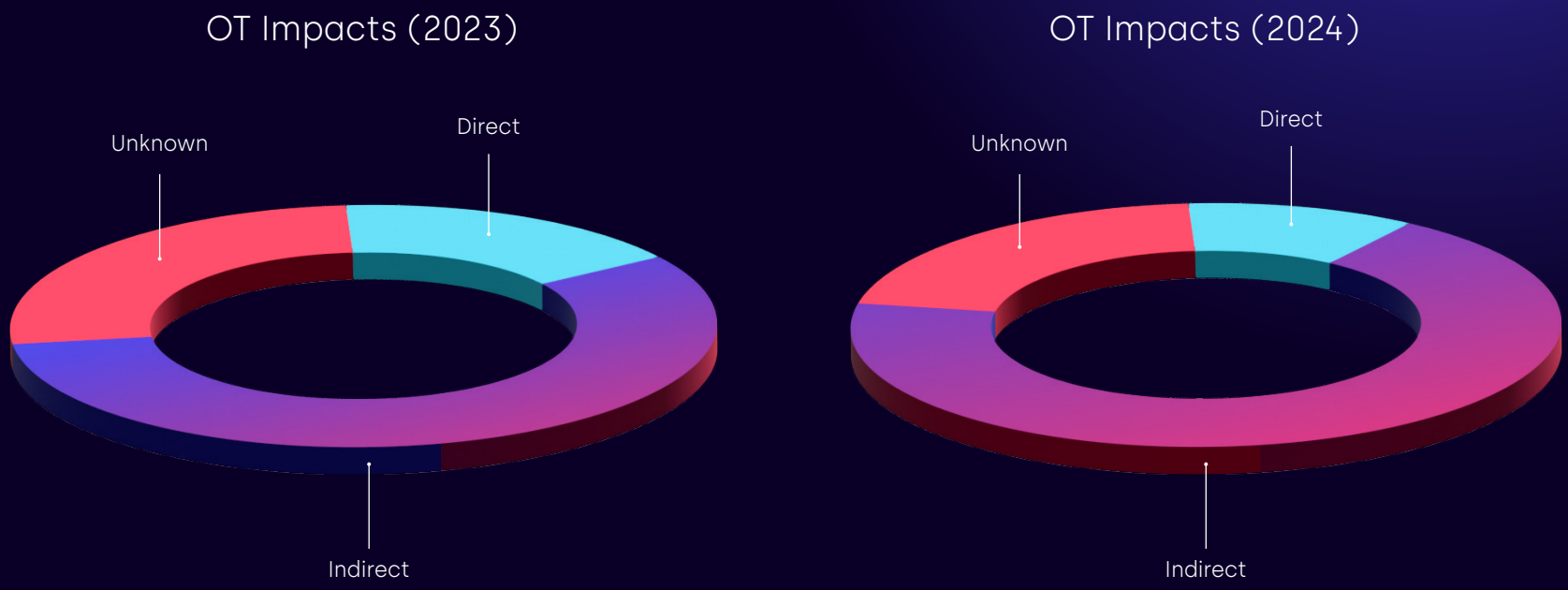


Figure 7: How cyber attacks caused physical consequences (2023 & 2024)

To generally clarify how these types of attacks are defined:

- **Direct attacks** are those where malware was found on OT systems or impacted OT systems directly, or where remote-controlled attacks reached into OT systems to sabotage them or shut them down.
- **Indirect attacks** are those where there was no direct impact on OT systems, but physical operations still suffered physical consequences because operations depended on access to or services from impaired IT systems.
- **Unknown attacks** are incidents where there was not enough detail in the public record to determine how the attack impaired operations.

Analyzing the entire 2010-2024 data set in more detail, we determine there are eight ways in which physical operations have been impacted – five direct and three indirect, namely:

Direct attack types:

1. **Attacks on OT** are local or remote attacks where attack software or manual attack actions directly affect OT automation systems or networks.

2. **Poor segmentation** are attacks where there is no evidence the OT network is distinct from an IT network – i.e. the network is "flat" – so any attack on IT is also an attack on OT.

3. **IT pivoting attacks** first compromise IT assets and then use the compromised assets to attack other IT or OT assets.

4. **Supply chain attacks** are where a threat actor surreptitiously inserts malware or vulnerabilities into software or firmware for assets deployed on OT networks.

5. **Malicious insiders** are where an insider uses their credentials and/or position of privilege to attack OT systems.

Indirect attack types:

6. **Abundance of caution shutdowns** occur when an attack compromises IT systems and the business pre-emptively shuts down OT systems for safety reasons, to reduce risk, to preserve forensic evidence, on the advice of third parties, or for other reasons.

7. **IT dependencies** are where OT systems or physical operations depend on services provided by IT networks and servers, and those IT assets are impaired or crippled by a cyber attack.

8. **3rd party** outages where an enterprise suffers no cyber attack, but one of their suppliers does, and the loss of production, or loss of trust in the supplier, or other consequence of the compromised supplier cause the affected enterprise to reduce, delay or halt production.

Of all the attacks in our data set (2010-2024) where the attack type could be determined reliably from the public record, OT shutdowns due to "abundance of caution" and OT dependencies on IT networks were the most common ways that attacks on IT networks impacted operations. When attacks deliberately targeted OT – Direct OT attacks – nearly all those attacks were attributed to either hacktivists or nation state threat actors.

Nearly all Direct OT attacks are attributed to either hacktivists or nation-state threat actors.

Implications For Cybersecurity Programs

What does this mean for cybersecurity programs? A naïve interpretation might suggest that, since most attacks with physical consequences target IT networks, incremental spend on cybersecurity programs should focus primarily on strengthening IT networks. However, the authors of this report argue that this interpretation is flawed for several reasons.

> IT networks are constantly exposed to the Internet, making them intrinsically vulnerable. Safety-critical networks require a level of security that goes beyond what is possible for IT networks.

1. Safety-critical OT networks must be designed and secured to be extremely robust in the face of all possible inputs and threats. IT networks are exposed to constant interaction with the Internet and thus it is not possible to secure IT networks to the extent that safety-critical networks must be secured. Furthermore, there is a general expectation that less-consequential IT networks can be more flexible about network and cybersecurity program designs than OT networks, but this flexibility and its benefits vanish if we demand they be secured to safety-critical standards.
2. The best way to eliminate "abundance of caution" shutdowns (attack type #6) is to strengthen OT security programs, and especially protections at the IT/OT interface to the point where it becomes practically impossible for cyber attacks to pivot from IT networks into OT networks.
3. The best way to eliminate "IT dependency" shutdowns (attack type #7) is to understand dependencies and take steps either to eliminate those dependencies, or to put network engineering and incident response measures in place to reduce to acceptable levels all cyber incident downtime for reliability-critical IT components.

> It should be physically impossible for cyberattacks to pivot from IT networks into high-consequence OT networks.

The norm today in industrial enterprises is IT cybersecurity programs are much more mature than OT cybersecurity programs. It is in this context that we observe cyber attacks with physical consequences nearly doubling annually. Doubling down on this practice of continuing to emphasize IT protections over OT will not reduce the slope of the OT incidents curve (in Figure 1).

Incident Costs

While costs continue to be difficult to identify, there were some noteworthy costs that were disclosed or could be calculated in 2024. In one high-profile attack, OT systems and services provider Halliburton had IT systems taken offline. The company has not shared many details about the attack, causing other customers to disconnect from Halliburton due to the lack of details provided. To date, costs related to the attack total a reported $35 million.

In another case, global contract manufacturer, Keytronic, reported an incident in May after disruptions at its Mexico and U.S. sites impacted business applications supporting operations and corporate functions. Keytronic was forced to shut down domestic and Mexican operations for two weeks during the incident response. To date, the attack has cost Keytronic over $17 million. The Stoli Group USA filed for Chapter 11 in US Bankruptcy Court after a malicious cyber attack forced the company to operate its global business manually while the systems are rebuilt. While there were multiple reasons for the bankruptcy, the cyber attack was cited as a top reason.

Supply Chain – CrowdStrike Incident

The July 2024 CrowdStrike failure was not a cyber attack, but the incident highlighted many industries' vulnerability to supply chain attacks. The incident was a defect in a software update pushed out to customers configured for automatic updates, causing some 8.5 million devices to crash and have difficulty rebooting. Thousands of flights were cancelled, Tesla halted production at a large factory for four hours, the Port of Houston closed briefly, and a Swedish mine briefly shut down and evacuated as a precaution, just to name a few.

> When worst-case consequences are unacceptable, all non-trivial changes and updates must be tested and evaluated for security as well as reliability.

The obvious lesson widely drawn from the incident is, when the consequences of malfunction or unavailability of computer equipment and networks are unacceptable, owners and operators should test software and security updates for reliability before deploying those updates. As the 2020 SolarWinds incident showed, however, the same lesson should be applied to malicious cyber attacks. All changed software or non-trivial updates must be tested and evaluated for security as well as reliability, to prevent malicious updates from impairing operations.

Cost estimates of the CrowdStrike incident to IT & OT owners and operators range from $5 billion to $10 billion.

Global Navigation & IRS Jamming and Spoofing

The 2024 data set includes three navigation system jamming and spoofing events, colloquially called "GPS" events[3]:

- Finnair cancelled all flights between Helsinki and Tartu, Estonia for 6 weeks because widespread GPS spoofing made the route unsafe, and until a certified alternative navigational system could be deployed.
- GPS jamming contributed to the crash of Azerbaijan Airlines Flight 8243 near Aktau, Kazahkstan and the death of 38 passengers.
- A nearly 64-hour stretch of GPS jamming over Poland, Sweden and Germany in March affected 1600 flights with Russia considered the prime suspect.

GPS jamming affected 1,600 flights over Poland, Sweden, and Germany in 64 hours.

Despite an international treaty banning GPS jamming, Russian forces routinely jam and spoof satellite navigation signals. Furthermore, while Inertial Reference Systems (IRS) are back-ups for GPS signal loss in many aircraft, IRS can be confused by GPS spoofing.

Many IRS use the higher accuracy of GPS positioning to periodically reset their internal position estimates to account for drift over time and other errors in the aircraft's position. Thus, when GPS signals are spoofed rather than jammed, IRS systems reset their own understanding of their current location to match the spoofed (false) GPS locations, causing potentially serious safety problems.

Owners and operators of systems that rely on GPS are advised to have plans in place to both detect and ride through GPS outages and falsified GPS signals.

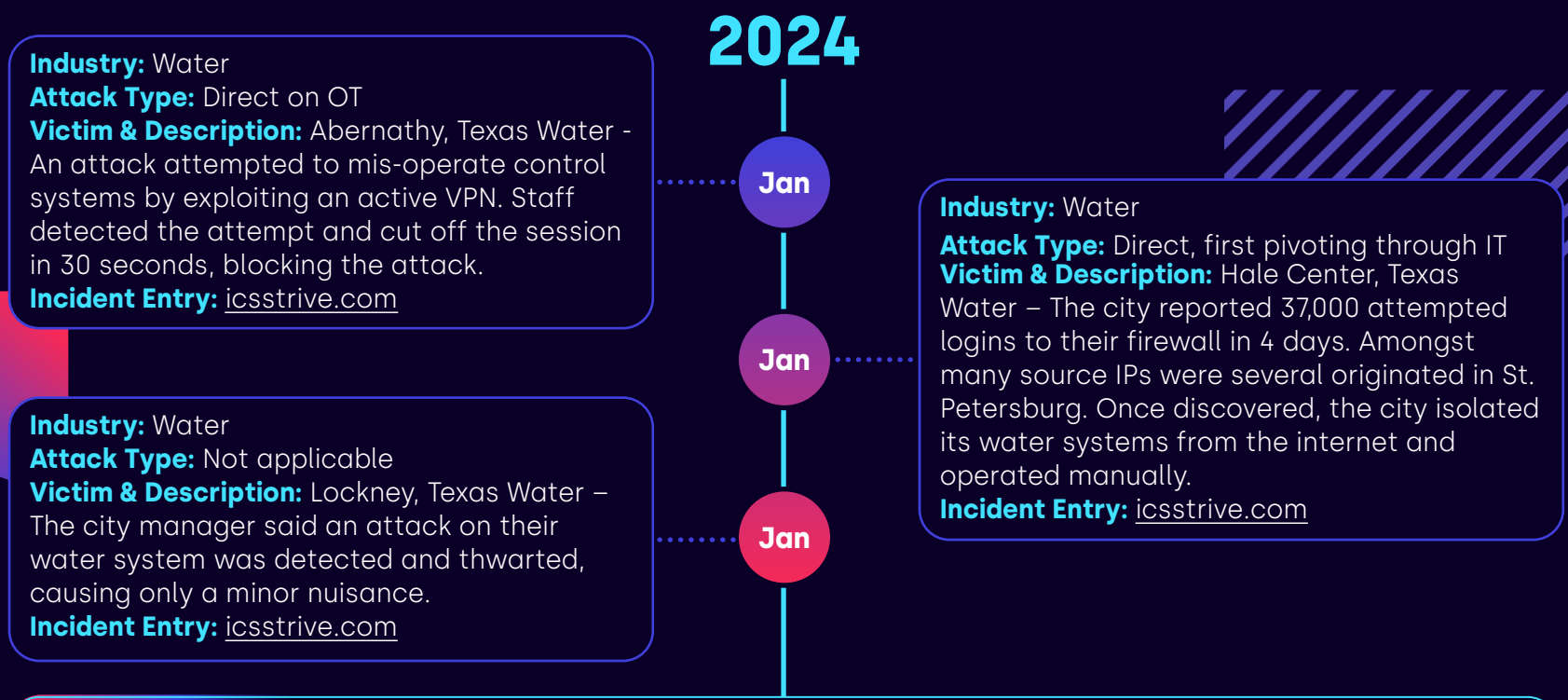
[3] When we use the acronym "GPS" in the report, we mean all satellite navigation which is termed global navigation satellite systems (GNSS). This includes the US GPS, EU Galileo, Russian GLONASS, and China's Beidou.

Near Misses

While near misses are not the focus of this report, we select and report on eleven such attacks that were significant indicators of threat activity.

For example, Sandworm (or CARR) attacks on water utilities appear to have come short of causing significant consequences. In Muleshoe Texas, however, they did cause water tanks to overflow for 30 minutes. After these incidents, credible evidence emerged from Google's Mandiant team revealing that CARR was directly supported by Unit 74455 of Russia's GRU military intelligence directorate.

In several of their attacks, CARR bragged and taunted their victims on Telegram and social media that they could have done much worse. These types of nation state attacks are often called grey zone attacks and are becoming more frequent. Grey zone attacks are often multiple incidents in sophisticated campaigns that are well resourced and deliberately planned to test an opponent's defenses and response time. These new nation-state grey-zone campaigns are like the aircraft sorties that routinely test an opponent's control over their air space. In such sorties, military aircraft routinely and deliberately fly along the edge of an opponent's airspace to test response times, strength, and other defensive capabilities and tactics. More frequent grey zone attacks do not necessarily imply physical conflict between nations are imminent, but they do represent an escalation in threat and risk to OT systems that should not be ignored.



Apr

Industry: Water
Attack Type: Direct, first pivoting through IT
Victim & Description: Tipton Municipal Utilities (TMU) -- Sandworm-linked group CARR infiltrated and claimed to have mis-operated an operator's HMI controlling the water treatment process. The utility reports remaining operational.
Incident Entry: icsstrive.com

June

Industry: Telecom
Attack Type: IT only
Victim & Description: SingTel -- Systems were breached in Singapore by Volt Typhoon group in an ongoing campaign against the USA and their allies. Experts believe this was a test-run for future attacks on the USA.
Incident Entry: icsstrive.com

Sep

Industry: Transport
Attack Type: Not applicable
Victim & Description: German Air Traffic Control (DFS) -- DFS suffered a cyber attack by Russia's Fancy Bear nation state threat actor. While no physical consequences occurred, and few details were released the threat actor's capabilities are so high this counts as a credible near miss.
Incident Entry: icsstrive.com

Sep

Industry: Water
Attack Type: Unknown
Victim & Description: Arkansas City Water -- Water treatment at Arkansas City reverted to manual operations in a cyber attack attributed to ransomware.
Incident Entry: icsstrive.com

Oct

Industry: Power
Attack Type: Unknown
Victim & Description: Fortum Oyj -- Finland's largest company owning and operating over one hundred hydro, CHP, condensing, nuclear, solar and wind generating plants reports daily attempts to penetrate their cyber systems and reported finding many drones hovering over their critical infrastructure sites.
Incident Entry: icsstrive.com

Oct

Industry: Telecom
Attack Type: Not applicable
Victim & Description: 21 global telcos -- Described as the "worst telecom hack" in history, a new Chinese nation state threat actor is found to have deeply penetrated telecom networks as far back as two years ago in dozens of countries. This campaign exfiltrated call metadata, text messages, and audio content for over 150 top US officials including Trump, Harris and Vance running in both presidential campaigns.
Incident Entry: icsstrive.com

Nov

Industry: Oil & Gas
Attack Type: Unknown
Victim & Description: RECOPE -- After a ransomware attack hit Costa Rica's state energy company, safety concerns were cited as the reason for switching to manual operations. This impacted service quality for loading and unloading cargo terminals, at both land (trucking) and sea (tankers).
Incident Entry: icsstrive.com

Dec

Industry: Oil & Gas
Attack Type: Not applicable
Victim & Description: Lukoil -- Cyber specialists of Ukraine's Main Intelligence Directorate (HUR) carried out a cyber attack on Russian oil company Lukoil, which impacted online and retail POS payments at the pumps and during the holiday shopping season.
Incident Entry: icsstrive.com

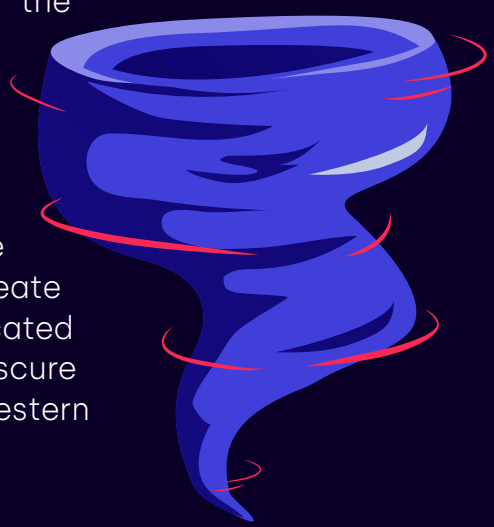
Volt Typhoon and Salt Typhoon

Other significant grey zone attack campaigns either disclosed in 2024 or continuing into 2024 include two significant campaigns by China. Western intelligence agencies and governments have repeatedly expressed alarm and have declared these the most significant threats to their national security. They include ongoing campaigns by two threat actor groups:

Volt Typhoon

Now recognized as a campaign of nation state attacks on privately-owned critical infrastructure in service and supply agreements to US government and global military operations:

- Early in 2024, the FBI obtained a rare court order to silently clean malware from devices owned by US citizens and organizations, and declared the infections eradicated.
- The FBI, however, cannot clean botnets from non-US owned devices and asked the wider public to be aware of the threat. The threat actor(s) then attempted to maintain persistence in the targeted networks.
- In the summer of 2024, the SingTel (Singapore) breach exposed efforts by the threat actor to create a SE Asia – located pivot point to obscure attack traffic on Western networks.



"Living off the land" attacks operate by remote control without using RAT malware. Instead, the attackers use normal tools built into operating systems to attack other systems. This makes attacks extremely difficult to detect because anti-virus software shows no malware on the machines, only the normal operating system tools.

Salt Typhoon

A campaign on telecommunication infrastructure was exposed in the USA and dozens of other nations, persisting in networks dating back at least two years:

- The attacks not only perpetrated widespread metadata collection but also carried out targeted communications interception on the highest levels of government, including Democratic Presidential candidate Kamala Harris, Republican Presidential candidate Donald Trump, and Republican Vice-Presidential candidate JD Vance in the 2024 presidential campaign.
- It's unclear how Salt Typhoon did this. Did they penetrate telecom switches and backbone routers? Did they install malware? Was this a supply chain attack or work of malicious insiders?
- Telecom is a type of OT that this report does not explicitly track, but the industry's equipment, expected system reliability, and importance to national security and public safety parallels that of industrial control systems.

The Volt Typhoon attack was also noteworthy in that it was a so-called "living off the land" attack. Such attacks operate by remote control but do not deploy the Remote Access Trojan (RAT) malware that is typically used to maintain remote control. Instead, the attackers use facilities built into the operating systems of compromised IT machines to maintain remote control. This makes the attacks extremely difficult to detect, because any anti-virus or other scan of the affected machines showed no malware resident on the machines, only normal operating system tools.

Volt Typhoon was seen reaching into OT networks and then pulling back to its IT persistence base. The consensus of US intelligence agencies is that the Chinese government is using these footholds in IT networks of US government-linked utilities to establish and maintain a capability to act in future kinetic conflicts.

New ICS-Capable Malware

2024 saw the discovery of three new ICS-capable malware variants. This is a material increase to the six such malwares discovered in the preceding 14 years (2010-2023):

- **2010:** Stuxnet – cyber-sabotage – autonomous malware destroyed~1000 uranium gas centrifuges
- **2013:** Havex – cyber-espionage – remote access trojan (RAT) with OPC scanning capabilities
- **2016:** CrashOverride – cyber-sabotage – RAT with the ability to issue commands in four ICS protocols, depending on the version of the malware – turned off the power to Kiev for an hour.
- **2017:** Triton – cyber-sabotage – RAT with the ability to write to SE Triconex Safety Instrumented System controllers – malfunctions triggered safety shutdowns at two petrochemical sites
- **2022:** Pipedream – cyber-sabotage – a RAT with a "Swiss army knife" of ICS hacking tools that was detected before it caused physical consequences
- **2023:** CosmicEnergy – cyber-sabotage – a RAT able to write IEC 60870-5-104 commands, though it may have been used only as an educational tool for Russian penetration testers
- **2024:** FrostyGoop – cyber-sabotage – a RAT able to write Modbus TCP commands – disrupted heating to 600 apartment buildings in Ukraine
- **2024:** IOControl – cyber-sabotage – a RAT targeting ARM-based Linux IoT devices – disrupted fuel pumps in thousands of Iranian gas stations
- **2024:** Fuxnet – cyber-sabotage – autonomous malware that carried out denial of service attacks via Meter-Bus (MBus) RS485 communications and bricked over 500 sensor gateways by repeatedly writing to their NAND-flash firmware repositories.

With discoveries of this kind of malware, ICS-capable malware is becoming an increasingly credible threat to industrial operations.

Three new ICS-capable malware variants were discovered in 2024, compared to just six found in the previous 14 years.

Defensive Developments in 2024

Tools, techniques and perspectives for defending industrial control systems continue to evolve as well. In the sections below, we sample three highlights of 2024.

> The multi-agency report Modern Approaches to Network Access Security now recommends hardware-enforced remote access for high-consequence OT networks, rather than VPNs and jump hosts.

Hardware-Enforced Remote Access

American, Canadian and New Zealand authorities issued a joint publication Modern Approaches to Network Access Security. The document is designed to improve remote access to both IT and OT networks. For example, for the first time these authorities recommend moving away from the traditional VPN and jump host designs that are still the foundation for other advice, including the NERC CIP 005 standard. The agencies encourage owners and operators to adopt more powerful techniques. The document recommends a range of Zero-Trust Cloud-based Tech for IT networks and low-consequence OT networks.

For high-consequence OT networks, the guide recommends hardware-enforced network segmentation, such as is provided by unidirectional gateway technology. For remote access into unidirectionally protected networks, the guide recommends:

- For attended OT sites, a timed hardware switch in series with the above-recommended software protections provides OT sites with physical control over when and for how long software-mediated remote access is enabled.
- Again, for attended OT sites, unidirectional remote screen view transmits real-time screen images through unidirectional hardware to remote service providers. Those providers can then interact with on-site personnel, usually over the phone, providing real-time advice to diagnose and correct complex problems.
- For unattended remote access to OT sites, the guidance recommends hardware-enforced remote access systems with independent unidirectional hardware control channels for keystrokes and mouse movement that are separate from and independent of unidirectional monitoring channels for screen images.

In all cases, the new recommendations specify remote access solutions that are much stronger than VPN and jump host technology.

OT Security Principles

The Principles of Operational Technology Cybersecurity is a joint publication of 16 government agencies in nine nations. The document is significant, in part because of the endorsement of the same set of concepts by such a wide array of agencies and nations, and in part because of the engineering-centric nature of the principles outlined there.

Many statements in this high-level document echo concepts in the Cyber-Informed Engineering (CIE) initiative – precisely the mix of engineering risk management and cyber risk management concepts that is being so well received by engineering and enterprise security teams in so many businesses with physical operations.

The first principle in the document for example is that safety is paramount – not confidentiality, integrity or availability of data. The document asks questions never before seen in government guidance – questions such as "If software is essential to the safety of a physical process, and there is a real risk that an adversary has taken over that software, how will the organization assure the safety of incident responders sent to the site to investigate the breach?" And the guidance acknowledges the importance of deterministic protections in addition to software-based protection.

> If software is essential to the safety of a physical process, and there is a real risk that an adversary has taken over that software, how will the organization assure the safety of incident responders sent to the site to investigate the breach?

The document is ground-breaking in that it is the first time that such a wide array of agencies and authorities have issued cybersecurity guidance with such a strong engineering focus and with such a clear explanation of the role of engineering principles, tools, and approaches in cybersecurity programs.

Credibility, not Likelihood

A key principle of CIE is that risk management should start with the highest-consequence threats, not the highest-frequency threats. To reflect this emphasis, a number of standards bodies and authorities that issue OT risk assessment and risk management guidance are considering a change to the terminology of their publications, focusing on the concept of "credibility" rather than "likelihood."

> Threats that were not considered credible a decade ago are now pervasive.

Standard thinking about cyber risk holds that given enough time, money and talent, any defensive posture can be breached by a sufficiently sophisticated attack. In our 2024 data we observe that attacks are becoming increasingly sophisticated.

Types of attacks that were not considered credible threats a decade ago have become pervasive. Effective discussion and decision making about sophisticated, high-consequence threats demands that decision-makers decide what types of attacks and consequences constitute credible threats to physical operations today and in the near future, and what defenses are reasonable to implement, given these credible threats.

The research team looks forward to much greater use of words like "judgement," "reasonable," and "credible" in future standards and guidance.

Conclusion

With only a small increase in incidents that caused physical consequences, one might be tempted to argue we are winning the cyber war, at least on OT networks. In fact, the sophistication and capabilities of our adversaries continue to increase with near-miss/living-off-the-land techniques applied at over 50 utilities, a steadily increasing number of impacted sites, and one third as many new ICS-focused/ICS-capable malware discoveries in 2024 as in all the previous decade and a half.

Increasingly capable cyber attacks are becoming credible threats. Owners and operators are advised to re-evaluate what threats they regard as credible today, as well as threats which are likely to become credible in the years ahead, and take reasonable actions to address those credible threats.

Owners and operators are advised to re-evaluate what threats they regard as credible and take reasonable actions to address those threats.

APPENDIX A – The Complete Data Set

Field Descriptions

Date: Date the incident was detected or occurred.
Victim: The impacted organization's name.
Region: Region of impacted sites. When sites are impacted in multiple regions, the region of the head office is reported.
Industry: Industry of the affected sites.
TA = Threat Actor: The type of threat actor, one of:

- R: Ransomware
- H: Hacktivist
- I: Insider
- NS: Nation state
- SC: Supply chain
- U: Unknown

Attribution: Specific threat actor publicly reported or claimed responsibility.

Sites: Total number of sites affected.
Cost: Lower-bound estimate of financial impact on victim organization, in USD unless otherwise indicated.
FD = Financial Disclosure: Entity to which financial disclosure was required or made, if any:

- SEC: Securities and Exchange Commission (US),
- NSE: National Stock Exchange (Mumbai, India),
- EU MAR: Market Abuse Regulation No 596/2014 Article 17 (EU),
- LSE: London Stock Exchange (UK).
- PIPC: Personal Information Protection Commission (Kojin Jōhō Hogo Iinkai)
- TASE: Tel Aviv Stock Exchange (הַבּוּרְסָה לְנְיָירוֹת עֵרֶךְ בְּתֵל אָבִיב)

Type = OT Attack Type: How the attack caused physical consequences:

- DO: Direct, on OT – malware or threat actor manipulated OT systems,
- DS: Direct, poor segmentation – no separate OT network existed,
- DIP: Direct, IT pivot – an attack "pivoted" through compromised IT assets to attack OT assets,
- DSC: Direct, supply chain – the attack inserted malware or vulnerabilities into products deployed on OT networks,
- DM: Direct, malicious insider – an insider used their credentials or privilege to bring about physical OT consequences,
- IA: Indirect, abundance of caution – the victim shuts down physical operations pre-emptively after the attack was detected,
- ID: Indirect, IT dependency – physical consequences were realized when only IT systems were compromised, because physical operations depended on one or more IT systems or services, and
- I3: Indirect, third party – victim suffered no cyber attack but shut down because a supplier was attacked.

OT / ICS Physical Consequences: how the victim suffered.
Incident Summary: summary of what happened.
References: Links to public reports on the incident.

Incidents in 2024

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-01-07	Beirut (Rafik-Hariri) Int'l Airport	Lebanon	Transport	U	Unknown	1			U	Disrupted the Flight Information Display System (FIDS) network and reduced the Baggage Handling System (BHS) to 20% capacity for 10+ days	A breach of the airport's cybersecurity resulted in baggage belts malfunctioning and a hostile message to Hezbollah showing on screens meant to display flight details. A source at national airline MEA confirmed the Flight Information Display System (FIDS) network had been penetrated.	https://icsstrive.com/incident/cyberattack-on-beirut-airport-lebanon/ https://today.lorientlejour.com/article/1364771/lasting-consequences-at-beirut-airport-following-cyberattack.html https://today.lorientlejour.com/article/1363591/cyberattack-at-beirut-airport-what-happened-and-what-are-the-potential-risks.html
2024-01-18	Muleshoe, Texas Water	USA	Water	NS	Cyber Army of Russia Reborn [CARR] & Sandworm [GRU Unit 74455] (Russia)	1			DIP	Impacted operations by mis-operating the control system and causing water tanks to overflow for 30+ mins	Originally attributed to hacktivist group CARR, Sandworm-supported hacktivists bragged online about their attack on Muleshoe's ICS. Mandiant/Google published detailed analysis linking CARR to nation-state group Sandworm and the Russian GRU. In late July, the US Treasury sanctioned Yuliya Pankratova and Denis Degtyarenko, holding them responsible for this incident and a series of similar "unsophisticated" attacks on critical infrastructure in the US and the EU.	https://icsstrive.com/incident/cyberattack-on-three-rural-texas-water-facilities/ https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/ https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm https://therecord.media/cyber-army-russia-us-sanctions
2024-01-20	Tietoevry Oyj / Rusta	Finland, Sweden, Norway, Germany	Transport	R	Akira	200	30M kr.		I3	Impacted logistics (inventory tracking and replenishment) and order fulfilment, materially impacted sales, for 2+ wks	Finnish cloud service provider Tietoevry was hit by a ransomware attack, which impacted their customers like Rusta. Rusta, a discount hard goods retailer, relied on Titoevery for all business functions including supply chain (logistics) management.	https://icsstrive.com/incident/numerous-customers-suffer-from-ransomware-attack-at-cloud-provider-tietoevry/ https://www.bleepingcomputer.com/news/security/tietoevry-ransomware-attack-causes-outages-for-swedish-firms-cities/ https://investors.rusta.com/en/rustas-business-systems-are-fully-operational-after-disruptions/ https://investors.rusta.com/en/update-on-operational-disruptions-in-rustas-it-system-2/

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-01-22	Lvivteplo energo	Ukraine	Power	U	FrostyGoop (Unknown)	600			DIP	Disconnected heating services to 324 "heating points" or 600 homes in Lviv's Sykhiv neighbourhood for 2 days	In July, a novel malware called FrostyGoop was found by Dragos to be exploiting a zero day in internet-facing Mikrotik routers at an un-named heating utility. This malware is reportedly the first to send Modbus commands directly into the victim's network to mis-operate ENCO controllers, among other capabilities. It is also uniquely located on the threat actor's systems, and not deployed in the victim's network, making it harder to detect. Ukraine's SBU confirmed FrostyGoop malware was responsible for this attack. Andy Greenberg (Wired) notes how attack TTP bears hallmarks of Unit 74455 of the GRU (Sandworm), but this cannot be confirmed.	https://icsstrive.com/incident/malware-caused-ukranian-energy-company-to-disconnect-heating-services-impacting-over-100000-people/ https://www.sans.org/blog/whats-the-scoop-on-frostygoop-the-latest-ics-malware-and-ics-controls-considerations/ https://www.wired.com/story/russia-ukraine-frostygoop-malware-heating-utility/ https://www.epravda.com.ua/news/2024/01/23/709063/
2024-02-02	Etesia SAS	France	Discrete Mfg.	R	Unknown	1	€100K		ID	Shutdown production for 2+ months, and placed the company into receivership for 6 months	A small equipment machinery manufacturer was hit by a cyberattack that caused its systems to be encrypted. This prevented systems, essential to production, from working.	https://icsstrive.com/incident/french-ride-on-mower-manufacturer-tries-to-recover-from-ransomware-attack/ https://www.servicedealer.co.uk/latest-news/etesia-suffer-crippling-cyber-attack https://www.linkedin.com/posts/etesia-uk_etesia-uk-statement-were-pleased-to-announce-activity-7178434317021286402-3xMb/ https://www.lesechos.fr/pme-regions/grand-est/espaces-verts-etesia-tente-de-se-relever-de-sa-cyberattaque-2087045
2024-02-02	Welch Food	USA	Food & Bev.	R	Unknown	1			ID	Shut down operations for 1 month and sent 200+ workers home	An unknown TA, alleged to be a "criminal group", attempted to extort Welch by encrypting plant systems critical to their juice, jam and jelly production. These critical systems were essential to operations at their North East (lit.) plant in Erie County, PA.	https://icsstrive.com/incident/weeks-of-operational-shutdown-at-welch-foods-plant https://www.goerie.com/story/news/2024/02/28/north-east-pa-welch-foods-plant-victim-cyber-attack-halted-production/72750164007/
2024-02-11	Ignitis ON	Lithuania	Power	U	Unknown	156			ID	Disabled publicly located and privately-owned charging stations for several hours	Ignitis' charging services are implemented on a cloud-based SaaS model, making their operations critically dependant on those external IT services. A suspected ransomware attack ad subsequent data breach on those cloud services caused their smartphone app to stop working, preventing customers from charging their cars as the app was critical to the charger's functionality. This attack also disabled and disconnected all Ignitis ON's publicly accessible charging stations across Lithuania.	https://icsstrive.com/incident/ignitis-on-customers-unable-to-charge-cars-in-lithuania/ https://www.delfi.lt/en/business/data-of-20-000-ignitis-on-clients-leaked-in-cyber-incident-95857777 https://balticnews.com/hackers-leak-data-data-of-around-20000-ignitis-on-customers-in-lithuania/ https://madeinvilnius.lt/en/news/Lithuanian-news/On-Sunday,-the-company-Ignitis-experienced-an-attack,-most-of-the-customers-cannot-charge-their-electric-cars/

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-02-12	Varta	Germany	Discrete Mfg.	U	Unknown	5		EU MAR	IA	Shut down production, for 2+ weeks	Following a cyberattack, Varta proactively shutdown their production plants and IT systems for "security reasons" and to "ensure data integrity."	https://icsstrive.com/incident/german-battery-maker-varta-group-hit-in-cyberattack/ https://www.csoonline.com/article/1307574/hackers-paralyze-battery-maker-varta-in-cyberattack.html https://www.securityweek.com/cyberattack-disrupts-production-in-varta-battery-factories/ https://www.csoonline.com/article/3494349/cyberattacke-auf-batterieherstellerhacker-legen-varta-lahm.html
2024-02-19	HAL Allergy Group	Netherlands	Pharma	R	RansomHouse	1			ID	Delayed order processing and delivery 32 days	A statement on HAL Allergy's website admits they were victims of a ransomware attack, that could result in large numbers of customers not receiving their prescription products. They blamed their lack of access to data for the service interruption. In an update on March 22, HAL said that orders have resumed shipping but offers few additional details on the nature of the attack.	https://icsstrive.com/incident/ransomware-attack-at-hal-allergy-impacts-customer-deliveries/ https://www.hal-allergy.com/2024/02/22/notification-statement/ https://www.hal-allergy.com/2024/03/22/first-deliveries-have-been-successfully-resumed/ https://www.redpacketsecurity.com/ransomhouse-ransomware-victim-hal-allergy/
2024-02-20	Continental Aeropace Tech	USA	Discrete Mfg.	R	Play / PlayCrypt	1			U	Shutdown operations	Company reports that it suffered an attack that impacted their daily operations at their Mobile, Alabama HQ. A customer publicly posted that their order for a new engine has been delayed, without being given any reason. PLAY ransomware later claimed responsibility for the attack and published exfiltrated data.	https://icsstrive.com/incident/continental-aerospace-discloses-cyberattack/ https://www.avweb.com/aviation-news/continental-hacked/ https://www.redpacketsecurity.com/play-ransomware-victim-continental-aerospace-Tech/
2024-02-21	Casino del Sol	USA	Bldg. Automation	U	Unknown	1			ID	Shut down ops for 7 days, including elec. access to rooms and phones	A hotel and casino in Tucson, AZ suffered a cyber attack that disabled door keycards and telephones in a widespread outage.	https://icsstrive.com/incident/cyberattack-causes-widespread-outage-at-casino-del-sol-az/ https://www.casino.org/news/casino-del-sol-in-tucson-fighting-cyber-attack/ https://www.kold.com/2024/02/28/tucson-area-casino-victim-attempted-cyberattack/ https://www.kvoa.com/news/cybersecurity-expert-sheds-light-on-casino-del-sol-cyberattack/article_7afbcd50-d753-11ee-981b-b31776f14851.html

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-02-22	Int'l Paper / IP Riegelwood Mill	USA	Process Mfg.	U	Unknown	1			IA	Shut down mill operations in an abundance of caution	IP Riegelwood Mill was targeted in an attack and decided to initiate an orderly shutdown in an abundance of caution. The attacker gained access through a third-party vendor.	https://icsstrive.com/incident/int'l-paper-takes-operations-offline-after-cyberattack/ https://cybermaterial.com/papers-riegelwood-mill-hit-by-cyberattack/ https://www.nrcolumbus.com/news/business/ip-riegelwood-mill-shuts-down-after-cyberattack/article_df5a0cec-d17e-11ee-9a58-7f96ccce8480.html
2024-02-23	Sprimoglass	Belgium	Process Mfg.	R	8BASE	1			U	Shut down production for 10+ days, furloughed 350+ workers	A ransomware attack brought production to a standstill at one of the largest glass manufacturers in Belgium, preventing a large proportion of workers from making glass. With over 600 computers in their OT network, it will take more than two weeks to restore all plant operations.	https://icsstrive.com/incident/production-halted-at-glass-plant-in-belgium/ https://www.hln.be/tech/hackers-eisen-aanval-sprimoglass-op-wij-straffen-bedrijven-die-privacy-van-werknemers-en-klanten-verwaarlozen~aca8516c/?referrer=https%3A%2F%2Fwww.google.com%2F https://www.hln.be/binnenland/na-cyberaanval-duvel-moortgat-ook-bij-tweede-grote-belgische-bedrijf-sprimoglass-ligt-productie-grotendeels-stil-om-zelfde-reden~a185872d/
2024-02-23	ThyssenKrupp Automotive Body Solutions	Germany	Discrete Mfg.	U	Unknown	3			IA	Halted production at 3 autobody plants (Heilbronn, Burghaun, and Wadern-Lockweiler)	After suffering an attack on their autobody manufacturing division, the company took IT systems offline in response, which halted production.	https://icsstrive.com/incident/hackers-breach-systems-at-steel-giant-thyssenkrupp/ https://www.bitdefender.com/blog/hotforsecurity/cybercriminals-halt-car-body-production-at-thyssenkrupp-automotive-division/ https://www.bleepingcomputer.com/news/security/steel-giant-thyssenkrupp-confirms-cyberattack-on-automotive-division/ https://www.saarbruecker-zeitung.de/saarland/saar-wirtschaft/hacker-angriff-auf-thyssenkrupp-auch-werk-im-saarland-betroffen_aid-107637793
2024-03-05	Duvel Moortgat	Belgium, USA	Food & Bev.	R	Stormous	5			IA	Shut down production of 5 beer brands in Belgium and USA	After detecting ransomware in their US Subsidiary's network, Duvel's security systems automatically halted global production as a precautionary safety measure. Shutdown breweries included four Belgian locations and their American subsidiary Boulevard Brewing. Duvel refused to pay the ransom and resumed production after restoring from backup.	https://icsstrive.com/incident/belgian-duvel-brewery-halts-production-after-ransomware-attack/ https://www.vrt.be/vrtnws/en/2024/03/11/cyber-attack-production-at-all-duvel-moortgat-plants-restarted/ https://www.techzine.eu/news/security/117352/ransomware-pauses-beer-production-at-duvel-la-chouffe-and-liefmans/ https://www.techzine.eu/news/security/119038/belgian-brewery-duvel-moortgats-data-made-public-because-company-refused-to-pay/
2024-03-07	Leicester City Council	UK	Power	R	Inc. Ransom	1			ID	Lost control over streetlights, leaving them permanently on for 2+ months	A ransomware attack shutdown IT systems at the city, forcing the street light system into an uncontrolled "default" mode, among other unspecified operational impacts.	https://icsstrive.com/incident/prolonged-effects-of-cyberattack-on-city-of-leicester-almost-two-months-after-initial-attack/ https://www.infosecurity-magazine.com/news/leicester-council-documents-leaked/ https://www.bbc.com/news/uk-england-leicestershire-68881057
2024-03-14	Radiant Logistics, Inc.	Canada	Transport	U	Unknown	3		SEC 8K	IA	Delayed delivery and logistical services for 1 wk in Canada	After detected a cyber attack impacting their Canadian operations, they isolated Canadian systems from the rest of their global network resulting in a local service outage.	https://icsstrive.com/incident/radiant-logistics-isolates-canadian-operations-after-cyberattack/ https://www.board-cybersecurity.com/incidents/tracker/20240320-radiant-logistics-inc-cybersecurity-incident/ https://therecord.media/radiant-logistics-cyberattack-canada-operations

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-03-16	BerlinerLuft Technik GmbH	Germany	Discrete Mfg.	R	Unknown	1			IA	Shut down production 3+ weeks and delayed product deliveries	This HVAC parts and equipment manufacturer shutdown and isolated systems in an abundance of caution to contain a cyber attack, which resulted in operational impacts. Ops resumed April 8th.	https://icsstrive.com/incident/operations-severely-disrupted-at-berlinerluft-manufacturing/ https://www.berlinerluft.de/info-cyberangriff/
2024-03-22	GPS Jamming and Spoofing	Poland, Sweden, Germany	Transport	NS	Unknown (Russia)	1600			DO	Jammed GPS for 63h40m total, impacting flights over Europe: first 24 hours over all three countries, then remainder solely over Poland	Russia is the prime suspect of a record-long 63-hour jam on GPS signals in the Baltic. From the evening of March 22 to the afternoon of March 25, interference was spread across three countries before settling on Poland for 40 hours, impacting more than 1600 flights.	https://icsstrive.com/incident/aircraft-unable-to-receive-gps-signals-in-baltic-sea-the-black-sea-and-eastern-mediterranean/ https://www.newscientist.com/article/2424678-unprecedented-gps-jamming-attack-affects-1600-aircraft-over-europe/ https://x.com/rundradion/status/1772366665583337827
2024-03-27	Intermarché	Belgium	Transport	R	Unknown	2			ID	Impacted logistics at some stores for 2 days	A cyber attack hit former Groupe Mestdagh-branch supermarkets of grocery-giant Intermarché, leading to supply problems at some stores. Attackers targeted IT systems that were not fully integrated after Mestdagh was recently acquired by their new parent a year prior and demanded a ransom. Operations were back to normal days later.	https://icsstrive.com/incident/intermarche-hackers-took-advantage-of-mestdagh-brand-take-over-phase/ https://www.retaildetail.be/nl/news/food/cyberaanval-op-mestdagh-winkels-van-intermarche/
2024-03-29	Omni Hotels & Resorts	USA, Canada	Bldg. Automation	R	Daixin Team	50	$40M		ID	Disrupted the entire hotel chain's ops. including keycard access to rooms, for 11 days	Customers who had been staying at Omni hotels when the incident started reported check-ins being done on paper, room keys not working, and being unable to pay with credit cards. They later resumed April 8th.	https://icsstrive.com/incident/national-outage-at-omni-hotels-after-cyberattack/ https://www.securityweek.com/cyberattack-causes-disruptions-at-omni-hotels/ https://www.theregister.com/2024/04/03/omni_hotels_it_outage/ https://www.bleepingcomputer.com/news/security/daixin-ransomware-gang-claims-attack-on-omni-hotels/
2024-03-30	Hoya Corporation	Japan	Discrete Mfg.	R	Hunters Int'l	2			IA	Shut down production and delayed order fulfillment for 3+ wks	A ransomware attack on its IT network caused the optical manufacturer to disconnect servers and bring in a response team. As a result, production and ordering systems were impacted. Hoya told customers to expect ordering delays.	https://icsstrive.com/incident/attack-shuts-down-production-at-lens-maker-hoya/ https://www.securityweek.com/lens-maker-hoya-scrambling-to-restore-systems-following-cyberattack/ https://www.bleepingcomputer.com/news/security/optics-giant-hoya-hit-with-10-million-ransomware-demand/ https://www.hoyavision.com/about-hoya/hoya-vision-care-news/news/it-system-incident-update-2/

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-04-09	Moscollector	Russia	Water	NS	Blackjack [Security Services of Ukraine] / Fuxnet	500			DIP	Destroyed or disabled thousands of IIoT devices deployed throughout underground utility corridors, impacting supply, monitoring and emergency response	BlackJack claimed to have significantly impacted Moscollector's IOT sensor gateway network deployed throughout underground utility corridors, providing telecommunications, district heating, water, and sewage services throughout Moscow. Claroty analyzed a Fuxnet malware sample from the attack adding credibility to BlackJack's claims. Fuxnet has the capability of sending spurious commands over RS-485/MBus protocols and bricking sensor gateways by destroying their flash memory chips.	https://icsstrive.com/incident/ics-malware-fuxnet-disrupts-russian-infrastructure/ https://www.securityweek.com/destructive-ics-malware-fuxnet-used-by-ukraine-against-russian-infrastructure/ https://claroty.com/team82/research/unpacking-the-blackjack-groups-fuxnet-malware https://moscollector.ru/%D0%BE-%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D0%B8/
2024-04-11	United Renewable Energy Co., Ltd. (URECO, 聯合再生)	Taiwan	Discrete Mfg.	U	Unknown	1			ID	Shut down production	This solar power panel module manufacturing company announced a cyberattack on their IT systems caused their factory to shut down, and that the financial cost of this shutdown was still being evaluated.	https://icsstrive.com/incident/taiwan-united-renewable-energy-corporation-confirms-cyberattack/ http://www.aastocks.com/tc/stocks/news/glh-news/GLH1482129L/1
2024-04-12	Barnett's Couriers	Australia	Transport	R	Unknown	1	Bankrupt		U	Shut down freight operations for 2+ weeks, and laid-off staff and contractors; then bankrupted and permanently closed the company	A North Wollongong, Australia trucking company was hit by a cyber attack. In an automated message, they informed customers and employees that they intended to resume operations by April 19th, but on Monday April 22, they gave notice of another week of expected downtime. In May, they announced the attack has made the business unprofitable, causing it to permanently close after operating for 40 years.	https://icsstrive.com/incident/barnetts-couriers-shuts-down-operations-after-cyberattack/ https://www.illawarramercury.com.au/story/8601158/wollongong-firm-barnetts-couriers-left-reeling-from-cyber-attack/ https://bigrigs.com.au/2024/05/08/illawarra-trucking-company-closes-doors-after-cyber-attack/ https://www.illawarramercury.com.au/story/8652381/police-investigating-cyber-attack-on-barnetts-couriers/
2024-04-15	Octapharma Group	**Switzerland**, USA	Pharma	R	BlackSuit	182			ID	Shutdown 180 donation centers for 6 days	A ransomware attack on a blood plasma processing company shut down operations at their donation centers and may have shutdown their European factories as a result. BlackSuit managed to gain initial access through VMWare ESXi servers.	https://icsstrive.com/incident/plasma-donation-company-octapharma-shuts-down-180-centers-worldwide/ https://therecord.media/plasma-donation-company-cyberattack-blacksuit https://www.theregister.com/2024/04/18/ransomware_octapharma_plasma/
2024-04-16	Norrmejerier	Sweden	Food & Bev.	R	Unknown	1			IA	Shutdown production 4+ days	After discovering their Umeå plant suffered a cyberattack, they chose to shutdown all production in an abundance of caution. Because of how high tech their industry is, nearly everything is computerized.	https://icsstrive.com/incident/production-shut-down-at-swedish-dairy/ https://www.svt.se/nyheter/lokalt/vasterbotten/cyberangrepp-mot-norrmejerier-i-umea-produktionen-nere https://www.mynewsdesk.com/se/norrmejerier_ek/news/norrmejerier-har-utsatts-foer-ett-cyberangrepp-482617

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-04-20	Puerto Nuevo Terminals consortium / Luis Ayala Colón-Tote Maritime	Puerto Rico	Transport	R	Unknown	1			U	Delayed cargo movement and truck dispatch for several days; caused traffic jam on Kennedy Ave into capital San Juan; caused empty shelves and shortages at retail	A ransomware attack on the main port consortium in Puerto Rico impacted operations. The FBI's office in Puerto Rico is investigating.	https://icsstrive.com/incident/ransomware-attack-at-puerto-nuevo-terminals-in-puerto-rico/ https://www.transportation.gov/sites/dot.gov/files/2024-07/20240711-FINAL-MARAD_Responses_House_CGMT_QFRs_April%2030_2024_508.pdf https://www.elnuevodia.com/english/news/story/fbi-assists-in-the-investigation-on-a-cyberattack-against-the-company-that-operates-cargo-docks-in-san-juan/ https://web.archive.org/web/20240526050313/https://www.sanjuandailystar.com/post/union-chief-empty-shelves-can-be-observed-following-cyberattack-at-docks
2024-04-22	Finnair / Tartu Airport	Estonia	Transport	NS	Unknown (Russia)	1			I3	Cancelled flights between Helsinki Finland and Tartu Estonia until June 2 (6 wks.)	A popular flight route between Helsinki and Tartu was suspended for 6 weeks after widespread GPS jamming and spoofing made operating the route safely impossible. After two Finnair flights in Estonia had to return to Helsinki after their GPS stopped working, the route was shelved until there was a certified alternative navigation system in place.	https://icsstrive.com/incident/finnair-suspends-flights-between-helsinki-and-tartu-after-gps-jamming/ https://www.cbc.ca/news/world/gps-interference-airlines-1.7213538 https://www.politico.eu/article/estonia-blames-russia-for-gps-interference-that-forces-finnair-to-suspend-flights/ https://www.reuters.com/world/europe/finnair-pauses-flights-tartu-estonia-amid-gps-interference-2024-04-29/
2024-04-22	Systembolaget, Skanlog	Sweden	Transport	R	North Korea	1			ID	Impacted wine and spirit distribution to retail stores nation-wide for 1 month	Skanlog, Sweden's critical distributor for government-owned retail liquor stores Systembolaget, was hit by ransomware that disrupted operations. Skanlog's CEO Mona Zuko claimed that a North Korean ransomware gang was responsible. As of May 17, System Bolaget still reported supply issues for wine	https://icsstrive.com/incident/ransomware-attack-on-skanlog-triggered-nationwide-alcohol-shortage/ https://www.euronews.com/next/2024/04/25/alcohol-sales-disrupted-in-sweden-after-reported-ransomware-attack https://therecord.media/sweden-ransomware-liquor-shortage-skanlog-systembolaget https://press.systembolaget.se/pressmeddelanden/2024/leveranser-fran-drabbad-distributor-aterupptas/
2024-04-23	BECOM Electronics GmbH	Austria	Discrete Mfg.	R	Unknown	1			IA	Shut down production	BECOM admitted to an attack and were able to prevent systems from being encrypted, but they did so by isolating systems and disconnecting from the internet. This had impacts on production.	https://icsstrive.com/incident/cyberattack-on-austrian-electronics-company-becom/ https://www.meinbezirk.at/oberpullendorf/c-wirtschaft/becom-electronics-wurde-ziel-eines-cyberangriffs_a6655617 https://burgenland.orf.at/stories/3254332/
2024-04-25	Kansas City Highway Traffic System (KC Scout)	USA	Transport	R	Play / PlayCrypt	1			U	Disrupted "KC Scout" motor vehicle emergency information and alert systems for 6+ wks.	On a day with many dangerous severe storms in the forecast, critical information on Kansas City metro area's highway traffic system KC Scout was disrupted by ransomware. Digital road sign boards that show real-time information, such as emergency road and lane closures, and road cameras that monitor road conditions, have faded to black reducing motorist's safety.	https://icsstrive.com/incident/kansas-city-scout-system-systems-shut-down/ https://www.foxweather.com/weather-news/cyberattack-missouri-dot-highway-signs-kc-scout https://www.modot.org/node/49616 https://www.kctv5.com/2024/06/11/still-crippled-by-cyberattack-kc-scout-test-initial-phases-restoration/

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-05-06	Port of Sao Francisco Do Sul (Porto de São Francisco do Sul)	Brazil	Transport	R	RansomHub	1			U	Shut down port for 1 day	This port in Brazil suffered an attack that encrypted systems and data. To prevent the spread of the malware, they shut down in an abundance of caution. They restored operations by the next day. RansomHub later took responsibility and threatened to release leaked data.	https://icsstrive.com/incident/cyberattack-at-brazilian-port-of-sao-francisco-do-sul/ https://portosaofrancisco.com.br/saiba-mais/id/293 https://www.halcyon.ai/attacks/ransomware-attack-on-administration-of-the-port-of-sao-francisco-do-sul
2024-05-06	Key Tronic Corporation (Keytronic)	**USA**, Mexico	Discrete Mfg.	R	BlackBasta	2	$17M	SEC 8K	IA	Shut down production in the US and Mexico for two weeks	A printed circuit board manufacturer shut down operations after detecting unusual activity on their IT network. Later, they filed $2.3m in related expenses and $15m in revenue losses with the SEC.	https://isssource.com/ransomware-attack-shuts-key-tronic-operations/ https://therecord.media/key-tronic-cyberattack-cost-17-million-sec https://www.techradar.com/pro/security/keytronic-confirms-data-breach-after-black-basta-ransomware-gang-strikes-again
2024-05-11	Wehrle-Werk AG	Germany	Process Mfg.	U	Unknown	1			U	Shut down production	Cybercriminals attacked the Emmendinger plant, impacting production and communications. Response teams were brought in to help with restoration.	https://icsstrive.com/incident/operations-down-at-water-complex-waste-water-plant-manufacturer-wehrle/ https://www.sentiguard.eu/wissen/wehrle-werk-ag-schraenkt-nach-hackerangriff-produktion-ein/
2024-05-11	LEMKEN	**Germany**, Netherlands, India	Discrete Mfg.	R	8BASE	4			IA	Shut down production	After detecting the attack on all worldwide locations, LEMKEN chose to protect themselves by shutting down all IT systems to prevent further access and called in a response team. On May 21, ransomware group 8BASE took responsibility and threatened to leak data.	https://icsstrive.com/incident/german-machinery-manufacturer-lemken-halts-production-sites/ https://lemken.com/en-en/news/agriculture-news/detail/lemken-affected-by-cyberattack https://www.farmersjournal.ie/machinery/news/lemken-resumes-production-after-cyberattack-822249 https://www.csoonline.com/article/3494185/produktion-lahmgelegt-hackerangriff-auf-lemken.html
2024-05-18	Matadero de Gijón	Spain	Food & Bev.	R	RansomHub	1			DO	Shut down operations and sent workers home	Ransomhub claimed they accessed the SCADA system at Matadero de Gijón, specifically their wastewater treatment systems, which shutdown the beef plant. Workers were sent home mid-shift. Production later resumed after systems were switched to manual operation.	https://icsstrive.com/incident/ransomhub-targets-scada-system-of-spanish-meat-processing-plant/ https://www.lne.es/gijon/2024/05/22/matadero-paralizado-lunes-hackeo-depuradora-102715618.html https://cybersecuritynews.com/ransomhub-ics-attack/ https://cyble.com/blog/ransomware-menace-amplifies-for-vulnerable-industrial-control-systems-heightened-threats-to-critical-infrastructure/
2024-05-28	CDEK	Russia	Transport	R	Head Mare	1			U	Disrupted shipments and deliveries for 3 days and caused further delivery delays	A ransomware attack on CDEK by Head Mare, a Russian-speaking ransomware group, interrupted logistical services and caused delivery delays by encrypting systems critical to operations.	https://icsstrive.com/incident/alleged-cyberattack-on-delivery-service-in-russia/ https://therecord.media/russian-delivery-company-cdek-down-cyberattack https://x.com/head_mare/status/1795072931489345946

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-06-04	Vietnam Post	Vietnam	Transport	R	Unknown	1			IA	Impacted postal and delivery services for 4 days	Ransomware infected systems at Vietnam Post and were quickly detected. Systems were shutdown to contain and stop the spread of the malware, impacting operations, which were restored days later.	https://icsstrive.com/incident/ransomware-attack-at-vietnam-post-takes-systems-offline/ https://therecord.media/vietnam-claims-restore-services-cyberattack https://theinvestor.vn/vietnam-postal-services-crippled-by-ransomware-attack-d10489.html https://baotintuc.vn/van-de-quan-tam/he-thong-dich-vu-buu-dien-viet-nam-co-ban-hoat-dong-tro-lai-sau-khi-bi-tan-cong-mang-20240608093324588.htm
2024-06-08	Kadokawa Corporation	Japan	Process Mfg.	R	BlackSuit	1	$3M		ID	Decreased production (printing), and reduced shipping volume down to 1/3 for 2 months	A large publisher in Japan suffered a ransomware attack that infected IT systems. This consequently impacted the physical printing and distribution of books, comics and magazines. Falling back to manual operations lessened, but did not avoid, physical consequences. Kyodonews reported that while Kadokawa paid a $3m ransom to BlackSuit in bitcoin, BlackSuit leaked 1.5TB of stolen data anyways.	https://icsstrive.com/incident/cyberattack-impacted-kadokawas-and-its-subsidiarys-operations/ https://www.animenewsnetwork.com/news/2024-07-30/kadokawa-gradually-resumes-shipping-of-books-in-august/.213718 https://english.kyodonews.net/news/2024/12/fffebe5585f1-japanese-publisher-paid-3-million-to-hacker-group-after-cyberattack.html
2024-06-08	Crown Equipment	USA	Discrete Mfg.	R	Unknown	24			ID	Shut down production and sent workers home for 3 wks	Forklift manufacturer shutdown after a ransomware attack. The TA gained initial access after an employee was social engineered, allowing the TA to plant a RAT on their system. On July 1st, Crown announced they resumed production at all 24 plants.	https://isssource.com/cyberattack-halts-oh-forklift-makers-operations/ https://therecord.media/crown-equipment-shuts-down-systems-forklifts https://www.bleepingcomputer.com/news/security/crown-equipment-confirms-a-cyberattack-disrupted-manufacturing/ https://www.daytondailynews.com/local/cyberattack-temporarily-halts-operations-at-crown-equipment/RIPZJ4HWKJDKJN65JQMTGVKUTE/
2024-06-12	GlobalWafers Co. / GW / 環球晶圓	Taiwan	Discrete Mfg.	U	Unknown	1			IA	Halted production and disrupted shipments for 6 days	The world's third-largest silicon wafer maker reported that a cyberattack caused them to lower risk and "shut down its operating systems," halting production and disrupting shipments. Everything was back to normal by June 18th. NB in March 2022, Pandora ransomware attacked GlobalWafers resulting in a data breach.	https://isssource.com/production-hurt-in-attack-on-silicon-wafer-maker https://www.tomshardware.com/news/silicon-wafer-giant-globalwafers-resumes-production-days-after-hack-attack https://focustaiwan.tw/sci-tech/202406170020
2024-06-17	Rekah / Ophir & Shalpharm Medicines and Cosmetics	Israel	Pharma	U	Unknown	1		TASE	IA	Halted pharmaceutical distribution nation-wide	Rekah suffered a cyberattack impacting pharmaceutical distribution throughout Israel after several systems were shutdown. Production was not affected.	https://icsstrive.com/incident/cyberattack-shuts-down-distribution-at-israeli-pharma-company-rekah/ https://www.isssource.com/israeli-pharma-firm-suffers-cyberattack/ https://www.calcalistech.com/ctechnews/article/sjyk8iab0

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-06-26	CO-OP Cardlock gas stations & retail food stores (Federated Co-operatives Limited, FCL)	Canada	Transport	U	Unknown	380			IA	Shut down cardlock and retail gas stations, and caused supply problems which varied by retail store location, for 3+ wks	Local CO-OP retail and cardlocks (unmanned fleet-only) gas stations shutdown across western Canada after a cybersecurity incident. Also, retail grocery locations saw empty shelves and logistical delivery delays. The company released few details, but admitted they were forced to shutdown "customer-facing systems" at locations across Western Canada.	https://icsstrive.com/incident/operations-disrupted-at-co-op-locations-in-western-canada/ https://www.cbc.ca/news/canada/saskatchewan/federated-co-operatives-limited-cybersecurity-incident-1.7249723 https://www.moosejawtoday.com/local-news/federated-co-operatives-limited-announces-all-systems-normal-following-cyberattack-9287743
2024-06-30	RideMovi	Italy	Transport	SC	Ride'n Godi	1			DSC	Rendered 80% of RideMovi's bike fleet damaged, untraceable, or unusable	A pirate app called *Ride'n Godi* allowed users to unlock bikes without needing to pay and subscribe to the official service *RideMovi*, severely disrupting this large bike sharing service in Bologna. Bikes were reported being left in unforeseen places, with empty batteries, or physically damaged, leaving them untraceable and inoperable.	https://icsstrive.com/incident/illegal-app-renders-80-of-bicycles-out-of-use-in-bologna-italy/ https://www.redhotcyber.com/post/bologna-gli-hacker-scrivono-unapp-illegale-che-paralizza-il-bike-sharing-l80-delle-biciclette-fuori-uso/ https://bologna.repubblica.it/cronaca/2024/06/27/news/bologna_app_pirata_bike_sharing-423289317/
2024-07-02	AKG Group (Heat Exchangers)	Germany	Discrete Mfg.	U	Unknown	11			IA	Shut down production for 11 days	After discovering that operators in India could not login to their computers, the company discovered it was the result of an attack. After the problem got worse, AKG chose to shutdown systems to contain the attack. This resulted in production outages until July 13.	https://icsstrive.com/incident/cyberattack-at-akg-group-shuts-down-of-it-infrastructure-and-restricts-production/ https://www.hna.de/lokales/hofgeismar/hofgeismar-ort73038/nach-cyber-angriff-produktion-bei-akg-laeuft-wieder-93184688.html
2024-07-08	Sibanye-Stillwater	USA	Metals & Mining	R	RansomHouse	1			ID	Shut down smelter operations in Columbus, OH, USA; halted some mining operations in Montana	South-Africa based Sibanye Stillwater suffered a ransomware attack which disrupted their IT systems globally. While the company claimed only business systems were impacted, a union official said some automated systems stopped working in Ohio. Also, their mine in Montana reported an operational shutdown due to the attack. In late July, RansomHouse claimed responsibility for the attack in a large data leak.	https://icsstrive.com/incident/sibanye-stillwater-reports-limited-disruptions-in-mining-and-metals-processing-operations/ https://www.ktvq.com/news/local-news/sibanye-stillwater-hit-by-ransomware-attack https://thecyberexpress.com/stillwater-data-breach-info-of-employees/
2024-07-10	Bassett Furniture	USA	Discrete Mfg.	R	Unknown	5	$2M	SEC 8K	ID	Shut down production at all plants for 27 days, impacting order fulfillment	Due to an attack on their IT network, some systems were encrypted. The company responded by investigating, isolating and shutting down some systems. As a result, manufacturing stopped, and orders could not be fulfilled. Customer facing IT -assets, like ordering and retail systems, were not impacted.	https://icsstrive.com/incident/ransomware-attack-shuts-down-large-us-furniture-company/ https://www.retaildive.com/news/bassett-furniture-cyberattack-shuts-down-manufacturing-facilities/721681/ https://www.woodworkingnetwork.com/news/woodworking-industry-news/bassett-furniture-hit-cyberattack-manufacturing-affected https://therecord.media/furniture-giant-manufacturing-shut-down-cyberattack

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-07-15	Cadre Holdings Inc.	USA	Discrete Mfg.	U	Unknown	1		SEC 8K	IA	Impacted production and order fulfillment	In a quarterly 10Q filling with the SEC, Cadre admitted that a cyber incident caused them to shutdown certain systems in an abundance of caution. This impacted their operations, incurred restoration and remediation costs, and is likely to negatively impact their financial results.	https://icsstrive.com/incident/safety-equipment-giant-cadre-holdings-shut-down-some-systems-after-cyberattack/ https://www.cadre-holdings.com/sec-filings/all-sec-filings/content/0001558370-24-011750/0001558370-24-011750.pdf https://www.securityweek.com/safety-equipment-giant-cadre-holdings-hit-by-cyberattack/
2024-07-22	Split (Saint Jerome) Airport	Croatia	Transport	R	Akira	1			ID	Canceled all flights and diverted planes for 2 days. Disrupted ground handling and the passenger information system, and forced airport to operate manually for days	Akira ransomware encrypted key IT systems at the airport, disrupting flights. Refusing to negotiate, they restored a critical IT system for aircraft handling two days later and resumed operations.	https://icsstrive.com/incident/operations-disrupted-at-split-airport/ https://seenews.com/news/split-airport-restoring-functions-after-cyberattack-1261006 https://glashrvatske.hrt.hr/en/domestic/split-airport-after-the-hacker-attack-we-will-not-negotiate-11673909 https://n1info.hr/english/news/split-airport-key-it-system-restored-after-cyber-attack/
2024-08-17	Microchip Technology	USA	Discrete Mfg.	R	Play / PlayCrypt	2		SEC 8K	IA	Disrupted operations at multiple sites, reduced production output, and impacted order fulfilment	In an SEC filing, Microchip said that a cyber incident impacted production and order fulfilment, causing them to isolate systems and shut down some services. On August 24th, Play claimed responsibility for the attack on their dark web leak site and threatened to publish stolen data.	https://icsstrive.com/incident/microchip-technology-manufacturing-operations-disrupted-after-cyberattack/ https://www.isssource.com/production-hurt-in-attack-on-silicon-wafer-maker https://www.bleepingcomputer.com/news/security/microchip-technology-discloses-cyberattack-impacting-operations/ https://www.reuters.com/technology/microchip-technologys-certain-operations-disrupted-by-cyber-incident-2024-08-20/
2024-08-19	BVI Electricity Corporation (BVIEC)	British Virgin Islands	Power	R	Unknown	1			ID	Prolonged power distribution outage for 10+ days	While recovering from Hurricane Ernesto, BVIEC has been working hard to restore power infrastructure for a week when they were suddenly hit by a ransomware attack that made restoration much more difficult. The attack hit both "internal and external operations," meaning both IT and OT networks. A large customer data breach followed.	https://icsstrive.com/incident/operations-disrupted-at-bvi-electricity-corporation-bviec/ https://www.virginislandsnewsonline.com/en/news/bviec-falls-victim-to-cyber-attack https://bvinews.com/bviec-warns-residents-check-your-credit-cards/ https://bvinews.com/bviecs-online-payment-platform-restored-after-cyber-attack/
2024-08-24	Seattle-Tacoma Int'l Airport (SeaTac) / Port of Seattle	USA	Transport	R	Rhysida	1			IA	Delayed Flights and shutdown or impaired the baggage handling system (BHS), check-in kiosks, and passenger flight information display system (FIDS) for weeks	After discovering a breach in their computer systems, and noticing some systems being encrypted, The Port of Seattle began disconnecting systems from the internet. This impacted passenger services at logistics at both the airport and seaport.	https://icsstrive.com/incident/cyberattack-disrupts-seattle-airport-for-days-affecting-labor-day-weekend-rush https://www.theregister.com/2024/08/26/seattle_airport_cyber attack https://therecord.media/seattle-port-rhysida-ransom-refused https://www.portseattle.org/news/port-cyberattack-archive

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-08-27	JAS Worldwide	Italy, USA	Transport	R	Unknown	1			U	Disrupted or delayed freight and logistics forwarding	After a ransomware attack, operations were impacted at one of the largest Int'l freighter forwarders. Post-incident, JAS reported that backlogged requests were being worked through, implying there were some delays.	https://icsstrive.com/incident/global-freight-forwarder-jas-confirms-malware-disrupts-operations/ https://theloadstar.com/jas-forwarding-recovers-from-cyber-attack-but-saw-many-stolen-credentials/ https://www.freightwaves.com/news/global-freight-forwarder-confirms-malware-attack-for-technical-disruptions https://www.freightcaviar.com/jas-worldwide-confirms-malware-attack-cause-of-technical-disruptions/
2024-08-30	Ekomobil	Turkey	Transport	H	Cund El Aksa	1			IA	Disrupted public bus services in the city of Kocaeli	A hacktivist group sent threatening messages to municipal bus commuters by hijacking the Ekomobil smart-phone app and displaying threatening messages. Also, bus card readers' displays were compromised to display a bomb threat. As a precaution, all bus services in the city were temporarily halted.	https://icsstrive.com/incident/bus-services-disrupted-after-turkish-transportation-app-hack/ https://www.turkiyetoday.com/turkiye/anti-semitic-group-hacks-turkish-transportation-app-46954/ https://www.cagdaskocaeli.com.tr/haber/21477453/e-komobil-hacklendi
2024-09-03	Elektroskandia Sverige AB	Sweden	Transport	R	BlackSuit	1	100M kr.		ID	Halted logistical operations for 2+ wks	IT systems at Elektroskandia's large central warehouse in Örebro were shutdown in a ransomware attack. This impacted logistical operations and prevented the company from picking or delivery orders.	https://icsstrive.com/incident/large-swedish-electrical-wholesalers-elektroskandia-loses-millions/ https://info.elektroskandia.se/underhall/ https://www.elinstallatoren.se/2024/10/elektroskandiachefen-om-hackerattacken-vi-sa-till-vara-kunder-att-ga-till-konkurrenterna/
2024-09-12	KANTSU (関通)	Japan	Transport	R	Unknown	1			U	Halted and delayed logistical operations for 1 month	Kantsu reported that ransomware was detected on their server which caused a system outage, impacting multiple systems related to the custody of customer items in their logistical system. The attack originated externally and pivoted into their IT and OT networks and delayed the storage and retrieval of warehoused items. Full operations were restored a month later on October 12th.	https://icsstrive.com/incident/cyberattack-at-japanese-logistics-company-kantsu/ https://www.kantsu.com/news/6573/ https://www.kantsu.com/news/6615/ https://www.kantsu.com/news/6620/
2024-09-14	ZACROS (藤森工業株式会社)	Japan	Discrete Mfg.	R	Argonauts Group	1		PIPC	ID	Impacted production and delivery operations	A leading Japanese manufacturer of packaging materials suffered a ransomware attack that affected servers critical to ERP and production management. A data breach resulted, which was reported to Japan's' PIPC, and acknowledged an impact on financial performance. The Argonauts ransomware group claimed responsibility and said they leaked data over ZACROS' refusal to pay a ransom.	https://icsstrive.com/incident/japanese-manufacturer-zarcos-hit-by-ransomware-attack/ https://securityonline.info/zacros-corporation-discloses-personal-information-leak-following-ransomware-attack/ https://www.cyjax.com/resources/blog/new-argonauts-extortion-group-emerges/ https://cybersecurity-info.com/news/zacros-ransomware/

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-09-22	Schumag AG	Germany	Discrete Mfg.	U	Unknown	1	Bankrupt		U	Shut down production, and filed for bankruptcy & restructuring	A precision engineering and tooling company filed for bankruptcy and self-directed restructuring in mid October, after a cyberattack a month prior caused production outages. The threat actor was not identified.	https://icsstrive.com/incident/german-steel-manufacturer-shuts-down-systems-and-cancels-annual-shareholder-meeting/ https://www.csoonline.com/article/3559206/schumag-von-cyberattacke-betroffen.html https://www.boerse-frankfurt.de/nachrichten/Schumag-Aktiengesellschaft-Cyberangriff-Absage-der-fuer-den-25-September-2024-einberufenen-ordentlichen-Hauptversammlung-63c6812b-71f9-4407-b14a-589dc8f3ab55
2024-09-27	Smeg	Italy	Discrete Mfg.	U	Unknown	1			IA	Shut down production due to dependencies on their SAP system, and furloughed hundreds of employees	High-End home appliances maker Smeg proactively halted production after a cyber attack, saying it was forced to suspend operations as its SAP system was interrupted, which then went on to impact logistics.	https://icsstrive.com/incident/production-at-standstill-at-italian-high-end-home-appliances-manufacturer/ https://cyberinsider.com/high-end-appliances-maker-smeg-halts-production-after-cyberattack/ https://www.wired.it/article/cyberattacco-smeg-elettrodomestici/
2024-09-28	Beirut (Rafik-Hariri) Int'l Airport	Lebanon	Transport	NS	Israel Defense Force [IDF] (Israel)	1			DO	Diverted civilian plane Qasem Air Flight No. QFZ9964 back to its origin of Tehran, Iran	After learning that an Iranian plane was due to land at the airport, Israel's IDF breached the control tower's communication network in a cyber attack and warned operators not to allow the plane to land. Otherwise, they would launch an attack on the airport. Lebanon's transport minister, Ali Hamieh intervened and directed the incoming plane to divert its flight path and return to Iran.	https://icsstrive.com/incident/israel-hacks-beirut-airport-control-tower/ https://www.jpost.com/middle-east/article-822208
2024-10-05	Casio	Japan	Discrete Mfg.	R	Underground	1			IA	Halted manufacturing, suspended repair services, and delayed product delivery inside Japan for over a month	After a ransomware attack on this Japan-based watchmaker both production and repair services were impacted. In response, Casio took servers offline which affected receiving and placing orders with suppliers, and the scheduling of product shipments.	https://icsstrive.com/incident/japanese-technology-giant-casio-computer-confirmed-cyberattack/ https://therecord.media/japan-casio-delays-watchmaker-ransomware https://techcrunch.com/2024/10/17/casio-says-no-prospect-of-recovery-yet-after-ransomware-attack/
2024-10-11	Hubergroup	Germany	Discrete Mfg.	U	Unknown	1			U	Limited production for 2+ weeks, delayed delivery	The Celle manufacturing plant suffered a cyber attack that had impacts on their SAP system, internet connectivity, production, and delivery for weeks. The company said other Int'l locations have not been impacted.	https://icsstrive.com/incident/cyberattack-at-german-printing-ink-manufacturer-hubergroup/ https://www.celleheute.de/post/cyberangriff-auf-hubergroup-regionale-it-systeme-beeintr%C3%A4chtigt/
2024-10-19	CERP Bretagne Atlantique	France	Pharma	R	Hunters Int'l	1800			ID	Shut down distribution and delayed orders 1 day	Due to a cyber attack, this key pharma wholesaler and distributor suffered a 24-hour outage before resuming orders and deliveries to pharmacies across Western France.	https://icsstrive.com/incident/french-pharmacy-wholesaler-hit-by-cyberattack/ https://www.letelegramme.fr/cotes-d-armor/saint-brieuc-22000/victime-dune-cyberattaque-le-grossiste-en-pharmacie-cerp-devrait-rapidement-retrouver-une-activite-normale-6686412.php https://www.zdnet.fr/actualites/apres-la-cyberattaque-la-reconstruction-pas-a-pas-du-grossiste-en-pharmacie-cerp-bretagne-atlantique-400030.htm

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-10-28	AEP GmbH	Germany	Pharma	R	Unknown	6000			ID	Disrupted pharmaceutical distribution and order fulfillment to 6,000 pharmacies across Germany for 9 days.	After the company's own systems detected a breach, some systems were encrypted before they pre-emptively "disconnected all external connections and shut down all affected IT systems". Services were restored Nov. 6th.	https://icsstrive.com/incident/ransomware-attack-threatens-disrupting-medicine-supply-to-pharmacies-in-germany/ https://therecord.media/ransomware-attack-hits-german-pharmaceutical-wholesaler-disruptions https://www.pharmazeutische-zeitung.de/massiver-cyberangriff-auf-aep-151028/ https://www.br.de/nachrichten/bayern/cyberattacke-auf-pharmagrosshaendler-lieferprobleme-fuer-apotheken,UShteGL
2024-10-31	Microlise Group plc (DHL, Serco, NISA)	UK	Transport	R	SafePay / LockBit	3		LSE	I3	Disrupted tracking services at DHL, globally, thereby impacting NISA and other logistical operations, some customer companies reported logistiical delays	Microlise, a software company that DHL relies on for its global delivery tracking operations, was hit by a ransomware attack. This impacted Nisa's logistics which relies, in turn, on DHL.	https://icsstrive.com/incident/tracking-in-prison-vans-and-courier-vehicles-affected-by-microlise-cyberattack/ https://www.betterretailing.com/dhl-cyber-attack/ https://www.securityweek.com/microlise-confirms-data-breach-as-ransomware-group-steps-forward/ https://motortransport.co.uk/cyberattack-on-microlise-hits-operators-triggering-call-for-stronger-continuity-plans/24912.article
2024-11-08	Ahold Delhaize (Stop & Shop, Food Lion, Hannaford, Giant Food, Giant Company)	USA	Transport	U	Unknown	2040			IA	Impacted and delayed food and pharmaceutical distribution to stores and online customers for 12+ days. A dozen New England locations report bare shelves and shortages.	Delhaize's US operations were impacted after a cyberattack on their IT systems. Security experts were brought in that recommended isolating and taking systems offline. The incident and subsequent response impacted logistical operations. Delhaize released very few incident details.	https://icsstrive.com/incident/operations-disrupted-at-us-branch-of-grocery-giant-ahold-delhaize/ https://cybernews.com/news/ahold-delhaize-cyberattack-stop-shop-hannaford-food-lion-impacted-/ https://www.theregister.com/2024/11/12/ahold_delhaize_cybersecurity_issue_blamed/ https://www.msn.com/en-us/money/companies/inventory-at-worcester-area-stop-shops-remains-limited-after-cyberattack/ar-AA1urPDb
2024-11-14	Vossko	Germany	Food & Bev.	R	BlackBasta	1			ID	Shut down production for 8 days.	This food processing company suffered a ransomware attack that shutdown production after first encrypting IT systems including databases. After bringing in external response team specialists including law enforcement, their systems were restored and rebuilt to strengthen them against future attacks. In December, BlackBasta took responsibility for the attack in a data breach.	https://icsstrive.com/incident/cyberattack-on-vossko-food-company-in-germany/ https://www.vossko.de/2024/11/22/cyberangriff-bei-vossko-systeme-und-produktion-wiederhergestellt/ https://www.comparitech.com/news/ransomware-gang-says-its-responsible-for-data-breach-at-pennsylvania-food-producer/
2024-11-18	Henley Standard, Higgs Group	UK	Process Mfg.	U	Unknown	1			U	Shut down production (printing), delayed publishing & distribution 4 days	A cyber attack impacted the publisher's production and IT systems, preventing the distribution of one weekly edition of their newspaper on time. They hoped to produce and distribute it, late, on Thursday, the 21st.	https://icsstrive.com/incident/local-uk-newspaper-production-shut-down-after-cyberattack/ https://www.henleystandard.co.uk/news/home/193821/this-week-s-paper-delayed.html

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-11-21	Morrisons, Sainsbury's, BIC (Panasonic Blue Yonder)	**UK**, USA	Transport	R	Termite/Babuk	3			I3	Impacted multiple Blue Yonder customers' logistical operations for 3+ weeks	A supply chain ransomware attack on MSP provider Blue Yonder impacted multiple customers including BIC, the pen manufacturer, who experienced shipping delays. Sainsbury's and Morrisons stated the attack impacted warehouse management systems.	https://icsstrive.com/incident/big-ripple-effects-after-supply-chain-software-supplier-blue-yonder-cyberattack/ https://therecord.media/starbucks-bic-morrisons-blue-yonder-supply-chain-attack-ransomware https://www.securityweek.com/starbucks-grocery-stores-hit-by-blue-yonder-ransomware-attack/ https://therecord.media/blue-yonder-cyberattack-customer-systems-returning
2024-11-21	Artivion	USA	Discrete Mfg.	R	Unknown	1		SEC 8K	IA	Disrupted order fulfillment	A ransomware attack impacted operations and forced the medical device manufacturer to take some systems offline in response.	https://icsstrive.com/incident/medical-device-maker-artivion-hit-in-ransomware-attack/ https://therecord.media/artivion-medical-device-company-cyberattack-notice-sec https://thecyberexpress.com/artivion-cyberattack/
2024-12-16	LKQ Corporation (Keystone, Tri Star, ADL)	**Canada**, USA	Discrete Mfg.	U	Unknown	1		SEC 8K	U	Impacted operations "for a few weeks"	LKQ, an aftermarket auto parts manufacturer, made an SEC 8K filing reporting their Canadian business unit fell victim to unauthorized access, impacting operations. On the date of their filing, they reported having resumed operating at near full capacity.	https://icsstrive.com/incident/auto-parts-company-lkq-hit-in-cyberattack-halts-operations/ https://www.securityweek.com/major-auto-parts-firm-lkq-hit-by-cyberattack/ https://www.isssource.com/cyberattack-halts-operations-at-auto-parts-maker-lkq/
2024-12-19	Pittsburg Regional Transit (PRT)	USA	Transport	R	Unknown	1			U	Disrupted rail services temporarily; delayed trains 20+ mins	A ransomware attack disrupted light passenger rail train operations on Thursday morning and launched an investigation. On Jan. 7th 2025, they announced a data breach had occurred but have not named those responsible or given more details.	https://icsstrive.com/incident/ransomware-attack-at-pittsburgh-regional-transit/ https://therecord.media/pittsburgh-regional-transit-attributes-disruptions-to-ransomware-attack https://www.wpxi.com/news/local/internet-outage-that-delayed-t-rail-cars-was-result-ransomware-attack-prt-says/4YCKQXPINJBQRB765RWXZZGCTY/ https://www.trains.com/trn/news-reviews/news-wire/pittsburgh-transit-agency-victim-of-ransomware-attack/
2024-12-25	Azerbaijan Airlines Flight J2-8243	Azerbaijan, Chechnya (Russia)	Transport	NS	Russia	1			DO	Disabled GPS navigation and ADS-B transponder; contributed to a crash; killed 38 passengers	En route to destination Grozny, an Embraer 190 lost both GPS navigation and their ADS-B transponder. This was deliberate, as Russian forces jammed GPS over Grozny while defending the city against possible Ukrainian drone attacks, but they had not yet closed the airspace to civilian flights. The aircraft contacted ATC and attempted landing twice but without GPS. Heavy fog caused ATC to order them to abort and return to Baku. Minutes later, the Embraer was hit by Russian anti-aircraft fire and lost controls ultimately crashing near Aktau while attempting an emergency landing.	https://icsstrive.com/incident/azerbaijani-jet-confused-for-ukrainian-drone/ https://www.cnn.com/2024/12/26/asia/kazakhstan-plane-crash-questions-intl/index.html https://www.iata.org/en/pressroom/2024-releases/2024-12-29-01/ https://en.wikipedia.org/wiki/Azerbaijan_Airlines_Flight_8243

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2024-12-26	Japan Airlines (JAL)	Japan	Transport	U	Unknown	74			ID	Canceled 4 domestic flights, delayed 70 domestic and Int'l flights up to 4 hours, and suspended ticket sales for several hours	A cyberattack impacted systems by overwhelming them with network requests during the busy year-end travel season. This caused the airline to temporarily halt operations because internal and external systems began malfunctioning, including baggage handling systems (BHS). JAL said system outages totaled 6 hours.	https://icsstrive.com/incident/ddos-attack-delays-flights-at-japan-airlines/ https://english.kyodonews.net/news/2024/12/33b9ee9a0030-urgent-jals-system-under-cyberattack-domestic-and-intl-flights-delayed.html https://www.securityweek.com/japan-airlines-was-hit-by-a-cyberattack-delaying-flights-during-the-year-end-holiday-season/ https://www.japantimes.co.jp/news/2024/12/26/japan/jal-cyberattack/
2024-12-29	Peikko Group Corp.	Finland	Discrete Mfg.	R	Akira	12			ID	Halted manufacturing and deliveries, with some countries' operations operating manually, for 12 days	An attack on a manufacturer of pre-cast and in-cast concrete floor structures impacted their Microsoft D365 ERP systems and Telka 3D structural modelling software. In turn, this impacted manufacturing and customer deliveries for days. On January 13, the Akira ransomware group took responsibility for the attack in a data breach.	https://icsstrive.com/incident/cyberattack-impacts-operations-at-finnish-manufacturer-peikko-group/ https://www.isssource.com/attack-slows-manufacturing-for-finlands-peikko-group/ https://www.peikko.com/news/peikko-encounters-a-cyber-attack/ https://www.breachsense.com/breaches/peikko-data-breach/

Incidents in 2023

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-01-09	VDM Metals	Germany	Process Mfg.	U	Unknown	4			U	Production halted; workers sent home 3 wks.	Attack crippled operations for weeks, requiring all on-premises and virtual IT systems to be rebuild or replaced. Specialty ZAC (cybercrime) police in NRW investigate.	https://icsstrive.com/incident/cyberattack-affects-all-locations-of-german-vdm-steel/ https://come-on.de/lennetal/werdohl/vdm-kaempft-sich-zurueck-92061669.html https://hellwegeranzeiger.de/unna/hacker-vdm-metals-lohnabschlag-cyberangriff-w687619-1000725900/ https://come-on.de/lennetal/werdohl/cyberangriff-auf-vdm-metals-92030607.html
2023-01-10	UK Postal Service (Royal Mail)	UK	Transport	R	LockBit 3.0	11500	£42M		ID	Disabled label printers; prevents sending Int'l letters or parcels for 6 wks.	After a LockBit ransomware attack, custom label printers and systems were disabled and hijacked to print ransom notes, halting all mail export services nation-wide.	https://icsstrive.com/incident/ransomware-attack-at-royal-mail-disrupts-international-operations-more-than-a-month/ https://www.telegraph.co.uk/business/2023/01/12/russia-linked-hackers-behind-royal-mail-cyber-attack/ https://bankinfosecurity.com/royal-mail-refused-absurd-lockbit-extortion-demand-a-21214 https://theguardian.com/business/2023/feb/21/royal-mail-international-deliveries-cyber-attack-ransom-strikes
2023-01-11	Morgan Advanced Materials	UK	Discrete Mfg.	U	Unknown	2	£8M	LSE	U	Halted production and shipping	Production and shipping were affected at multiple sites following a cyberattack.	https://icsstrive.com/incident/uk-manufacturer-morgan-advanced-materials-hit-in-cyberattack/ https://therecord.media/morgan-advanced-materials-cyberattack-shares-drop https://therecord.media/british-company-that-helps-make-semiconductors-hit-by-cyber-incident https://cybernews.com/news/morgan-advanced-materials-cyberattack/
2023-01-13	Super Bock Group	Portugal	Food & Bev.	U	Unknown	1			U	Impaired operations, product supply, and delivery	Portugal's largest brewer gave notice that a cyberattack has impaired operations, causing "major restrictions in its supply chain."	https://icsstrive.com/incident/cyberattack-at-super-bock-brewery-affects-operations/ https://theportugalnews.com/news/2023-01-31/restrictions-with-super-bock-after-cyber-attack/74342 https://theregister.com/2023/02/02/super_bock_cyberattack/?utm_source=twitter&utm_medium=twitter&utm_campaign=auto&utm_content=article https://linkedin.com/posts/superbockgroup_superbockgroup-activity-7025903123470725122-ZHY2/
2023-01-17	Exco Tech	Canada	Discrete Mfg.	R	LockBit 3.0	3			IA	Shutdown production at 3 plants for 2 weeks	An attack on three plants in Exco's large mould group, prompting a pre-emptive shutdown to contain the incident. LockBit claimed responsibility.	https://icsstrive.com/incident/production-at-canadian-tool-manufacturer-exco-technologies-interrupted/ https://insurancebusinessmag.com/ca/news/cyber/canadian-manufacturer-takes-debilitating-cyber-hit-434108.aspx https://excocorp.com/2023/01/23/exco-technologies-limited-announces-cyber-security-incident/ https://itworldcanada.com/article/canadian-tool-manufacturer-hit-by-cyber-attack/523620

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-01-17	Fritzmeier Gruppe & M1 Sporttechnik	Germany	Discrete Mfg.	U	Unknown	15			U	Halted production for 7 days & took 4 wks. for full restoration	A criminal investigation is ongoing into a cyberattack at this auto, truck and bike manufacturer that halted production and took weeks to return to normal levels.	https://icsstrive.com/incident/operations-paralyzed-across-all-locations-of-german-automotive-supplier-fritzmeier-gruppe/ https://merkur.de/lokales/muenchen-lk/aying-ort28266/fritzmeier-hacker-angriff-internet-telefon-aying-firma-cybercrime-92037641.html https://merkur.de/lokales/muenchen-lk/hackerangriff-auf-fritzmeier-group-noch-keine-spur-zu-den-erpressern-92105466.html https://radmarkt.de/update-fritzmeier-group-cyber-attacke-m1-produktion-laeuft-wieder/
2023-01-18	Benetton Group (United Colors of Benetton)	Italy	Transport	U	Unknown	1			ID	Delayed and impaired product shipments and orders for 4 days, and furloughed employees	An attack impaired Benetton's main logistical centre in Castrette di Villorba, where it ships products to over 5K global outlets, and is fundamental to its business.	https://icsstrive.com/incident/operations-disrupted-at-italian-clothing-giant-benetton/ https://thecyberexpress.com/italian-clothing-giant-benetton-cyber-attack/ https://trevisotoday.it/economia/benetton-attacco-hacker-22-gennaio-2023.html
2023-01-29	Tribhuvan (Kathmandu) Int'l Airport	Nepal	Transport	U	Unknown	1			ID	Delayed Int'l arrival and departure flights for 3 hours	A DDoS attack on Nepal's Government Integrated Data Centre took down services at the Dept. of Immigration and Passport office, impaired airport kiosks and travel document processing, thereby delaying Int'l flights.	https://icsstrive.com/incident/weekend-ddos-attack-on-400-nepal-government-sites-airport-most-affected/ https://nepalitimes.com/latest/open-season-on-hacking-into-gov-np
2023-02-01	MKS Instruments & Applied Materials	USA	Discrete Mfg.	R	Unknown	1	$450M	SEC	IA	temporarily suspended manufacturing operations	"The incident has affected [...] production-related systems, and as part of the containment effort, the company has elected to temporarily suspend operations" -- SEC filing.	https://icsstrive.com/incident/mks-suspends-operations-to-contain-ransomware-attack/ https://csoonline.com/article/3687098/mks-instruments-falls-victim-to-ransomware-attack.html https://therecord.media/applied-materials-supply-chain-mks-ransomware-attack https://www.bankinfosecurity.com/mks-instruments-ransomware-attack-results-in-200m-sales-hit-a-21442
2023-02-02	Häfele (Hafele, Haefele)	Germany	Discrete Mfg.	R	LockBit 3.0	180			IA	Halted order fulfilment; forced to pre-emptively shut down systems	The kitchen and furniture fitting manufacturer shutdown their IT systems worldwide and disconnected from the internet after the attack.	https://icsstrive.com/incident/ransomware-attack-at-german-furniture-company-hafele/ https://itsecurityguru.org/2023/05/03/hafele-recovers-from-ransomware-attack-using-sase/ https://kbbreview.com/52078/news/hafele-it-systems-down-after-cyber-attack/ https://techepages.com/hafele-suffers-ransomware-attack/
2023-02-09	Ziegler Feuerwehrfahrzeuge	Germany	Discrete Mfg.	R	ALPHV / BlackCat	2			IA	Halted ops 11d, with complete restoration taking 24 days more	All systems went offline following the attack. Remediation and restoration efforts took weeks to check, clean and replace all hardware and software components before resuming ops.	https://icsstrive.com/incident/ransomware-attack-halts-operations-at-ziegler-fire-engine-manufacturer/ https://b2b-cyber-security.de/en/alphv-publishes-data-from-ziegler-fire-brigade-vehicles/ https://hz.de/lokales/giengen/nach-cyberangriff-im-februar-alle-systeme-wiederhergestellt https://hz.de/lokales/giengen/alle-systeme-offline-giengener-unternehmen-nur-stark-eingeschraenkt-arbeitsfaehig

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-02-11	Gates Industrial Corporation plc	USA	Discrete Mfg.	R	BlackBasta	30		SEC, State of Maine	IA	Impacted production and shipments	Worldwide production facilities were shutdown in an abundance of caution after a ransomware attack and were unable to produce or ship product.	https://icsstrive.com/incident/gates-industrial-corporation-takes-systems-offline-temporarily/ https://cybernews.com/security/gates-corporation-ransomware/ https://bizjournals.com/denver/news/2023/02/27/gates-corp-malware-attack-recovery-systems.html https://breachsense.com/breaches/gates-data-breach/
2023-02-23	Dole Food Company	USA	Food & Bev.	R	Unknown	4	$11M	SEC	IA	Shut down North American production, halted and delayed shipments up to 2 wks.	Following the attack, Dole shutdown systems throughout North America and operated some manually, leading to fresh food shortages, like lettuce, throughout North America.	https://icsstrive.com/incident/dole-suffers-ransomware-attack/ https://bleepingcomputer.com/news/security/fruit-giant-dole-suffers-ransomware-attack-impacting-operations https://malwarebytes.com/blog/news/2023/03/food-giant-dole-reveals-more-about-ransomware-attack https://cybersecuritydive.com/news/dole-ransomware-breached-data-workers/653650/
2023-02-24	Rosenbauer	Austria	Discrete Mfg.	R	LockBit 3.0	1			IA	Shut down production at all locations, including Neidling factory, for 2+ weeks	As a precaution, the company shut down all IT systems. However, they also said that affected production, including at their Neidling factory west of St. Polten.	https://icsstrive.com/incident/all-rosenbauer-group-locations-affected-by-cyberattack-claimed-by-lockbit/ https://www.noen.at/st-poelten/neidling-nach-cyber-attacke-rosenbauer-faehrt-it-schrittweise-wieder-hoch-neidling-358205756 https://www.noen.at/st-poelten/auch-werk-in-noe-betroffen-cyber-attacke-auf-feuerwehr-ausruester-rosenbauer-neidling-cyberangriff-rosenbauer-it-infrastruktur-redaktion-356154463 https://feuerwehrmagazin.de/nachrichten/news/rosenbauer-ziel-einer-cyber-attacke-120280
2023-03-01	Steico Group	Germany	Discrete Mfg.	U	Unknown	1		EU MAR	U	Shut down production for several days	Steico discloses in an EU market filing that a cyberattack halted both operations and IT systems.	https://icsstrive.com/incident/steico-group-operations-disrupted-after-cyberattack/ https://csoonline.com/de/a/cyberangriff-auf-deutschen-baustoffproduzent,3674479 https://web.archive.org/web/20230306060223/www.steico.com/de/ https://bnnbloomberg.ca/steico-owner-is-said-to-weigh-sale-of-wood-insulation-maker-1.1919432
2023-03-14	Fiege Logistik (Logistics)	Italy	Transport	R	LockBit 3.0	3			U	Disrupted logistic operations in Italy for 3 days	Lockbit took out 15% of Fiege's Italian logistics. After rushing to isolate the 3 sites, the spread stopped, and restoration began.	https://icsstrive.com/incident/ransomware-attack-at-fiege-logistik-italian-sites/ https://eurotransport.de/artikel/hacker-greifen-fiege-logistik-an-interne-daten-im-darknet-aufgetaucht-11221630.html https://redpacketsecurity.com/lockbit-3-0-ransomware-victim-fiege-com/ https://verkehrsrundschau.de/nachrichten/transport-logistik/cyber-angriff-auf-fiege-3349093
2023-03-17	Alliance Healthcare	Spain	Transport	U	Unknown	850			U	Disrupted distribution of medicine to pharmacies; 1/4 of pharmacies in Catalonia hardest hit	The attack impacted the distribution of medicine to 850 pharmacies, causing supply chain disruptions and delays throughout Spain.	https://icsstrive.com/incident/cyberattack-at-drug-distributor-alliance-healthcare-impacts-pharmacies-in-spain/ https://cybernews.com/news/cyberattack-alliance-healthcare/ https://scmagazine.com/news/cyberattack-hits-spanish-pharmaceutical-company-alliance-healthcare https://thelocal.es/20230323/cyberattack-disrupts-spanish-medicine-distribution

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-03-17	Hahn Group	Germany	Discrete Mfg.	U	Unknown	1			IA	Shut down production 10+ days	After an attack, all systems were switched off as a safety precaution, and rebuilt from a clean-room environment, with full restoration expected to take weeks.	https://icsstrive.com/incident/hahn-group-shuts-down-network-and-systems-after-cyberattack/ https://csoonline.com/de/a/automationsspezialist-von-cyberattacke-betroffen,3674530 https://hahn.group/en/2023/04/14/update-cyber-attack/ https://
2023-03-24	NZZ Mediengruppe Zürich	Switzerland	Process Mfg.	R	Play / PlayCrypt	2			ID	Shut down printing for 2+ weeks, then capacity reduced, for both NZZ and customer CH-Media-Verlag	A Play ransomware attack halted NZZ's printing presses and impacted their customers who depend on their print services.	https://icsstrive.com/incident/swiss-german-language-newspaper-nzz-shut-down-production/ https://swissinfo.ch/eng/business/hacker-group-publishes-stolen-swiss-media-data/48504626 https://breakinglatest.news/technology/nzz-has-to-shut-down-the-newspaper-production-system-after-a-cyber-attack/
2023-03-25	SAF-Holland Group	Germany	Discrete Mfg.	R	ALPHV / BlackCat	2	€41M	EU MAR	U	Interrupted production for 7-14 days, caused 3-month backlog	Filed a 17. 596/2014 MAR report to the EU Parliament following an attack that halted production at multiple locations and disclosed heavy sales losses and remediation expenses.	https://icsstrive.com/incident/cyberattack-at-saf-holland-causes-three-month-production-backlog/ https://eqs-news.com/news/adhoc/saf-holland-se-saf-holland-se-affected-by-cyberattack/1783179 https://www.breachsense.com/breaches/saf-holland-data-breach/ https://globaltrailermag.com/2023/05/09/unexpected-strong-financial-year-start-for-saf-holland/
2023-03-27	CommScope	USA	Discrete Mfg.	R	Vice Society	1			U	Shut down production for 2 days	According to employees, CommScope suffered a ransomware incident that resulted in "several days of widespread disruption, including plant production."	https://icsstrive.com/incident/vice-society-disrupts-operations-at-commscope-and-publishes-employee-pii/ https://techcrunch.com/2023/04/27/commscope-ransomware-data/ https://techcrunch.com/2023/04/17/hackers-publish-sensitive-employee-data-stolen-during-commscope-ransomware-attack/ https://therecord.media/commscope-network-infrastructure-cyberattack-vice-society
2023-03-31	Ustra Deutschlandticket	Germany	Transport	R	Unknown	1			ID	Delayed start and operation of new rail service for 3+ days	A new passenger rail service in Hannover suffered an attack disabling digital signage, telephone, computer, and ticket systems. The service's start was delayed despite trains being capable of moving down the track.	https://icsstrive.com/incident/public-transportation-deutschlandticket-launch-in-germany-disrupted-by-ransomware-attack/ https://bild.de/regional/hannover/hannover-aktuell/cyberattacke-auf-uestra-hacker-stoppen-deutschland-ticket-in-hannover-83439654.bild.html https://csoonline.com/de/a/cyberattacke-auf-hannoversche-verkehrsbetriebe,3674537 https:// https:// https:// https://
2023-04-05	Israel Postal Company	Israel	Transport	H	Anonymous Sudan / #OPIsrael	1			ID	Halted some postal services, including Int'l mail and local courier, for 6+ days	As part of the annual #OPIsrael hacktivist campaign, several services including the sending of Int'l mail and courier services were interrupted, then proactively shut down, while the Cyber Directorate was brought in to assist with investigations and recovery.	https://icsstrive.com/incident/disruption-at-israel-postal-company-after-cyberattack-last-for-6-days/ https://jns.org/cyberattack-shutters-galilee-farm-water-controllers/ https://calcalistech.com/ctechnews/article/hj000lsgm3

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-04-08	Bobst	Switzerland	Discrete Mfg.	R	BlackBasta	1			IA	Disrupted operations 9 days	The sewing machine manufacturer suffered an attack that impacted operations over the Easter long weekend, forcing them to isolate systems and halting production.	https://icsstrive.com/incident/operations-disrupted-at-machine-manufacturer-bobst/ https://24heures.ch/bobst-resiste-a-deux-piratages-informatiques-788144530362 https://inside-it.ch/mutmassliche-abb-hacker-stecken-auch-hinter-angriff-auf-bobst-20230607 https://letemps.ch/economie/cyber/bobst-reussi-dejouer-deux-cyberattaques-ciblees
2023-04-09	Galil Sewage Corp.	Israel	Water	H	GhostSec / #OPIsrael	1			DO	Disabled and defaced water pump controllers 1-day, interrupting wastewater treatment	Internet-exposed Unitronics pump controllers, in operation at farms and the Galil's wastewater facility in the Jordan valley, were defaced and disabled by hacktivists of the annual #OPIsrael campaign. While farms were unaffected and able to run manually, it took Galil a day to resume treatment ops.	https://icsstrive.com/incident/israel-water-monitoring-systems-in-cyber-attack/ https://jns.org/cyberattack-shutters-galilee-farm-water-controllers/ https://securityweek.com/irrigation-systems-in-israel-disrupted-by-hacker-attacks-on-ics/ https://labs.yarix.com/2023/08/ghostsec-the-hacktivist-collective-targeting-icss/
2023-04-12	Fincantieri Marinette Marine (FMM)	USA	Discrete Mfg.	R	Unknown	1			ID	Disabled CNC manufacturing machines 1-2 days; delayed production	Ransomware infected the network, encrypting not only file servers essential to the shipyard's CNC machines, but other services like email, implying an OT dependency on IT services, or a flat network.	https://icsstrive.com/incident/ransomware-attack-delays-shipyard-production-at-marinette-marine-shipyard/ https://news.usni.org/2023/04/20/ransomware-attack-hits-marinette-marine-shipyard-results-in-short-term-delay-of-frigate-freedom-lcs-construction
2023-04-12	Lürssen	Germany	Discrete Mfg.	R	Unknown	1			U	Shut down shipyard operations in Bremen	Ransomware shutdown large parts of shipyard operations at the superyacht and military ship builder for an undisclosed amount of time.	https://icsstrive.com/incident/operations-halted-at-german-superyacht-maker-by-ransomware-attack/ https://therecord.media/german-builder-of-superyachts-and-military-boats https://news.yahoo.com/german-superyacht-maker-targeted-ransomware-123518896.html
2023-04-15	Evotec SE	Germany	Pharma	R	ALPHV / BlackCat	1	> €10M		IA	Shut down proteomics machines, interrupted new drug control studies, lost customers, caused production delays	Pre-emptively chose to shutdown systems to protect company and partner data, temporarily ceasing operations, including proteomics machines and ongoing automated drug control studies. Evotec lost contract customers requiring rapid results which sought out other firms.	https://icsstrive.com/incident/german-biotechnology-company-evotec-shuts-down-it-systems/ https://scbio.org/biotech-ceo-gets-hands-on-after-cyberattack-to-protect-business/ https://therecord.media/german-drug-company-says-cyberattack-causing-delays
2023-04-20	Badische Stahlwerke (BSW) (Baden Steel Works)	Germany	Process Mfg.	U	Unknown	1			IA	Shut down production, furloughed 850 employees	Police are investigating after BSW reported "unauthorized access to its network," then pre-emptively initiated a controlled shut-down of all systems, affecting production.	https://icsstrive.com/incident/german-steelmaker-hacked/ https://stadtanzeiger-ortenau.de/kehl-stadt/c-lokales/hacker-angriff-auf-badischen-stahlwerke_a87063 https://csoonline.com/de/a/cyberattacke-auf-badische-stahlwerke,3674567 https://bo.de/lokales/ortenau/hackerangriff-auf-badische-stahlwerke-in-kehl#

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-04-25	Americold	USA	Bldg. Automation	R	Cactus	250			IA	Shut down all 250 warehouses globally for 1+ wks, halting all inbound and most outbound cold storage	The cold storage company shut down their network to contain a ransomware attack and began to rebuild. Meanwhile, they were unable to accept logistical inbound and all-but critically perishable outbound deliveries at their cold storage facilities. Employees and customers reported on reddit that global ops were shutdown.	https://icsstrive.com/incident/operations-impacted-at-americold-after-network-breach/ https://bleepingcomputer.com/news/security/cold-storage-giant-americold-discloses-data-breach-after-april-malware-attack/ https://therecord.media/cold-storage-company-americold-reports-cyberattack https://reddit.com/r/supplychain/comments/12zjaup/americold_north_america_shutdown/
2023-04-27	Elysée Cosmétiques	France	Process Mfg.	R	Unknown	1	€3M		U	Shut down production 13+ days; furloughed 300 employees	The manufacturer of cosmetic aerosols reported that Russian cybercriminals attacked their centralized servers in Germany and shutdown production.	https://icsstrive.com/incident/french-cosmetics-factory-at-standstill-after-cyberattack/ https://radiomelodie.com/a/18085-elysee-cosmetiques-face-a-une-cyberguerre-selon-son-directeur-general https://republicain-lorrain.fr/economie/2023/05/04/serveurs-pirates-par-des-russes-l-usine-elysee-cosmetiques-a-l-arret
2023-04-29	Maxim Cosmetics	Germany	Process Mfg.	R	BlackBasta	1			IA	Shut down production	An attack encrypted the corporate network, caused the cosmetics manufacturer to pre-emptively shut down all systems and begin remediation. This caused a production shutdown also implying an OT dependency on IT systems.	https://icsstrive.com/incident/emergency-operational-shutdown-at-maxim-german-cosmetics-manufacturer/ https://ksta.de/region/rhein-erft/pulheim/pulheimer-kosmetikhersteller-maxim-will-sich-gegen-neuen-hackerangriff-schuetzen-567732 https://csoonline.com/de/a/ransomware-angriff-auf-kosmetikhersteller-maxim,3680898 https://breachsense.com/breaches/maxim-data-breach/
2023-05-06	Orqa FPV	Croatia	Discrete Mfg.	SC	Swarg	1			DM	Bricked manufactured devices, after a specified date had been reached (time-bomb attack)	A contracted developer planted malicious code into the firmware of Orqa's drone goggles, designed to brick devices after a timestamp is reached. Later, the bad actor offers an unauthorized binary firmware fix, for sale online, marketed as a "license extension and renewal" update. A complex case of ransomware deployed into the supply chain by a malicious insider.	https://icsstrive.com/incident/contractor-inserts-cyber-time-bomb-attack-in-firmware-of-orqa-drone-goggle/ https://cyware.com/news/drone-goggles-maker-orqa-hit-with-time-bomb-ransomware-attack-821e7295 https://theregister.com/2023/05/03/orqa_goggles_borked/ https://bleepingcomputer.com/news/technology/drone-goggles-maker-claims-firmware-sabotaged-to-brick-devices/
2023-05-07	ABB	Switzerland	Discrete Mfg.	R	BlackBasta	1			IA	Lost production and shut down external network connections to customers, in an abundance of caution	Windows AD was attacked by ransomware causing ABB to shut their VPN connections to customers to contain the spread. Manufacturing was also disrupted.	https://icsstrive.com/incident/abb-hit-in-cyberattack-operations-suffer/ https://bleepingcomputer.com/news/security/multinational-tech-firm-abb-hit-by-black-basta-ransomware-attack/ https://cyberplace.social/@GossiTheDog/110355364010961428 https://securityweek.com/industrial-giant-abb-confirms-ransomware-attack-data-theft/

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-05-10	Suzuki Motorcycle India	India	Discrete Mfg.	U	Unknown	1	20,000 units		U	lost production of 20,000+ units, 10+ days downtime	Shutdown manufacturing facilities due to a cyberattack.	https://icsstrive.com/incident/cyberattack-halts-production-at-factories-of-suzuki-motorcycle-india/ https://auto.hindustantimes.com/auto/two-wheelers/suzuki-motorcycle-india-plant-shut-after-cyber-attack-production-affected-41684581981220.html https://autocarpro.in/news/exclusive-suzuki-motorcycle-india-plant-shut-for-a-week-due-to-cyber-attack-115136 https://livemint.com/news/india/hit-by-cyberattack-suzuki-motorcycle-india-halts-production-at-its-factories-report-11684537524538.html
2023-05-11	The Philadelphia Inquirer	USA	Process Mfg.	U	Unknown	1			IA	Lost production for 3 days; halted printing and distribution	Suffered a cyberattack, impacting both IT and OT systems, and prevented the printing and distribution of the regular Sunday May 14 edition.	https://icsstrive.com/incident/philadelphia-inquirer-unable-to-print-sunday-paper/ https://theguardian.com/us-news/2023/may/15/philadelphia-inquirer-cyber-attack https://inquirer.com/news/philadelphia/philadelphia-inquirer-hack-cyber-disruption-20230514.html
2023-05-12	Lacroix	France	Discrete Mfg.	R	Unknown	3			ID	3 factories in France, Germany and Tunisia shut for 10 days	Intercepted a targeted attack on the French (Beaupréau), German (Willich) and Tunisian (Zriba) sites. Downtime was mostly restoration from backups, as all systems were encrypted.	https://icsstrive.com/incident/lacroix-hit-in-cyberattack/ https://techmonitor.ai/technology/cybersecurity/lacroix-cyberattack-factories-closed https://securityweek.com/lacroix-closes-production-sites-following-ransomware-attack/ https://cybernews.com/news/lacroix-data-breach/
2023-05-20	Granules India	India	Pharma	R	LockBit 3.0	1		NSE	ID	Shut down production 40+ days, reported a 'significant loss of revenue'	Regulatory and quality standards could not be met due to major disruptions in the company's IT systems.	https://icsstrive.com/incident/significant-revenue-loss-at-indian-pharmaceutical-giant-after-cyberattack/ https://reuters.com/business/healthcare-pharmaceuticals/paracetamol-maker-granules-india-q1-profit-hurt-by-cyber-attack-disruptions-2023-08-09/ https://thehindubusinessline.com/companies/cyber-attack-has-caused-significant-loss-to-revenue-profitability-granules-india/article67022628.ece https://techcrunch.com/2023/06/15/lockbit-ransomware-granules-india/
2023-06-10	Haynes Int'l	USA	Process Mfg.	R	LockBit 3.0	1	quarterly $18M net revenue or $3.7M EBITDA loss	SEC	U	Shut down production for 11 days and delayed shipments	The attack temporarily disrupted manufacturing ops. and production shipments.	https://icsstrive.com/incident/haynes-international-cyberattack-estimated-cost-is-18-20-million/ https://finance.yahoo.com/news/haynes-hit-cybersecurity-incident-disrupts-035900431.html https://twitter.com/FalconFeedsio/status/1687789436266848256 https://channelchek.com/news-channel/haynes-international-hayn-lowering-estimates-to-reflect-near-term-impact-of-a-cyberattack
2023-06-13	Brunswick Corporation	USA	Discrete Mfg.	U	Unknown	2	up to $85M		U	Halted production & distribution for 17 workdays	An attack on the Mercury Marine outboard motor maker forced them to shutdown during restoration. The CEO stated lost production cannot be recovered due to a full production schedule until end-of-year.	https://icsstrive.com/incident/brunswick-corp-recovering-from-serious-cyberattack/ https://maritime-executive.com/article/brunswick-corp-works-to-recover-from-cyberattack https://boatingindustry.com/top-news/2023/06/27/brunswick-provides-operations-update-following-cyber-attack/ https://cyware.com/news/marine-industry-giant-brunswick-corporation-lost-85-million-in-cyberattack-ceo-confirms-e32f91b2/

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-06-15	KNP Logistics Group	UK	Transport	R	Akira	1	Bankrupt		ID	730 jobs lost, bankrupted company, forced to sell off assets and subsidiaries	An attack forced KNP to lay off 730 workers and close the company, because the ransomware impacted key systems and processes, preventing them from securing additional investment and funding.	https://icsstrive.com/incident/uk-based-knp-logistics-business-shuts-down-700-jobs-lost/ https://bbc.com/news/uk-england-cambridgeshire-66997691 https://therecord.media/knp-logistics-ransomware-insolvency-uk https://cybertalk.org/ransomware-forces-large-logistics-firm-to-close/
2023-06-16	Rheinische Post Mediengruppe	Germany	Process Mfg.	U	Unknown	1			U	Halted print (and online) newspaper production and distribution for at least 1 day	One of the top 5 newspaper publishers in Germany was forced to halt operations and pre-emptively cut themselves off from the internet following a cyberattack.	https://icsstrive.com/incident/cyberattack-causes-widespread-operational-disruption-at-rheinische-post-mediagruppe/ https://tagesschau.de/wirtschaft/unternehmen/rheinische-post-hackerangriff-100.html https://zeit.de/news/2023-06/19/cyberangriff-auf-mediengruppe-zeitungen-mit-notausgaben?utm_referrer=https%3A%2F%2Ficsstrive.com%2F
2023-06-22	Livingston Int'l	Canada	Transport	R	Royal	125			DS	Shut down operations at CAN-US border, and delayed shipments by truck for 2 days	Livingston stated they shutdown because protecting clients' systems and data was of paramount importance, highlighting the lack of segmentation between business data and physical ops.	https://icsstrive.com/incident/giant-north-american-freight-forwarder-livingstone-hit-by-ransomware-attack/ https://trucknews.com/transportation/customs-broker-systems-shutdown-causes-border-delays/1003176137/ https://thecyberexpress.com/royal-ransomware-group-adds-livingston-victim/
2023-07-02	Montpellier-Méditerranée (Fréjorgues) Airport	France	Transport	U	Unknown	1			U	Shut down all internal systems, forcing airport ops to operate manually for several hours; cancelled and delayed flights for a week	The attack, while only causing the airport to operate manually for several hours, had a much longer-term impact of cancelling and delaying flights for a week.	https://icsstrive.com/incident/operations-disrupted-at-montpellier-airport-after-weekend-cyberattack/ https://midilibre.fr/2023/07/02/nos-systemes-ont-ete-hs-durant-plusieurs-heures-une-cyberattaque-tres-violente-contre-laeroport-de-montpellier-11316240.php
2023-07-04	Port of Nagoya	Japan	Transport	NS	Unknown (China)	2			ID	Shut down port for 3 days and a Toyota parts export plant 1 day	Caused disruption to the circulation of goods to and from Japan. Toyota auto shipments and a parts export plant were also affected. Originally attributed to LockBit 3.0 ransomware, sources suggested a month later to the Financial Times that this was a disguised attack by the Chinese government, testing Japan's critical infra.	https://icsstrive.com/incident/container-processing-halted-at-the-port-of-nagoya/ https://bleepingcomputer.com/news/security/japans-largest-port-stops-operations-after-ransomware-attack/ https://cnn.com/2023/07/06/tech/japan-port-ransomware-attack/index.html https://www.ft.com/content/de0042f8-a7ce-4db5-bf7b-aed8ad3a4cfd
2023-07-14	Wildeboer	Germany	Discrete Mfg.	R	Unknown	1			ID	Production halted and 350 employees temporarily laid off with benefits (Kurtzarbeit) for 4+ wks.	While the company says the attack affected its IT systems, production was halted, suggesting operations depends on IT. 350 employees were temporarily laid off and put on state-sponsored benefits.	https://icsstrive.com/incident/ransomware-attack-shuts-down-operations-at-german-manufacturer-wildeboer/ https://csoonline.com/de/a/deutscher-bauproduzent-wildeboer-von-hackerangriff-betroffen,3681028 https://wildeboer.de/en/important-information-attack-on-wildeboer-it-systems/ https://ga-online.de/artikel/1391624/Ostfriesisches-Unternehmen-nach-Cyberattacke-immer-noch-lahmgelegt

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-07-20	Campbell Soup Co.	USA	Food & Bev.	U	Unknown	1			ID	Shut down production 3 days, sent employees home	Campbell's Napoleon, OH plant shutdown due to "IT related complications," exposing an OT dependency on IT systems.	https://icsstrive.com/incident/campbell-soup-shuts-down-oh-site-after-cyberattack/ https://toledoblade.com/business/labor/2023/08/03/three-day-campbell-s-napoleon-plant-outage-due-to-it-problems-company-says/stories/20230803129 https://cybersecuritydive.com/news/campbell-soup-cyberattack-limited-impact/694758/
2023-07-23	Tempur Sealy Int'l	USA	Discrete Mfg.	R	ALPHV / BlackCat	1		SEC	U	Temporarily interrupted operations, losing 1 wk production; sent workers home	In an SEC 8K disclosure filing, Tempur Sealy admitted to the attack. Workers took to social media to talk of being sent home amid production outages.	https://icsstrive.com/incident/tempur-sealy-international-suffers-cyberattack/ https://thecyberexpress.com/tempur-sealy-cyber-attack-blackcat-ransomware/ https://therecord.media/mattress-giant-tempur-sealy-cyberattack
2023-08-15	Clorox	USA	Discrete Mfg.	R	ALPHV/Scattered Spider	1	$49M	SEC	IA	Disrupted operations, delayed production >1 month, lost CISO	In an SEC filing, the company said damage to the IT network "caused widescale disruption of Clorox's operations." Clorox's CISO left during the crisis and the role was filled by a temp.	https://icsstrive.com/incident/cleaning-products-maker-clorox-suffers-attack/ https://theregister.com/2023/09/19/the_clorox_company_admits_cyber/ https://finance.yahoo.com/news/clorox-cyber-chief-leaves-recovery-191819607.html https://www.bnnbloomberg.ca/clorox-security-breach-linked-to-group-behind-casino-hacks-1.1980331
2023-08-25	Polish Rail	Poland	Transport	H	2 Polish citizens	20			DO	Halted 20+ trains and denied service for 2+ hours	Two Polish citizens shut down trains using simple radio equipment, through an outdated system designed to wireless engage onboard emergency brakes. This un-authenticated, un-encrypted VHF 150MHz-band radio protocol was already scheduled for replacement by 2025.	https://icsstrive.com/incident/polish-railways-hack-paralyzed-freight-and-passenger-trains/ https://bbc.com/news/world-europe-66630260?blaid=4990964 https://wired.com/story/poland-train-radio-stop-attack/ https://railjournal.com/technology/unauthorised-radio-stop-signal-disrupts-pkp-operations/
2023-08-29	20+ Civilian and private Jets	Iraq	Transport	U	Unknown	20			DO	Loss of navigation, diverted aircraft from intended path into restricted or dangerous airspace, & endangered lives and flight safety	A novel type of GPS and IRS signal spoofing attack caused over 20 aircraft to suffer complete loss of navigational capability over restricted or dangerous airspace, and unintended flight path divergences in airspace along the Iran / Iraq border.	https://icsstrive.com/incident/fake-gps-signals-in-middle-east-lead-multiple-aircrafts-astray/ https://timesofindia.indiatimes.com/world/rest-of-world/fake-gps-signals-sent-20-aircraft-off-course-in-iranian-airspace/articleshow/104074703.cms?from=mdr https://ops.group/blog/gps-spoofing-update-08nov2023/ https://gcmap.com/featured/20230929
2023-09-06	KIA Motors	USA	Discrete Mfg.	R	Unknown	1			I3	Shut down production for 1 day: disrupted shifts and deliveries	A 3rd party data and services provider to KIA was hit by ransomware, which halted and canceled the first and second shifts at KIA's Georgia plant.	https://icsstrive.com/incident/kia-motors-ga-plant-hit-in-cyber-incident/ https://wrbl.com/news/cybersecurity-incident-disrupting-kia-production-in-west-point-georgia/ https://lagrangenews.com/2023/09/06/kia-hack-temporarily-shuts-down-production/

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-09-08	MGM Resorts	USA	Bldg. Automation	R	ALPHV/Scattered Spider	19	$110M		IA	Shut down ops for 10 days, including phys. access and phones, to all MGM Resort properties in Vegas	Attackers gained initial access through by social engineering a help desk operator, then subsequently encrypting up to 100 Vmware ESXi servers. After discovering signs of intrusion on Sep 10, MGM chose to contain and isolate many systems, exacerbating the situation. Guests reported that hotel room locks were unsecured and telephones inoperable.	https://icsstrive.com/incident/mgm-shuts-down-operations-for-10-days-across-las-vegas-properties/ https://thedeepdive.ca/mgm-resorts-battles-ongoing-cyberattack-disruption-scattered-spider-claims-responsibility/ https://apnews.com/article/mgm-cyberattack-las-vegas-100-million-clorox-087726961b5366065b6231d1d223b4eb https://blog.morphisec.com/mgm-resorts-alphv-spider-ransomware-attack
2023-09-10	ALPS Alpine Co. Ltd.	USA	Discrete Mfg.	R	Blackbyte	2			IA	Partially impacted North American production and shipping for 2+ days	ALPS' North American production operations and delivery were impacted by a ransomware incident. When they discovered the breach, they took steps to isolate systems from the network and began restoration.	https://icsstrive.com/incident/operational-impact-at-electronics-company-alps-alpine-group/ https://www.alpsalpine.com/cms.media/September_12th_Cyber_Attack_ver1_11_31306d3123.pdf https://www.alpsalpine.com/cms.media/September_14th_Cyber_Attack_ver07_5d102b80e5.pdf https://redpacketsecurity.com/blackbyte-ransomware-victim-alps-alpine/
2023-09-14	Canada Border Services Agency (CBSA)	Canada	Transport	H	NoName057(16)	10			DO	Shut down automated border arrival check-in kiosks at multiple Canadian airports for a "few hours" causing significant delays in processing travellers	La Presse reported that the automated kiosk systems should be on a closed circuit and not connected to the internet. Nevertheless, the attack caused significant real-world delays and wait times at heavily automated Canadian airports.	https://icsstrive.com/incident/borderchecks-point-outages-in-canada/ https://lapresse.ca/actualites/2023-09-18/une-attaque-informatique-revendiquee-contre-l-agence-des-services-frontaliers.php https://thecyberexpress.com/cyber-attacks-on-canadian-airports-disrupt-ops/ https://lapresse.ca/actualites/national/2023-09-19/agence-des-services-frontaliers/la-panne-dans-les-aeroports-provenait-bien-d-une-attaque-informatique.php
2023-09-18	Somagic	France	Discrete Mfg.	R	MedusaLocker	1			ID	Shut down production	Employees were surprised when they showed up at work on Monday morning only to discover all their IT systems were rendered unusable and encrypted, halting production.	https://icsstrive.com/incident/operational-impact-at-electronics-company-alps-alpine-group/ https://csidb.net/csidb/incidents/8182c50d-ec4b-4cc9-8ecb-d589e8563b69/ https://lejsl.com/economie/2023/09/21/l-entreprise-bressane-somagic-victime-d-une-cyberattaque-de-grande-ampleur https://redpacketsecurity.com/medusalocker-ransomware-victim-somagic/
2023-09-23	Johnson Controls and subsidiaries York, Tyco, Coleman, Ruskin, and Simplex	USA	Discrete Mfg.	R	Dark Angels	6	$27M	SEC	ID	Shut down manufacturing and disrupted operations, weakened US DHS physical security	VMWare ESXi encryptor malware, designed to spread through a compromised Windows AD server, infected interconnected IT systems at Johnson Controls and subsidiaries. This prompted Johnson to make 3 SEC filings, and lead to a DHS investigation to examine claims that federal building's schematics and security info were leaked.	https://icsstrive.com/incident/massive-ransomware-attack-at-johnson-controls/ https://bleepingcomputer.com/news/security/building-automation-giant-johnson-controls-hit-by-ransomware-attack/ https://cnn.com/2023/09/28/politics/dhs-investigating-ransomware-attack/index.html https://reddit.com/r/HVAC/comments/16t2876/comment/k2cwwvl

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-09-28	Leonardo	Russia	Transport	H	IT Army (Ukraine)	227			DS	Delayed flights at 3 Russian carriers at Airports in Russia, up to 1 hour	A massive DDoS attack on the Leonardo online booking system, used by 50 air carriers in Russia, caused delays of up to 1 hour in Moscow. Big air carriers include Rossiya, Pobeda, and Aeroflot.	https://icsstrive.com/incident/dodds-attack-at-russian-flight-booking-system-leonardo-disrupts-airports/ https://therecord.media/russia-flight-booking-system-leonardo-ddos
2023-10-10	Simpson Manufacturing	USA	Discrete Mfg.	U	Unknown	1		SEC	IA	Caused "wide scale disruption" to operations for 3 days	After the building materials manufacturer realized their IT network problems were in fact a cyberattack, the manufacturer chose to shutdown systems and ops and begin remediation.	https://icsstrive.com/incident/simpson-manufacturing-a-building-materials-maker-attacked/ https://bleepingcomputer.com/news/security/simpson-manufacturing-shuts-down-it-systems-after-cyberattack/ https://ir.simpsonmfg.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=16995846
2023-10-14	Henry Schein	USA	Discrete Mfg.	R	ALPHV / BlackCat	1	$500M	SEC	U	Up to three ransomware attacks encrypted systems and impacted manufacturing and distribution operations for 3+ months	Henry Schein's operations were encrypted on three separate occasions by a ransomware gang. First initially, then by Nov. 3 as negotiations faltered, then a third time on Nov. 22, just as systems were nearing full restoration.	https://icsstrive.com/incident/cyber-incident-at-healthcare-solutions-giant-henry-schein/ https://www.bleepingcomputer.com/news/security/henry-schein-discloses-data-breach-a-year-after-ransomware-attack https://www.bleepingcomputer.com/news/security/healthcare-giant-henry-schein-hit-twice-by-blackcat-ransomware https://cybernews.com/news/alphv-blackcat-re-encrypt-henry-schein-ransom-negotiations-third-time-
2023-10-16	10+ Civilian and private Jets	Egypt	Transport	U	Unknown	10			DO	Loss of navigation, diverted aircraft from intended path into restricted or dangerous airspace, & endangered lives and flight safety	(Similar to 2023-8-29 incident) A novel type of GPS and IRS signal spoofing attack caused 10 aircraft to suffer complete loss of navigational capability, caused unintended flight path divergences over Cairo.	https://icsstrive.com/incident/wide-concern-over-gps-spoofing-incidents-previously-thought-to-be-impossible-in-middle-east/ https://ops.group/blog/gps-spoofing-update-08nov2023/ https://www.forbes.com/sites/erictegler/2023/12/05/gps-spoofing-in-the-middle-east-is-now-capturing-avionics/?sh=6550d5c23a6f https://www.businessinsurance.com/Henry-Schein-cuts-annual-profit-forecast-as-cyberattack-impact-lingers/
2023-10-25	4+ Civilian and private Jets	Israel	Transport	U	Unknown	4			DO	Loss of navigation, diverted aircraft from intended path into restricted or dangerous airspace, & endangered lives and flight safety	(Similar to 2023-8-29 incident) A novel type of GPS and IRS signal spoofing attack caused 4 aircraft to suffer complete loss of navigational capability and caused unintended flight path divergences over Israel, Lebanon, and Jordan.	https://icsstrive.com/incident/wide-concern-over-gps-spoofing-incidents-previously-thought-to-be-impossible-in-middle-east/ https://ops.group/blog/gps-spoofing-update-08nov2023/ https://www.forbes.com/sites/erictegler/2023/12/05/gps-spoofing-in-the-middle-east-is-now-capturing-avionics/?sh=6550d5c23a6f
2023-10-30	Ace Hardware	USA	Transport	U	Unknown	17			ID	Shut down order fulfilment and warehouse distribution operations company-wide, sent workers home for over a week	Ace Hardware's warehousing was hit by a cyberattack that had a wide-ranging impact on the company including warehouse managing systems and other software crucial to physical ops.	https://icsstrive.com/incident/cyberattack-cripples-operations-at-ace-hardware-in-us https://www.theregister.com/2023/10/31/ace_hardware_cyberattack/ https://www.reddit.com/r/sysadmin/comments/17jwvtz/ace_hardware_corp_cybersecurity_incident_10302023/ https://www.bleepingcomputer.com/news/security/ace-hardware-says-1-202-devices-were-hit-during-cyberattack/

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-11-01	Bircher Farm	Switzerland	Food & Bev.	R	Unknown	1	6K Fr.		I3	Caused livestock loss (death) of one animal (1 cow)	The third-party company that supplies robotic milking machines also monitors the cattle herd's health. As this third-party was compromised by ransomware, it was encrypted and stopped operating. Even though the milking machine at Val Bircher's farm were switched to manual operation, an alarm failed to alert to a pregnant cow that had a calf die in her womb. The cow was unable to be saved and had to be put down by a vet.	https://icsstrive.com/incident/small-swiss-farmer-refuses-to-pay-ransomware/ https://www.csoonline.com/article/3484349/ransomware-attack-paralyzes-milking-robots-cow-dead.html https://www.schweizerbauer.ch/politik-wirtschaft/betriebsfuehrung/gehackter-melkroboter-loesegeldforderung-und-eine-tote-kuh
2023-11-10	DP World Australia	Australia	Transport	U	Unknown	4	>$1M		IA	Shut down 4 ports in Australia for 3 days: Melbourne, Freemantle, Botany, Brisbane; caused 10-day backlog of 30K containers	Ports pre-emptively disconnected systems from the internet, which stopped the initial attack on Australian port ops. This resulted in operational downtime. No trace of ransomware was found in systems and the incident investigation continues.	https://icsstrive.com/incident/cyberattack-crippled-facilities-of-large-australia-port-operator/ https://msn.com/en-ae/news/world/dp-world-australia-makes-significant-progress-to-restore-operations-after-cyber-attack/ar-AA1jMEHJ https://theguardian.com/australia-news/2023/nov/13/australian-port-operator-hit-by-cyber-attack-says-cargo-may-be-stranded-for-days https://reuters.com/technology/cybersecurity/dp-world-says-hackers-stole-australian-ports-employee-data-2023-11-28/
2023-11-15	Stellantis / Yanfeng Automotive Interiors	USA, Mexico	Discrete Mfg.	U	Qlin	4	$26M		I3	Disrupted Stellantis' production of Jeep and RAM trucks at 3 plants in Detroit and 1 in Mexico, due to lack of parts supplied from Yanfeng	Stellantis manufacturing plants shut down after a cyberattack hit their external supplier Yangfeng, a vehicle interior manufacturer. In April '24, Stellantis demanded millions in damages from supplier Yanfeng over the incident and related shutdown, which kicked off a bitter contract dispute between the two parties.	https://icsstrive.com/incident/yanfeng-cyberattack-disrupts-production-at-stellantis/ https://automotivelogistics.media/oems/yanfeng-cyberattack-disrupts-production-at-stellantis/44893.article https://carscoops.com/2023/11/stellantis-production-disrupted-after-cyberattack-on-chinese-interior-supplier/ https://carscoops.com/2024/04/stellantis-demands-26m-in-damages-from-chinese-supplier-sparking-lawsuit
2023-11-30	Drum / Binghamstown Group Water Scheme Co-Operative Society	Ireland	Water	NS	CyberAv3ngers (Iran) / Islamic Revolutionary Guard Corps (IRGC)	1			DS	Shut down water distribution to 180 residents for 2 days	Residents lost water after an attack on Unitronics water pump controllers at a local station. The Erris area utility said they did not have the budget for cybersecurity like firewalls, and that after the attack, they struggled to bypass the pump to run manually, leading to the outage.	https://icsstrive.com/incident/pro-iran-hackers-cut-water-supply-for-2-days-in-remote-irish-town/ https://westernpeople.ie/news/hackers-hit-erris-water-in-stance-over-israel_arid-4982.html https://securityweek.com/cyberattack-on-irish-utility-cuts-off-water-supply-for-two-days/
2023-12-07	Serwis Pojazdów Szynowych (SPS)	Poland	Transport	SC	Newag SA	1			DSC	Impaired operations: Sabotaged rolling stock when serviced by third-party workshops	After SPS was contracted to maintain rolling stock for operator Koleje Dolnośląskie, they discovered deliberate code in firmware designed to "brick" controllers, planted by the manufacturer Newag, to enforce vendor maintenance lock-in.	https://icsstrive.com/incident/polish-train-builder-denies-sabotaging-plc-code/ https://theregister.com/2023/12/08/polish_trains_geofenced_allegation/ https://badcyber.com/dieselgate-but-for-trains-some-heavyweight-hardware-hacking/

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2023-12-13	Erfo	Germany	Discrete Mfg.	U	Unknown	1	Bankrupt		U	Shut down production and filed for bankruptcy	This textile fashion brand and manufacturer reported that a cyber attack impacted not only IT but OT systems, impacting production. The impacts were so severe, they pushed the brand to file for insolvency with local courts and seek out new investment to continue operating.	https://icsstrive.com/incident/hackers-paralyzed-operations-of-textile-manufacturer-erfo/ https://www.csoonline.com/article/3495589/erfohackerangriff-fuhrt-zu-insolvenz-bei-textilkonzern.html
2023-12-17	Socadis	Canada	Transport	U	Unknown	1			IA	Halted deliveries and distribution, 4+ days	The company was a victim of a spear phishing attack and isolated all systems to avoid spreading the malware to industry partners.	https://icsstrive.com/incident/large-canadian-book-distributor-suspends-operations-after-cyberattack/ https://ledevoir.com/economie/804162/informatique-cyberattaque-paralyse-maillon-important-livre-quebecois? https://lapresse.ca/arts/litterature/2023-12-20/probleme-de-cybersecurite/les-activites-du-distributeur-de-livres-socadis-sur-pause.php https://facebook.com/socadis/posts/831533385645938?ref=embed_post
2023-12-18	Iranian Gas Stations	Iran	Oil & Gas	H	Predatory Sparrow (Gonjeshke Darande)	2150			DO	Disrupted 70% of national gas stations	Predatory Sparrow took responsibility for another attack on most gas stations in Iran (different from the last one in 2021). Analysis by DarkCell AB suggest that this recent attack is remarkably similar except the attack vector and entry point are different.	https://icsstrive.com/incident/iranian-petrol-stations-hit-by-cyberattack/ https://bbc.com/persian/articles/c51zv8ek8vxo https://reuters.com/world/middle-east/software-problem-disrupts-iranian-gas-stations-fars-2023-12-18/ https://sites.google.com/darkcell.se/www/sparrows
2023-12-18	Yusen Logistics	Japan	Transport	R	ALPHV / BlackCat	2			ID	Delayed delivery; impacted logistics and partner BSH (UK)	Reported a "major problem with IT infrastructure" after an attack impacted invoicing and delivery. Home appliance retailer BSH, a Yusen partner in the UK, was similarly impacted.	https://icsstrive.com/incident/cyberattack-at-yusen-logistics-partner-of-big-kitchen-manufacturers-spells-delays-for-applicance-retailers/ https://kbbreview.com/56802/news/appliance-delivery-woes-return-big-brands-as-tech-glitch-hits-logistics-partner/ https://kbbreview.com/56927/news/appliance-supplier-confirms-delays-due-to-cyber-attack/ https://ransomwareattacks.halcyon.ai/attacks/blackcat-alphv-attacks-yusen-logistics

Incidents in 2022

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2022-01-07	CPH Chemie & Papier Holding	Switzerland, Germany	Process Mfg.	R	Unknown	1			IA	6 days of downtime; lost 8,400 tons in paper output	Newsprint, packaging, and lightweight coated paper (LWC) producer in Perlen and Müllheim was forced into a controlled shutdown after a cyberattack.	https://icsstrive.com/incident/hackers-paralyze-only-newsprinting-facility-in-switzerland/ https://euwid-paper.com/news/markets/cph-to-restart-operations-in-perlen-and-muellheim-by-tomorrow https://www.pulpapernews.com/20220111/13176/cyber-attack-it-systems-cph-group
2022-01-28	Kenyon Produce (KP) Snacks	UK	Food & Bev.	R	Conti	1			ID	Halted production, delayed deliveries for 2 months, & capped orders	Hit by Conti ransomware, the snack maker "cannot safely process orders or dispatch goods." Orders were capped while existing stocks consumed.	https://icsstrive.com/incident/uk-snack-provider-hit-by-ransomware-attack/ https://foodprocessing.com/industrynews/2022/hackers-cripple-kp-snacks
2022-01-29	Marquard & Bahls subsidiaries Mabanaft & Oiltanking	Germany	Oil & Gas	R	ALPHV / BlackCat	11			U	Declared force majeure, halted operations for 2 weeks	BlackCat (ALPHV) ransomware halted loading and unloading of fuel and bulk oil at port and had a minor impact on automotive fuel distribution in Germany.	https://icsstrive.com/incident/german-oil-tank-farm-shut-down/ https://bbc.com/news/technology-60215252
2022-01-30	SEA-Tank & SEA-Invest Group	Belgium, Africa	Oil & Gas	R	ALPHV / BlackCat	24			U	Halted operations at all European and African ports	Every SEA-Tank or SEA-Invest port terminal in Europe and Africa could not unload fuel due to a reported BlackCat (ALPHV) ransomware attack.	https://isssource.com/oil-terminals-in-europe-suffer-cyberattack
2022-02-02	Evos Group	Malta, Belgium, Netherlands	Oil & Gas	U	Unknown	3			U	Delayed unloading fuel at 3 ports: Terneuzen, Ghent, and Birzebbuga	Cyberattack delayed loading and unloading of fuel and bulk oil at port for the storage logistics company. The Malta operation was just recently acquired from Oiltanking.	https://icsstrive.com/incident/malta-oil-terminal-run-by-evos-one-of-several-european-facilities-hit-by-a-cyberattack/ https://insurancejournal.com/news/international/2022/02/03/652169.htm
2022-02-03	Swissport	Switzerland	Transport	R	ALPHV / BlackCat	1			ID	Delayed 22 flights, cargo, and freight services for 20 min	BlackCat (ALPHV) ransomware attack forced Swissport to revert to manual ops and backup procedures.	https://icsstrive.com/incident/ransomware-attack-at-swiss-airport-services-firm https://spiegel.de/netzwelt/web/swissport-hackerangriff-stoert-zeitweise-flugbetrieb-in-der-schweiz-a-44285ac8-ad73-42ea-b751-91559c2ff4c8
2022-02-21	Jawaharlal Nehru Port Container Terminal (JNPCT)	India	Transport	R	Unknown	1			ID	Diverted incoming vessels and halted in-progress loading/unloading at port	Management Information System (MIS) knocked out by ransomware at JNPCT, one of five marine facilities at the Nhava Sheva container gateway.	https://icsstrive.com/incident/ransomware-attack-cripples-indian-port-container-terminal-jncpt/ https://theloadstar.com/ransomware-attack-hits-nhava-sheva-container-terminal
2022-02-22	Expeditors	USA	Transport	R	Unknown	1	$60M		ID	Shut down operations for 3+ weeks	Cannot ship freight or manage customs processing, thereby halting ops. The financial cost to restore systems and in lost business was significant. Occurred two days before the Invasion of Ukraine.	https://icsstrive.com/incident/expeditors-intl-hit-by-ransomware-attack/ https://bleepingcomputer.com/news/security/expeditors-shuts-down-global-operations-after-likely-ransomware-attack

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2022-02-24	Caledonian Modular	UK	Discrete Mfg.	R	Unknown	1	Bankrupt		U	Shut down manufacturing ops.	Modular building manufacturer's lost production output due to the attack and was a major factor in the company's March insolvency. Occurred the day of the Invasion of Ukraine.	https://icsstrive.com/incident/cyber attack-significantly-reduced-caledonian-modulars-operating-capability/ https://theconstructionindex.co.uk/news/view/jrl-buys-caledonian-modular-out-of-administration
2022-02-27	Bridgestone	N. & S. America	Process Mfg.	R	LockBit	23			IA	10 days lost production, and workers sent home, at all 23 tire plants in the Americas	LockBit ransomware prompted the shut down all plants in the western hemisphere, in an abundance of caution, and begin recovery.	https://icsstrive.com/incident/tire-manufacturer-bridgestone-hit-in-ransomware-attack
2022-02-28	Belarus Railway	Belarus	Transport	H	Cyber Partisans (Belarus)	1			DO	Halted trains in Minsk, Orsha, and Osipovichi	The Belarusian "Cyber Partisans" encrypt and disable routing and switching devices, stranding trains at station, to slow Russian troops transiting to the Ukrainian front.	https://icsstrive.com/incident/belarus-rail-network-disrupted-by-hacktivist-group/ https://bqprime.com/amp/technology/belarus-hackers-allegedly-disrupted-trains-to-thwart-russia
2022-02-28	Toyota, Hino, Daihatsu, Kojima Industries	Japan	Discrete Mfg.	R	Unknown	14			I3	Shut down all Japanese auto and truck plants for 1 day, and lost production of 10K units	When 3rd party supplier Kojima was hit by ransomware, Toyota chose to shut down all their Japanese plants in an abundance of caution.	https://isssource.com/toyota-halts-production-after-cyberattack-on-supplier
2022-02-28	Rosetti Energy	Russia	Power	H	AutoEnterprise (Ukraine)	2			DO	Deactivated all EV charging stations between Moscow and St. Petersberg	Hacktivists remotely disable all electric vehicle charging stations along the M-11 motorway and reprogram displays criticizing Russian President Putin.	https://icsstrive.com/incident/russian-electric-vehicle-chargers-hacked-on-m11-highway-as-political-protest https://www.vice.com/en/article/russian-electric-vehicle-chargers-hacked-tell-users-putin-is-a-dickhead/
2022-03-11	H.P. Hood Dairy LLC	USA	Food & Bev.	U	Unknown	13			IA	Shut down production 1 week, disposed all dairy product, canceled orders & deliveries	Cyberattack prompted taking Hood's 13 plants offline in an abundance of caution and could not receive materials to manufacture dairy products.	https://icsstrive.com/incident/dairy-plant-operations-offline-no-milk-at-schools-in-new-england/ https://boston.com/news/local-news/2022/03/18/most-hood-plants-up-and-running-after-cyber-event
2022-03-20	ELTA (Hellenic Post)	Greece	Transport	R	Unknown	1			ID	Disrupted postal services for 17 days, nationally	Unpatched vulnerability led to reverse shell & ransomware deployment, disrupting all mail, financial, and bill payment services processed through the Greek Post.	https://icsstrive.com/incident/ransomware-attack-halts-public-postal-services-in-greece/ https://therecord.media/greeces-national-postal-service-restoring-systems-after-ransomware-attack
2022-03-23	METRANS Rail, HUPAC, Italian State Railways (FS), Italian Rail Network (RFI)	Italy	Transport	R	Hive/Cryptolocker	3			U	Suspended all METRANS, HUPAC and LINEAS freight rail operations in Italy 1 day	A ransomware attack impacted the IT systems at Italian State Railways (FS) and subsidiary Trenitalia and Italian Rail Network (RFI), disrupting ticket sales, passenger information screens, and tablets for railway staff. As a result, Tenitalia shut down IT services, but passenger train services remained operational. However, Czech-based freight operator METRANS said this caused the suspension of all their Italian train operations. HUPAC and LINEAS also said their rail freight ops. were suspended for 24 hours.	https://icsstrive.com/incident/widespread-fallout-after-cyberattack-hits-italys-national-railway-company/ https://www.railjournal.com/infrastructure/italian-railway-it-system-suffers-major-cyber-attack/ https://metrans.eu/hacker-attack-on-the-italian-railway-infrastructure/ https://www.railfreight.com/railfreight/2022/03/25/cyber-attack-on-italian-railway-company-stops-traffic

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2022-03-24	TAVR Corporate Group	Russia	Food & Bev.	U	Unknown	1			U	Shut down production and recorded a "significant economic loss"	TAVR makes 50K tons of meat and sausage in Rostov-on-don, close to the Ukraine border. A rep assessed the event as "meticulously planned and significant sabotage."	https://icsstrive.com/incident/operational-impact-after-cyberattack-at-tavr-food-processing-group-in-russia
2022-04-16	Bulgarian State Post Office	Bulgaria	Transport	R	Unknown	1			DIP	2+ week outage of 26 national postal services, including deliveries	Russian-originated ransomware attack to the Bulgarian Post, where attackers moved laterally into all IT and OT systems affecting all 26 offered services.	https://icsstrive.com/incident/complete-state-postal-system-outage-in-bulgaria/ https://euractiv.com/section/politics/short_news/russian-style-hackers-ruin-bulgarian-post-office
2022-04-17	Costa Rican Customs Service	Costa Rica	Transport	R	Conti & Hive	1			ID	Slowed shipments for > 1 month, and shut down Customs' systems	Small part of a massive Conti and Hive ransomware attack on Costa Rica's government, and container freight shipments to slow to a trickle at the port of Limón.	https://icsstrive.com/incident/costa-rica-declares-national-emergency-in-response-to-ransomware-attack/ https://fas.usda.gov/data/costa-rica-costa-rica-customs-delays-affect-imports
2022-04-18	Sunwing Airlines	Canada	Transport	U	Unknown	1			ID	Shut down check-in systems, delay or cancel 188 flights	Discount holiday carrier's passengers stranded during the busy Easter long weekend, where "a system that is running all the time, which never fails, was hacked."	https://icsstrive.com/incident/check-in-systems-offline-for-days-at-sunwing-airlines/ https://infosecurity-magazine.com/news/cyberattackers-hit-sunwing-airlines
2022-05-05	AGCO	USA & Europe	Discrete Mfg.	R	Unknown	1			ID	Shut down maj. of production in for 15+ days, and sent workers home	Attack on major tractor and equipment manufacturer occurs at the start of planting season, during peak global demand for new equipment and parts from dealers.	https://icsstrive.com/incident/ransomware-attack-at-agco/ https://theregister.com/2022/05/09/farm_machinery_giant_agco_hit
2022-05-25	SpiceJet	India	Transport	R	Unknown	1			ID	Grounded or delayed planes for 5+ hours	Attempted ransomware attack on SpiceJet caused major delays for air travellers, causing a cascading effect on future flight schedules.	https://icsstrive.com/incident/spicejets-low-cost-airline-in-india-systems-and-operations-impacted-by-ransomware-attack
2022-05-31	Foxconn Baja California	Mexico	Discrete Mfg.	R	LockBit	1			U	Disrupted production for 2 weeks, & forced production capacity adjustment	LockBit gang ransomed the plant in Tijuana, which supplies most of California's brand-labeled consumer electronics. 2nd time in 2 years this plant was hit by ransomware.	https://icsstrive.com/incident/foxconn-hit-in-ransomware-attack-for-second-time/ https://therecord.media/foxconn-mexico-factory-operations-gradually-returning-to-normal-after-ransomware-attack
2022-05-31	CMC Electronics	Canada	Discrete Mfg.	R	ALPHV/Unknown	1			IA	Disrupted and delayed ops.	ALPHV ransomware encrypted systems and "disrupted operations" to a key supplier of avionics of Canada's Department of National Defense.	https://icsstrive.com/incident/alphv-ransomware-gang-attacks-canadian-defense-contractor/ https://itworldcanada.com/article/canadian-military-provider-suffered-ransom-attack-says-news-report/487654
2022-06-22	Yodel	UK	Transport	U	Unknown	1			ID	Delayed parcel delivery for millions of customers	Suspected but unconfirmed ransomware attack shuts down critical operations, including delivery tracking, for millions awaiting home delivery of goods and services.	https://icsstrive.com/incident/millions-of-yodel-customers-in-uk-face-parcel-delivery-delays/ https://bleepingcomputer.com/news/security/yodel-parcel-company-confirms-cyberattack-is-disrupting-delivery
2022-06-25	Apetito (Wiltshire Food Farms parent)	UK	Food & Bev.	R	Hive	1			ID	5-day halt to food deliveries, and rebuilt systems	Hive ransomware hits Meals-on-wheels serving institutions and the vulnerable. Apetito reverted to manual procedures and a complete system rebuild to restore ops.	https://icsstrive.com/incident/apetitos-security-systems-breached-in-sophisticated-cyberattack

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2022-06-25	Macmillan Publishers	UK, USA	Transport	R	Unknown	2			ID	Halted orders & shipments; backlogged regional warehouses for months	Ransomware attack on a major publisher closed offices in NYC and London, disrupting order processing, and causing months of delivery backlogs at regional warehouses.	https://icsstrive.com/incident/cyber attack-forces-macmillan-publishers-to-take-operations-offline-and-close-physical-offices
2022-06-27	Khuzestan Steel (KSC), Mobarakeh Steel (MSC), & Hormozgan Steel (HOSCO)	Iran	Metals & Mining	H	Predatory Sparrow (Gonjeshk e Darande)	1			DO	Damaged equipment and halted production at the KSC plant.	Predatory Sparrow group claimed responsibility set the KSC plant on fire and posted CCTV of the incident on twitter. Damage reports on MSC and HOSCO remain unconfirmed.	https://icsstrive.com/incident/khuze stan-steel-hit-in-cyber-attack-production-halts/ https://timesofisrael.com/large-cyberattack-on-iranian-industrial-sector-targets-three-steel-plants
2022-06-29	Knauf	UK	Process Mfg.	R	BlackBasta	2			IA	Shut down production for 3+ weeks; Delayed existing and canceled all new orders	After a BlackBasta ransomware attack, Knauf pre-emptively shut down to facilitate recovery and forensics, and operated both plants manually.	https://icsstrive.com/incident/large st-building-material-producer-attacked-by-black-basta/ https://techmonitor.ai/technology/cybersecurity/knauf-cyberattack-blackbasta-ransomware
2022-07-18	Eglo	Austria	Discrete Mfg.	R	Unknown	1			U	Shut down production, order processing and shipping for 12 days	Lighting manufacturer's CEO confirmed the ransomware attack but noted that no ransom note had been received by the time they begun recovery.	https://icsstrive.com/incident/hacke rs-paralyzed-computer-system-at-austrian-light-manufacturer-eglo/ https://diepresse.com/6167688/tirol er-leuchtenhersteller-eglo-von-cyber-angriff-getroffen
2022-07-29	Semikron-Danfoss	Germany	Discrete Mfg.	R	Unknown	8			U	Shut down production for months	A power-electronics semiconductor maker for ICS, EVs and wind turbines suffered a LV ransomware attack, and was not fully restored months after the incident.	https://icsstrive.com/incident/semik ron-holding-production-after-cyber-attack/ https://bleepingcomputer.com/new s/security/semiconductor-manufacturer-semikron-hit-by-lv-ransomware-attack
2022-08-05	Ontario Cannabis Retail Corporation (OCS)	Canada	Transport	U	Unknown	1			U	Halted delivery & distribution province-wide for 5 days	Through the OCS crown corporation, the provincial government of Ontario controls and regulates the supply of cannabis to all retail stores.	https://icsstrive.com/incident/us-supply-chain-cyberattack-affects-ontario-cannabis-retail-corporation-ocs-deliveries/ https://cbc.ca/news/canada/toront o/ontario-cannabis-store-1.6549657
2022-08-08	Bombardier Recreationa l Products (BRP)	Austria, Canada, Finland, USA	Discrete Mfg.	R	RansomExx	4			I3	Shut down production and halted order fulfillment for 1 week	The malware infection was traced to a service provider. RansomExx gang published all exfiltrated data from BRP after they refused to pay the ransom.	https://icsstrive.com/incident/brp-suspends-operations-following-ransomware-attack/ https://bleepingcomputer.com/new s/security/ransomexx-claims-ransomware-attack-on-sea-doo-ski-doo-maker
2022-08-13	Apex Capital / TCS Fuel	USA	Transport	R	BlackByte	1			ID	Shut down operations for 1 week	BlackByte ransomware on TCS Fuel impacted small-business truckers, who were unable to fuel their trucks or access funds to pay their owner-operators.	https://icsstrive.com/incident/syste m-outage-at-apex-capital-affects-medium-and-small-size-trucking-companies
2022-09-02	Novosibirsk City Transport Traffic Managemen t System	Russia	Transport	H	Team OneFist (Ukraine)	1			DO	Shut down and disrupted public transportation for 2+ days	Pro-Ukrainian activists Team OneFist causes traffic chaos, by halting and damaging the public transit scheduling system and signage, to prevent a quick recovery.	https://icsstrive.com/incident/novos ibirsk-transportation-system-attacked-by-pro-ukranian-hacker-group/ https://ibtimes.com/russians-novosibirsk-forced-pound-pavements-team-onefist-paralyzes-traffic-exclusive-3611628
2022-09-03	Yandex Taxi	Russia	Transport	H	Anonymou s [OpRussia]	1			DO	Disrupted Moscow traffic for 3+ hours	Hacktivists caused traffic chaos, in an attack that simultaneously dispatched all Yandex's Taxi cars to the same location, resulting in a massive traffic jam.	https://icsstrive.com/incident/chao s-in-moscow-traffic-caused-by-yandex-taxis-software-hack https://securityaffairs.com/135280/hacktivism/anonyomus-hacked-yandex-taxi.html

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2022-09-05	Läderach	Switzerland	Food & Bev.	R	Unknown	1			DS	Halted production, logistics and administration for 67 days	A ransomware attack on the chocolatier causes a long-term outage and impacts logistics. After Läderach refuses to pay the ransom, all data is leaked.	https://icsstrive.com/incident/operations-impacted-at-swiss-chocolate-manufacturer-laderach
2022-09-26	Electricity Company of Ghana (ECG)	Ghana	Power	R	Unknown	1			ID	5+ days of power outages for pre-paid customers	A ransomware attack disables ECG's billing system and the IT network, leaving commercial and residential customers in the dark and unable to purchase power.	https://icsstrive.com/incident/ransomware-attack-at-electric-company-of-ghana-left-customers-without-power-for-days
2022-10-05	HiPP	Germany	Food & Bev.	U	Unknown	1			DS	Shut down production for days, and 1000 employees sent home	Pfaffenhofen, Bavaria based baby food manufacturer, which sells worldwide, was hit by an attack which shutdown both IT and OT systems.	https://icsstrive.com/incident/ot-systems-impacted-at-german-baby-food-manufacturer/ https://csoonline.com/de/a/hipp-gehackt,3674208
2022-10-12	Undisclosed Ukrainian Power Facilities	Ukraine	Power	NS	Sandworm [GRU Unit 74455] (Russia)	1			DO	Caused two power outages	Sandworm (Russian GRU Main Intelligence Directorate) caused two separate power outages on Oct. 12 and 14th. Coincided with a kinetic strike on critical infra. Mandiant released details in a November 2023 public report.	https://icsstrive.com/incident/russian-sandworm-behind-operational-disruption-of-ukraine-energy-facility-in-october-2022/ https://mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology
2022-10-14	Heilbronner Stimme & Stimme Mediengruppe	Germany	Process Mfg.	R	Unknown	1			DS	Shut down operations and sent employees home; impacted regional partners	Printing presses halted after a ransomware attack, stopping distribution of the Heilbronner Stimme and other regional publications printed under contract.	https://icsstrive.com/incident/ransomware-attack-cripples-printing-systems-at-german-newspaper/ https://bleepingcomputer.com/news/security/ransomware-attack-halts-circulation-of-some-german-newspapers
2022-10-28	Aurubis AG	Germany, USA	Metals & Mining	U	Unknown	1			IA	Production and delivery halted, and employees sent home, in Buffalo, NY	Europe's largest copper smelter admitted to isolating from the internet, and operating manually, but local news in Buffalo reported their copper wire plant was shutdown.	https://icsstrive.com/incident/hackers-shut-down-production-at-cartonnerie-gondardennes-in-france/ https://hackread.com/copper-producer-aurubis-cyberattack
2022-10-29	Danish Rails (DSB) / Supeo	Denmark	Transport	R	Unknown	1			I3	Shut down train service for several hours	Denmark's largest rail operator halted due to cyberattack on 3rd party Supeo. Supeo was unable to offer their critical, real-time safety data to train drivers.	https://isssource.com/trains-halted-in-denmark-after-cyberattack https://reuters.com/technology/danish-train-standstill-saturday-caused-by-cyber-attack-2022-11-03/
2022-10-31	Cartonnerie Gondardennes	France	Process Mfg.	R	Unknown	1			DS	Shut down production for 3 days, and workers sent home	This cardboard maker avoided paying a ransom as systems were decrypted by a local journalist and cyber expert Damien Bancal.	https://icsstrive.com/incident/hackers-shut-down-production-at-cartonnerie-gondardennes-in-france/ https://lavoixdunord.fr/1250765/article/2022-11-07/le-piratage-cartonnerie-gondardennes-decrypte-par-damien-bancal-journaliste
2022-11-02	Jeppesen, a wholly owned Boeing subsidiary	Global	Transport	R	Unknown	1			I3	Delayed flights at multiple airlines & impacted flight planning for 14 days	Ransomware shutdown 6 Electronic Flight Bag (EFB) apps & services provided by Jeppesen, increasing pilot's workloads in flight planning and navigation.	https://icsstrive.com/incident/cyberattack-attack-at-boeing-subsidiary-causes-widespread-flight-disruptions https://ops.group/blog/jeppesen-ransomware-attack-update
2022-11-05	Uponor Oyj	Finland	Discrete Mfg.	R	Unknown	1			IA	Shut down production for 1 week, then reduced capacity for 2+ weeks	The manufacturer of HVAC, plumbing, and infrastructure products shutdown all OT systems as a precaution, and restoration took weeks.	https://icsstrive.com/incident/operational-shutdown-at-uponor-intelligent-plumbing-climate-solutions

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2022-11-05	PGT Innovations	USA	Discrete Mfg.	R	Unknown	2	$12M		U	Impacted production at 2 plants, and contributed to a $12m loss	A ransomware attack impacted 2 window and door manufacturing plants in Florida and contributed to $12m quarterly revenue loss.	https://icsstrive.com/incident/ransomware-attack-at-window-and-door-manufacturer-pgt-innovations
2022-11-06	Maple Leaf Foods	Canada	Food & Bev.	R	BlackBasta	1			U	Disrupted operations and services at multiple sites	BlackBasta lists MapleLeaf as one of its victims on the dark web, but Maple Leaf releases little else about the attack other than the impact to ops.	https://icsstrive.com/incident/system-outage-at-maple-leaf-food-manufacturer-in-canada/ https://just-food.com/news/canadas-maple-leaf-foods-hit-by-cyberattack
2022-11-17	Taxis Coop Québec	Canada	Transport	R	Unknown	1			IA	Shut down taxi dispatch system for 2.5 hours in the early morning	Ransomware breached Taxi Coop Quebec's ride hailing back-end systems, so staff pre-emptively shut down all servers and began recovery.	https://icsstrive.com/incident/taxi-ride-hailing-service-in-quebec-hacked/ https://ici.radio-canada.ca/nouvelle/1933690/taxi-coop-quebec-cyberattaque-informatique
2022-11-17	Europea Microfusioni Aerospaziali (EMA)	Italy	Discrete Mfg.	R	Unknown	1			U	Shut down production line for 6+ days, and sent employees home	EMA, a precision investment casting leader, was hit by ransomware production lines were shutdown. 40 techs and specialists were sent in to assist.	https://icsstrive.com/incident/cyberattack-shuts-down-operations-at-precision-casting-foundry-europea-microfusioni-aerospaziali
2022-11-21	Communauto	Canada	Transport	U	Unknown	1			DS	Shut down ride-sharing operations & services for 1 day	A cyberattack prevented users from starting or ending a ride, during an existing industry shortage of vehicles, frustrating users struggling to reserve a car.	https://icsstrive.com/incident/cyberattack-hits-communauto-operations-already-struggling-with-frustrated-customers
2022-11-25	Prophete / VSF Fahrradmanufaktur, Rabeneick and Kreidler	Germany	Discrete Mfg.	R	Unknown	1	Bankrupt		ID	Shut down operations for 3+ weeks and lead to insolvency	Ransomware attack meant that parts did not arrive, bicycles were not fully assembled and delivered, and shareholder injections could not be secured.	https://icsstrive.com/incident/downtime-caused-by-cyberattack-final-straw-for-german-bicycle-manufacturer
2022-11-25	Cobolux	Luxembourg	Food & Bev.	R	Unknown	1	€400K		ID	1 day production loss; Estimated €400K - €500K in damages and restoration costs	Ransomware attack made it impossible to continue operating, because meat products could not be labeled, a regulated and food safety requirement.	https://icsstrive.com/incident/production-halted-at-meat-processing-factory-in-luxembourg
2022-12-10	UNOX	Italy	Discrete Mfg.	U	Unknown	1			IA	Shut down production for 2 days	Hit by a cyberattack, the company activated emergency procedures, suspended production as a safety measure, and initiated "appropriate checks."	https://icsstrive.com/incident/italian-oven-manufacturer-suspends-production-after-cyberattack
2022-12-11	Fruttagel	Italy	Food & Bev.	R	ALPHV / BlackCat	1			U	Shut down production for 4+ days	A BlackCat (ALPHV) ransomware attack on Fruttagel halted production and prevented customer deliveries.	https://icsstrive.com/incident/production-outage-after-massive-ransomware-attack-at-italian-fruttagel
2022-12-13	Empresas Públicas de Medellín (EPM)	Colombia	Water	R	ALPHV / BlackCat	1			ID	Trucked in water for 28k customers on pre-paid service plans	A BlackCat (ALPHV) ransomware attack shut off water for 28K customers unable to pre-pay for service, due to an OT dependence on IT and billing systems.	https://isssource.com/ransomware-attack-at-colombian-utility
2022-12-22	Technolit GmbH, in Grossenlüder	Germany	Discrete Mfg.	U	Unknown	1			U	Shut down operations and sent employees home	A German manufacturer and distributor of welding supplies and products was shutdown by an unknown cyberattack.	https://icsstrive.com/incident/cyberattack-at-technolit-gmbh-employees-sent-home
2022-12-27	Copper Mountain Mining Corporation (CMMC)	Canada	Metals & Mining	R	Unknown	1			IA	Shut down operations for 5 days (pre-emptive), then reduced production for 4 days	CMMC shutdown mining ops out of an abundance of caution, after an attack possibly enabled by passwords leaked on the dark web weeks earlier.	https://isssource.com/copper-miner-hit-in-ransomware-attack

Incidents in 2021

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2021-01-23	Westrock	USA	Process Mfg.	R	Unknown	1			IA	Forced manual ops, reduced production by 85K tons, and delayed shipments	After the packaging manufacturer was hit by ransomware, they shutdown systems in an abundance of caution, which impacted production and shipment volumes.	https://icsstrive.com/incident/ransomware-attack-on-westrock/ https://ir.westrock.com/press-releases/press-release-details/2021/WestRock-Provides-Update-on-Ransomware-Incident-8dfde2fca/default.aspx https://securityweek.com/packaging-giant-westrock-says-ransomware-attack-impacted-ot-systems
2021-01-26	Palfinger AG	Europe, N. & S. America, Asia	Discrete Mfg.	R	Unknown	31			IA	Lost nearly 2 weeks crane production at all plants	The world's largest crane manufacturer. All global plants were affected.	https://icsstrive.com/incident/austria-crane-maker-under-attack/ https://bitdefender.com.au/blog/hotforsecurity/worlds-largest-crane-maker-suffers-global-cyber-attack-operations-at-a-halt https://www.internationalcranes.media/news/palfinger-attack-highlights-escalation-in-cyber-crimes/8013885.article
2021-02-18	Beneteau SA	France	Discrete Mfg.	R	Unknown	2			IA	Shut down for 3-4 weeks at several plants	Boat manufacturer hit by ransomware, impacting OT. Production shutdown or delayed at "several sites". Wiped out 2021 growth, according to CEO.	https://icsstrive.com/incident/french-boat-maker-beneteau-hit-by-cyberattack/ https://boatindustry.com/news/36934/beneteau-2021-growth-almost-evaporated-in-cyber-attack https://press.beneteau-group.com/assets/210221-beneteau-information-regarding-a-cyberattack-5e06-49529.html
2021-03-11	Molson Coors	USA, Canada, UK	Food & Bev.	R	Unknown	13	$120M		IA	Disrupted brewery production and shipments, delaying 120-$140m in earnings	Took all systems offline to contain the spread. By end of the month was still dealing with delays and disruptions UK, Canada, and USA.	https://icsstrive.com/incident/major-brewer-molson-coors-hit-by-cyberattack/ https://bleepingcomputer.com/news/security/molson-coors-brewing-operations-disrupted-by-cyberattack https://securityweek.com/molson-coors-cyberattack-storms-could-cost-company-140-million
2021-03-20	Sierra Wireless	Canada	Discrete Mfg.	R	Unknown	1			IA	Halted production at all manufacturing sites	IoT, cellular, and wireless device manufacturer with an unknown number of manufacturing sites.	https://isssource.com/sierra-wireless-hit-by-ransomware-attack
2021-03-25	Asteelflash Group SA	France	Discrete Mfg.	R	REvil	20			IA	Shut down multiple printed circuit board plants	A leading Electronics Manufacturing Services (EMS) company suffered a REvil ransomware attack.	https://icsstrive.com/incident/revil-ransomware-shut-down-multiple-plants-at-asteelflash
2021-04-01	JBI Bike	USA	Transport	R	Unknown	11			ID	Delayed shipments for 7+ days	A wholesale bicycle and parts distributor, with 11 warehouses, where only some were back up a week after the attack.	https://icsstrive.com/incident/jbi-bicycle-retailer-halts-shipments-due-to-cyberattack/ https://bicycleretailer.com/industry-news/2021/04/07/jbi-back-online-limited-capacity-after-ransomware-attack#.ZBip3PbMKdY
2021-04-04	Bakkier Logistiek	Netherlands	Transport	R	Unknown	1			ID	Disrupted new orders, delayed shipments to retail outlets for 5 days	Caused shortages of packaged cheese at retail.	https://icsstrive.com/incident/ransomware-attack-at-bakker-logistiek-caused-cheese-shortage-in-dutch-supermarkets

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2021-05-07	Colonial Pipeline	USA	Oil & Gas	R	DarkSide	1	$52M		IA	Shut down pipeline for 6 days, paid a $4.4M ransom, & lost (WF) estimated $50m in revenue (FBI recovered $2.2M)	DarkSide ransomware behind attack on the largest gasoline pipeline in USA, triggering widespread gasoline shortages in US Northeast.	https://icsstrive.com/incident/colonial-pipeline-ops-shut-down-after-ransomware-attack
2021-05-20	Ardagh Group	UK	Process Mfg.	R	Unknown	1	$34M		ID	Slowed production and delayed shipments	Metal and glass beverage packaging facilities remained operational, but some processes reverted to manual operation causing shipment delays.	https://isssource.com/eu-packaging-maker-hit-by-cyberattack
2021-05-21	Siegfried Group	Switzerland, Germany	Pharma	U	Unknown	2			U	Shut down operations and impacted production	A cyberattack cause several sites to shutdown operations. The company said production shortfalls are expected to be made up by end-of-year.	https://icsstrive.com/incident/swiss-drug-manufacturer-siegfried-shuts-down-production-after-cyberattack/ https://www.siegfried.ch/siegfried-restarts-production-after-cyber-attack/ https://cen.acs.org/business/specialty-chemicals/Siegfried-Brenntag-Symrise-hit-cyberattacks/99/i20
2021-05-30	JBS SA	Australia, Canada, USA	Food & Bev.	R	REvil	5	$11M		IA	Several large meatpacking plants shut down and sent workers home	Plants in Nebraska, Colorado, Texas, Brooks, and Australia canceled production shifts. REvil the top suspect.	https://icsstrive.com/incident/attack-shuts-operations-of-global-meat-provider/ https://cbc.ca/news/business/jbs-meat-cyberattack-1.6048942 https://www.cbc.ca/news/canada/calgary/jbs-canada-cyberattack-1.6060121 https://cnn.com/2021/07/13/tech/revil-ransomware-disappears/index.html
2021-07-09	Iran Rails	Iran	Transport	H	Predatory Sparrow (Gonjeshke Darande)	1			DO	Impaired service by reprogramming signs and wiping computers	Targeted by the Predatory Sparrow group, infected with wiper malware, and reprogrammed rail signage causing "unprecedented chaos."	https://icsstrive.com/incident/irans-rail-service-delayed-with-fake-messages/ https://nytimes.com/2021/08/14/world/middleeast/iran-trains-cyberattack.html https://theguardian.com/world/2021/jul/11/cyber-attack-hits-irans-transport-ministry-and-railways
2021-07-22	Transnet	South Africa	Transport	R	Unknown	4			U	Declared Force Majeure and halted operations for 7 days	Transnet said ports at Durban, Ngqura, Port Elizabeth and Cape Town were affected.	https://icsstrive.com/incident/attacks-shuts-south-africa-port-ops/ https://reuters.com/article/us-transnet-cyber-idUSKBN2EZ0RQ
2021-09-17	New Cooperative	USA	Food & Bev.	R	BlackMatter	1			IA	Delayed grain receipts & shipments, & shut down fertigation optimization system	A BlackMatter ransomware attack impacted grain transactions during harvest season. Systems were pre-emptively shutdown to stop the spread.	https://icsstrive.com/incident/ia-ag-cooperative-hit-in-ransomware-attack
2021-09-19	Crystal Valley Cooperative	USA	Food & Bev.	R	Unknown	1			IA	Shut down for 4 days and reverted to manual ops.	During harvest season were unable to mix fertilizer, fulfil livestock feed orders, and switched to manual ops for receiving grain by issuing paper receipts.	https://icsstrive.com/incident/ransomware-attack-forces-agricultural-grain-firm-in-minnesota-to-take-systems-offline
2021-09-21	Weir Group	UK	Discrete Mfg.	R	Unknown	1	£20M		IA	Disrupted manufacturing, engineering, and shipping	When the attack was detected, "systems promptly responded by shutting down core operations." Loss projected at £20-30m.	https://icsstrive.com/incident/weir-group-ransomware-incident
2021-10-09	Ferrara	USA	Food & Bev.	R	Unknown	2			U	Shut down operations and delayed shipments for more than two weeks	Candymaker suffered production shutdowns prior to Halloween, but had only resumed production in "select facilities" two weeks later.	https://icsstrive.com/incident/ransomware-strikes-candymaker/ https://cyberscoop.com/candy-corn-hack-halloween https://manufacturing.net/home/news/13165782/ferrero-to-acquire-ferrara-candy-company

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2021-10-22	Schreiber Foods	USA, Europe, S. America	Food & Bev.	R	Unknown	30			U	Shut down production and delivery for 5 days, and disrupted dairy supply chain	Large cheese and yogurt manufacturer could not receive, produce, or ship dairy product due to an attack on their plants and distribution centers	https://icsstrive.com/incident/ransomware-attack-disrupted-entire-milk-supply-chain-at-scheiber-foods-for-days/ https://cyberscoop.com/schreiber-foods-cyber-event-ransomware-agriculture-food https://wisfarmer.com/story/news/2021/10/26/schreiber-foods-hit-cyberattack-plants-closed/8558252002
2021-10-24	Eberspaecher Group	Germany	Discrete Mfg.	R	Unknown	80	$60M		ID	Impacted parts production, closed factories, and impacted workers	Attack encrypted systems across their global IT network, impacted manufacturing, and cited in annual report as reason for a 2022 net loss.	https://icsstrive.com/incident/cyberattack-cost-eberspacher-automotive-supplier-60million-says-ceo/ https://rvbusiness.com/report-eberspaecher-still-delivering-parts-amid-cyberattack/ https://www.eberspaecher.com/fileadmin/data/corporatesite/pdf/en/7_company/EB_Annual_Report_01.pdf
2021-10-26	Gas stations in Iran	Iran	Oil & Gas	H	Predatory Sparrow (Gonjeshke Darande)	4300			ID	Long line-ups and closed stations for 4-5 days	Predatory Sparrow group disabled system supporting cards used to buy discounted gasoline.	https://icsstrive.com/incident/iran-says-cyberattack-closes-gas-stations-across-country/ https://bbc.com/news/world-middle-east-59062907 https://iranprimer.usip.org/blog/2021/nov/02/israel-iran-cyber-war-gas-station-attack
2021-11	Madix Inc	USA	Discrete Mfg.	R	Unknown	2			U	Shut down production, sent employees home	Manufacture of store fixtures halted at both Goodwater and Eclectic plants.	https://icsstrive.com/incident/ransomware-hits-store-fixture-manufacturer/ https://newsbreak.com/news/2435633463049-ransomware-attack-at-alabama-manufacturing-plants-send-hundreds-of-employees-home-with-no-specified-date-of-return
2021-11-07	Diamond Comic Book Distributors	USA	Transport	R	Unknown	1			DS	Delayed retail shipments by 2-4 days, twice	A top distributor for Marvel, Dark Horse and Image comics temporarily halted scheduled orders after a ransomware attack prevented delivery.	https://icsstrive.com/incident/ransomware-attack-at-diamond-comic-distributors-disrupts-retailer-shipments
2021-11-08	Estrella Damm Brewery	Spain	Food & Bev.	R	Unknown	2			DS	Shut down production for 5 days at all breweries (impacted bottling)	Had this occurred in the summer, consequences would have been more severe as stocks only last 3 days.	https://icsstrive.com/incident/barcelonas-damm-brewery-ransomware-attack
2021-12-01	Bay & Bay Transportation	USA	Transport	R	Conti	1			IA	Lost 1.5 weeks of production	Hit by Conti ransomware, systems were taken offline and remediated.	https://icsstrive.com/incident/mn-trucking-and-logistics-company-hit-by-ransomware-attack-again/ https://freightwaves.com/news/minnesota-trucking-company-hit-in-2nd-ransomware-attack
2021-12-21	Nortura	Norway	Food & Bev.	R	Unknown	2			IA	Production halted at several sites for more than a week	Shutdown meat processing plants after a ransomware attack, with one report of animals destined for slaughter being diverted to competitors.	https://icsstrive.com/incident/norwegian-food-producer-hit-in-cyberattack https://web.archive.org/web/20220701083242/norwaytoday.info/news/slaughter-pigs-sent-to-a-competitor-after-the-data-attack-on-nortura
2021-12-28	Amedia	Norway	Process Mfg.	U	Unknown	1			U	Shut down printing presses for 1.5 days	Norway's largest local news publisher was forced to shut down their presses after an unspecified cyberattack shut them down.	https://icsstrive.com/incident/norway-media-company-amedia-hit-in-cyberattack

Incidents in 2020

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2020-01-13	Picanol	Belgium, Romania, China	Discrete Mfg.	R	Unknown	3	€1M		U	Shut down manufacturing plants for 1 weeks, and sent workers home	As a manufacturer of weaving machines, Picanol's manufacturing plants are heavily automated. Financial impact amounts paid for external experts.	https://icsstrive.com/incident/ransomware-attack-shuts-down-production-at-loom-manufacturer-in-belgium/ https://picanolgroup.com/en/investors/press-releases/press-release-cyber-attack-update-january-31-2020
2020-01-31	Toll Group	Australia	Transport	R	Unknown	1			IA	Shut down systems and reverted to manual ops.	Australian-based global logistics company suffered a targeted ransomware attack, and shutdown automation in an abundance of caution.	https://icsstrive.com/incident/toll-group-has-large-portion-of-it-infrastructre-taken-out-by-ransomeware-attack/ https://zdnet.com/article/deliveries-stranded-across-australia-as-toll-confirms-ransomware-attack https://zdnet.com/article/toll-group-shuts-down-it-systems-in-response-to-cybersecurity-incident
2020-02-24	KHS Bicycles	USA	Discrete Mfg.	R	Unknown	1			ID	Delayed shipments for 2 days	Could not process B2B orders and ship bikes following a ransomware attack over the weekend.	https://icsstrive.com/incident/khs-bicycle-shipments-delayed-for-2-days-after-cyberattack/ https://bicycleretailer.com/industry-news/2020/02/25/khs-bicycles-systems-hacked-distributor-halts-shipments#.YG3-wC1h3ox
2020-03-04	EVRAZ manufacturing	USA & Canada	Process Mfg.	R	Unknown	2			ID	Shut down operations at several plants, and sent 900+ workers home for 3+ days	After an attack on IT systems, production was halted at least two sites in Canada. Ops depend on IT which are "necessary to ensure standards and traceability."	https://icsstrive.com/incident/evraz-infection/ https://cbc.ca/news/canada/saskatchewan/evraz-regina-shut-down-ransomware-attack-1.5487017 https://globalnews.ca/news/6640313/evraz-regina-cyberattack-layoffs
2020-05-09	Shahid Rajaee port	Iran	Transport	NS	Unknown	1			DO	Halted port terminal, abruptly and inexplicably	Sophisticated attack by Israel and retaliation for Iran's attacks on Israeli water systems in April, which were caught and defeated in real-time.	https://icsstrive.com/incident/shahid-rajaee-port-terminal-maratime-attack/ https://timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april https://timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps
2020-06-04	Fisher & Paykel Appliances	New Zealand	Discrete Mfg.	R	Unknown	1			U	Shut down appliance manufacturing and distribution ops.	Victim of the Netfilim ransomware group. They refused to pay, then suffered a large data leak.	https://icsstrive.com/incident/large-amount-of-data-leaked-after-at-new-zealand-manufacturer-refused-to-pay/ https://stuff.co.nz/business/121849569/appliance-repairer-in-the-dark-after-ransomware-attack-on-fp-appliances
2020-06-09	Honda	Japan, Turkey, UK, USA	Discrete Mfg.	R	EKANS	4			DS	Shut down global plant manufacturing ops. for 4 days and delayed vehicle shipments	Victim of EKANS ("Snake") ransomware that spread to at least 4 plants. The malware spread from IT servers to the control network suggesting poor network segmentation.	https://icsstrive.com/incident/honda-manufacturing-attack https://telegraph.co.uk/technology/2020/06/09/hondas-global-factories-brought-standstill-cyber-attack
2020-06-09	Lion	Australia	Food & Bev.	R	REvil	45			IA	Shut down brewery operations for 2+ weeks	Hit by two separate REvil ransomware attacks weeks apart, during the early months of the Covid-19 pandemic.	https://icsstrive.com/incident/aussie-brewer-lion-production-hit-after-ransomware-attack/ https://zdnet.com/article/lion-warns-of-beer-shortages-following-ransomware-attack https://smh.com.au/technology/cyber-crisis-deepens-at-lion-as-second-attack-bites-beer-giant-20200618-p5540c.html
2020-07-05	X-FAB	Germany, France, Malaysia, USA	Discrete Mfg.	R	Maze	6			IA	Shut down all plants: down 2 weeks at 5 sites, and 1 week for another	X-FAB is a leading MEMS analog/mixed-signal chip fab and fell victim to a Maze ransomware attack.	https://icsstrive.com/incident/x-fab-group-targeted-by-cyberattack/ https://businesswire.com/news/home/20200705005045/en/X-FAB-Affected-by-Cyber-Attack

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2020-09-06	Tower Semiconductor	Israel	Discrete Mfg.	R	Unknown	2			IA	Shut down "several" plants	Tower Semi manufactures integrated circuits, and has 2 plants in Israel, 2 in the USA, and 3 in Japan. Further details were not made public.	https://icsstrive.com/incident/cyberattack-at-israeli-tower-semiconductor-manufacturer/ https://cisomag.com/tower-semiconductor-cyberattack
2020-09-15	Bluescope Steel	Australia	Discrete Mfg.	R	Unknown	2			U	Shut down production, and reverted to manual operations for some processes	Ransomware infection was first detected in their USA-based subsidiary, but the attack eventually impacted global production ops.	https://icsstrive.com/incident/bluescope-event/ https://abc.net.au/news/2020-05-15/bluescope-steel-cyber-attack-shut-down-kembla-ransomware/12251316 https://securityweek.com/australian-steel-maker-bluescope-hit-cyberattack/
2020-10-17	IPG Photonics	USA	Discrete Mfg.	R	RansomExx	2			U	Shut down global parts manufacturing and shipping	The Oxford, MA based industrial, medical, and military laser manufacturer was hit by RansomExx malware.	https://icsstrive.com/editorials/ransomware-hits-ma-laser-maker https://bleepingcomputer.com/news/security/leading-us-laser-developer-ipg-photonics-hit-with-ransomware
2020-10-19	Société de transport de Montréal (STM)	Canada	Transport	R	RansomExx	1	$2M		DS	Shut down on-call, door to door, paratransit services for nearly a week	Montreal's transit service was hit by RansomExx ransomware, and they refused to pay the $2.8 mil demanded.	https://icsstrive.com/incident/montreals-transit-service-hit-by-ransomexx-ransomware/ https://cbc.ca/news/canada/montreal/stm-refused-to-pay-2-8-million-ransomware-attack-1.5782838 https://stm.info/en/press/news/2020/the-stm-completes-cyber-attack-investigation
2020-10-22	Steelcase	USA	Discrete Mfg.	R	Ryuk	1	$60M		IA	Shut down all plants for 2 weeks; delayed $60m in shipments to the 4th quarter	Office furniture maker was the victim of a Ryuk ransomware attack that shutdown global order management, manufacturing and distribution systems.	https://icsstrive.com/incident/ransomware-shuts-furniture-maker/ https://bleepingcomputer.com/news/security/steelcase-furniture-giant-hit-by-ryuk-ransomware-attack https://mibiz.com/sections/manufacturing/cyberattack-delays-60-million-in-shipments-for-steelcase-as-pandemic-continues-to-batter-office-furniture-orders
2020-10-22	Dr Reddy's Laboratories	India, UK, Brazil, Russia, USA	Pharma	R	Unknown	5			IA	Shut down production at 5 plants and stocks fell 3%	A week after agreeing to produce the Sputnik V Covid-19 vaccine for final trials, Dr Reddy's was subject to a ransomware attack.	https://icsstrive.com/incident/covid-vaccine-maker-dr-reddy-laboratories-hit-by-cyber-attack/ https://businessinsider.in/india/news/dr-reddys-shares-fell-over-3-the-drug-maker-isolated-all-data-service-centers-after-a-cyber-attack/articleshow/78806238.cms https://thehindu.com/business/Industry/oct-22-data-breach-involved-a-ransomware-attack-dr-reddys/article32962438.ece
2020-10-25	Stelco	Canada	Discrete Mfg.	U	Unknown	1			U	Shut down steel production, temporarily	The company has reported the incident to law enforcement and did not give further details.	https://icsstrive.com/incident/canadian-stelco-temporarily-suspended-operations/ https://insurancebusinessmag.com/ca/news/cyber/stelco-reveals-information-systems-were-subjected-to-a-criminal-attack-237287.aspx
2020-12-13	Symrise	Germany	Process Mfg.	R	Cl0p	1			IA	Shut down production out of abundance of caution	The flavor and fragrance manufacturer was hit by a Cl0p ransomware attack which limited sales growth below target.	https://icsstrive.com/incident/german-flavor-manufacturer-symrise-preventively-shut-down-operations/ https://bleepingcomputer.com/news/security/flavors-designer-symrise-halts-production-after-clop-ransomware-attack https://handelsblatt.com/unternehmen/industrie/mdax-konzern-hacker-legen-symrise-lahm-warum-der-fall-besonders-schwerwiegend-ist/26718680.html
2020-12-15	Forward Air	USA	Transport	R	Hades	1	$7.5M		ID	Shut down operations and delayed shipments for a week	Hades ransomware gang attack impacted data exchange with customers, leading to delivery delays which impacted financial results.	https://icsstrive.com/incident/ransomware-attack-at-forward-air/ https://freightwaves.com/news/news-alert-forward-air-reveals-ransomware-attack-warns-of-revenue-hit https://freightwaves.com/news/news-alert-forward-airs-systems-coming-back-online https://zdnet.com/article/trucking-company-forward-air-said-its-ransomware-incident-cost-it-7-5-million

Incidents from 2018-2019

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2018-08-03	Taiwan Semiconductor Manufacturing Co (TSMC)	Taiwan	Discrete Mfg.	R	WannaCry	3	$255 m		I3	Shut down operations at Tainan, Hsinchu and Taichung; Lost 3% in quarterly revenue	WannaCry ransomware caused the outage. Supplier installed software on some machines accidentally infected with the malware, without running AV.	https://icsstrive.com/incident/tsmc-hit-by-wannacry-variant/ https://itpro.com/security/31629/tsmc-cyber-attack-was-apparently-caused-by-wannacry
2019	Unknown gas pipeline	USA	Oil & Gas	R	Unknown	1			DS	Shut down pipeline for 2 days	Attackers used spear phishing to gain initial access to the IT network, easily pivoting into the OT network due to poor segmentation. Then, they planted ransomware.	https://icsstrive.com/incident/us-natural-gas-compression-facility-shut-down-entire-pipeline-for-2-days/ https://securityweek.com/operations-us-natural-gas-facilities-disrupted-ransomware-attack https://cisa.gov/news-events/cybersecurity-advisories/aa20-049a
2019-02-28	Hoya Corporation	Thailand	Discrete Mfg.	U	Unknown	1			ID	Partially shut down production for 3 days, dropping output by 60%	Around 100 computers were infected by credential stealing malware, and subsequently infected with a cryptojacker (mining) malware. Following the initial attack, workers were not able to keep up with orders and so manufacturing output fell for 3 days before resuming.	https://icsstrive.com/incident/hoya-corporation-hit-by-cyberattack/ https://www.bleepingcomputer.com/news/security/cyber-attack-shuts-down-hoya-corps-thailand-plant-for-three-days/ https://english.kyodonews.net/news/2019/04/7d3dc3094e3a-hoya-hit-by-cyberattack-in-feb-disrupting-thai-factory-operations.html
2019-03-18	Norsk Hydro	Norway	Metals & Mining	R	LockerGoga	10	$71m		ID	Halted production at all rolled (sheet) & extruded aluminum plants and at their building products plant	Infected by LockerGoga ransomware. initially spread at Norsky Hydro through phishing email on the IT network, then deploying via the AD controller.	https://icsstrive.com/incident/production-lines-stopped https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency https://industrialcybersecuritypulse.com/facilities/throwback-attack-norsk-hydro-gets-hit-by-lockergoga-ransomware
2019-07-26	City Power Johannesburg	South Africa	Power	R	Unknown	1			ID	Power outage for 250k customers and delayed restoration	Ransomware encrypts the IT system, preventing customers on pre-paid plans from purchasing electricity, and hampering line crews' efforts to restore localized blackouts.	https://icsstrive.com/incident/ransomware-attack-at-electricity-provider-for-johannesburg-sa/ https://twitter.com/CityPowerJhb/status/1154277777950093313 https://bbc.com/news/technology-49125853
2019-09-27	Rheinmetall	Germany	Discrete Mfg.	U	Unknown	3	€6M		ID	Disrupted production significantly for 2 weeks at locations in United States, Mexico, and Brazil	Rheinmetall's civilian automotive production business was impacted after a malware attack, requiring a complete rebuild of the IT network expected to take a minimum of 2 weeks.	https://icsstrive.com/incident/malware-attack-disrupts-multiple-sites-of-rheinmetal-ag-causing-shares-to-drop/ https://www.reuters.com/article/us-rheinmetall-malware-idUSKBN1WC0LH

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2019-10-13	Pilz	Germany	Discrete Mfg.	R	BitPaymer	1			IA	Shut down systems, reverted to manual ops., and slowed production for 1 week	Slowdown due to impaired order tracking, due to BitPaymer ransomware attack.	https://icsstrive.com/incident/ransomware-attack-automation-supplier-pilz-down/ https://drivesncontrols.com/news/fullstory.php/aid/6191/Pilz_is_recovering_from_a__91major_92_ransomware_attack.html
2019-12-16	Unknown MTSA facility	USA	Transport	R	Ryuk	1			DS	Infected ICS that monitors cargo transfer and encrypted files, lost critical process control and monitoring systems, forced an operational shutdown for more than 30 hours	A MTSA-regulated facility suffered a ransomware attack that encrypted both IT and OT systems. The USCG said that initial access was gained likely through phishing, encrypted both IT and OT networks, forcing an operational shutdown.	https://icsstrive.com/incident/ransomware-takes-down-maritime-facility/ https://www.bleepingcomputer.com/news/security/us-coast-guard-says-ryuk-ransomware-took-down-maritime-facility/ https://maritime-executive.com/article/uscg-cyberattack-penetrated-operating-controls-of-isps-facility https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf?ver=2019-12-23-134957-667
2019-12-20	RavnAir Alaska	USA	Transport	R	Unknown	1			ID	Canceled Dash-8-100 flights for 24 hours	Canceled Dash-8 flights because cyberattack caused outage of the Dash-8 maintenance system and its backup, which is required for flight.	https://icsstrive.com/incident/airline-hit-by-cyber-attack-cancels-flights/ https://theregister.com/2020/01/02/ravnair_ransomware_dhc_dash_8

Incidents from 2010-2017

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2010-07-15	Natanz Nuclear Enrichment Plant	Iran	Process Mfg.	NS	Unknown/Stuxnet	1			DO	Destroyed 1000 centrifuges at Natanz	Plant was infected by the Stuxnet worm in a targeted attack designed to disrupt Iran's nuclear enrichment program.	https://icsstrive.com/incident/malware-targets-uranium-enrichment-facility/ https://en.wikipedia.org/wiki/Stuxnet
2012-04-22	Iran's main oil export terminals	Iran	Oil & Gas	NS	Unknown/Flame	6			DO	Shut down 6 terminals	6 terminals ops. affected by Flame malware. News outlets confirm outage, despite Iran downplaying the attack's effects.	https://icsstrive.com/incident/iranian-oil-terminal-offline-after-malware-attack/ https://www.bbc.com/news/technology-17811565 https://computerworld.com/article/2727219/attacks-on-iranian-oil-industry-led-to-flame-malware-find.html
2012-07-22	Natanz and Fordow Nuclear Enrichment Plants	Iran	Process Mfg.	U	Unknown	2			DO	Shut down 2 plants	Mikko Hypponen at F-Secure reports a scientist claiming to be with Iran's Atomic Energy Organization asked for help following an attack on Siemens PLCs.	https://icsstrive.com/incident/natanz-and-fordo-facilities-closed-down-automation-network-after-new-worm-targeted-irans-nuclear-program/ https://web.archive.org/web/20150511100332/ https://www.washingtonpost.com/blogs/worldviews/post/iranian-nuclear-facilities-are-hit-by-acdc-virus/2012/07/25/gJQAqfRz8W_blog.html https://web.archive.org/web/20160428132811/ http://www.bloomberg.com/news/articles/2012-07-25/iranian-nuclear-plants-hit-by-virus-playing-ac-dc-website-says
2012-10	Unknown Power Plant	USA	Power	U	Unknown / Mariposa BotNet	1			DO	Delayed turbine restart (thus power generation) by 3 weeks	10 plant PCs were infected by Mariposa malware variant, transmitted through a USB stick. Occurred during scheduled shutdown for maintenance.	https://icsstrive.com/incident/virun-infection-in-turbo-control-system-at-us-electric-utility/ https://us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf
2014-12-22	German steel mill	Germany	Metals & Mining	U	Unknown	1			DO	Caused "massive damage" to plant equipment	Sophisticated attack using spear phishing and ICS knowledge to disable the control system, causing an uncontrolled shutdown of the blast furnace.	https://icsstrive.com/incident/cyber-attack-at-german-steel-mill-damages-equipment/ https://bbc.com/news/technology-30575104
2015-12-23	Prykarpattyaobl energo, Chernivtsioblen ergo, and Kyivoblenergo	Ukraine	Power	NS	Sandworm [GRU Unit 74455]/BlackEnergy 3 (Russia)	32			DO	Power outage lasts up to 6 hours affecting 230K people	First publicly known attack on a power grid occurs when threat actor Sandworm deploys BlackEnergy 3 malware into the utility's network.	https://icsstrive.com/incident/225k-customers-without-power-in-ukraine-power-grid-hack/ https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack https://arstechnica.com/information-technology/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation
2016-08-16	AW North Carolina	USA	Discrete Mfg.	R	Unknown	1	$1M		DS	Shut down ops. for 4 hours, and caused a ripple delay effect in the auto supply chain	Just-in-time transmission component supplier to Toyota, Honda and others is hit by ransomware that slipped through firewall and AV software defenses.	https://icsstrive.com/incident/ransomware-attack-at-aw-north-carolina-shuts-down-operations-for-4-hours/ https://www.isssource.com/users-learning-but-ransomware-still-a-problem/ https://industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-aw-north-carolina-attack-shows-dangers-of-ransomware-and-just-in-time-manufacturing https://apnews.com/article/nc-state-wire-north-america-us-news-ap-top-news-north-carolina-e316bd63f21a4fd181b3fb4a8dd7a5ba

Date	Victim	Region	Industry	Threat Actor	Threat Actor	Sites	Cost	SEC	OT Attack Type	OT / ICS Physical Consequences	Incident Summary	References
2016-12-13	Ukrzaliznytsia (Ukrainian State Railway)	Ukraine	Transport	NS	Sandworm [GRU Unit 74455]/BlackEnergy 3 & KillDisk (Russia)	1			DIP	Impacted online ticket purchasing and train scheduling; delayed both passenger and freight traffic during the holiday season	A SandWorm attack on Ukrainian rail used the KillDisk wiper malware to disable online ticketing systems, creating chaos and confusion for passengers and rail staff.	https://icsstrive.com/incident/ukrainian-railway-company-ukrzaliznytsia-hit-by-cyberattack/ https://www.industrialcybersecuritypulse.com/hacks-attacks/throwback-attack-ukrainian-railway-hit-by-cyberattack-stranding-passengers/
2016-12-17	Pivnichna substation, Kyiv	Ukraine	Power	NS	Sandworm [GRU Unit 74455]/Industroyer (Russia)	1			DO	Power outage for 20% of Kyiv for over 1 hour	Sandworm suspected in deploying Industroyer (also: CrashOverride) malware, by exploiting a vulnerability in Siemens SIPROTEC relays.	https://icsstrive.com/incident/attack-on-kyiv-power-substation-shut-down-remote-terminals/ https://en.wikipedia.org/wiki/2016_Kyiv_cyberattack https://arstechnica.com/information-technology/2017/06/crash-override-malware-may-sabotage-electric-grids-but-its-no-stuxnet
2017-05-12	Renault-Nissan	France, Slovenia, Romania, India	Discrete Mfg.	R	WannaCry / EternalBlue	5			DS	Shut down plants in Douai, Sandouville, Slovenia, Pitesti, and Chennai for 1 day	WannaCry ransomware, spread by the EternalBlue exploit originally developed by the NSA and later leaked by ShadowBrokers, hit 5 plants for 1 day.	https://icsstrive.com/incident/wannacry-affects-operations-at-several-renault-plants/ https://industrialcybersecuritypulse.com/facilities/throwback-attack-wannacry-ransomware-takes-renault-nissan-plants-offline
2017-06-27	Many, incl. AP Moller-Maersk, JNPT Gateway Terminals India (GTI), Merck Pharmaceutical, Royal Canin	Global	Multi	NS	NotPetya	1	$10B		I3	Outages throughout many industries: one incident, countless victims; Shut down ops. At JNPT GTI Terminal.	NotPetya malware, created by Russian actors targeting Ukraine, spreads indiscriminately through networks using the EternalBlue exploit, permanently encrypting data.	https://icsstrive.com/incident/petya-ransomware-attack-affects-operations-at-terminal-of-indias-largest-container-port-jnpt/ https://wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world https://timesofindia.indiatimes.com/india/indias-largest-container-port-jnpt-hit-by-ransomware/articleshow/59346704.cms https://www.ebervet.com/pet-food-impacted-cyber-attack/
2017-08	Petro Rabigh Petrochemical Refinery	Saudi Arabia	Oil & Gas	NS	Central Scientific Research Institute of Chemistry and Mechanics [CNIIHM]/Triton (Russia)	1			DO	Shut down one plant, twice	Triton malware employed to infect and reprogram Triconex safety systems. This triggered an automatic shutdown, alerting operations. Occurred twice.	https://icsstrive.com/incident/safety-instrumented-system-is-disabled-by-malware/ https://theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safety-systems-energy-plant https://cbsnews.com/news/russia-cyberattacks-60-minutes-2022-04-17

APPENDIX B – Sources and Acknowledgements

The authors thank and acknowledge the contributions of many incident repositories, reports, blogs, reporters, and other data sources that the authors drew upon to create this data set, including but not limited to:

Alerts and advisories From the Canadian Centre for Cyber Security	**cyber.gc.ca/en/alerts-advisories**
BlackFog - The State of Ransomware 2024	blackfog.com/the-state-of-ransomware-2024
Center for Strategic & Int'l Studies: Significant Cyber Incidents	csis.org/programs/strategic-Tech-program/significant-cyber incidents
CERT-EU Cyber Security Briefs and Threat Intelligence Reports	cert.europa.eu/publications/threat-intelligence/2023
Check Point Research - 2024	research.checkpoint.com/2024
CIO Magazine (Germany): "These companies have already been hit"	www.cio.de/a/diese-unternehmen-hat-s-schon-erwischt
Cloudian - Ransomware Attack List and Alerts	cloudian.com/ransomware-attack-list-and-alerts
Cyber Management Alliance - Cybersecurity Blog	cm-alliance.com/cybersecurity-blog
Cyber Security Incident Database (dot net)	csidb.net
Cybercrime Info NL - Actuele cyberaanvallen, datalekken, dreigingen en trends - Deze week	ccinfo.nl/menu-nieuws-trends/actuele-cyberaanvallen
CyberMaterial - Incidents	cybermaterial.com/incidents
DataBreaches.Net The Office of Inadequate Security	databreaches.net
DSGVO Portal Data breaches, cyber attacks and vulnerabilities	dsgvo-portal.de/sicherheitsvorfall-datenbank
European Repository of Cyber Incidents (EuRepoC)	eurepoc.eu
Halcyon Recent Ransomware Attacks	ransomwareattacks.halcyon.ai
ICS STRIVE Industrial Control System incident repository	icsstrive.com
ICS-SCADA incidents	securityaffairs.co/wordpress/category/ics-scada

Jam Cyber List of Successful Cyber Attacks and Data Breaches	jamcyber.com/discover/cyber-attacks
KonBriefing / Cyberattacks, Hacker attacks, Ransomware attacks	konbriefing.com/en-topics/cyberattacks.html
Monthly Data Breaches and Cyber Attacks Archive	itgovernance.co.uk/blog/category/monthly-data-breaches-and-cyber-attacks
NHL Stenden's MCAD Maritime Cyber Attack Database (Dr. Stephen McCombie)	maritimecybersecurity.nl
Office of the Information and Privacy Commissioner of Alberta - Breach Notification Decisions	oipc.ab.ca/decisions/breach-notification-decisions
Publicly disclosed U.S. ransomware attacks in 2023	techtarget.com/searchsecurity/feature/Publicly-disclosed-US-ransomware-attacks-in-2023
Ransomware Attack List and Alerts	cloudian.com/ransomware-attack-list-and-alerts
Ransomware Report: Latest Attacks And News	cybersecurityventures.com/ransomware-report
Red Hot Cyber - Italian Cyber Attacks	redhotcyber.com/post/category/attacchi-informatici-italiani
RedPacket Security: Ransomware	www.redpacketsecurity.com/category/ransomware
TechTarget's LeMagIT – Recherche	lemagit.fr/recherche
Ti Safe Incident Hub	hub.tisafe.com/base-de-dados
Upstream AutoThreat Intelligence Cyber Incident Repository	upstream.auto/research/automotive-cybersecurity
Dominic Aliveri, Cybersecurity analyst and security researcher	@AlvieriD (Twitter/X)
Eduardo Kovacs, Contributing Editor, SecurityWeek	@EduardKovacs (Twitter/X)
FalconFeeds.io's Twitter/X feed	@FalconFeedsio (Twitter/X)