WATERFALL®
Stronger Than Firewalls

2023 Threat Report

ICSSTRIVE
&
Waterfall Security Solutions

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

Executive Summary

The Waterfall / ICSSTRIVE annual threat report documents public reports of deliberate cyber attacks – not instrument errors or human errors and omissions – attacks that caused physical consequences in process manufacturing, discrete manufacturing, and critical industrial infrastructures. These attacks with physical consequences turned from a theoretical problem in the 2010-2019 decade, into a very real problem this decade. In 2022, these attacks increased 140% over the previous year and impacted over 150 industrial operations. At this rate of growth, we expect cyber attacks to shut down 15,000 industrial sites in 2027, that is: in less than five years.

Hacktivist attacks that deliberately cause physical consequences are increasing – 2022 saw six such attacks, the largest of any year in history. Of the remaining attacks, the vast majority are ransomware, and in most ransomware attacks, only the IT network was impaired, not the OT network. None the less, in all ransomware attacks we track, there were physical consequences, either because physical operations relied on crippled IT systems for minute-by-minute operations, or because ransomware victims did not trust the strength of their OT security systems and so shut down operations “in an abundance of caution.”

Looking forward, we predict that because of the steadily increasing number of critical infrastructure outages, governments in many jurisdictions will order critical infrastructure owners and operators to implement dramatically stronger cybersecurity measures. Worse, we note that natural language artificial intelligence tools such as ChatGPT have the potential to enhance cyber attack capabilities and so materially accelerate the growth of cyber attacks with physical consequences. On the other hand, we also observe that the new Cyber-Informed Engineering initiative has the potential to materially improve the strength of OT security postures, even in the face of nation-state-grade ransomware and AI-powered cyber attacks.

Finally, as an aid to interested readers and other researchers, Appendix A includes a comprehensive list of all cyber attacks with physical consequences in the industries we track since 2010, with links to public resources describing the attacks.

Contents

Introduction

The ICSSTRIVE and Waterfall Security Solutions 2023 Threat Report documents credible public disclosures of cyber attacks with physical consequences to operational technology (OT) in discrete manufacturing and process industries world-wide in all of 2022. In 2022, we saw 57 attacks that met these strict criteria, an increase of more than 150% over the preceding year. Most of these attacks were ransomware targeting IT networks but resulted nevertheless in consequences for physical operations in the victim organizations.

This report documents these and other findings from attacks recorded in 2022. We also look at the most important developments in cyber defenses throughout 2022. Defensive tools and techniques are developing rapidly, and modern defenses must be deployed more widely to affect overall trends in production outages and other physical consequences.

What We Track

This report is the result of Waterfall Security Solutions' cooperation with ISSSource and their ICSSTRIVE OT incident repository. This report is focused on cyber attacks with physical consequences in:

- Discrete manufacturing: operations that combine small parts into larger manufactured objects, such as automobiles or laptop computers,
- Process industries: industries where physical operations can me modeled as a continuous process; transforming raw materials into a more useable form, as in mining or refining, and
- Critical industrial infrastructure: industrial operations that are essential to society and the economy, and deserving of special protection like transportation, power, and utilities.

We do not track cyber attacks with physical consequences in other industries, such as telecommunications outages, canceled surgeries at hospitals, or most retail store shutdowns. We also do not track general cyber attacks on the financial sector or governments, their agencies, or their militaries unless they involve an element of industrial automation for physical processes. It is not that these attacks are not important — they are. We confine our tracking and analysis to the industries that we do, because it is these industries with which the authors are most familiar.

That said, drawing a line through any continuum involves making what may seem arbitrary distinctions. Right or wrong, for this year we do not report on retail grocery store outages, even though we do report on food & beverage (human consumables) manufacturing. We do, however, report on gas station outages, because such outages are generally considered part of the "downstream" oil & gas industry. We do report on electric power distribution outages, because power distribution is considered critical infrastructure and a process industry, even though electric distribution is also arguably electricity retailing. Similarly, we do report on both postal system outages, and power and gas distribution outages. We report on postal system outages because the postal system is a transportation system. While both the post and distribution utilities are government-owned in most jurisdictions, we do not report on other government service outages, such as tax departments, the courts of law, or financial systems.

OT Incidents with Physical Consequences in 2022

With Physical Consequences

The research team for the 2023 report found that fifty-seven (57) incidents out of 218 incidents on the ICSSTRIVE website resulted in physical consequences and matched our inclusion criteria. A more detailed version of this list is included as part of Appendix A.

2022	Industry	OT Incident Description
Jan	Transport	**Bay & Bay Transportation** — 1.5 weeks production lost while all systems taken offline and remediated
Jan	Process Mfg	**CPH Chemie & Papier** — Newsprint paper producer: 6 days of downtime, lost 8,400 tons in paper output
Jan	Food & Bev	**KP Snacks** — Production halted, delayed deliveries 2 months, and capped orders while existing stocks consumed
Jan	Oil & Gas	**Mabanaft & Oiltanking** — Both units declared Force majeure: halted loading and unloading of fuel & bulk oil at the ports
Jan	Oil & Gas	**SEA-Tank & SEA-Invest** — Ops. at all ports in Europe and Africa impacted. SEA-Tank terminal in Antwerp cannot unload fuel at port.
Feb	Oil & Gas	**Evos** — Delays in unloading fuel at three ports: Terneuzen (Netherlands), Ghent (Belgium), and Birzebbuga (Malta)
Feb	Transport	**Swissport** — 22 flights, cargo, and freight services delayed or canceled for 20 min
Feb	Transport	**JNPCT** — Diverted incoming vessels and halted in-progress loading/unloading at port
Feb	Transport	**Expeditors** — Operations shut down for 3+ weeks as they cannot ship freight or manage customs processing
Feb	Discrete Mfg	**Caledonian Modular** — Lost production was a contributing factor in the company's insolvency the following month
Feb	Discrete Mfg	**Bridgestone** — 10 days lost production, and workers sent home at all 23 tire plants in the Americas
Feb	Transport	**Belarus Railway** — Rail routing and switchgear disabled by hacktivists – trains halted in Minsk, Orsha, and Osipovichi
Feb	Discrete Mfg	**Kojima Industries & Toyota** — Shut down all 14 Japanese Toyota-owned vehicle plants 1 day, resulting in 10K unit production loss
Feb	Power	**Rosetti Energy** — Deactivated all electric vehicle charging stations between Moscow and St. Petersberg along the M-11 motorway
Mar	Food & Bev	**H.P. Hood Dairy** — Shut down production for 1 week – forced disposal of all dairy product: orders, and deliveries canceled
Mar	Transport	**Hellenic Post** — 17-day nation-wide disruption to all mail, financial, and bill payment services processed through the Greek Post
Mar	Food & Bev	**TAVR** — Production halted and a “significant economic loss recorded”
Apr	Transport	**Bulgarian State Post** — 2+ week outage of 26 national postal services, including deliveries
Apr	Transport	**Costa Rican Customs Service** — National Customs systems outage of > 1 month cause shipments to slow to a trickle
Apr	Transport	**Sunwing Airlines** — 5+ day outage of check-in systems delays 188 flights & strands or delays thousands of passengers
May	Discrete Mfg	**AGCO** — Production shutdown for 15+ days at the start of planting season, sent workers home
May	Transport	**SpiceJet** — 5+ hour outage where planes are grounded or delayed
May	Discrete Mfg	**Foxconn Baja California** — Operations affected by disrupting production for 2 weeks, then forced production capacity adjustment
May	Discrete Mfg	**CMC Electronics** — Disrupted operations to a key supplier of avionics to Canada's Department of National Defense
Jun	Transport	**Yodel** — Millions of customers face parcel delivery delays
Jun	Food & Bev	**Apetito / Wiltshire Food Farms** — 5-day halt to food deliveries destined for vulnerable Meals-on-Wheels customers
Jun	Discrete Mfg	**Macmillan Publishers** — Unable to ship orders, with several months of delivery backlogs reported at regional warehouses
Jun	Metals & Min	**Khuzestan Steel Co.** — Equipment damage due to fire and production halted
Jun	Process Mfg	**Knauf** — 3+ weeks production shutdown – existing orders delayed, and all new orders cancelled
Jul	Discrete Mfg	**Eglo** — Shut down production, order processing and shipping for 12 days
Jul	Discrete Mfg	**Semikron** — Production halted and not fully restored for months after the incident
Aug	Transport	**Ontario Cannabis** — 5-day province-wide halt to delivery & distribution of the government-controlled cannabis supply
Aug	Discrete Mfg	**Bombardier (BRP)** — 1 week production shutdown, and halts all sales orders and fulfillment
Aug	Transport	**Apex Capital / TCS Fuel** — 1-week impact to small trucking businesses relying on TCS Fuels for refilling trucks and paying operators
Sep	Transport	**Novosibirsk TMS** — 2+ days traffic chaos, due to traffic scheduling system being disabled then damaged, to hamper restoration
Sep	Transport	**Yandex Taxi** — 3+ hours traffic chaos in Moscow, caused by attack that dispatched all Yandex Taxi's cars to the same location
Sep	Food & Bev	**Läderach** — 67-day interruption to production, logistics and administration
Sep	Power	**Electricity Company of Ghana** — 5+ days of power outages for pre-paid commercial and residential customers
Oct	Food & Bev	**HiPP** — Production shut down for days, and 1000 employees sent home
Oct	Discrete Mfg	**Stimme Mediengruppe** — Printing operations shut down and employees sent home, also impacted other regional publishing partners
Oct	Metals & Min	**Aurubis** — Production and delivery halted, and employees sent home at the Buffalo, NY plant

Oct	Transport	**Danish Rails** — Trains shut down, for several hours, at state-owned and largest rail operator
Oct	Process Mfg	**Cartonnerie Gondardennes** — Shut down prod. for 3 days and workers sent home until systems decrypted
Nov	Transport	**Jeppesen** — Jeppesen's flight planning tools shut down, causing multiple airline carriers to suffer flight delays
Nov	Discrete Mfg	**Uponor** — Shut down production and deliveries for 1 week, then reduced capacity for 2+ weeks
Nov	Discrete Mfg	**PGT Innovations** — Impacted manufacturing at 2 plants and contributed to $12m quarterly revenue loss
Nov	Food & Bev	**Maple Leaf Foods** — Disrupted ops. and services at multiple sites
Nov	Transport	**Taxis Coop Québec** — 2.5 hours dispatch system outage in the early morning hours
Nov	Discrete Mfg	**EMA** — 6+ day production line outage, and employees sent home
Nov	Transport	**Communauto** — 1-day ops. outage to ride-sharing services
Nov	Discrete Mfg	**Prophete** — 3–4-week operational shutdown with interruption of invoicing and delivery services caused company insolvency
Nov	Food & Bev	**Cobolux** — 1 day production loss; Estimated €400K - €500K in damages and restoration costs
Dec	Discrete Mfg	**UNOX** — 2-day production shutdown
Dec	Food & Bev	**Fruttagel** — 4+ day production shutdown
Dec	Water	**Empresas Públicas de Medellín (EPM)** — Water distribution outage for 28k pre-paid customers; company had water trucked in
Dec	Discrete Mfg	**Technolit** — Operations shut down and employees sent home
Dec	Metals & Min	**CMCC** — 5 days pre-emptive shutdown, followed by 4 days of reduced production

Some of the year's highest-profile and most noteworthy incidents include:

- Outages at widely known businesses, including fourteen of Toyota's automobile manufacturing plants, twenty-three of Bridgestone Tire's plants, and outages at Maple Leaf Foods and Macmillan Publishers,
- Flight delays for tens of thousands of air travelers in four separate attacks,
- Physical operations impacted in four attacks on metals and mining, with one of the attacks resulting in a fire and material equipment damage,
- Malfunctions of loading and unloading of cargo containers, fuel, and bulk oil for half a dozen seaports on three continents, and
- Contributing to the bankruptcy of two victim organizations.

While none of these incidents made front page news the way we saw with the Colonial Pipeline incident in 2021, 2022 did see these high-profile critical infrastructure sites impacted with physical consequences.

Near Misses

While the core focus of the Threat Report is physically consequential OT cyber incidents, there were several near misses that are worth examining for deeper insights into the nature of threats to critical industrial infrastructure. We define near misses as cyber attacks that had the potential for physical consequences if the circumstances of the attack had been slightly different. Six noteworthy near misses that met our criteria were:

2022	Industry	Near Miss Description
Feb	Food & Bev	**Seliatino Agrohub** — Hacktivists tried to spoil 40K tons of frozen meat products in the Moscow region by changing temperature setpoints from -24 to +30 °C, but the attack is detected by operations, settings put back, and networks disconnected
Apr	Power	**Seven Indian State Load Despatch Centres (SLDCs)** — An 8 month long, Chinese state-sponsored attack on Indian load distribution centers in the Ladakh region ultimately fails, amid an ongoing border dispute between the two nuclear powers
Apr	Power	**Anonymous Electric Utility —** ESET and CERT-UA determined with high confidence that Unit 74455 of Russia's GRU (a.k.a. Sandworm) targeted high-voltage substations in Ukraine with Industroyer2 malware, but the attack was detected and stopped while in progress
July	Power	**DTEK's Kryvorizka Power Plant —** A combined kinetic and cyber attack on Ukraine's grid -- where both Russian missile strikes and an attempted cyber attack by threat group XakNet on the plant's OT network -- ultimately fails to destabilize the grid
Aug	Water	**South Staffs Water & Thames Water —** Cl0p ransomware gang breaches IT & OT systems at South Staffs Water in the UK, but in a strange mix-up attempts to double-extort Thames Water, elsewhere in the country. Neither water utility suffers OT consequences
Oct	Transport	**Secretariat of Infrastructure, Communications and Transportation (SICT) —** Cyber attack shuts down IT systems at Mexico's agency that licenses commercial truck operators, threatening impair international trade and halt operations for truckers with expiring permits. An emergency decree to extend all permits and papers to December 31st and subsequent lack of media reports on the issue suggests the issue was resolved by the New Year.

These incidents were noteworthy because:

- Five of the six attacks intended to damage industries such as the power grid, international transport and trade, and the food supply and were ideologically or politically motivated, not just financially motivated,
- Three of the six were nation-state attacks on the power grid between adversaries with sizable militaries and in two cases nuclear weapons capabilities,
- One attack, on an unnamed Ukrainian electric utility, deployed a sophisticated new malware called Industroyer2, that was subsequently well documented and studied by industrial cyber security experts, and
- All these attacks targeted critical infrastructure, which means they sought to sabotage operations or endeavors essential to the well-being of societies and economies.

The April 8th, 2022, Industroyer2 attack on an undisclosed electric utility company in Ukraine is deserving of some elaboration. While the attack was detected and stopped before physical operations were impacted, the circumstances were major news. This is because the threat actors were credibly identified as the Sandstorm group – Unit 74455 of Russia's GRU – by experts at Slovakia's ESET and the Ukrainian government's Cyber Emergency Response Team (CERT-UA). In this nation-state attack, Sandstorm attempted to cause a blackout in Ukraine by deploying a brand-new malware, an evolution over the previous Industroyer (aka CrashOverride) malware deployed by the same threat group six years prior. Industroyer2 is highly configurable and can be recompiled for each new victim and environment. Because this malware does not contain a mechanism useful for targeted ransomware, but instead is specifically tailored to target ICS power grid infrastructure, this incident stood out in a year where ransomware dominated.

Threat Analysis

Attack Trends

Figure (1) shows 2022's attack numbers in the context of attacks meeting the same criteria from 2010 onwards. The graph shows that in the decade from 2010-2019, such attacks were a largely theoretical problem. In that decade, there were many reported attacks on industrial operations, but almost all were cyber-espionage attacks that stole information, not cyber-sabotage attacks that impaired operations. Governments were concerned that espionage attacks demonstrated material weaknesses in industrial defenses, but owners and operators were by and large less concerned about becoming a target or suffering any material impact to their operations.

This changed in the current decade. Since 2020, public reports of cyber attacks with physical consequences in our focused industries have more than doubled annually. This is exponential growth. The number of impacted sites is growing at roughly the same rate as more than 150 sites were impacted this year. However, there are larger variations in the number of impacted sites from year to year than in the number of attacks impacting those sites. At the current rate, the number of attacks and the number of affected sites are increasing roughly ten-fold every 2.5 years. If this trend continues, we can expect a 100-fold increase in attacks and impacted sites in 2027 vs 2022.

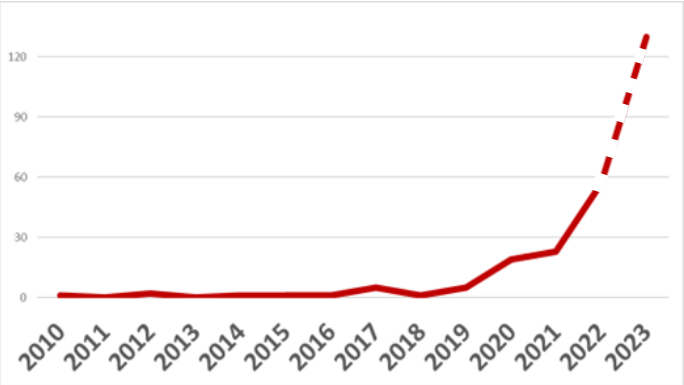

Figure (1): Consequential Cyber Attacks

This is arguably a "state change" in the global cyber threat environment. Given the trend since the beginning of the decade, it appears very unlikely that we will ever return to a year like 2013 where there was no cyber attack with physical consequences, or 2018 where there was only the one such attack.

Threat Actors

While public reports of these attacks generally contain few detail about the perpetrators, figure (2) illustrates what we do know about the threat actors. In 17% of 2022's attacks, the nature of the threat actor was not identified or reported in the public record. What was reported was that a cyber attack caused outages or consequences and to whom. Another 74% of the attacks were ransomware and the remaining 9% were by hacktivists. In looking at these incidents with physical consequences, none showed clear evidence of material state sponsorship.

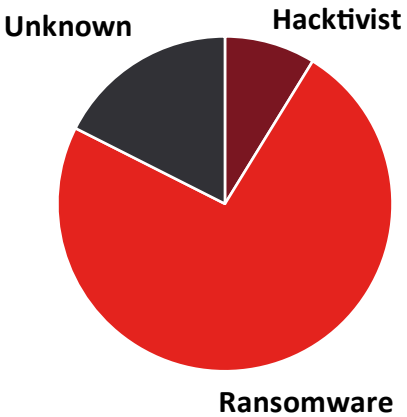

Figure (2): Attack Type

Hacktivism

2022 was the year that attacks by hacktivists became consequential to physical operations, comprising over 1 in every 10 attacks (11%). Contrast this with 2021, where

there was only a single incident of hacktivists causing physical consequences to an industrial target: the attack on Iran Rails. None of 2022's hacktivist attacks had a financial demand attached. Rather, each hacktivist group had a political or ideological agenda and set out to disrupt critical infrastructure or services in every case.

All six hacktivist incidents fall into two on-going conflicts: one incident reflects the conflict between Iran and Israel, and the others were part of the Russo-Ukrainian conflict. Of the total, four attacks disrupted transportation industry operations (rails, public transportation, or taxi services), one targeted a steel mill and caused a fire and equipment damage, and the last targeted EV charging stations belonging to a power utility. While there there were additional reports of attacks on Russia and Belarus by the hacktivist group Team One Fist, the only information available on these attacks was reports from the attackers themselves. If credible corroborating reports become available, a future threat report will update the attack list to include these incidents.

Criminal Ransomware

In 2022, 42 ransomware attacks were identified with physical consequences in discrete manufacturing, process industries and industrial critical infrastructure. That is nearly as many as the 47 such attacks in all previous study years combined (2010-2021). Of the known ransomware attacks in 2022, 17 (40%) are attributed to a known ransomware type or group. Attribution by the numbers was (6) by BlackCat or ALPHV; (2) each by Conti, Lockbit, Hive, and Black Basta; and (1) each to Black Byte, RansomEXX, and LV.

Most ransomware attacks in this report caused operational shutdowns not deliberately, but because either IT systems that were essential to continued operation of OT systems were crippled by the attack, or because the victim organization chose to shut down operations to prevent the spread of ransomware to those systems in "an abundance of caution."

Note that in the last decade, only two (2) cases on record did not have a public attribution of the threat actor. A general trend through last year was that more victims are choosing not to disclose information or details about the cyber attack they suffered. In some cases, these incidents were only disclosed by third parties with first-hand knowledge of the attack. Given that two companies cited one of these attacks as a factor in their insolvency, and that increasingly ransomware gangs employ double or triple extortion techniques, it makes sense that organizations are being more tight-lipped. Victim motivation to avoid public disclosure can include refusing to give criminals the upper hand in any possible ransom negotiations and protecting themselves from legal and regulatory consequences.

Geography

Figure (3) is one perspective on the geographic distribution of victim sites. Attributing a geography to each of these cyber attacks is problematic, because so many victims had multiple affected sites in multiple geographies and jurisdictions. Appendix A attributes a geography to each according to:

- If sites in only one country were affected, we list that country.
- If sites in many countries were affected, we list the country of the victim's head office.

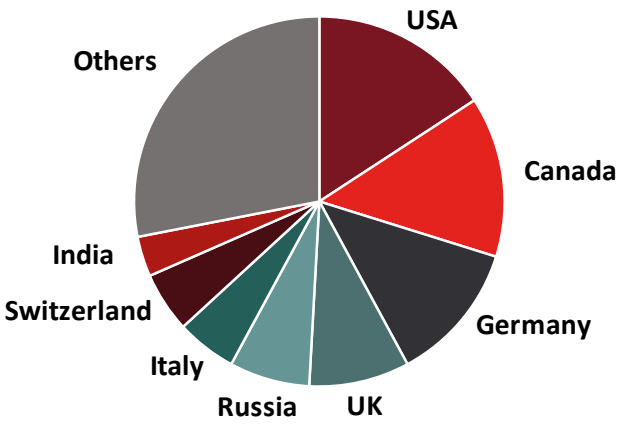

Figure (3): Geographical Distribution in 2022

While numerous public reports detail widespread IT-style cyber attacks on Ukrainian targets, no such attacks in 2022 had physical OT consequences that qualify for this threat report. It is important to recall two near-miss attacks on Ukraine's power grid. This may indicate that the cyber landscape mirrors the situation on the battlefield, with Ukrainian defenses successfully countering OT cyber attacks, disabling and uncovering OT malware such as Industroyer2 before they reached their intended targets.

Conversely, Russia and its allies experienced multiple attacks with physical consequences in 2022. Besides the March 24th ransomware attack on TAVR, most of these attacks were politically motivated rather than financially driven, and are identified as hacktivist attacks in this report.

Industries

Figure (5) illustrates the year's industry breakdown. Transportation, discrete manufacturing, and food & beverages are 2022's top three victim targeted industries, the same as the previous year. One possible reason for this distribution is that "discrete manufacturing" is in fact not one industry but many, and market research suggests that there are at least as many discrete manufacturing sites on the planet as the sum of all critical industrial infrastructure and process manufacturing sites. It is therefore perhaps not surprising that this collection of industries suffers a comparable fraction of outages due to cyber attacks. We will look at finer differentiation of this sector in future reports.

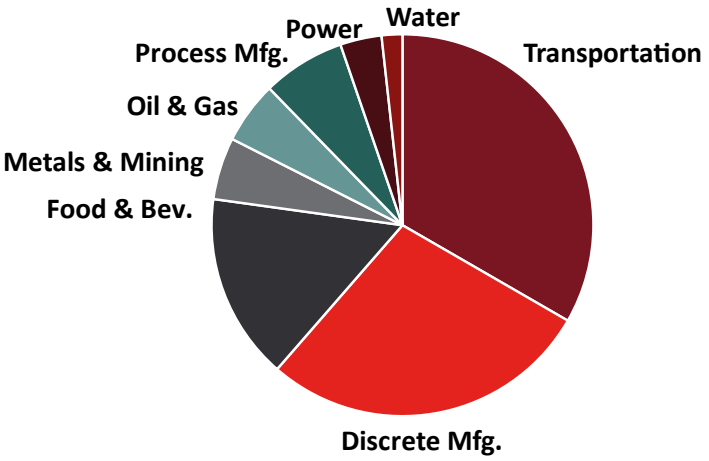

Figure (5): Breakdown by Industry Distribution

Another factor contributing to industry targeting may be IT/OT interdependencies. In the transportation industry, IT systems are often essential to minute-by-minute operations, because it is the IT systems that track packages, containers, and contents. In a large fraction of ransomware attacks, IT networks are the first networks compromised, and the first networks whose contents and systems are encrypted and impaired. Thus, industries whose physical operations and OT automation systems are heavily dependent on IT systems are more likely to suffer physical consequences when ransomware enters their IT networks.

Note: we look deeper at IT / OT interdependencies later in the report.

Key Takeaways

Attack Sophistication

When we observe cyber attacks with physical consequences more than doubling annually, it is no surprise that authorities all over the world are issuing new guidance and even new regulations. In last year's Waterfall / ICSSTRIVE threat report, we observed that the most sophisticated ransomware groups were using attack tools and techniques that less than 5 years ago were being used exclusively by nation-state threat actors. This year's US National Cybersecurity Strategy document confirms this conclusion:

> *Once available only to a small number of well-resourced countries, offensive hacking tools and services, including foreign commercial spyware, are now widely accessible. These tools and services empower countries that previously lacked the ability to harm U.S. interests in cyberspace and enable a growing threat from organized criminal syndicates.*

Therefore, at least some of what we see nation states doing to each other today, we should expect ransomware criminal groups to be doing to anyone with money within less than five years. In addition, as nation-state-grade attacks in the hands of ransomware criminals target an ever-widening swatch of industrial operations, the US national strategy recommends that we must change how we think about cybersecurity, concluding:

> *A single person's momentary lapse in judgment, use of an outdated password, or errant click on a suspicious link should not have national security consequences. Our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations and individual citizens.*

This recommendation captures the need for increased security, for new perspectives on security and for new approaches to implementing cybersecurity measures.

IT Dependencies in OT

When we see transportation systems failing because ransomware attacks impair IT networks, it is no surprise that the TSA is targeting IT/OT interdependencies explicitly in its new directives. TSA Security Directive 2021-02C is the latest directive for pipelines and is very similar to the new TSA Security Directive 1580/82-2022-01 that applies to rail systems. The approach to cybersecurity that the TSA created in response to the Colonial Pipeline attack seems to be turning into the template for directives the TSA is issuing to other industries.

Both directives include strong language for the IT/OT interface and for IT/OT dependencies. Both TSA directives start by defining network and system criticality in terms of the worst-case consequences of cyber compromise. The directives then require specific security measures at the IT/OT criticality boundary. Worst-case consequences of compromise on OT networks tend to be physical – production downtime, equipment damage or worse. Worst-case consequences on IT networks tend to be business consequences – clean-up costs, the theft of proprietary data and Personally Identifiable Information (PII) leakage lawsuits. At the connection between these two networks with very different kinds of consequences, the TSA requires very specific security measures:

- OT networks must continue operating at “necessary capacity,” even when IT networks are compromised,
- Owners and operators must eliminate all OT dependencies on IT services and if they cannot, must document residual dependencies and compensating measures to the TSA,
- Owners and operators must eliminate all OT to IT domain trust relationships, and if they cannot, must develop policies to manage the risks due to those dangerous trusts, and
- OT networks must be designed so that they can be isolated from IT networks during incident response procedures.

In discussing these directives with industry stakeholders throughout the last 12 months, it has become clear that it can be very difficult to eliminate all OT dependencies on IT systems. However, we cannot simply ignore any dependencies that must remain. Instead, we must recognize that IT systems that are essential to continued physical operations are in fact reliability-critical components. These reliability-critical systems may be hosted on the IT network instead of the OT network but must be managed and secured as if they were OT systems. For example:

- If a pipeline depends on a custody transfer and billing system in IT: modify our customer contracts so that if we must declare *force majeure*, custody transfer billing enters an “approximation” mode. The OT system caches all billing-relevant data in a historian or other repository until the billing system recovers and can reconcile accounts.
- If a passenger rail system depends on customers having access to a ticketing system, then host the entire ticketing system on a virtual machine, keep a known-good copy of the VM stored where attackers cannot reach it, and log ticket purchase transactions to write-once media. Then if the IT network fails, we can promptly restore the ticketing system and replay the transaction logs to restore functionality.
- If a factory needs new production orders and specifications to execute against when the current production run is complete, then keep a queue of 7-10 days of such orders stored in the OT system in case the IT system is compromised.

Note: if quick recovery of an IT system is essential, such as in the ticketing example above, we must also eliminate dependencies that the reliability-critical IT system may have on other external systems. For example, we should remove critical systems from management by the main Active Directory system, so that if the main IT AD system is impaired, then the critical ticketing system can come up and function correctly even without the rest of the IT network functioning.

External Dependencies

2022 saw 14 Toyota plants shut down because Kojima Industries, a Toyota supplier, was shut down by a ransomware attack. News reports indicated that the Toyota plants shut down because:

- Just-in-time manufacturing meant that Toyota had no inventory of Kojima’s parts and so Toyota factories had no choice but to stop production for lack of those parts, and
- Just-in-time coordination software at Toyota and throughout the Toyota supply chain had connections to the compromised Kojima network and systems, Toyota and most of the connected manufacturers shut down in “an abundance of caution” while they were inspected for copies of the ransomware.

A more general lesson therefore is about dependencies on external systems and suppliers. If a supplier cannot deliver goods or services essential to physical operations at a manufacturer or other industrial operation, then the affected operation must shut down. And if a supplier or cloud

services provider with connections into a manufacturer is compromised, then again that manufacturer and in fact every industrial operation with connections to that compromised provider risks an “abundance of caution” shutdown. Whether a client of the compromised supplier or service shuts down depends of course on the strength of cybersecurity at each client.

Predictions

Use of Artificial Intelligence for Stage 2 in the ICS Cyber Kill Chain

In November 2022, ChatGPT was released, and since then artificial intelligence tools have become mainstream. Simultaneously, other tools based on Large Language Models (LLMs) have emerged, targeting various activities. It is expected that attackers will incorporate these tools into their offensive arsenals. We also predict that these tools will be used to create OT malware for Stage 2 of the ICS kill chain – the payload – to achieve physical consequences.

Creating OT payloads that are able to bring about consequences more serious than a shutdown of physical operations is challenging. To date, such payloads have been crafted exclusively by nation-state actors able to hire personnel with deep engineering expertise. Moreover, many OT environments differ significantly across industries and even across sites within the same organization. This means that even engineering-sophisticated attackers may spend months studying a specific environment to launch an effective attack. Malware with payloads targeting OT systems is rare, and only STUXNET, HAVEX, BlackEnergy, Industroyer, CrashOveride, TRISIS, and PipeDream are known examples.

The emergence of AI tools that offer in depth knowledge on various subjects increases the risk that AI could potentially create these payloads on demand, creating payloads for Stage 2 that involve more intricate actions which could result in nation-state grade physical consequences.

Enhanced Global Response and Legislation

The predictable reaction for a government when the safety of its citizens is involved is to enact legislation to reduce the impact of the threat. As discussed earlier, the US TSA issued new regulations for the nation's most important pipelines less than two months after the Colonial Pipeline outage. With consequential cyber attacks increasing ten-fold every 2.5 years, it is inevitable that there will be additional attacks causing outages of high-profile critical infrastructures throughout the next half decade. Owners and operators should expect governments in many jurisdictions to issue new cybersecurity regulations because of this trend, as those governments become aware of the state change in the threat environment.

We are already seeing governments expressing a need for change. The first pillar of the Biden-Harris National Cybersecurity Strategy for example, is to defend critical infrastructure and essential services from attacks, while the new NIS2 legislation in Europe is an effort intended to harmonize cybersecurity policies for all European nations.

We expect the impact of these initiatives on OT cybersecurity programs to include:

- An increased focus on segmenting critical OT systems from IT networks to prevent consequences based on IT dependencies and "abundance of caution" shutdowns,
- New legislation requiring more transparency when reporting attacks and their resultant consequences – NIS2 already requires that an early warning must be issued within 24 hours, followed by an incident notification within 72 hours, and a complete incident report within one month, and
- Wider collaboration, both at the state and international levels, with the creation of new organizations to oversee the response to global attacks, such as the newly established European Cyber Crisis Liaison Organization Network (EU-CyCLONe).

We expect the future of cybersecurity regulation for OT networks in at least critical industrial infrastructure to focus on preventing outages and recovering more quickly from outages, rather than protecting information.

Emergence of Engineered Cybersecurity

The publication of the US Department of Energy's Cyber-Informed Engineering (CIE) Strategy was another highlight of 2022. That strategy recognizes that, in a world where very sophisticated and consequential cyber attacks are becoming the norm, and attacks with physical consequences are more than doubling annually, the engineering profession has powerful tools available to address physical risks due to cyber attacks. For example:

- Safety engineering: spring-loaded, over-pressure valves and other mechanical safeties can make over-pressure explosions and other safety consequences physically impossible – eliminating those consequences as cyber risks.
- Digital protection: digital circuits with gate arrays and ASICs but no CPUs can carry out complex equipment-protection and other functions, and the function of these digital circuits cannot be subverted by a cyber attack.
- Network engineering: monitor-only IIoT networks can protect against compromised cloud systems, and unidirectional gateway technology can protect against any external compromise penetrating to a protected system: this class of protection can enable monitoring of industrial systems, without introducing risks of cyber-sabotage to those systems.

All these approaches are unique to the engineering profession – where is an over-pressure valve in the NIST Cybersecurity Framework for example? Or in the IEC 62443 standards? And unlike conventional IT-grade protections, the CIE approach yields defenses that are engineering-grade and can be empirically modeled to work predictably and consistently for decades, even when under attack, and even as the attacks evolve into the future.

Summary

In short, key take-aways from the 2022 data set and analysis include:

- Industrial cybersecurity has transformed from a mostly theoretical problem last decade to a very real and rapidly growing problem this decade,
- Cyber attacks with physical consequences in the industries we track are increasing exponentially – if this rate of growth persists, we will see at least 4,500 incidents per year, affecting over 15,000 industrial sites by the end of 2027,
- Most of these attacks are ransomware, but hacktivists are increasing their activities,
- The transportation industry suffered the greatest number of attacks this year, with many of those attacks involving OT dependencies on IT systems,
- The US TSA has issued new directives for rails that mirror their 2021 pipeline directives, and many of the measures in these directives directly target IT/OT connections and IT/OT interdependencies,
- Large language-model-based tools, such as ChatGPT, have the potential to significantly enhance the capabilities of attackers in orchestrating cyber attacks with physical consequences,
- We should expect new regulations and legislation in many jurisdictions as cyber attacks increasingly impact national security and the daily lives of citizens, and
- The new CIE strategy shows promise for developing an engineering body of knowledge for designing out cyber risk to physical operations and public safety.

The industrial security threat environment suffered a significant transformation after 2020 – attacks with physical consequences are now increasing exponentially. The US administration has already reacted to the first symptoms of this transformation by modifying their defensive strategies. Other authorities world-wide will have no choice but to follow suit in the years ahead.

Appendix A – 2010-2022 Data Set

The following is a detailed listing of all cyber attacks with physical consequences in our tracked industries in the public record, from the beginning of 2010 to 2022's year end. Estimates of the number of sites affected, and impact costs are lower bounds where we report the lowest reasonable numbers that are supported by public reports of the incident.

Date	Victim	Region	Industry	Threat Actor	Sites	Cost	OT / Physical Consequences	Incident Summary	References	
2010 07-15	Stuxnet	Iran	Process Mfg.	Nation State	1		Destroyed 1000 centrifuges at Natanz	Plant was infected by the Stuxnet worm in a targeted attack designed to disrupt Iran's nuclear enrichment program	https://en.wikipedia.org/wiki/Stuxnet	
2012 04-22	Iran's main oil export terminals	Iran	Oil & Gas	Nation State	6		Shutdown 6 terminals	6 terminals ops. affected by Flame malware. News outlets confirm outage, despite Iran downplaying the attack's effects	bbc.com/news/world-middle-east-59062907	iranprimer.usip.org/blog/2021/nov/02/israel-iran-cyber-war-gas-station-attack
2012 10-?	Unknown Power Plant	USA	Power	Unknown	1		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	us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf	
2014 12-22	German steel mill	Germany	Metals & Mining	Unknown	1		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	bbc.com/news/technology-30575104	
2015 12-13	Prykarpattyaoblenergo, Chernivtsioblenergo, and Kyivoblenergo	Ukraine	Power	Nation State	32		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	en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack	arstechnica.com/information-technology/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation
2016 12-17	Pivnichna substation, Kyiv	Ukraine	Power	Nation State	1		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	en.wikipedia.org/wiki/2016_Kyiv_cyberattack	arstechnica.com/information-technology/2017/06/crash-override-malware-may-sabotage-electric-grids-but-its-no-stuxnet
2017 05-12	Renault-Nissan	France, Slovenia, Romania, India	Discrete Mfg.	Ransomware	5		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	industrialcybersecuritypulse.com/facilities/throwback-attack-wannacry-ransomware-takes-renault-nissan-plants-offline	
2017 06-27	AP Moller-Maersk / Gateway Terminals India (GTI)	India	Transportation	Ransomware	1		Shutdown operations at the JNPT GTI Terminal	JNPT's GTI container terminal depends on Maersk's systems located in the Hague, which fell victim to a Petya ransomware attack	timesofindia.indiatimes.com/india/indias-largest-container-port-jnpt-hit-by-ransomware/articleshow/59346704.cms	
2017 06-27	Countless	Global	All	Nation State	1	$10B	Outages throughout many industries: one incident, countless victims	NotPetya malware, created by Russian actors targeting Ukraine, spreads indiscriminately through networks using the EternalBlue exploit, permanently encrypting data	wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world	
2017 08-?	Unknown Petrochemical Plant	Saudi Arabia	Oil & Gas	Nation State	1		Shutdown one plant, twice	Triton malware employed to infect and reprogram Triconex safety systems. This triggered an automatic shutdown, alerting operations. Occurred twice	theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safety-systems-energy-plant	
2017 08-16	AW North Carolina	USA	Discrete Mfg.	Ransomware	1	$1M	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	industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-aw-north-carolina-attack-shows-dangers-of-ransomware-and-just-in-time-manufacturing	apnews.com/article/nc-state-wire-north-america-us-news-ap-top-news-north-carolina-e316bd63f21a4fd181b3fb4a8dd7a5ba

Date	Victim	Region	Industry	Threat Actor	Sites	Cost	OT / Physical Consequences	Incident Summary	References	
2018 08-03	Taiwan Semiconductor Manufacturing Co (TSMC)	Taiwan	Discrete Mfg.	Ransomware	3	$255M	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	itpro.com/security/31629/tsmc-cyber-attack-was-apparently-caused-by-wannacry	
2019 ?-?	Unknown gas pipeline	USA	Oil & Gas	Ransomware	1		Shutdown pipeline for 2 days	Attackers used spear phishing to gain initial access to the IT network, then pivoted into the OT network due to poor segmentation. Then, they planted ransomware	securityweek.com/operations-us-natural-gas-facilities-disrupted-ransomware-attack	
2019 03-18	Norsk Hydro	Norway	Metals & Mining	Ransomware	170	$71M	Halted production at 170 sheet aluminum plants	Infected by the LockerGoga ransomware, initially spread at Norsky Hydro through phishing emails on the IT network	news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency	
2019 07-26	City Power Johannesburg	South Africa	Power	Ransomware	1		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	twitter.com/CityPowerJhb/status/1154277777950093313	bbc.com/news/technology-49125853
2019 10-13	Pilz	Germany	Discrete Mfg.	Ransomware	1		Shutdown systems, reverted to manual ops., and slowed production for 1 week	Slowdown due to impaired order tracking, due to BitPaymer ransomware attack	drivesncontrols.com/news/fullstory.php/aid/6191/Pilz_is_recovering_from_a__91major_92_ransomware_attack.html	
2019 12-20	RavnAir Alaska	USA	Transportation	Ransomware	1		Canceled Dash-8-100 flights for 24 hours	Canceled Dash-8 flights because a cyber attack caused outage of the Dash-8 maintenance system and its backup, which is required for flight	theregister.com/2020/01/02/ravnair_ransomware_dhc_dash_8	
2020 01-13	Picanol	Belgium, Romania, China	Discrete Mfg.	Ransomware	3	€1M	Shutdown manufacturing plants for 1 weeks, and sent workers home	Picanol is a manufacturer of weaving machines, and their manufacturing plants are heavily automated. Financial impact amounts paid for external experts	picanolgroup.com/en/investors/press-releases/press-release-cyber-attack-update-january-31-2020	
2020 01-31	Toll Group	Australia	Transportation	Ransomware	1		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	zdnet.com/article/deliveries-stranded-across-australia-as-toll-confirms-ransomware-attack	zdnet.com/article/toll-group-shuts-down-it-systems-in-response-to-cybersecurity-incident
2020 02-02	Miltenyi Biotech	Germany	Discrete Mfg.	Ransomware	28		Impaired global order processing for 2 weeks	Mount Locker ransomware impacted manufacturer and distributor of biotechnology & COVID-19 products. 150 GB data was exfiltrated and 1GB leaked publicly	bleepingcomputer.com/news/security/biotech-research-firm-miltenyi-biotec-hit-by-ransomware-data-leaked	
2020 02-24	KHS Bicycles	USA	Discrete Mfg.	Ransomware	1		Delayed shipments for 2 days	Could not process B2B orders and ship bikes following a ransomware attack over the weekend	bicycleretailer.com/industry-news/2020/02/25/khs-bicycles-systems-hacked-distributor-halts-shipments#.YG3-wC1h3ox	
2020 03-04	EVRAZ manufacturing	USA & Canada	Discrete Mfg.	Ransomware	2		Shutdown operations at several plants, and sent 900+ workers home for 3+ days	After an attack on IT systems, production was halted at least two sites in Canada. IT systems depend on OT and "necessary to ensure standards and traceability"	cbc.ca/news/canada/saskatchewan/evraz-regina-shut-down-ransomware-attack-1.5487017	globalnews.ca/news/6640313/evraz-regina-cyberattack-layoffs
2020 05-09	Shahid Rajaee port	Iran	Transportation	Nation State	1		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	timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april	timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps
2020 06-04	Fisher & Paykel Appliances	New Zealand	Discrete Mfg.	Ransomware	1		Shutdown appliance manufacturing and distribution ops.	Victim of the Netfilim ransomware group. They refused to pay and suffered a large data leak	stuff.co.nz/business/121849569/appliance-repairer-in-the-dark-after-ransomware-attack-on-fp-appliances	
2020 06-09	Honda	Japan, Turkey, UK, USA	Discrete Mfg.	Ransomware	4		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.com/incident/honda-manufacturing-attack	telegraph.co.uk/technology/2020/06/09/hondas-global-factories-brought-standstill-cyber-attack
2020 06-09	Lion	Australia	Food & Beverage	Ransomware	45		Shutdown brewery operations for 2+ weeks	Hit by two separate REvil ransomware attacks weeks apart, during the early months of the Covid-19 pandemic	zdnet.com/article/lion-warns-of-beer-shortages-following-ransomware-attack	smh.com.au/technology/cyber-crisis-deepens-at-lion-as-second-attack-bites-beer-giant-20200618-p5540c.html

Date	Victim	Region	Industry	Threat Actor	Sites	Cost	OT / Physical Consequences	Incident Summary	References	
2020 07-05	X-FAB	Germany, France, Malaysia, USA	Discrete Mfg.	Ransomware	6		Shutdown all plants: down 2 weeks at 5 sites, and 1 week for another	X-FAB is a leading MEMS analog/mixed-signal chip fab and fell victim to a Maze ransomware attack	businesswire.com/news/home/20200705005045/en/X-FAB-Affected-by-Cyber-Attack	
2020 09-06	Tower Semiconductor	Israel	Discrete Mfg.	Ransomware	2		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	cisomag.com/tower-semiconductor-cyberattack	
2020 09-15	Bluescope Steel	Australia	Discrete Mfg.	Ransomware	2		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.	abc.net.au/news/2020-05-15/bluescope-steel-cyber-attack-shut-down-kembla-ransomware/12251316	
2020 10-17	IPG Photonics	USA	Discrete Mfg.	Ransomware	2		Shutdown global parts manufacturing and shipping	The Oxford, MA based industrial, medical, and military laser manufacturer was hit by RansomExx malware	icsstrive.com/editorials/ransomware-hits-ma-laser-maker	bleepingcomputer.com/news/security/leading-us-laser-developer-ipg-photonics-hit-with-ransomware/
2020 10-19	Société de transport de Montréal (STM)	Canada	Transportation	Ransomware	1	$2M	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	cbc.ca/news/canada/montreal/stm-refused-to-pay-2-8-million-ransomware-attack-1.5782838	stm.info/en/press/news/2020/the-stm-completes-cyber-attack-investigation
2020 10-22	Steelcase	USA	Discrete Mfg.	Ransomware	1	$60M	Shutdown all plants for 2 weeks; delayed $60m in shipments to the 4th quarter	Office furniture maker the victim of a Ryuk ransomware attack that shutdown global order management, manufacturing, and distribution systems	bleepingcomputer.com/news/security/steelcase-furniture-giant-hit-by-ryuk-ransomware-attack	mibiz.com/sections/manufacturing/cyberattack-delays-60-million-in-shipments-for-steelcase-as-pandemic-continues-to-batter-office-furniture-orders
2020 10-22	Dr Reddy's Laboratories	India, UK, Brazil, Russia, USA	Discrete Mfg.	Ransomware	5		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	businessinsider.in/india/news/dr-reddys-shares-fell-over-3-the-drug-maker-isolated-all-data-service-centers-after-a-cyber-attack/articleshow/78806238.cms	thehindu.com/business/Industry/oct-22-data-breach-involved-a-ransomware-attack-dr-reddys/article32962438.ece
2020 10-25	Stelco	Canada	Discrete Mfg.	Unknown	1		Shutdown steel production, temporarily	The company has reported the incident to law enforcement and did not give further details.	insurancebusinessmag.com/ca/news/cyber/stelco-reveals-information-systems-were-subjected-to-a-criminal-attack-237287.aspx	
2020 12-13	Symrise	Germany	Discrete Mfg.	Ransomware	1		Shutdown production out of abundance of caution	The flavor and fragrance manufacturer was hit by a Cl0p ransomware attack	bleepingcomputer.com/news/security/flavors-designer-symrise-halts-production-after-clop-ransomware-attack	handelsblatt.com/unternehmen/industrie/mdax-konzern-hacker-legen-symrise-lahm-warum-der-fall-besonders-schwerwiegend-ist/26718680.html
2020 12-15	Forward Air	USA	Transportation	Ransomware	1		Shutdown operations and delayed shipments for a week	Hades ransomware gang attack impacted both IT and OT systems leading to delivery delays which may impact financial results	freightwaves.com/news/news-alert-forward-air-reveals-ransomware-attack-warns-of-revenue-hit	freightwaves.com/news/news-alert-forward-airs-systems-coming-back-online
2021 01-23	Westrock	USA	Discrete Mfg.	Ransomware	1		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	ir.westrock.com/press-releases/press-release-details/2021/WestRock-Provides-Update-on-Ransomware-Incident-8dfde2fca/default.aspx	
2021 01-26	Palfinger AG	Europe, N. & S. America, Asia	Discrete Mfg.	Ransomware	31		Lost nearly 2 weeks crane production at all plants	The world's largest crane manufacturer. All global plants were affected.	bitdefender.com.au/blog/hotforsecurity/worlds-largest-crane-maker-suffers-global-cyber-attack-operations-at-a-halt	
2021 02-18	Beneteau SA	France	Discrete Mfg.	Ransomware	2		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.	boatindustry.com/news/36934/beneteau-2021-growth-almost-evaporated-in-cyber-attack	

Date	Victim	Region	Industry	Threat Actor	Sites	Cost	OT / Physical Consequences	Incident Summary	References	
2021 03-11	Molson Coors	USA, Canada, UK	Food & Beverage	Ransomware	13	$120M	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	bleepingcomputer.com/news/security/molson-coors-brewing-operations-disrupted-by-cyberattack	securityweek.com/molson-coors-cyberattack-storms-could-cost-company-140-million
2021 03-20	Sierra Wireless	Canada	Discrete Mfg.	Ransomware	1		Halted production at all manufacturing sites	IoT, cellular, and wireless device manufacturer with an unknown number of manufacturing sites	isssource.com/sierra-wireless-hit-by-ransomware-attack	
2021 03-25	Asteelflash Group SA	France	Discrete Mfg.	Ransomware	20		Shutdown multiple printed circuit board plants	A leading Electronics Manufacturing Services (EMS) company suffered a REvil ransomware attack	icsstrive.com/incident/revil-ransomware-shut-down-multiple-plants-at-asteelflash	
2021 04-01	JBI Bike	USA	Transportation	Ransomware	11		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	bicycleretailer.com/industry-news/2021/04/07/jbi-back-online-limited-capacity-after-ransomware-attack#.ZBip3PbMKdY	
2021 04-04	Bakkier Logistiek	Netherlands	Transportation	Ransomware	1		Disrupted new orders, delayed shipments to retail outlets for 5 days	Caused shortages of packaged cheese at retail	icsstrive.com/incident/ransomware-attack-at-bakker-logistiek-caused-cheese-shortage-in-dutch-supermarkets	
2021 05-07	Colonial Pipeline	USA	Oil & Gas	Ransomware	1	$4.4M	Shutdown pipeline for 6 days and paid a $4.4M ransom	DarkSide ransomware behind attack on the largest gasoline pipeline in USA, triggering widespread gasoline shortages in US Northeast	icsstrive.com/incident/colonial-pipeline-ops-shut-down-after-ransomware-attack	
2021 05-20	Ardagh Group	UK	Process Mfg.	Ransomware	1	$34M	Slowed production and delayed shipments	Metal and glass beverage packaging facilities remained operational, but some processes reverted to manual operation causing shipment delays	isssource.com/eu-packaging-maker-hit-by-cyberattack	
2021 05-30	JBS SA	Australia, Canada, USA	Food & Beverage	Ransomware	5		Several large meatpacking plants shut down and sent workers home	Plants in Nebraska, Colorado, Texas, Brooks, and Australia canceled production shifts	cbc.ca/news/business/jbs-meat-cyberattack-1.6048942	
2021 07-09	Iran Rails	Iran	Transportation	Hacktivist	1		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”	nytimes.com/2021/08/14/world/middleeast/iran-trains-cyberattack.html	theguardian.com/world/2021/jul/11/cyber-attack-hits-irans-transport-ministry-and-railways
2021 07-22	Transnet	South Africa	Transportation	Ransomware	4		Declared Force Majeure and halted operations for 7 days	Transnet said ports at Durban, Ngqura, Port Elizabeth and Cape Town were affected	reuters.com/article/us-transnet-cyber-idUSKBN2EZ0RQ	
2021 09-17	New Cooperative	USA	Agriculture	Ransomware	1		Delayed grain receipts & shipments, & shutdown fertigation optimization system	BlackMatter ransomware attack impacted grain transactions during harvest season. Systems were pre-emptively shutdown to stop the spread	icsstrive.com/incident/ia-ag-cooperative-hit-in-ransomware-attack	
2021 09-19	Crystal Valley Cooperative	USA	Agriculture	Ransomware	1		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.com/incident/ransomware-attack-forces-agricultural-grain-firm-in-minnesota-to-take-systems-offline	
2021 09-21	Weir Group	UK	Discrete Mfg.	Ransomware	1	£20M	Disrupted manufacturing, engineering, and shipping	When the attack was detected, "systems promptly responded by shutting down core operations." Loss projected at £20-30m	icsstrive.com/incident/weir-group-ransomware-incident	
2021 10-09	Ferrara	USA	Food & Beverage	Ransomware	2		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	cyberscoop.com/candy-corn-hack-halloween	manufacturing.net/home/news/13165782/ferrero-to-acquire-ferrara-candy-company
2021 10-22	Schreiber Foods	USA, Europe, S. America	Food & Beverage	Ransomware	30		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	cyberscoop.com/schreiber-foods-cyber-event-ransomware-agriculture-food	wisfarmer.com/story/news/2021/10/26/schreiber-foods-hit-cyberattack-plants-closed/8558252002
2021 11-?	Madix Inc	USA	Discrete Mfg.	Ransomware	2		Shutdown production, sent employees home	Manufacture of store fixtures halted at both Goodwater and Eclectic plants	newsbreak.com/news/2435633463049-ransomware-attack-at-alabama-manufacturing-plants-send-hundreds-of-employees-home-with-no-specified-date-of-return	

Date	Victim	Region	Industry	Threat Actor	Sites	Cost	OT / Physical Consequences	Incident Summary	References	
2021 11-07	Diamond Comic Book Distributors	USA	Transportation	Ransomware	1		Delayed retail shipments by 2-4 days, twice	Diamond is a top distributor for Marvel, Dark Horse, and Image comics. Scheduled orders were temporarily halted after a ransomware attack the prevented delivery.	icsstrive.com/incident/ransomware-attack-at-diamond-comic-distributors-disrupts-retailer-shipments	
2021 11-08	Estrella Damm Brewery	Spain	Food & Beverage	Ransomware	2		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.com/incident/barcelonas-damm-brewery-ransomware-attack	
2021 12-21	Nortura	Norway	Food & Beverage	Ransomware	2		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.com/incident/norwegian-food-producer-hit-in-cyberattack	web.archive.org/web/20220701083242/norwaytoday.info/news/slaughter-pigs-sent-to-a-competitor-after-the-data-attack-on-nortura
2021 12-28	Amedia	Norway	Discrete Mfg.	Unknown	1		Shutdown printing presses for 1.5 days	Norway's largest local news publisher was forced to shut down their presses after an unspecified cyber attack shut them down.	icsstrive.com/incident/norway-media-company-amedia-hit-in-cyberattack	
2022 01-01	Bay & Bay Transportation	USA	Transportation	Ransomware	1		Lost 1.5 weeks of production	Hit by Conti ransomware, and systems taken offline and remediated	freightwaves.com/news/minnesota-trucking-company-hit-in-2nd-ransomware-attack	icsstrive.com/incident/mn-trucking-and-logistics-company-hit-by-ransomware-attack-again
2022 01-07	CPH Chemie & Papier Holding	Switzerland, Germany	Process Mfg.	Ransomware	1		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 cyber attack	euwid-paper.com/news/markets/cph-to-restart-operations-in-perlen-and-muellheim-by-tomorrow	icsstrive.com/incident/hackers-paralyze-only-newsprinting-facility-in-switzerland
2022 01-28	Kenyon Produce (KP) Snacks	UK	Food & Beverage	Ransomware	1		Halted production, delayed deliveries for 2 months, & capped orders	Hit by Conti ransomware, the snack maker "cannot safely process orders or dispatch goods." Orders will be capped while existing stocks consumed	foodprocessing.com/industrynews/2022/hackers-cripple-kp-snacks	isssource.com/ransomware-attack-at-uk-snack-provider
2022 01-29	Marquard & Bahls subsidiaries Mabanaft & Oiltanking	Germany	Transportation	Ransomware	11		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	bbc.com/news/technology-60215252	icsstrive.com/incident/german-oil-tank-farm-shut-down
2022 01-30	SEA-Tank & SEA-Invest Group	Belgium, Africa	Transportation	Ransomware	24		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	isssource.com/oil-terminals-in-europe-suffer-cyberattack	icsstrive.com/incident/oil-terminals-in-europe-suffer-cyberattack
2022 02-02	Evos Group	Malta, Belgium, Netherlands	Transportation	Unknown	3		Delayed unloading fuel at 3 ports: Terneuzen, Ghent, and Birzebbuga	Cyber attack 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	insurancejournal.com/news/international/2022/02/03/652169.htm	icsstrive.com/incident/malta-oil-terminal-run-by-evos-one-of-several-european-facilities-hit-by-a-cyberattack
2022 02-03	Swissport	Switzerland	Transportation	Ransomware	1		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.com/incident/ransomware-attack-at-swiss-airport-services-firm	spiegel.de/netzwelt/web/swissport-hackerangriff-stoert-zeitweise-flugbetrieb-in-der-schweiz-a-44285ac8-ad73-42ea-b751-91559c2ff4c8
2022 02-21	Jawaharlal Nehru Port Container Terminal (JNPCT)	India	Transportation	Ransomware	1		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	theloadstar.com/ransomware-attack-hits-nhava-sheva-container-terminal	*icsstrive.com/incident/ransomware-attack-cripples-indian-port-container-terminal-jncpt*
2022 02-22	Expeditors	USA	Transportation	Ransomware	1	$60M	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	bleepingcomputer.com/news/security/expeditors-shuts-down-global-operations-after-likely-ransomware-attack	icsstrive.com/incident/expeditors-intl-hit-by-ransomware-attack
2022 02-24	Caledonian Modular	UK	Discrete Mfg.	Ransomware	1		Shutdown manufacturing ops.	Modular building manufacturer's lost production output due to the attack was a major factor in the company's March insolvency	theconstructionindex.co.uk/news/view/jrl-buys-caledonian-modular-out-of-administration	https://https://icsstrive.com/incident/cyberattack-significantly-reduced-caledonian-modulars-operating-capability/
2022 02-27	Bridgestone	N. & S. America	Discrete Mfg.	Ransomware	23		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.com/incident/tire-manufacturer-bridgestone-hit-in-ransomware-attack	icsstrive.com/incident/tire-manufacturer-bridgestone-hit-in-ransomware-attack
2022 02-28	Belarus Railway	Belarus	Transportation	Hacktivist	1		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	bgprime.com/amp/technology/belarus-hackers-allegedly-disrupted-trains-to-thwart-russia	

Date	Victim	Region	Industry	Threat Actor	Sites	Cost	OT / Physical Consequences	Incident Summary	References	
2022 02-28	Kojima Industries, Toyota, Hino, & Daihatsu	Japan	Discrete Mfg.	Ransomware	14		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	isssource.com/toyota-halts-production-after-cyberattack-on-supplier	
2022 02-28	Rosetti Energy	Russia	Power	Hacktivist	2		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 President Putin	icsstrive.com/incident/russian-electric-vehicle-chargers-hacked-on-m11-highway-as-political-protest	
2022 03-11	H.P. Hood Dairy LLC	USA	Food & Beverage	Unknown	13		Shutdown production 1 week, disposed all dairy product, canceled orders & deliveries	Cyber attack prompted taking Hood's 13 plants offline in an abundance of caution, and could not receive materials to manufacture dairy products	boston.com/news/local-news/2022/03/18/most-hood-plants-up-and-running-after-cyber-event	icsstrive.com/incident/dairy-plant-operations-offline-no-milk-at-schools-in-new-england
2022 03-20	ELTA (Hellenic Post)	Greece	Transportation	Ransomware	1		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	therecord.media/greeces-national-postal-service-restoring-systems-after-ransomware-attack	icsstrive.com/incident/ransomware-attack-halts-public-postal-services-in-greece
2022 03-24	TAVR Corporate Group	Russia	Food & Beverage	Ransomware	1		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.com/incident/operational-impact-after-cyberattack-at-tavr-food-processing-group-in-russia	
2022 04-16	Bulgarian State Post Office	Bulgaria	Transportation	Ransomware	1		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	euractiv.com/section/politics/short_news/russian-style-hackers-ruin-bulgarian-post-office	icsstrive.com/incident/complete-state-postal-system-outage-in-bulgaria
2022 04-17	Costa Rican Customs Service	Costa Rica	Transportation	Ransomware	1		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	fas.usda.gov/data/costa-rica-costa-rica-customs-delays-affect-imports	icsstrive.com/incident/costa-rica-declares-national-emergency-in-response-to-ransomware-attack
2022 04-18	Sunwing Airlines	Canada	Transportation	Unknown	1		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"	infosecurity-magazine.com/news/cyberattackers-hit-sunwing-airlines	icsstrive.com/incident/check-in-systems-offline-for-days-at-sunwing-airlines
2022 05-05	AGCO	USA & Europe	Discrete Mfg.	Ransomware	1		Shutdown majority 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	theregister.com/2022/05/09/farm_machinery_giant_agco_hit	icsstrive.com/incident/ransomware-attack-at-agco
2022 05-25	SpiceJet	India	Transportation	Ransomware	1		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.com/incident/spicejets-low-cost-airline-in-india-systems-and-operations-impacted-by-ransomware-attack	
2022 05-31	Foxconn Baja California	Mexico	Discrete Mfg.	Ransomware	1		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	therecord.media/foxconn-mexico-factory-operations-gradually-returning-to-normal-after-ransomware-attack	isssource.com/foxconn-recovering-from-ransomware-attack-again
2022 05-31	CMC Electronics	Canada	Discrete Mfg.	Ransomware	1		Disrupted and delayed ops.	BlackCat (ALPHV) ransomware encrypted systems and "disrupted operations" to a key supplier of avionics of Canada's Department of National Defense	itworldcanada.com/article/canadian-military-provider-suffered-ransom-attack-says-news-report/487654	icsstrive.com/incident/alphv-ransomware-gang-attacks-canadian-defense-contractor
2022 06-22	Yodel	UK	Transportation	Unknown	1		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	bleepingcomputer.com/news/security/yodel-parcel-company-confirms-cyberattack-is-disrupting-delivery	icsstrive.com/incident/millions-of-yodel-customers-in-uk-face-parcel-delivery-delays
2022 06-25	Apetito (parent of Wiltshire Food Farms)	UK	Food & Beverage	Ransomware	1		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.com/incident/apetitos-security-systems-breached-in-sophisticated-cyberattack	
2022 06-25	Macmillan Publishers	UK, USA	Discrete Mfg.	Ransomware	2		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.com/incident/cyberattack-forces-macmillan-publishers-to-take-operations-offline-and-close-physical-offices	

Date	Victim	Region	Industry	Threat Actor	Sites	Cost	OT / Physical Consequences	Incident Summary	References	
2022 06-27	Khuzestan Steel (KSC), Mobarakeh Steel (MSC), & Hormozgan Steel (HOSCO)	Iran	Metals & Mining	Hacktivist	1		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. Any potential damages to MSC and HOSCO remain unconfirmed	timesofisrael.com/large-cyberattack-on-iranian-industrial-sector-targets-three-steel-plants	icsstrive.com/incident/khuzestan-steel-hit-in-cyber-attack-production-halts
2022 06-29	Knauf	UK	Process Mfg.	Ransomware	2		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	techmonitor.ai/technology/cybersecurity/knauf-cyberattack-blackbasta-ransomware	icsstrive.com/incident/largest-building-material-producer-attacked-by-black-basta
2022 07-18	Eglo	Austria	Discrete Mfg.	Ransomware	1		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	diepresse.com/6167688/tiroler-leuchtenhersteller-eglo-von-cyber-angriff-getroffen	icsstrive.com/incident/hackers-paralyzed-computer-system-at-austrian-light-manufacturer-eglo
2022 07-29	Semikron-Danfoss	Germany	Discrete Mfg.	Ransomware	8		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	bleepingcomputer.com/news/security/semiconductor-manufacturer-semikron-hit-by-lv-ransomware-attack	icsstrive.com/incident/semikron-holding-production-after-cyber-attack
2022 08-05	Ontario Cannabis Retail Corporation (OCS)	Canada	Transportation	Unknown	1		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	cbc.ca/news/canada/toronto/ontario-cannabis-store-1.6549657	icsstrive.com/incident/us-supply-chain-cyberattack-affects-ontario-cannabis-retail-corporation-ocs-deliveries
2022 08-08	Bombardier Recreational Products (BRP)	Austria, Canada, Finland, USA	Discrete Mfg.	Ransomware	4		Shutdown production and halted order fulfillment for 1 week	RansomExx gang published all files (30 GB) exfiltrated from BRP after they refused to pay the ransom. The malware infection was traced to a service provider.	bleepingcomputer.com/news/security/ransomexx-claims-ransomware-attack-on-sea-doo-ski-doo-maker	icsstrive.com/incident/brp-suspends-operations-following-ransomware-attack
2022 08-13	Apex Capital / TCS Fuel	USA	Transportation	Ransomware	1		Shutdown ops. 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.com/incident/system-outage-at-apex-capital-affects-medium-and-small-size-trucking-companies	
2022 09-02	Novosibirsk City Transport Traffic Management System	Russia	Transportation	Hacktivist	1		Shutdown and disrupted public transportation for 2+ days	Pro-Ukrainian activists Team OneFist causes traffic chaos, by halting and damaging the public transit scheduling system and signage, so as to prevent quick recovery	ibtimes.com/russians-novosibirsk-forced-pound-pavements-team-onefist-paralyzes-traffic-exclusive-3611628	icsstrive.com/incident/novosibirsk-transportation-system-attacked-by-pro-ukranian-hacker-group
2022 09-03	Yandex Taxi	Russia	Transportation	Hacktivist	1		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.com/incident/chaos-in-moscow-traffic-caused-by-yandex-taxis-software-hack	theverge.com/2022/9/3/23335694/hackers-traffic-jam-russia-moscow-ride-hailing-app-yandex-taxi
2022 09-05	Läderach	Switzerland	Food & Beverage	Ransomware	1		Halted production, logistics and administration for 67 days	A ransomware attack on the chocolate maker causes a long-term outage, and impacts logistics. After Läderach refuses to pay the ransom, all data is leaked	icsstrive.com/incident/operations-impacted-at-swiss-chocolate-manufacturer-laderach	
2022 09-26	Electricity Company of Ghana (ECG)	Ghana	Power	Ransomware	1		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.com/incident/ransomware-attack-at-electric-company-of-ghana-left-customers-without-power-for-days	
2022 10-05	HiPP	Germany	Food & Beverage	Unknown	1		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	csoonline.com/de/a/hipp-gehackt,3674208	icsstrive.com/incident/ot-systems-impacted-by-cyberattack-at-hipp-a-german-baby-food-manufacturer
2022 10-14	Heilbronner Stimme & Stimme Mediengruppe	Germany	Discrete Mfg.	Ransomware	1		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	bleepingcomputer.com/news/security/ransomware-attack-halts-circulation-of-some-german-newspapers	icsstrive.com/incident/ransomware-attack-cripples-printing-systems-at-german-newspaper
2022 10-28	Aurubis AG	Germany, USA	Metals & Mining	Unknown	1		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	hackread.com/copper-producer-aurubis-cyberattack	icsstrive.com/incident/worlds-largest-copper-smelter-largely-maintains-operations-after-cyberattack
2022 10-29	Danish Rails (DSB) / Supeo	Denmark	Transportation	Ransomware	1		Shutdown train service for several hours	Denmark's largest rail operator halted due to cyber attack on 3rd party Supeo who were unable to offer their critical, real-time safety data to train drivers	isssource.com/trains-halted-in-denmark-after-cyberattack	

Date	Victim	Region	Industry	Threat Actor	Sites	Cost	OT / Physical Consequences	Incident Summary	References	
2022 10-31	Cartonnerie Gondardennes	France	Process Mfg.	Ransomware	1		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	lavoixdunord.fr/1250765/article/2022-11-07/le-piratage-cartonnerie-gondardennes-decrypte-par-damien-bancal-journaliste	icsstrive.com/incident/hackers-shut-down-production-at-cartonnerie-gondardennes-in-france
2022 11-02	Jeppesen, a Boeing subsidiary	Global	Transportation	Ransomware	1		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.com/incident/cyberattack-attack-at-boeing-subsidiary-causes-widespread-flight-disruptions	ops.group/blog/jeppesen-ransomware-attack-update
2022 11-05	Uponor Oyj	Finland	Discrete Mfg.	Ransomware	1		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.com/incident/operational-shutdown-at-uponor-intelligent-plumbing-climate-solutions	
2022 11-05	PGT Innovations	USA	Discrete Mfg.	Ransomware	2	$12M	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.com/incident/ransomware-attack-at-window-and-door-manufacturer-pgt-innovations	
2022 11-06	Maple Leaf Foods	Canada	Food & Beverage	Ransomware	1		Disrupted operations and services at multiple sites	BlackBasta lists Maple Leaf as one of its victims on the dark web, but Maple Leaf releases little else about the attack other than the impact to ops	just-food.com/news/canadas-maple-leaf-foods-hit-by-cyberattack	icsstrive.com/incident/system-outage-at-maple-leaf-food-manufacturer-in-canada
2022 11-17	Taxis Coop Québec	Canada	Transportation	Ransomware	1		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	ici.radio-canada.ca/nouvelle/1933690/taxi-coop-quebec-cyberattaque-informatique	icsstrive.com/incident/taxi-ride-hailing-service-in-quebec-hacked
2022 11-17	Europea Microfusioni Aerospaziali (EMA)	Italy	Discrete Mfg.	Ransomware	1		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.com/incident/cyberattack-shuts-down-operations-at-precision-casting-foundry-europea-microfusioni-aerospaziali	
2022 11-21	Communauto	Canada	Transportation	Unknown	1		Shutdown ride-sharing operations & services for 1 day	A cyber attack prevented users from starting or ending a ride, during an existing industry shortage of vehicles, frustrating users struggling to reserve a car	icsstrive.com/incident/cyberattack-hits-communauto-operations-already-struggling-with-frustrated-customers	
2022 11-25	Prophete / VSF Fahrradmanufaktur, Rabeneick and Kreidler	Germany	Discrete Mfg.	Ransomware	1		Shutdown operations for 3+ weeks and lead to insolvency	Ransomware attack meant that parts did not arrive, and bicycles were not fully assembled and delivered. Additional shareholder injections could not be secured triggering bankruptcy	icsstrive.com/incident/downtime-caused-by-cyberattack-final-straw-for-german-bicycle-manufacturer	
2022 11-25	Cobolux	Luxembourg	Food & Beverage	Ransomware	1	€400K	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.com/incident/production-halted-at-meat-processing-factory-in-luxembourg	
2022 12-10	UNOX	Italy	Discrete Mfg.	Unknown	1		Shutdown production for 2 days	Hit by a cyber attack, the company activated emergency procedures, suspended production as a safety measure, and initiated "appropriate checks"	icsstrive.com/incident/italian-oven-manufacturer-suspends-production-after-cyberattack	
2022 12-11	Fruttagel	Italy	Food & Beverage	Ransomware	1		Shutdown production for 4+ days	A BlackCat (ALPHV) ransomware attack on Fruttagel halted production and prevented customer deliveries. Ransom goes unpaid so Blackcat leaked all 720GB of exfiltrated data	icsstrive.com/incident/production-outage-after-massive-ransomware-attack-at-italian-fruttagel	
2022 12-13	Empresas Públicas de Medellín (EPM)	Colombia	Water	Ransomware	1		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	isssource.com/ransomware-attack-at-colombian-utility	
2022 12-22	Technolit GmbH, in Grossenlüder	Germany	Discrete Mfg.	Unknown	1		Shutdown operations and sent employees home	A German manufacturer and distributor of welding supplies and products was shutdown by an unknown cyber attack	icsstrive.com/incident/cyberattack-at-technolit-gmbh-employees-sent-home	
2022 12-27	Copper Mountain Mining Corporation (CMCC)	Canada	Metals & Mining	Ransomware	1		Shutdown operations for 5 days (pre-emptive), then reduced production for 4 days	CMCC shutdown mining ops out of an abundance of caution, after an attack possibly enabled by passwords leaked on the dark web weeks earlier	isssource.com/copper-miner-hit-in-ransomware-attack	

Appendix B – Acknowledgements

Waterfall Security Solutions and ICSSTRIVE would like to recognize and thank the many people who contributed materially to this report:

Andrew Ginter,
VP Industrial Security | Waterfall Security Solutions

Gregory Hale
Editor & Founder | Industrial Safety and Security Source

Rees Machtemes
Director of Industrial Security | Waterfall Security Solutions

Monique Walhof
Consultant | Industrial Safety & Security Source

Jesus Molina
Director of Industrial Security, Waterfall Security Solutions

Courtney Schneider
Cyber Policy Research Manager, Waterfall Security Solutions

We would also like to thank the many news outlets who report on cybersecurity, and the incident repositories we specifically searched for public incident disclosures and other information, including:

https://icsstrive.com
https://konbriefing.com/en-topics/cyberattacks.html
https://cybersecurityventures.com/intrusion-daily-cyber-threat-alert
https://cybersecurityventures.com/ransomware-report
https://cloudian.com/ransomware-attack-list-and-alerts
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
https://www.itgovernance.co.uk/blog/category/monthly-data-breaches-and-cyber-attacks
https://securityaffairs.co/wordpress/category/ics-scada
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
https://spin.ai/resources/ransomware-tracker/
https://cybersecurityventures.com/intrusion-daily-cyber-threat-alert/


WATERFALL®
Stronger Than Firewalls
waterfall-security.com