waterfall

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

2024 Threat Report

OT Cyberattacks with Physical Consequences

By: Rees Machtemes, Director Industrial Security, Waterfall Security Solutions
Greg Hale, Editor & Founder, Industrial Safety and Security Source
Monique Walhof, Consultant, Industrial Safety and Security Source
Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

Table of Contents

Executive Summary

In the past year, one half of all cyberattacks that caused physical consequences impacted manufacturing, and most of those attacks were ransomware. In addition, GPS spoofing and supply chain incidents are important new developments in the Operational Technology (OT) cyber threat environment.

This 2024 Threat Report is a collaboration between Waterfall Security Solutions and ICS STRIVE, the OT incident threat database. We document cyberattacks with physical consequences in Operational technology (OT) networks, consequences such as production outages, equipment damage, environmental disasters and injuries or casualties. To be included in the report, the incidents must be deliberate attacks, with physical consequences, in the public record, in covered industries: building automation, transportation, manufacturing, heavy industry and critical industrial infrastructures.

Key findings:

- In 2023 there were 68 attacks that met the inclusion criteria, impairing operations at over 500 sites. This is a 19% increase in attacks over the previous year.
- In the period 2019-2023, these attacks are almost doubling annually – we see an average compound annual growth rate of over 90% per year.
- Ransomware remains the predominant threat, responsible for over half of the attacks where a threat actor type could be attributed reliably from the public record.
- Ransomware attacks did not increase as much as predicted in 2023 because attackers are more often holding data to ransom rather than encrypting systems and holding decryption keys to ransom. That said, this trend is expected to stabilize this year and we will most likely see a resumed exponential increase in physical consequences due to ransomware attacks for the foreseeable future.
- The discrete manufacturing sector was the hardest hit, followed by transportation and process manufacturing.
- The most expensive incidents cost victims from tens of millions of dollars to hundreds of millions.
- In roughly one quarter of all attacks since 2010, where public reports included enough detail, the threat actors impaired or manipulated OT systems directly. In the remaining attacks, physical consequences were an indirect result of compromising IT systems or other kinds of systems.
- Hacktivist and nation-state attack groups continue to impair OT systems and physical operations directly and deliberately.

Other developments, good and bad, in the year 2023 include:

- Attack complexity is increasing, including for example the emergence of serious GPS spoofing attacks and an increasing number of supply chain attacks with physical consequences.
- The regulatory landscape is evolving – in 2023 for the first year we report a significant number of attack disclosures due to new securities markets and other incident disclosure rules and regulations.
- Cyber-Informed Engineering (CIE) has emerged as the most important new perspective on OT security defensive postures in over a decade.

In short, reports of attacks with physical consequences, the number of reportedly affected sites, and the dollar cost consequences all increased this year and are expected to continue increasing for the foreseeable future.

In 2023 there were 68 attacks with physical consequences, affecting over 500 physical sites.

» Introduction

This threat report is a cooperative effort between Waterfall Security Solutions and the ICS STRIVE incident repository. The foundation of the report is a data set with strict inclusion criteria. This data set documents cyber incidents that:

- Are deliberate in nature – not errors and omissions, not equipment or software failures,
- Result in physical consequences including production outages, equipment damage, environmental disasters and injuries or casualties – not just data theft or clean-up costs,
- Have taken place in manufacturing, building automation, heavy industry, and critical industrial infrastructures, including transportation of people and goods, and
- Are found on public record – no private disclosures.

The complete data set of all such incidents can be found in Appendix A.

Note that this report does not track cyberattacks in other industries or critical infrastructures, not even those with physical consequences such as telecommunications outages, canceled surgeries at hospitals, or most retail store shutdowns. We do not track data-theft or denial-of-service cyberattacks on the financial sector or governments, their agencies, or their militaries, unless such attacks involve an element of industrial automation for physical processes that meets our section criteria above.

These attacks are now nearly doubling annually.

Readers interested in these other kinds of attacks may wish to consult the ICS STRIVE incident repository, which tracks a wider variety of incidents than is covered in this report, and/or consult the other incident data sources listed in Appendix B.

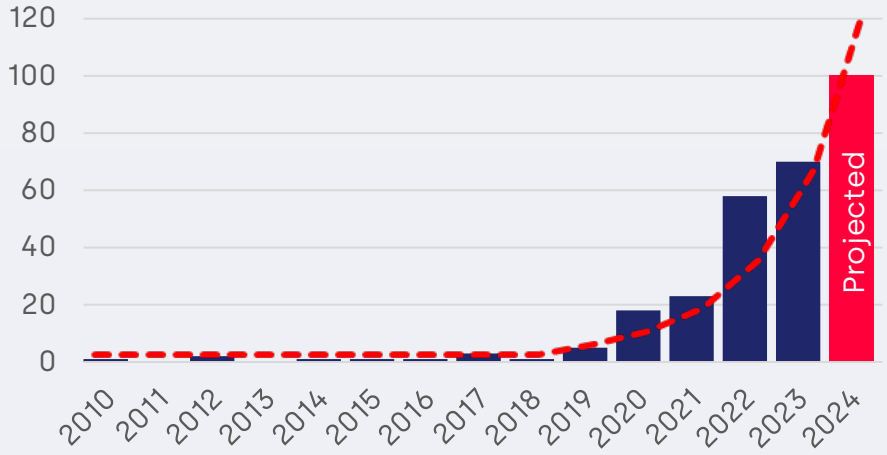

Figure (1) Incidents since 2010

» OT Incidents

Per the strict inclusion criteria for this report, there were 68 attacks with physical consequences found in 2023 affecting over 500 physical sites. This is a 19% increase over the 57 attacks reported in the previous year. Figure (1) shows that after a decade (2010-2019) with very few attacks with physical consequences, we observe that such attacks are now nearly doubling annually. When the exponential growth interval is one year, it is equivalent to compounded annual growth with the formula:

$$CAGF = \left(\frac{V_i}{V_f}\right)^{\frac{1}{n}}$$

CAGF: compound annual growth factor
V_i = Initial value
V_f = Final value
n = number of years between V_i & V_f

I.e.:

$$\left(\frac{68}{5}\right)^{\frac{1}{4}} = 1.92x$$

- 68 attacks in 2023
- 5 attacks in 2019
- 13.6x increase in 4 years
- 1.92x average compound increase / year

This is a slower rate of increase than was predicted last year given that ransomware and industrial cyber sabotage attacks continue increasing in frequency, not decreasing. Some factors that may help account for this year's total include: increased visibility due to SEC[1] and other[2] new disclosure rules, changing tactics on the part of ransomware criminal groups, and the changing mix of threat actors.

SEC & other financial disclosures

In 2023, we saw a significant number of cyberattacks with physical consequences detailed in regulatory filings because of new financial industry rules mandating such disclosures. There were 11 (16%) such disclosures made in 2023.What we can say with confidence is at least 4 (6%) of attacks in our data set appear in the public record exclusively because of such financial disclosures. In the remaining 7 (10%) of incidents where disclosures were made to a regulator, the filings either enhanced public knowledge with the impact details, or simply fulfilled legal obligations by reporting what was already made public.

Ransomware accounts for 80% of attacks where the threat actor is known.

These changes in reporting rules do not account for the smaller than expected increase in attacks this year, as the new rules for public incident disclosure would tend to increase the number of reported incidents, not reduce that number.

Threat actors

Ransomware accounts for 80% of 2023's attacks where the threat actor is known. The number of hacktivist attacks were flat over last year at six (6) such attacks with physical consequences.

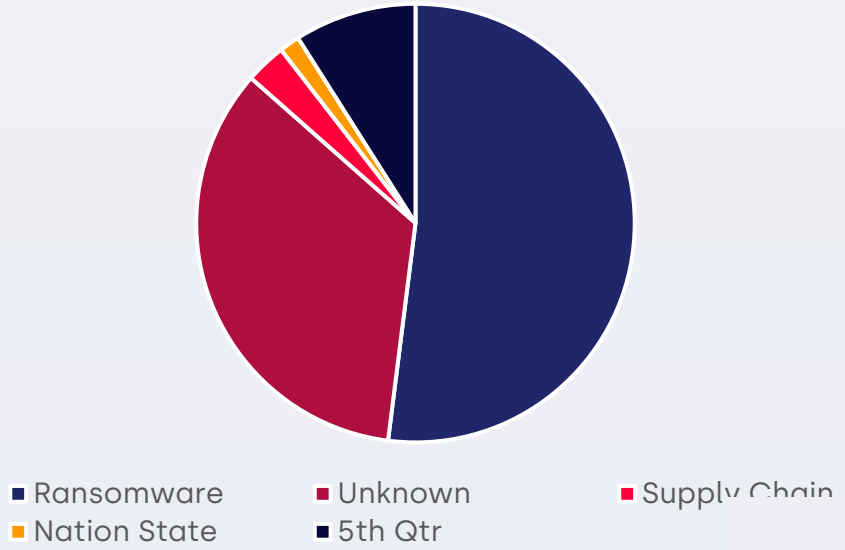

Figure (2) Threat actors

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, U.S. Securities and Exchange Commission, 2023, https://www.sec.gov/corpfin/secg-cybersecurity

[2] Cyber security incidents to be reported quarterly to stock exchanges, Vinod Kothari Consultants, 2023, https://vinodkothari.com/2023/10/cyber-security-incidents-to-be-reported-quarterly-to-stock-exchanges

This year, hacktivist attacks constitute a higher portion (15% vs 10%) of known attacks because the proportion of unknown attacks has increased materially, possibly due to the influence of SEC and related reporting requirements. Many businesses disclose the minimum that the law requires, and the law does not require publishing enough information to understand what kind of threat actor targeted a business, nor details beyond financial impacts.

> Hacktivists see producing physical consequences in critical infrastructures as a powerful way to draw attention

Furthermore, disclosing or failing to disclose a cyberattack is tricky to get right and carries significant business risk. Making disclosure can expose an organization to lawsuits, while failure to disclose can bring significant legal consequences and penalties. The latter is not lost on threat actors, who were observed leveraging their victims[3] over these disclosure rules in 2023. Therefore, it is not surprising that in the last two years organizations have disclosed only the minimum required and left out many incident details.

Hacktivist attacks are noteworthy, because while some ransomware criminal groups have claimed – whether we believe them or not – that they will not deliberately bring about physical consequences in critical infrastructures, hacktivist motivations appear to be the opposite. Hacktivists generally seek to make a political statement and produce physical consequences in critical infrastructures as a powerful way to draw attention to their political agendas.

That hacktivist activity appears to be flat year over year is somewhat surprising. However, hacktivist activity only became consequential to critical industrial infrastructures in 2021 and total hacktivist incidents since 2010 only broke into the teens this year. Random deviations in the form of two or three hacktivist attacks can make a disproportionate impact on year-over-year rates of change.

This year's data set also saw the first nation-state attack with physical consequences in several years: Iran's attack on a small water utility co-op near Erris, Ireland. This year also saw several supply chain attacks in the data set for the first time since NotPetya in 2017 – see the "Supply Chain" section below for details.

Ransomware & nation-state tactics

Ransomware attacks can be very sophisticated. Some ransomware groups are backed by nation states – e.g. North Korea is cited as sponsoring ransomware groups[4] to produce income for the sanctioned regime. Other ransomware groups are wealthy enough to afford their own nation-state-grade attack tools[5] . There was a time last decade when many organizations could look around and ask, "are we really important enough for a nation-state to target?" Today, nation-state-grade ransomware targets anyone with money.

> Are we really important enough to be a nation-state to target? Nation-state-grade ransomware targets everyone with money.

[3] Ransomware Group Files SEC Complaint over Victim's Failure to Disclose Data Breach, SecurityWeek, 2023, Edward Kovacs, https://www.securityweek.com/ransomware-group-files-sec-complaint-over-victims-failure-to-disclose-data-breach

[4] Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups, U.S. Department of the Treasurys Office of Foreign Assets Control (OFAC), 2019, https://home.treasury.gov/news/press-releases/sm774

[5] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

The tactics of ransomware criminal groups are evolving[6]. Authorities and experts are reporting that increasingly, ransomware attacks are no longer employing data encryption and denial as primary leverage for ransom, but instead prioritizing data exfiltration[7] . In the past, ransomware groups would generally search for and find the most valuable, confidential and embarrassing data they could, and then:

a. Steal a copy of that data, and

b. Encrypt the servers, databases and systems that held or managed the data.

The criminals would then demand money to (a) stop the release of the sensitive data to the Internet and (b) provide encryption keys to restore functionality to the encrypted systems. In the course of these attacks, some physical operations failures came about because IT or OT systems critical to operations were encrypted and thereby disabled, and other failures came about because the victim organization feared the attackers were about to encrypt operations-critical equipment and so shut down physical operations in an "abundance of caution."

> "We have seen both Iran-based and North Korea-based actors, leveraging commodity ransomware tools to damage targeted systems, often including critical infrastructure."
>
> Microsoft Digital Defense Report 2022, p 32

[6] Clop ransomware claims responsibility for MOVEit extortion attacks, BLEEPINGCOMPUTER, 2023, https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks

[7] How Data Exfiltration is Changing the Ransomware Landscape, BLACKFOG, 2024, https://www.blackfog.com/data-exfiltration-changing-ransomware-landscape

> We predict 100 attacks with physical consequences in 2024.

Again, in 2023, we saw an increasing fraction of ransomware criminals stealing sensitive data and demanding money to prevent disclosure of that data, without encrypting systems. While the data is not conclusive, it seems reasonable to conclude that a smaller fraction of ransomware attacks encrypting systems is the biggest single driver behind this year's OT incident count increasing by only 19% over last year.

Nation-state tactics are also evolving synergistically with ransomware tactics. Recently, nation-states have been observed using ransomware-developed tools in their attacks. While these new attacks do not show in this data-set, credible reports of critical infrastructure attacks have been made by Microsoft[8] and SentinelLABS[9] . This new synergy between nation-state and hacktivists leveraging each other's tools, tactics and procedures further reinforces that attacks are increasing in sophistication and unpredictability.

2024 OT incidents projection

General IT industry reports say ransomware attacks continued to increase dramatically in 2023, yet our incident data set shows only a modest increase in ransomware attacks with OT consequences. For example, the insurer Corvus reviewed claims data and examined ransomware data leak sites suggesting 7600 organizations were attacked in 2023, which is a 70% increase over 2022. If the modest year over year increase in OT consequences is in fact due to changing ransomware tactics (See section "RANSOMWARE & NATION-STATE TACTICS" above), then it seems reasonable to predict 100 attacks with physical

[8] Microsoft Digital Defense Report 2022, Microsoft, 2022,https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

[9] From Wiper to Ransomware | The Evolution of Agrius, SentinelLABS, 2021, https://www.sentinelone.com/labs/from-wiper-to-ransomware-the-evolution-of-agrius

consequences in 2024. We reason that not all businesses or other targets of ransomware attacks have information that is sensitive enough to justify paying a ransom. Thus, some fraction of ransomware criminals and attacks will always choose to encrypt systems or otherwise impair their operation, in addition to holding confidentiality to ransom. If we expect that:

1. Over the next 12-24 months, as the fraction of criminals exclusively holding confidentiality to ransom stabilizes, and
2. The overall rate of ransomware attacks continues to increase,

then we will most likely see ransomware attacks with OT consequences again start to increase at historical rates.

That hacktivist attacks made up nearly 10% of all attacks in the last three years, that many near miss incidents were attributed to nation-states, and the global geopolitical environment continues to deteriorate is also factored into our prediction. We assess that while the overall threat environment is unpredictable, politically motivated incidents will continue increasing in number and proportion alongside criminal ransomware.

Industries

Over 50% of last year's incidents impacted process and discrete manufacturing operations, most often causing production shutdowns, work stoppages, and/or shipping delays.

> "You never know when your opponent is going to suddenly make a technological leap that renders you highly vulnerable."
>
> Admiral James G. Stavridis, interview with Wired

Over 50% of incidents impacted process and discrete manufacturing.

This is a near-doubling of manufacturing incidents (37 vs. 19) over the previous year. In contrast, Food and Beverage industry attacks dropped from nine (9) in 2022 to only three (3) in 2023.

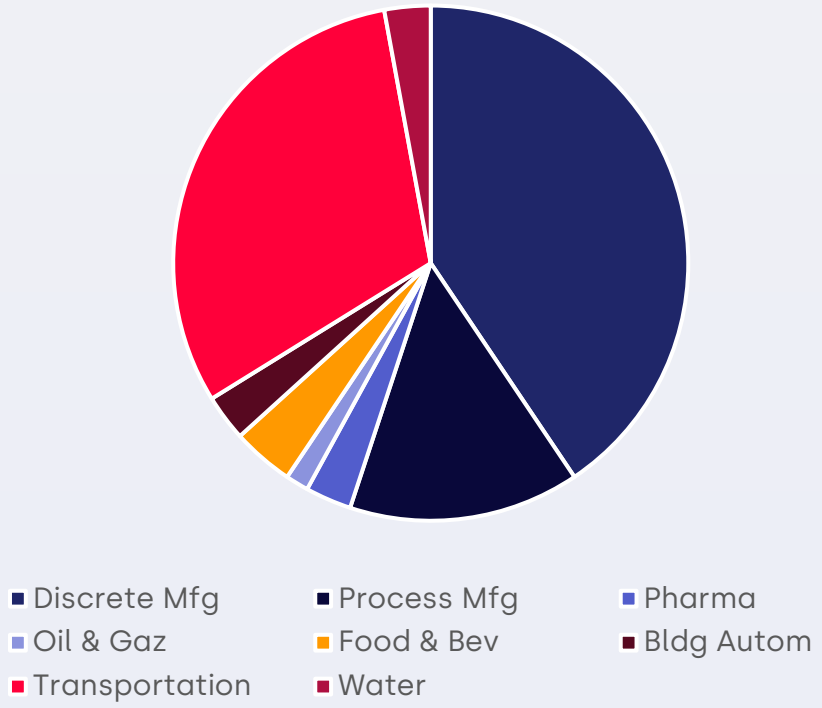

Figure (3) Industries

It is not clear what to draw from these numbers. Yes, few manufacturing operations are considered critical infrastructures, so it seems reasonable to expect that most manufacturing operations are protected less thoroughly than are water, power, or oil & gas operations. This fact might account for a greater number of manufacturing operations falling prey to cyberattacks. While many Food and Beverage enterprises are also considered critical infrastructures, far fewer of them were impacted physically this year than the previous year.

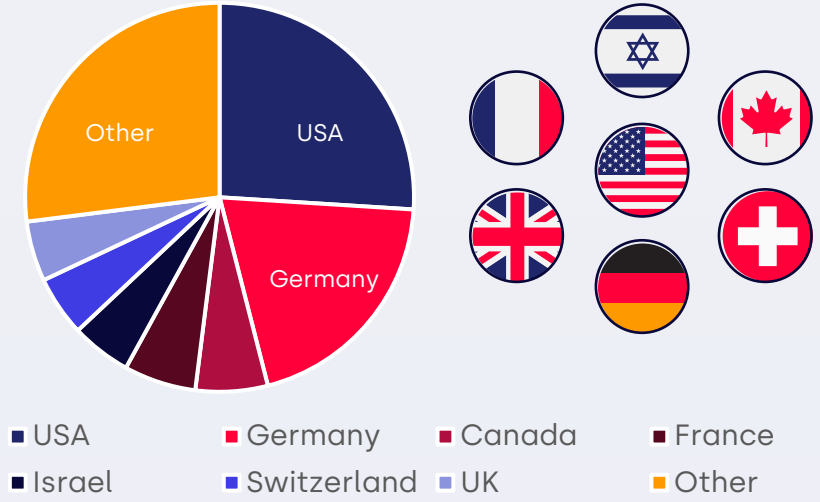

Figure (4) Attacks by Geography

Geographies

The number of attacks with physical consequences attributed to different countries varies widely year on year. Perhaps the only constant is that historically the United States has almost always been the "leader" – suffering the most such attacks in any given year. This is no surprise – consider simple demographics. The United States is the world's third largest country by population and is much more heavily industrialized and computer-automated than any of the other nations in the world's top ten countries by population.

Attacks with physical impacts are being felt globally.

Germany is second this year, which is new but perhaps not surprising, given the strong manufacturing base and highly sophisticated economy in Germany coupled with the fraction of attacks this year that specifically target manufacturing.

Attacks with physical impacts are being felt globally. While nearly 60% of incidents impacted the four top countries, the remainder constitutes 18 other countries with victims.

Costs

With increased scrutiny coming from the Securities and Exchange Commission (SEC), the financial impacts of cyberattacks are becoming more widely available in the public record. Some examples of impacts in this year's data set:

- $27 million for Johnson Controls,
- $49 million for Clorox, and
- Up to $450 million tied to the MKS Instruments attack. In that case $200 million was attributed to MKS, while their customer Applied Materials said it lost $250 in revenue as they were dependent on MKS for supplies, which were reduced.

Some incidents this year cost over $200M USD.

An Akira ransomware attack on UK-based KNP Logistics Group forced the company to declare bankruptcy.

Critical infrastructures aside, given these increasingly large financial impacts, many business decision makers are considering whether it is simply good business practice to increase budgets for cybersecurity programs, to prevent these kinds of impacts.

» How Was OT Impacted?

This year, for attacks where the attack pattern could be determined from public records, one quarter (12 / 50 = 24%) of attacks with physical consequences were attacks that directly impacted OT automation systems. The remainder caused physical consequences only indirectly. If we look at all attacks since 2010, the breakdown is very similar – 28% impacted OT automation systems directly, and the remainder impacted physical operations only indirectly.

Overall:

- 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 the business' operations still suffered physical consequences following a cyberattack, and
- Unknown attacks are incidents where there was not enough detail in the public record to determine how the attack impaired operations.

Analyzing the entire 2010-2023 data set in more detail, we determine that there are eight main (8) ways in which physical operations were impacted, five (5) direct and three (3) indirect, namely:

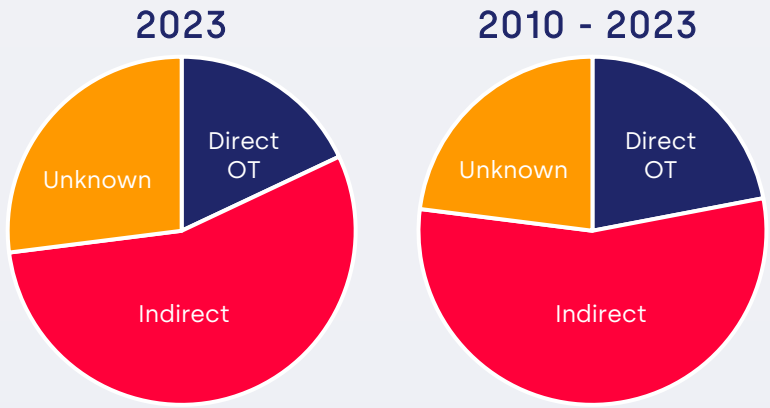

Figure (5) How Attacks Impacted Physical Operations

Direct attack types are:

1. **On OT:** local or remote attacks where attack software or manual attack actions directly affect OT automation systems or networks,
2. **Poor segmentation:** there is no evidence the OT network is distinct from an IT network – i.e. a "flat" network" – so that any attack on IT is also an attack on OT,
3. **IT pivot:** an attack first compromises IT assets and then uses the compromised asset to "pivot" the attack to OT assets,
4. **Supply chain:** a threat actor surreptitiously inserts malware or vulnerabilities into software or firmware for assets deployed on OT networks, and
5. **Malicious insider:** an insider uses their credentials and/or position of privilege to attack OT systems.

24% of attacks impacted OT systems directly, the remainder indirectly.

"Abundance of caution" shutdowns and IT dependencies are the biggest ways attacks impact operations.

Indirect attack types are:

1. **Abundance of caution:** where an attack impairs IT and the business decides to preemptively shutdown OT systems for safety reasons, to reduce risk, preserve forensic evidence, on the advice of third parties, or for other reasons,
2. **IT dependency:** 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 cyberattack, and
3. **3rd party:** where an enterprise suffers no cyberattack, 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.

The best way to eliminate "abundance of caution" shutdowns is to strengthen OT security programs especially protections at the IT/OT interface.

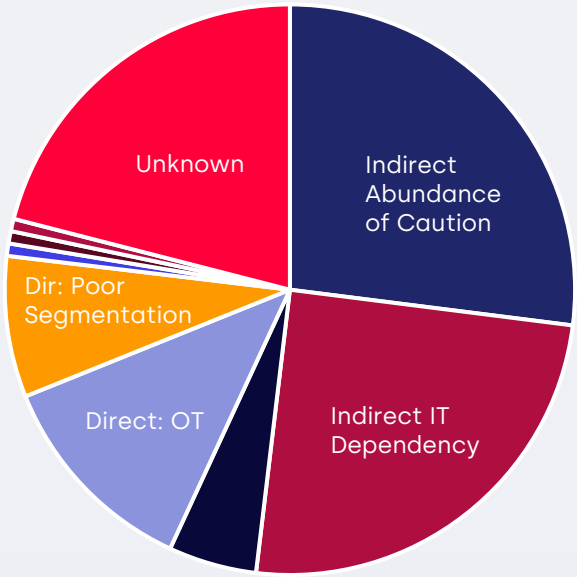

Figure (6) Details – Direct vs. Indirect Attacks

Of all the attacks in our data set (2010-2023) where the attack type could be determined reliably from the public record, OT shutdowns due to "abundance of cation" and OT dependencies on IT networks were by far the biggest ways that attacks on IT networks impacted operations. When attacks deliberately targeted OT – Direct OT – all those attacks were attributed to either hacktivists or nation states.

All attacks from 2010 to 2023 that deliberately targeted OT were attributed to hacktivist or nation state actors, not ransomware.

Implications for cybersecurity programs

What does this mean for cybersecurity programs? A naïve interpretation of the numbers above is that, since most attacks with physical consequences are attacks on IT networks, incremental spend on cybersecurity programs should be applied disproportionately to making IT networks more robust. These authors maintain this naïve interpretation is mistaken in many regards:

- IT networks are exposed to constant interaction with the Internet, but OT networks and systems are not so exposed. This means that IT networks are much harder and more expensive to secure than OT networks – secure to the high standards demanded of critical infrastructures, safety-critical systems, and manufacturing systems where the consequences of compromise can be in the hundreds of millions of dollars.
- 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 cyberattacks to pivot from IT networks into OT networks.
- 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 downtime for reliability-critical IT components.

The norm today in industrial enterprises is IT cybersecurity programs that are much more mature than OT cybersecurity programs. It is in this context that we observe cyberattacks 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).

» Important Developments

Supply chain

There are two cases of supply chain tampering in this year's data set: The first impacting Polish Rail (SPS), and the second ORQA FPV in Croatia.

In the first case, Poland's national railway SPS accused Newag SA of embedding code in trains it manufactured to "lock up the train with bogus error codes after some date, or if the train wasn't running for a period of time." One version of the PLC code was found to contain GPS coordinates to "contain the behavior to third-party workshops" for maintaining the train. In other words, the vendor is accused of self-sabotaging the code to guarantee regular services revenue for its authorized repair depots. The manufacturer denies the accusation and claims "unknown hackers" tampered with their products.

The best way to eliminate IT dependency shutdowns is to eliminate dependencies or implement network engineering measures to reduce downtime to acceptable levels.

A second incident targeted ORQA, a manufacturer that produces first-person view (FPV) virtual reality headsets for remote-controlling drones that range from racing drones to combat drones used by Ukrainian defenders. All ORQA's headsets shut down in May. A time bomb was found in the headset firmware. The author of that part of the firmware claims ORQA had the code under license, which had expired. ORQA claims that they are under no such obligation and that the time bomb is by a "greedy former contractor." No matter the details of the commercial dispute, a deliberate time-bomb was present in the code and the manufacturer, ORQA, had to scramble to fix the problem for their customers.

There are two cases of supply chain tampering in this year's data and a near miss in Ukraine.

In a 2023 near-miss, a credible report by the security service of Ukraine[10] stated that an unidentified Ukrainian water and gas telemetry equipment manufacturer suffered an attack that attempted to insert malware into a software update – see August incident in Table 1. The attack was discovered before the update was issued, and so there were no physical consequences.

These incidents show that supply chain attacks are increasing in diversity. No longer are such attacks limited to vendors such as Huawei and ZTE, who are presumed to be under the influence of potentially adversarial governments, nor nation-state attacks on software and firmware providers, as was the case with SolarWinds and the Ukrainian manufacturer. In both Newag SA and ORQA cases, apparently trustworthy suppliers are accused of deliberately inserting malicious capabilities into code that controls physical operations.

GPS & IRS spoofing

In September, commercial flights passing through Airway UM688 in northern Iraq reported GPS spoofing attacks, where an adversary transmitted false GPS signals to the aircraft to confuse their navigation systems' understanding of where the aircraft were and where they were headed. These attacks diverted aircraft from their planned courses, with one operator almost entering Iranian airspace without clearance, and so risking a reaction by the Iranian military. Inertial Reference Systems (IRS) in the affected aircraft were ineffective in detecting or mitigating the attacks, because the IRS used GPS signals to periodically reset their understanding of their location and direction. Some twenty aircraft reported these incidents, with GPS jamming appearing to originate in three different sources within the affected region. This report has therefore counted these incidents as three separate attacks – three actions on the part of the threat actor.

GPS blocking and spoofing is driving commercial aircraft off course and disabling navigation in ferries.

These attacks come in addition to long-standing concerns of GPS jamming[11] in commercial fishing, shipping and ferries. In addition to long-distance GPS jamming, there is a more widespread problem of people purchasing GPS jammers and installing them in trucks and taxis to frustrate corporate tracking of the vehicles, and in stolen vehicles[12] to frustrate GPS technology. Such jammers have been responsible for the loss of GPS signals in airports with nearby motorways, and very recently, such jammers are thought to be the reason that passenger and vehicular ferries have lost GPS[13] navigation capabilities.

GPS jammers are in widespread use – industrial users are advised to evaluate their dependence on these timing and positioning systems.

Industrial users should be aware that GPS jammers are coming into more widespread use, by malicious adversaries, corporate drivers, thieves, and those who transport stolen vehicles. Many industrial systems rely on GPS signals for more than just location information, where microsecond-synchronized timing is crucial, such as the protective relaying critical to the reliability of the electrical grid and of equipment in that grid. Operators of such systems are advised to evaluate the extent of their dependence on such timing and positioning systems and establish robust fail-safe operation modes when these systems are jammed or falsified.

[10] Exclusive: How a defend-forward operation gave Ukraine's SBU an edge over Russia, The Record, 2023, Dina Temple-Raston & Sean Powers, https://therecord.media/illia-vitiuk-interview-ukraine-sbu-defend-forward

[11] Ensuring safe navigation during GPS outage, SAFETY4SEA, 2017, https://safety4sea.com/ensuring-safe-navigation-during-gps-outage

[12] Car Thieves Use GPS Jammers to Make Clean Getaway, Wired, 2010, https://www.wired.com/2010/02/car-thieves-use-gps-jammers-to-make-a-clean-getaway

[13] Police suspect jammer devices on HGVs caused ferry's GPS system failure, trans.iNFO, 2022, https://trans.info/jammer-ferry-282005

Near misses

While near misses are not the focus of this report, twelve (12) significant near misses were observed in 2023. This year, there were near misses in critical infrastructure industries, including power generation, oil & gas, and transportation industries.

2023	Industry	Attack Type	Victim & Description	ICS STRIVE Incident entry
Feb	Power	Unknown	A national grid in Asia — China's Redfly infiltrated networks, persisted for 6 months, then tried to into OT	icsstrive.com/incident/china-linked-hackers-breach-power-grid-in-undisclosed-asian-country
May	Power, Oil & Gas	Unknown	22 Danish Critical Energy Infrastructure Companies — A widespread attack discovered by SektorCERT	icsstrive.com/incident/largest-recorded-cyberattacks-at-danish-energy-infrastructure
May	Power, Water	Indirect, pivot from IT	US Government Infrastructure (Power, Water, and more) — Chinese nation-state attackers found in multiple private and public utilities. Using living-off-the-land techniques, they remain hidden for years until being excised in early 2024.	icsstrive.com/incident/chinese-identified-hackers-targeting-hawaii-water-utilities-and-unidentified-oil-gas-pipeline-in-us
Jun	Discrete Manuf.	Unknown	YKK — LockBit attacked the Japanese zipper manufacturer, who contained the attack before in spread to operations.	icsstrive.com/incident/lockbit-attacks-us-networks-of-largest-zipper-manufacturer-in-japan
Jul	Bldg. Automation	Indirect, abundance of caution	Ventia — A large contractor who operates critical infrastructure in Australia and New Zealand, was attacked and IT systems impacted, but no infrastructure was interrupted	icsstrive.com/incident/australian-infrastructure-services-provider-takes-down-systems
Aug	Discrete Manuf.	Direct, supply chain	Undisclosed utility meter manufacturer —The Security Service of Ukraine (SBU), reported that Russia had targeted a water and gas utility telemetry manufacturer in a supply chain attack. The attack was detected and defeated before there were physical consequences.	icsstrive.com/incident/russian-cyberattack-targets-water-and-gas-utility-meter-manufacturer-in-ukraine
Sep	Power	Direct, on OT	Undisclosed energy facility — CERT-UA disclosed stopping an attack on a 'critical energy facility' before there were physical consequences	icsstrive.com/incident/russian-cyberattack-targets-water-and-gas-utility-meter-manufacturer-in-ukraine
Sep	Transport	Indirect, via 3rd party	ORBCOMM — The GPS solutions & ELD provider was hit by ransomware, impairing fleet visibility and logging for large freight firms. The US Federal Motor Carrier Safety Administration relaxed requirements allowing firms to operate as long as they keep paper logs.	icsstrive.com/incident/us-largest-freight-transportation-companies-impacted-by-orbcomm-software-outage
Nov	Water	Indirect, abundance of caution	Service public de l'assainissement francilien (SIAAP) — SIAAP' manages wastewater for the city of Paris. A "massive" attack hit their IT systems. Operations survived by severing all IT and third-party connections.	icsstrive.com/incident/cyberattack-disrupts-paris-wastewater-operations
Nov	Power	Indirect, via 3rd party	Holding Slovenske Elektrarne (HSE) — generates 60% of Slovenia's power, suffered a Rhysida ransomware attack. HSE was able to repel the attack to avoid power outages.	icsstrive.com/incident/ransomware-attack-at-slovenian-power-company-hse
Nov	Water	Direct, on OT	Municipal Water Authority of Aliquippa — Iran-backed hacktivists compromised Unitronics Vision controllers in a booster station. Water supply and safety was not affected, because the utility reverted to manual control.	icsstrive.com/incident/iranian-linked-cyber-gang-shut-down-aliquippa-drinking-water-supply-line-pump
Dec	Water	Direct, on OT	10 US Water utilities — US agencies confirmed an Iranian threat actor Cyber Av3ngers breached a pump station controller in Pennsylvania and compromised similar systems in many other states. There were no confirmed reports that the water supply was impacted.	icsstrive.com/incident/florida-water-agency-confirms-it-responded-to-cyberattack

Table (1) Near Misses

There were many near misses in critical infrastructure industries, including power generation, oil & gas, and transportation.

Volt Typhoon

American, Australian, Canadian, British and New Zealander authorities issued an alert that the Chinese nation-state attack group "Volt Typhoon" had compromised IT environments in communications, energy, transportation and water infrastructures[14] . No physical consequences were attributed to this set of attacks, but in one case, the attackers did demonstrate the ability to move from the IT network into control system networks.

We assess with high confidence that Volt Typhoon actors are prepositioning themselves to enable the disruption of OT functions across multiple critical infrastructure sectors.

Cynthia Kaiser, Deputy Assistant Director, FBI Cyber

These targeted attacks use "living off the land" techniques, where attackers gain a foothold through phishing, credential stealing, known vulnerability exploits or zero-day exploits of Internet-facing equipment.

They maintain the foothold through credential stealing and credentialed access to VPNs. Inside the target, they move very cautiously, preferring to use existing Windows and other tools to carry out their attacks, rather than download attack technology to compromised networks. This makes the attacks very difficult to detect. Victim organizations have been found with this attack group in their networks for over five years. The authorities report that, with a high degree of confidence, these attacks are intended to create the ability to impact operations in future cyber and kinetic conflicts.

SektorCERT Denmark

The Danish SektorCERT reported two waves of attacks on 22 large and small critical infrastructure providers via unpatched vulnerabilities in Zyxel firewalls deployed between IT networks and the Internet. The SektorCERT report describes the first wave as exploiting a Zyxel vulnerability published two weeks before the first attack, and the second as exploiting a Zyxel zero day. The CERT further reported that in response to the attacks, utilities went into "island mode," disconnecting their firewalls from the Internet until they could be repaired.

22 large and small critical infrastructure providers were breached by exploiting a vulnerability in their Internet-facing firewalls.

[14] PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, CISA, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Forescout subsequently reported[15] that the second attack exploited a vulnerability that had been known for some time, and that the second "wave" appeared to be part of an indiscriminate, widespread campaign to compromise Zyxel firewalls and other targets. Forescout also indicated that "island mode" meant that electric utilities disconnected from the grid, but this latter appears to be a misunderstanding of the terminology used by the SektorCERT.

Lessons to draw from this attack include:

- Nation-state-backed attacks target both large and small utilities, and
- Almost all enterprises with important physical operations should deploy only systems with auto-update capabilities into Internet-facing roles and should enable those updates.

Nation states are still able to exploit zero days, but the risk of random downtime due to possible malfunction of automatic updates is less impactful than the risk of downtime or equipment damage resulting from deliberate attacks by our enemies, at the moment of their choosing.

Water utilities

In this year's data set, there are two incidents resulting in physical consequences in the water sector, but that does not tell the whole story.

In Israel in April, Internet-connected Unitronics pump controllers, in operation at farms and the Galil's wastewater facility in the Jordan valley were defaced and disabled by hacktivists as part of the annual #OPIsrael campaign. While the farms were able to operate manually and were not affected by the attack, it took a day before Galil could resume treatment operations.

[15] Clearing the Fog of War – A critical analysis of recent energy sector cyberattacks in Denmark and Ukraine, Forescout, 2024, Jos Wetzels, https://www.forescout.com/blog/analysis-of-energy-sector-cyberattacks-in-denmark-and-ukraine

> They knocked (our controller offline). It took all day Friday to circumvent it so we could let the water flow manually.
>
> Noel Walsh, interview with Western People

At the end of November near Erris, Ireland, 180 households in Binghamstown and Drum lost water for two days. A cyberattack led to a loss of water pressure at the local pumping station operated by the Drum/Binghamstown Group Water Scheme Co-Operative Society. The attacker's identity has not yet been confirmed but was likely carried out by the Iranian group CyberAv3ngers, looking to deface Unitronics pump controllers, as in similar attacks seen in 2023 on Israel and the US.

> Hacktivists are discovering that small water systems are critical and are on average poorly protected.

Near misses in the water sector include the Municipal Water Authority of Aliquippa, Pennsylvania's booster stations that suffered a shutdown pump after a hack attack in November by an Iranian-backed Cyber Av3ngers. An alarm went off as soon as the hack had occurred, but it did not result in a shortage or any risk to the drinking water.

In November, the wastewater system in Paris, France suffered a cyberattack, but nothing shut down and the network of 275 miles of pipes serving nine million people was unaffected. In December, a north Texas water utility serving two million people suffered a cyberattack that shut down some business operations, but water services continued normally. Also in December, there was an attack on IT targets in the St. Johns River Management District in Florida. A spokesperson for St. Johns confirmed it "identified suspicious activity in its information technology environment" and that "containment measures have been successfully implemented."

Considering these attacks are made against often understaffed, underbudgeted and overwhelmed water departments, the US federal government and some private sector organizations are starting to develop programs to help this vital but beleaguered critical infrastructure area. Assistance for small water systems is likely to become very important within the next few years, since hacktivists have evidently discovered these small critical infrastructures are on average poorly protected.

» Defensive Developments

Defenses are evolving in parallel with the threat environment. There are developments in the field of engineering-grade protections, and cybersecurity regulations as critical industrial infrastructures are becoming more widespread and stringent.

Cyber-Informed Engineering

The Cyber-Informed Engineering (CIE) initiative at Idaho National Laboratory is arguably the most important development in the field of cybersecurity since the term "OT Security" was coined. CIE, informally, is positioned as "a coin with two sides." One side of the coin is cybersecurity, where the goal is teaching engineers about cyber threats and defenses.

The other side of the coin is engineering – powerful engineering tools and approaches for managing risk to physical operations – tools that simply do not exist in ISO 27001, IEC 62443 or other cybersecurity standards, frameworks, and best practices.

Cyber-Informed Engineering is the most important development in OT security since the term "OT security" was coined in 2005.

In September 2023, the CIE Implementation Guide[16] was published. In our opinion, the guide is more of a framework than a recipe or a body of knowledge. A framework is a list of questions you should ask, or topics you should consider. The Implementation Guide is literally a list of questions, among other things – some 880 questions for engineering and enterprise security teams to ask when they are designing an OT security program. Additional deliverables are in progress.

Free copies of Andrew Ginter's book Engineering-Grade OT Security: A manager's guide can be requested at waterfall-security.com

[16] Cyber-Informed Engineering Implementation Guide Version 1.0, U.S. Department of Energy, 2023, https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf

Engineering-Grade OT Security

Andrew Ginter's new book Engineering-Grade OT Security: A Manager's Guide[17] was published late in 2023. The book complements the CIE methodology by exploring the question "how much is enough?" How much engineering? How much cybersecurity? For which kinds of systems? And most importantly, why?

One central argument in the book is that one pervasive threat on the Internet is nation-state-grade ransomware – an argument based in part on this Waterfall / ICS STRIVE series of threat reports. Thus, if the consequences of compromise of an OT system are unacceptable, as may be the case for critical industrial infrastructures or safety-critical systems, then engineering teams have a professional obligation to deploy, to the greatest extent practical, engineering-grade protections for the correct and continuous operation of the OT systems. Engineering-grade protections are the only ones powerful enough to defeat remote-control attacks by nation-state adversaries and nation-state-grade ransomware.

Regulations

Member states of the European Union either have already introduced or are preparing new regulations for critical infrastructures – regulations to comply with the unions new NIS2 directive. In the United States, Transportation Security Administration (TSA) temporary security directives for OT security in pipelines and rail systems are being transitioned to permanent regulations and Environmental Protection Agency regulations have been enacted and then struck down by the courts.

The number of attacks is increasing, as is the number of sites affected and the financial impact on affected organizations.

None of this should come as a surprise. As cyberattacks on critical infrastructures with physical consequences continue to increase in number, severity and the number of sites affected, governments all over the world will look hard at additional regulations. A priority for all businesses involved in OT security should be to ensure that government agencies creating these new regulations understand the emerging CIE body of knowledge, and design regulations to recognize and encourage the contribution that engineering-grade designs and controls make to strong OT security defenses, in addition to the much more widely known IT-grade family of cybersecurity defenses.

[17] Engineering-Grade OT Security: A Manager's Guide, 2023, Andrew Ginter, https://waterfall-security.com/engineering-grade-ot-security

» Conclusions

The threat of cyberattacks to physical operations continues to increase overall. In addition, whether by locking up systems or threatening to divulge secret information from a database, ransomware continues to present huge problems and will continue to increase over the next few years. That said, this year's data saw a "pause" in the rate of increase in ransomware attacks, possibly the result of a fraction of such criminal groups switching tactics and only threatening to release sensitive data into the wild rather than encrypting systems and data. We expect this development to stabilize in 2024, with most of the ransomware groups who are likely to change to non-encryption attacks making that change in strategy before the end of the year. After that change happens in the groups who will make it, and as ransomware attacks overall continue to increase, we expect to see physical consequences due to ransomware increasing substantially again in 2024 and 2025.

In the meantime, the costs of compromise continue to increase. The total cost of incidents on enterprises affected by physical consequences is frequently in the tens of millions of dollars, and sometimes in the hundreds of millions. In addition, GPS blocking, GPS spoofing and supply chain attacks are emerging as worrying new kinds of threats to address. Many installations have come to rely deeply on GPS location and timing signals with little thought of contingency plans, and supply chain attacks are able to impact physical operations in dozens or hundreds of sites and enterprises nearly simultaneously.

Finally, we continue seeing important near misses as part of nation-state campaigns such as Volt Typhoon and an evolution of nation-state and hacktivist OT disruption payloads. These two trends show the possibility of increased cyber-physical warfare and physical consequences in the future.

Some good news is that Cyber-Informed Engineering and related initiatives continue apace. Marrying powerful safety, protection and network engineering approaches with more conventional cybersecurity and detection, response and recovery techniques is essential to reliable and resilient operations.

Combining safety, protection and network engineering with cybersecurity detection, response and recovery approaches yields reliable and resilient operations.

» 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) ,[18]
- **LSE:** London Stock Exchange (UK).

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 cyberattack 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.

[18] REGULATION (EU) No 596/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014, European Union, 2023,
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02014R0596-20240109#tocId177

» Incidents 2023

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
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 station 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.	ICSStrive, Industrial Cyber, Reuters, Times of Israel, Time, BBC, Google Sites
2023-12-18	Yusen Logistics	Japan	Transportation	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.	ICSStrive, KBB Review, KBB Review, Halcyon
2023-12-17	Socadis	Canada	Transport	U		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.	ICSStrive, Le Devoir, La Presse, CSIDB, Facebook
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.	ICSStrive, The Register, Bad Cyber
2023-11-30	Drum / Binghamstown Group Water Scheme Co-Operative Society	Ireland	Water	NS	CyberAv3ngers (Iran) / Islamic Revolutionary Guard Corps (IRGC)	1			DS	Shutdown 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.	ICSStrive, Western People, Security Week,
2023-11-15	Stellantis / Yanfeng Automotive Interiors	USA	Discrete Mfg.	U		2			I3	Disrupted production	Stellantis manufacturing plants shut down after a cyberattack hit their external supplier Yangfeng, a vehicle interior manufacturer.	ICSStrive, Automotive Logistics, Car Scoops

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2023-11-10	DP World Australia	Australia	Transport	U		4	>$ 1m		IA	Shutdown 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.	ICSStrive, MSN, AFR, The Guardian, CNBC TV, Reuters, Bleeping Computer
2023-10-25	4+ Civilian and private Jets	Israel	Transport	U		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.	ICSStrive, OPS Group, Forbes
2023-10-16	10+ Civilian and private Jets	Egypt	Transport	U		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.	ICSStrive, OPS Group, Forbes
2023-10-10	Simpson Manufacturing	USA	Discrete Mfg.	U		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.	ICSStrive, Bleeping Computer, Simpson Mfg
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.	ICSStrive, The Record
2023-09-23	Johnson Controls and subsidiaries York, Tyco, Coleman, Ruskin, and Simplex	USA	Discrete Mfg.	R	Dark Angels	6	$27m	SEC	ID	Shutdown 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.	ICSStrive, Bleeping Computer, BitDefender, ISSSource, Reddit, CNN

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2023-09-18	Somagic	France	Discrete Mfg.	R	MedusaLocker	1			ID	Shutdown 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.	ICSStrive, CSIDB, LEJSL, Red Packet Security, Halcyon
2023-09-14	Canada Border Services Agency (CBSA)	Canada	Transport	H	NoName057(16)	10			DO	Shutdown 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.	ICSStrive, The Record, CCCS, La Presse, La Presse, Cyber Express, Financial Post
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.	ICSStrive, CSIDB, Alps Alpine, Alps Alpine, Alps Alpine, Red Packet Security
2023-09-08	MGM Resorts	USA	Bldg. Automation	R	ALPHV / Scattered Spider	19	$110m		IA	Shutdown 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.	ICSStrive, The Deep Dive, Reuters, Tech Crunch, Morphisec Blog, CSO Online, AP News,
2023-09-06	KIA Motors	USA	Discrete Mfg.	R		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.	ICSStrive, WRBL, Lagrange News,
2023-08-29	20+ Civilian and private Jets	Iraq	Transport	U		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.	ICSStrive, OPS Group, OPS Group, The Hindu, Times of India, Forbes, GC Map

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
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.	ICSStrive, BBC, Wired, Rail Journal,
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.	ICSStrive, The Register, The Register, The Record, ISSSource, Yahoo Finance, Bloomberg
2023-07-23	Tempur Sealy International	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.	ICSStrive, Cyber Express, The Record
2023-07-20	Campbell Soup Co.	USA	Food & Bev.	U		1			ID	Shutdown production 3 days, sent employees home	Campbell's Napoleon, OH plant shutdown due to "IT related complications," exposing an OT dependency on IT systems.	ICSStrive, Toledo Blade, Cybersecurity Dive
2023-07-14	Wildeboer	Germany	Discrete Mfg.	R		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.	ICSStrive, CSO Online Wildeboer, GA Online
2023-07-04	Port of Nagoya	Japan	Transport	R	LockBit 3.0	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.	ICSStrive, Bank Info Security, Bleeping Computer, CNN, Asahi, Reuters

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2023-07-02	Montpellier-Méditerranée (Fréjorgues) Airport	France	Transport	U		1			U	Shutdown 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.	ICSStrive, Midilibre
2023-06-22	Livingston International	Canada	Transport	R	Royal	125			DS	shutdown 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.	ICSStrive, Truck News, Cyber Express
2023-06-16	Rheinische Post Mediengruppe	Germany	Process Mfg.	U		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.	ICSStrive, Tages Schau, Zeit
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.	ICSStrive, BBC, The Record, Cybertalk
2023-06-13	Brunswick Corporation	USA	Discrete Mfg.	U		2	up to $85m		U	Halted production & distribution for 17 work days	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.	ICSStrive, Maritime Executive, Boating Industry, CyWare
2023-06-10	Haynes International	USA	Process Mfg.	R	LockBit 3.0	1	quarterly $18m net or $3.7m EBITDA loss	SEC	U	Shutdown production for 11 days and delayed shipments	The attack temporarily disrupted manufacturing ops. and production shipments.	ICSStrive, Global News Wire, Yahoo Finance, Breach Sense, Red Packet Security, Twitter, Channel Chek

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2023-05-20	Granules India	India	Pharma	R	LockBit 3.0	1		NSE	ID	shutdown 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.	ICSStrive, SC Magazine, Reuters, The Hindu Business Line, Tech Crunch, NSE India, NSE India
2023-05-12	Lacroix	France	Discrete Mfg.	R		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.	ICSStrive, Tech Monitor, Security Week, SC Magazine, Cybernews WS
2023-05-11	The Philidelphia Inquirer	USA	Process Mfg.	U		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.	ICSStrive, The Guardian, Inquirer
2023-05-10	Suzuki Motorcycle India	India	Discrete Mfg.	U		1	20,000 units		U	lost production of 20,000+ units, 10+ days downtime	Shutdown manufacturing facilities due to a cyberattack.	ICSStrive, Hindustan Times, Auto Car Pro, Live Mint
2023-05-07	ABB	Switzerland	Discrete Mfg.	R	Black Basta	1			IA	Lost production, and shutdown 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.	ICSStrive, Bleeping Computer, Bleeping Computer, Security Week, Cyber Place, Cyber News
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. This can also be viewed as a form of ransomware and a supply chain attack.	ICSStrive, CyWare, The Register, Bleeping Computer

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2023-04-29	Maxim Cosmetics	Germany	Process Mfg.	R	Black Basta	1			IA	Shutdown 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.	ICSStrive, KSTA, CSO Online, Breach Sense, Republicain Lorrain
2023-04-27	Elysée Cosmétiques	France	Process Mfg.	R		1	€3.25 m		U	Shutdown production 13+ days; furloughed 300 employees	The manufacturer of cosmetic aerosols reported that Russian cybercriminals attacked their centralized servers in Germany and shutdown production.	ICSStrive, Radio Melodie, Republicain Lorrain
2023-04-25	Americold	USA	Bldg. Automation	R	Cactus	250			IA	Shutdown 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.	ICSStrive, Bleeping Computer, The Record, Reddit, Bleeping Computer,
2023-04-20	Badische Stahlwerke (BSW) (Baden Steel Works)	Germany	Process Mfg.	U		1			IA	Shutdown 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.	ICSStrive, Stadtanzeiger Ortenau, CSO Online, Bo
2023-04-15	Evotec SE	Germany	Pharma	R	ALPHV / BlackCat	1	> €10m		IA	Shutdown 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.	ICSStrive, SCBIO, The Record
2023-04-12	Fincantieri Marinette Marine (FMM)	USA	Discrete Mfg.	R		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.	ICSStrive, USNI News,

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2023-04-12	Lürssen	Germany	Discrete Mfg.	R		1			U	Shutdown shipyard operations in Bremen	Ransomware shutdown large parts of shipyard operations at the superyacht and military ship builder for an undisclosed amount of time.	ICSStrive, The Record, Yahoo
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.	ICSStrive, JNS, Security Week, Yarix Labs
2023-04-08	Bobst	Switzerland	Discrete Mfg.	R	Black Basta	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.	ICSStrive, 24 Heurs, Inside IT, Archyde, Le Temps
2023-04-05	Israel Postal Company	Israel	Transport	H	Anonymous Sudan / #OPIsrael	1			ID	Halted some postal services, including international mail and local courier, for 6+ days	As part of the annual #OPIsrael hacktivist campaign, several services including the sending of international mail and courier services were interrupted, then proactively shut down, while the Cyber Directorate was brought in to assist with investigations and recovery.	ICSStrive, JNS, CalCalisTech
2023-03-31	Ustra Deutschlandticket	Germany	Transport	R		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.	ICSStrive, Bild, CSO Online, Haz
2023-03-27	CommScope	USA	Discrete Mfg.	R	Vice Society	1			U	Shutdown production for 2 days	According to employees, CommScope suffered a ransomware incident that resulted in "several days of widespread disruption, including plant production."	ICSStrive, Tech Crunch, Tech Crunch, The Record

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
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.	ICSStrive, EQS News, CSO Online, Global Trailer Mag, Twitter
2023-03-24	NZZ Mediengruppe Zürich	Switzerland	Process Mfg.	R	Play (PlayCrypt)	2			ID	Shutdown 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.	ICSStrive, Swiss Info, Breaking Latest
2023-03-17	Alliance Healthcare	Spain	Transport	U		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.	ICSStrive, Cyber News, SC Magazine, Catalan News, The Local
2023-03-17	Hahn Group	Germany	Discrete Mfg.	U		1			IA	Shutdown 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.	ICSStrive, CSO Online, Hahn Group
2023-03-14	Fiege Logistik (Logistics)	Italy	Transport	R	LockBit 3.0	3			U	Disrupted logistic operations at 3 locations 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.	ICSStrive, EuroTransport, Red Packet Security, Verkehrsrundschau, Inside IT
2023-03-01	Steico Group	Germany	Discrete Mfg.	U		1		EU MAR	U	Production shutdown for several days	Steico discloses in an EU market filing that a cyberattack halted both operations and IT systems.	ICSStrive, CSO Online, Steico, BNN Bloomberg
2023-02-24	Rosenbauer	Austria	Discrete Mfg.	R	LockBit 3.0	1			IA	Production shutdown 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.	ICSStrive, Non, Non, Feuerwehr Magazin, Red Packet Security,

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2023-02-23	Dole Food Company	USA	Food & Bev.	R		4	$10.5m		IA	Shutdown 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.	ICSStrive, Bleeping Computer, CNN, CBS News
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.	ICSStrive, Cyber News, Biz Journals
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.	ICSStrive, B2B Cyber Security, Hz, Hz
2023-02-02	Häfele (Hafele, Haefele)	Germany	Discrete Mfg.	R	LockBit 3.0	180			IA	halted order fulfilment; forced to pre-emptively shutdown systems	The kitchen and furniture fitting manufacturer shutdown their IT systems worldwide and disconnected from the internet after the attack.	ICSStrive, IT Security Guru, KBB Review
2023-02-01	MKS Instruments	USA	Discrete Mfg.	R		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.	ICSStrive, CSO Online, Comparitech
2023-01-29	Tribhuvan (Kathmandu) International Airport	Nepal	Transport	U		1			ID	Delayed international 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 international flights.	ICSStrive, Nepal Times
2023-01-18	Benetton Group (United Colors of Benetton)	Italy	Transport	U		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.	ICSStrive, Cyber Express, Treviso Today

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2023-01-17	Exco Technologies	Canada	Discrete Mfg.	R	LockBit 3.0	3			IA	Production shutdown 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.	ICSStrive, Insurance Business Mag, Exco Corp
2023-01-17	Fritzmeier Gruppe & M1 Sporttechnik	Germany	Discrete Mfg.	U		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.	ICSStrive, Merkur, Merkur
2023-01-13	Super Bock Group	Portugal	Food & Bev.	U		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."	ICSStrive, Portugal News, The Register
2023-01-11	Morgan Advanced Materials	UK	Discrete Mfg.	U		2	£8m	LSE	U	Halted production and shipping	Production and shipping were affected at multiple sites following a cyberattack.	ICSStrive, The Record, The Record
2023-01-10	UK Postal Service (Royal Mail)	UK	Transport	R	LockBit 3.0	11500	£42m		ID	Disabled label printers; prevents sending international 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.	ICSStrive, Security Week, Bank Info Security
2023-01-09	VDM Metals	Germany	Process Mfg.	U		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.	ICSStrive, Come On, Hellwegeranzeiger

» Incidents 2022

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2022-12-27	Copper Mountain Mining Corporation (CMMC)	Canada	Metals & Mining	R		1			IA	Shutdown 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.	ICSStrive
2022-12-22	Technolit GmbH, in Grossenlüder	Germany	Discrete Mfg.	U		1			U	Shutdown operations and sent employees home	A German manufacturer and distributor of welding supplies and products was shutdown by an unknown cyberattack.	ICSStrive
2022-12-13	Empresas Públicas de Medellín (EPM)	Colombia	Water	R		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.	ICSStrive
2022-12-11	Fruttagel	Italy	Food & Bev.	R		1			U	Shutdown production for 4+ days	A BlackCat (ALPHV) ransomware attack on Fruttagel halted production and prevented customer deliveries.	ICSStrive
2022-12-10	UNOX	Italy	Discrete Mfg.	U		1			IA	Shutdown production for 2 days	Hit by a cyberattack, the company activated emergency procedures, suspended production as a safety measure, and initiated "appropriate checks."	ICSStrive
2022-11-25	Prophete / VSF Fahrradmanufaktur, Rabeneick and Kreidler	Germany	Discrete Mfg.	R		1	Bankrupt		ID	Shutdown 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.	ICSStrive
2022-11-25	Cobolux	Luxembourg	Food & Bev.	R		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.	ICSStrive
2022-11-21	Communauto	Canada	Transport	U		1			DS	Shutdown 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.	ICSStrive

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2022-11-17	Taxis Coop Québec	Canada	Transport	R		1			IA	Shutdown 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.	ICSStrive, Radio Canada
2022-11-17	Europea Microfusioni Aerospaziali (EMA)	Italy	Discrete Mfg.	R		1			U	Shutdown 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.	ICSStrive
2022-11-06	Maple Leaf Foods	Canada	Food & Bev.	R		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.	ICSStrive, Just Food
2022-11-05	Uponor Oyj	Finland	Discrete Mfg.	R		1			IA	Shutdown 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.	ICSStrive
2022-11-05	PGT Innovations	USA	Discrete Mfg.	R		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.	ICSStrive
2022-11-02	Jeppesen, a wholly-owned Boeing subsidiary	Global	Transport	R		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.	ICSStrive, Ops Group
2022-10-31	Cartonnerie Gondardennes	France	Process Mfg.	R		1			DS	Shutdown 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.	ICSStrive, Lavoix Dunord
2022-10-29	Danish Rails (DSB) / Supeo	Denmark	Transport	R		1			I3	Shutdown 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.	ISS Source
2022-10-28	Aurubis AG	Germany, USA	Metals & Mining	U		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.	ICSStrive, HackRead

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2022-10-14	Heilbronner Stimme & Stimme Mediengruppe	Germany	Process Mfg.	R		1			DS	Shutdown 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.	ICSStrive, Bleeping Computer
2022-10-12	Undisclosed Ukrainian Power Facilities	Ukraine	Power	NS		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.	ICSStrive, Mandiant
2022-10-05	HiPP	Germany	Food & Bev.	U		1			DS	Production shutdown 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.	ICSStrive, CSO Online
2022-09-26	Electricity Company of Ghana (ECG)	Ghana	Power	R		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.	ICSStrive
2022-09-05	Läderach	Switzerland	Food & Bev.	R		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.	ICSStrive
2022-09-03	Yandex Taxi	Russia	Transport	H		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.	ICSStrive
2022-09-02	Novosibirsk City Transport Traffic Management System	Russia	Transport	H		1			DO	Shutdown and disrupted public transportation for 2+ days	Pro-Ukrainian activists Team OneFist cause traffic chaos, by halting and damaging the public transit scheduling system and signage, to prevent a quick recovery.	ICSStrive, IB Times
2022-08-13	Apex Capital / TCS Fuel	USA	Transport	R		1			ID	Shutdown 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.	ICSStrive
2022-08-08	Bombardier Recreational Products (BRP)	Austria, Canada, Finland, USA	Discrete Mfg.	R		4			I3	Shutdown 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.	ICSStrive, Bleeping Computer

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2022-08-05	Ontario Cannabis Retail Corporation (OCS)	Canada	Transport	U		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.	ICSStrive, CBC
2022-07-29	Semikron-Danfoss	Germany	Discrete Mfg.	R		8			U	Shutdown 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.	ICSStrive, Bleeping Computer
2022-07-18	Eglo	Austria	Discrete Mfg.	R		1			U	Shutdown 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.	ICSStrive, Die Presse
2022-06-29	Knauf	UK	Process Mfg.	R		2			IA	Shutdown 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.	ICSStrive, Tech Monitor
2022-06-27	Khuzestan Steel (KSC), Mobarakeh Steel (MSC), & Hormozgan Steel (HOSCO)	Iran	Metals & Mining	H		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.	ICSStrive, Times of Israel
2022-06-25	Apetito (Wiltshire Food Farms parent)	UK	Food & Bev.	R		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.	ICSStrive
2022-06-25	Macmillan Publishers	UK, USA	Transport	R		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.	ICSStrive
2022-06-22	Yodel	UK	Transport	U		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.	ICSStrive, Bleeping Computer

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2022-05-31	Foxconn Baja California	Mexico	Discrete Mfg.	R		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.	ICSStrive, The Record
2022-05-31	CMC Electronics	Canada	Discrete Mfg.	R		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.	ICSStrive, IT World Canada
2022-05-25	SpiceJet	India	Transport	R		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.	ICSStrive
2022-05-05	AGCO	USA & Europe	Discrete Mfg.	R		1			ID	Shutdown 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.	ICSStrive, The Register
2022-04-18	Sunwing Airlines	Canada	Transport	U		1			ID	Shutdown 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."	ICSStrive, Infosecurity Magazine
2022-04-17	Costa Rican Customs Service	Costa Rica	Transport	R		1			ID	Slowed shipments for > 1 month, and shutdown 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.	ICSStrive, USDA
2022-04-16	Bulgarian State Post Office	Bulgaria	Transport	R		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.	ICSStrive, Euractiv
2022-03-24	TAVR Corporate Group	Russia	Food & Bev.	U		1			U	Shutdown 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.”	ICSStrive

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2022-03-20	ELTA (Hellenic Post)	Greece	Transport	R		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.	ICSStrive, The Record
2022-03-11	H.P. Hood Dairy LLC	USA	Food & Bev.	U		13			IA	Shutdown 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.	ICSStrive, Boston
2022-02-28	Belarus Railway	Belarus	Transport	H		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.	ICSStrive, BQPrime
2022-02-28	Toyota, Hino, Daihatsu, Kojima Industries	Japan	Discrete Mfg.	R		14			I3	Shutdown 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.	ICSStrive
2022-02-28	Rosetti Energy	Russia	Power	H		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.	ICSStrive
2022-02-27	Bridgestone	N. & S. America	Process Mfg.	R		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.	ICSStrive
2022-02-24	Caledonian Modular	UK	Discrete Mfg.	R		1	Bankrupt		U	Shutdown manufacturing ops.	Modular building manufacturer's lost production output due to the attack was a major factor in the company's March insolvency.	ICSStrive, The Construction Index
2022-02-22	Expeditors	USA	Transport	R		1	$60M		ID	Shutdown 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.	ICSStrive, Bleeping Computer

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2022-02-21	Jawaharlal Nehru Port Container Terminal (JNPCT)	India	Transport	R		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.	ICSStrive, The Loadstar
2022-02-03	Swissport	Switzerland	Transport	R		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.	ICSStrive, Der Spiegel
2022-02-02	Evos Group	Malta, Belgium, Netherlands	Oil & Gas	U		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.	ICSStrive, Insurance Journal
2022-01-30	SEA-Tank & SEA-Invest Group	Belgium, Africa	Oil & Gas	R		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.	ISS Source
2022-01-29	Marquard & Bahls subsidairies Mabanaft & Oiltanking	Germany	Oil & Gas	R		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.	ICSStrive, BBC
2022-01-28	Kenyon Produce (KP) Snacks	UK	Food & Bev.	R		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.	ICSStrive, Food Processing
2022-01-07	CPH Chemie & Papier Holding	Switzerland, Germany	Process Mfg.	R		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.	ICSStrive, Euwid Paper, PULPAPERnews

» Incidents 2021

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2021-12-28	Amedia	Norway	Process Mfg.	U		1			U	Shutdown 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.	ICSStrive
2021-12-21	Nortura	Norway	Food & Bev.	R		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.	ICSStrive, Norway Today
2021-12-01	Bay & Bay Transportation	USA	Transport	R		1			IA	Lost 1.5 weeks of production	Hit by Conti ransomware, systems were taken offline and remediated.	ICSStrive, Freight Waves
2021-11-08	Estrella Damm Brewery	Spain	Food & Bev.	R		2			DS	Shutdown 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.	ICSStrive
2021-11-07	Diamond Comic Book Distributors	USA	Transport	R		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.	ICSStrive
2021-11	Madix Inc	USA	Discrete Mfg.	R		2			U	Shutdown production, sent employees home	Manufacture of store fixtures halted at both Goodwater and Eclectic plants.	ICSStrive, News Break
2021-10-26	Gas stations in Iran	Iran	Oil & Gas	H		4300			ID	Long line-ups and closed stations for 4-5 days	Predatory Sparrow group disabled system supporting cards used to buy discounted gasoline.	ICSStrive, BBC, Iran Primer
2021-10-24	Eberspaecher Group	Germany	Discrete Mfg.	R		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.	ICSStrive, RV Business, Eberspaecher

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2021-10-22	Schreiber Foods	USA, Europe, S. America	Food & Bev.	R		30			U	Shutdown 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	ICSStrive, Cyber Scoop, WIS Farmer
2021-10-09	Ferrara	USA	Food & Bev.	R		2			U	Shutdown 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.	ICSStrive , Cyber Scoop, Manufacturing
2021-09-21	Weir Group	UK	Discrete Mfg.	R		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.	ICSStrive
2021-09-19	Crystal Valley Cooperative	USA	Food & Bev.	R		1			IA	Shutdown 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.	ICSStrive
2021-09-17	New Cooperative	USA	Food & Bev.	R		1			IA	Delayed grain receipts & shipments, & shutdown fertigation optimization system	A BlackMatter ransomware attack impacted grain transactions during harvest season. Systems were pre-emptively shutdown to stop the spread.	ICSStrive
2021-07-22	Transnet	South Africa	Transport	R		4			U	Declared Force Majeure and halted operations for 7 days	Transnet said ports at Durban, Ngqura, Port Elizabeth and Cape Town were affected.	ICSStrive, Reuters
2021-07-09	Iran Rails	Iran	Transport	H		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."	ICSStrive, New York Times, The Guardian
2021-05-30	JBS SA	AustraliaCanada, USA	Food & Bev.	R		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.	ICSStrive, CBC, CBC, CNN
2021-05-21	Siegfried Group	Switzerland, Germany	Pharma	U		2			U	Shutdown 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.	ICSStrive, Siegfried, Chemical & Engineering News

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2021-05-20	Ardagh Group	UK	Process Mfg.	R		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.	ISS Source
2021-05-07	Colonial Pipeline	USA	Oil & Gas	R		1	$52.2M		IA	Shutdown 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.	ICSStrive
2021-04-04	Bakkier Logistiek	Netherlands	Transport	R		1			ID	Disrupted new orders, delayed shipments to retail outlets for 5 days	Caused shortages of packaged cheese at retail.	ICSStrive
2021-04-01	JBI Bike	USA	Transport	R		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.	ICSStrive, Bicycle Retailer
2021-03-25	Asteelflash Group SA	France	Discrete Mfg.	R		20			IA	Shutdown multiple printed circuit board plants	A leading Electronics Manufacturing Services (EMS) company suffered a REvil ransomware attack.	ICSStrive
2021-03-20	Sierra Wireless	Canada	Discrete Mfg.	R		1			IA	Halted production at all manufacturing sites	IoT, cellular, and wireless device manufacturer with an unknown number of manufacturing sites.	ISSSource
2021-03-11	Molson Coors	USA, CanadaUK	Food & Bev.	R		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.	ICSStrive, Bleeping Computer, Security Week
2021-02-18	Beneteau SA	France	Discrete Mfg.	R		2			IA	Shutdown 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.	ICSStrive, Boat Industry Beneteau Group
2021-01-26	Palfinger AG	Europe, N. & S. America, Asia	Discrete Mfg.	R		31			IA	Lost nearly 2 weeks crane production at all plants	The world's largest crane manufacturer. All global plants were affected.	ICSStrive, Bitdefender, International Cranes
2021-01-23	Westrock	USA	Process Mfg.	R		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.	ICSStrive, Westrock, Security Week

Incidents 2020

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2020-12-15	Forward Air	USA	Transport	R		1	$7.5M		ID	Shutdown operations and delayed shipments for a week	Hades ransomware gang attack impacted data exchange with customers, leading to delivery delays which impacted financial results.	ICSStrive, FreightWaves, FreightWaves, ZDNet
2020-12-13	Symrise	Germany	Process Mfg.	R		1			IA	Shutdown production out of abundance of caution	The flavor and fragrance manufacturer was hit by a Cl0p ransomware attack which limited sales growth below target.	ICSStrive, Bleeping Computer, Handelsblatt
2020-10-25	Stelco	Canada	Discrete Mfg.	U		1			U	Shutdown steel production, temporarily	The company has reported the incident to law enforcement and did not give further details.	ICSStrive, Insurance Business Mag
2020-10-22	Steelcase	USA	Discrete Mfg.	R		1	$60M		IA	Shutdown 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.	ICSStrive, Bleeping Computer, Mibiz
2020-10-22	Dr Reddy's Laboratories	India, UK, Brazil, Russia, USA	Pharma	R		5			IA	Shutdown 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.	ICSStrive, Business Insider, The Hindu
2020-10-19	Société de transport de Montréal (STM)	Canada	Transport	R		1	$2M		DS	Shutdown 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.	ICSStrive, CBC, STM
2020-10-17	IPG Photonics	USA	Discrete Mfg.	R		2			U	Shutdown global parts manufacturing and shipping	The Oxford, MA based industrial, medical, and military laser manufacturer was hit by RansomExx malware.	ICSStrive, Bleeping Computer
2020-09-15	Bluescope Steel	Australia	Discrete Mfg.	R		2			U	Shutdown 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.	ICSStrive, ABC, Security Week

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2020-09-06	Tower Semiconductor	Israel	Discrete Mfg.	R		2			IA	Shutdown "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.	ICSStrive, CSO Magazine
2020-07-05	X-FAB	Germany, France, Malaysia, USA	Discrete Mfg.	R		6			IA	Shutdown all plants: down 2 week 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.	ICSStrive, Business Wire
2020-06-09	Honda	Japan, Turkey, UK, USA	Discrete Mfg.	R		4			DS	Shutdown 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.	ICSStrive, Telegraph
2020-06-09	Lion	Australia	Food & Bev.	R		45			IA	Shutdown brewery operations for 2+ weeks	Hit by two separate REvil ransomware attacks weeks apart, during the early months of the Covid-19 pandemic.	ICSStrive, ZDNet, SMH
2020-06-04	Fisher & Paykel Appliances	New Zealand	Discrete Mfg.	R		1			U	Shutdown appliance manufacturing and distribution ops.	Victim of the Netfilim ransomware group. They refused to pay, then suffered a large data leak..	ICSStrive, Stuff
2020-05-09	Shahid Rajaee port	Iran	Transport	NS		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.	ICSStrive, Times of Israel, Times of Israel
2020-03-04	EVRAZ manufacturing	USA & Canada	Process Mfg.	R		2			ID	Shutdown operations at several plants, and sent 900+ workers home for 3+ days	After a attack on IT systems, production was halted at at least two sites in Canada. Ops depend on IT which are "necessary to ensure standards and traceability."	ICSStrive, CBC, Global News
2020-02-24	KHS Bicycles	USA	Discrete Mfg.	R		1			ID	Delayed shipments for 2 days	Could not process B2B orders and ship bikes following a ransomware attack over the weekend.	ICSStrive, Bicycle Retailer
2020-01-31	Toll Group	Australia	Transport	R		1			IA	Shutdown systems, and reverted to manual ops.	Australian-based global logistics company suffered a targeted ransomware attack, and shutdown automation in an abundance of caution.	ICSStrive, ZDNet, ZDNet
2020-01-13	Picanol	Belgium, RomaniaChina	Discrete Mfg.	R		3	€1M		U	Shutdown 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.	ICSStrive, Picanol Group

» Incidents 2018-2019

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2019-12-20	RavnAir Alaska	USA	Transport	R		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.	ICSStrive, The Register
2019-10-13	Pilz	Germany	Discrete Mfg.	R		1			IA	Shutdown systems, reverted to manual ops., and slowed production for 1 week	Slowdown due to impaired order tracking, due to BitPaymer ransomware attack.	ICSStrive, Drives and Controls
2019-09-27	Rheinmetall	Germany	Discrete Mfg.	U		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.	ICSStrive, Reuters
2019-07-26	City Power Johannesburg	South Africa	Power	R		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.	ICSStrive, Twitter, BBC
2019-03-18	Norsk Hydro	Norway	Metals & Mining	R		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.	ICSStrive, Microsoft, Industrial Cybersecurity Pulse,
2019	Unknown gas pipeline	USA	Oil & Gas	R		1			DS	Shutdown 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.	ICSStrive, Security Week, CISA
2018-08-03	Taiwan Semiconductor Manufacturing Co (TSMC)	Taiwan	Discrete Mfg.	R		3	$255 m		I3	Shutdown 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.	ICSStrive, IT Pro

» Incidents 2016-2017

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2017-08	Petro Rabigh Petrochemical Refinery	Saudi Arabia	Oil & Gas	NS		1			DO	Shutdown one plant, twice	Triton malware employed to infect and reprogram Triconex safety systems. This triggered an automatic shutdown, alerting operations. Occurred twice.	ICSStrive, The Guardian, CBS News
2017-06-27	Many, incl. AP Moller-Maersk, JNPT Gateway Terminals India (GTI), Merck Pharmaceutical	Global	All	NS		1	$10B		I3	Outages throughout many industries: one incident, countless victims; Shutdown ops. At JNPT GTI Terminal.	NotPetya malware, created by Russian actors targeting Ukraine, spreads indiscriminately through networks using the EternalBlue exploit, permanently encrypting data.	ICSStrive, Wired, Times Of India
2017-05-12	Renault-Nissan	France, Slovenia, Romania, India	Discrete Mfg.	R		5			DS	Shutdown plants in Douai, Sandouville, Slovenia, Pitesti, and Chennai for 1 day	WannaCry ransomware, spread by the ExternalBlue exploit, hit 5 plants for 1 day.	ICSStrive, Industrial Cybersecurity Pulse
2016-12-17	Pivnichna substation, Kyiv	Ukraine	Power	NS		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.	ICSStrive, Wikipedia, Ars Technica
2016-08-16	AW North Carolina	USA	Discrete Mfg.	R		1	$1M		DS	Shutdown 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.	ICSStrive, ISS Source, Industrial Cybersecurity Pulse

» Incidents 2010-2015

Date	Victim	Region	Industry	TA	Attribution	Sites	Cost	FD	Type	OT / ICS Physical Consequences	Incident Summary	References
2015-12-23	Prykarpattyaoblenergo, Chernivtsioblenergo Kyivoblenergo	Ukraine	Power	NS		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.	ICSStrive, Wikipedia, Ars Technica
2014-12-22	German steel mill	Germany	Metals & Mining	U		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.	ICSStrive, BBC
2012-10	Unknown Power Plant	USA	Power	U		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.	ICSStrive, US CERT
2012-07-22	Natanz and Fordow Nuclear Enrichment Plants	Iran	Process Mfg.	U		2			DO	Shutdown 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.	Washington Post, Washington Post
2012-04-22	Iran's main oil export terminals	Iran	Oil & Gas	NS		6			DO	Shutdown 6 terminals	6 terminals ops. affected by Flame malware. News outlets confirm outage, despite Iran downplaying the attack's effects.	ICSStrive, BBC, Computer World
2010-07-15	Natanz Nuclear Enrichment Plant	Iran	Process Mfg.	NS		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.	ICSStrive, Wikipedia

» 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:

CERT-EU Cyber Security Briefs and Threat Intelligence Reports	https://cert.europa.eu/publications/threat-intelligence/2023
CIO Magazine (Germany): "These companies have already been hit"	https://www.cio.de/a/diese-unternehmen-hat-s-schon-erwischt
Cybercrime Magazine's Ransomware Report: Latest Attacks And News	https://cybersecurityventures.com/ransomware-report
European Repository of Cyber Incidents (EuRepoC)	https://eurepoc.eu
ICS STRIVE Industrial Control System incident repository	https://icsstrive.com
KonBriefing / Cyberattacks, Hacker attacks, Ransomware attacks	https://konbriefing.com/en-topics/cyberattacks.html
Monthly Data Breaches and Cyberattacks Archive	https://itgovernance.co.uk/blog/category/monthly-data-breaches-and-cyber-attacks
Ransomware Attack List and Alerts	https://cloudian.com/ransomware-attack-list-and-alerts
RedPacket Security: Ransomware (news and breaches)	https://www.redpacketsecurity.com/category/ransomware
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)