Waterfall / ICS STRIVE 2026
OT Cyber Threat Report

waterfall

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

Waterfall / ICS STRIVE 2026 OT Cyber Threat Report

Authors:

Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

Gregory Hale, Editor & Founder, Industrial Safety and Security Source, ICS STRIVE

Monique Walhof, Consultant, Industrial Safety and Security Source, ICS STRIVE

Contents

Key Takeaways

Cyber incidents causing physical impacts in heavy industry and critical infrastructure dropped by 25% in 2025, falling from 76 publicly recorded cases in 2024 to 57. Most of this decline appears due to an overall reduction in ransomware attacks because of a number of factors that are not likely to continue to "hold back the tide" – expect consequential breaches to start increasing again in 2026-2027.

Nation-state and hacktivist attacks doubled, with most such attacks targeting critical infrastructures. Particularly noteworthy attacks in 2025 included:

- **Jaguar / LandRover:** the most costly production shutdown in almost a decade
- **Collins Aerospace:** a crippled software system caused flight cancellations and delays for weeks – highlighting the need for rapid recovery or manual fall-backs for critical systems operated and managed by third parties
- **Grounded and mis-directed ships:** again highlighted the need for multiple independent checks on important external inputs, such as GPS signals
- **Polish distributed generation:** a near miss, because the lights stayed on, an example of the Russian nation state targeting European critical infrastructures, and a cautionary tale about "bricking" control equipment.

In this time of costly breaches and nation states targeting critical infrastructures, OT security teams cannot assume that cyber attacks with physical consequences will somehow simply go away, nor that software-only defenses are adequate, given the sophistication of today's ransomware, hacktivist and nation-state attacks. To this end, noteworthy developments in recent cybersecurity practice include:

Database of "unhackable" mitigations

- The Cyber-Informed Engineering (CIE) initiative released a database of engineering-grade mitigations for cyber attacks, many of which deserve the title "unhackable," and

Secure OT connectivity principles

- The UK NCSC and partners released innovative guidance that recognizes network segmentation and especially "unhackable" hardware-enforced segmentation as a key part of OT security, not just a compensating measure.

These tools are powerful ways to address today's automation and cyber realities. Reality is that we continue deploying more automation and increasingly connect that automation to the Internet and to cloud-based services, steadily increasing our risk profile. All this is in the context of legal and ethical obligations to make reasonable decisions when those decisions affect other people's safety, critical infrastructures, or large amounts of shareholders' money. Experts and authorities increasingly recommend that reasonable defenses include engineering-grade, hardware-enforced, deterministic protections such as unidirectional gateway technology and hardware-enforced remote access, in addition to IT-grade software protections.

Introduction & Methodology

This report documents cyber attacks with physical consequences. Security teams seeking funding for cybersecurity initiatives and business decision makers responsible for allocating such funding each need accurate data as to what breaches have occurred in the past, because those failures of security programs influence what attacks should be considered credible threats in the future. Planning for the future is especially important and especially challenging for industrial operations where every change poses a threat of errors and omissions that might materially impair safe, reliable or efficient / profitable physical operations. Given that changes to such operations can take place only at long intervals, it is especially important to use today's threat data and trends to anticipate the threat environment our defenses will face towards the end of their deployment life cycle.

In 2025, there were **57** breaches that met the strict inclusion criteria for this report: a surprising 25% decline over 2024.

In support of understanding today's threats and projecting tomorrow's, this report documents attacks that breached cybersecurity defenses targeting physical operations and infrastructure that:

- Are deliberate in nature – not errors and omissions, and neither equipment nor software failures,
- Produce physical consequences including production delays or outages, equipment damage, environmental disasters, injuries, or casualties – not just data theft or computer system clean-up costs,
- Impact manufacturing, building automation, heavy industry, and critical industrial infrastructures, including the transportation of people and goods,
- Are found in public – not private – disclosures, and
- Which the research team agrees meet the above criteria with a high degree of confidence.

This report's data is therefore a conservative estimate, certainly under-reporting actual attack activity. Many incidents were excluded due to disclosure restrictions, insufficient confidence in authenticity, or lack of access to reports in certain languages or regions. Additionally, numerous attacks very likely went unreported or were deemed unreliable in censored conflict zones.

The incident database and numbers in this report regarding breaches and outages are certain to be an underestimate.

Any reader wishing to verify the year's data can consult Appendix A, which contains the full data set of all incidents the research team counted in 2025. Readers interested in data from previous years should consult Appendix A in the 2025 Waterfall / ICS STRIVE *OT Cyber Threat Report*.

Note – why include IT incidents? A large fraction of ransomware attacks impair only IT assets, and still delay, shut down, or otherwise impact physical industrial operations. Businesses with physical operations need to know what cyber threats can impact their industrial operations, no matter which kinds of computers are targeted. To this end, this report documents all cyber attacks / breaches that impacted physical operations, no matter which cyber assets were compromised or impaired in the attack. For interested readers, the Section *How Operations Were Impacted* details how IT breaches most often impair physical operations.

Note – why track these industries and not others? This report includes industries that are in a sense related. When a cyber attack shuts down a pharmaceuticals plant, or an electronics factory, or even a shipping line, other industries take note. Power plants, refineries and pipeline operators for example, tend to track incidents in pharmaceuticals, discrete manufacturing and shipping, because they see themselves as similar kinds of targets. The same is generally not true for hospitals, telephone networks or department store chains. Hospitals and retail stores are set up and defended very little like industrial operations are, and in telephone networks, information is the asset, not physical equipment.

Finally, this report includes not only a discussion of breaches and trends, but an overview of defensive highlights in 2025, including:

- New advice from multiple agencies that encourages hardware-enforced protection and hardware-enforced remote access for OT systems, and
- An update on Cyber-Informed Engineering, the most important new development in OT security in 20 years.

As the threat environment evolves, new kinds of attacks are becoming credible threats that must be addressed in security programs. This report highlights both the attacks and the new ways those attacks are being addressed

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

Summary: This report tracks cyber attacks that caused physical consequences in heavy industry and critical industrial infrastructure in the public record. We include attacks that affect only IT assets, so long as they have physical / production consequences, because physical consequences from all cyber causes are of concern to owners and operators. We track these industries and not others, because this family of industries tends to have similar control system technologies, and so see breaches of each other's sites as significant threat intensity data points.

OT Incident Macro Trends

In 2025, there were 57 breaches that met the strict inclusion criteria for this report. As can be seen in *Figure (1)*, this is a 25% reduction over the 76 comparable breaches in 2024. In the sections and discussion that follow, we explore aspects of these attacks and trends and pull these aspects together into conclusions in the Section *Analysis – Where Did the Attacks Go?*

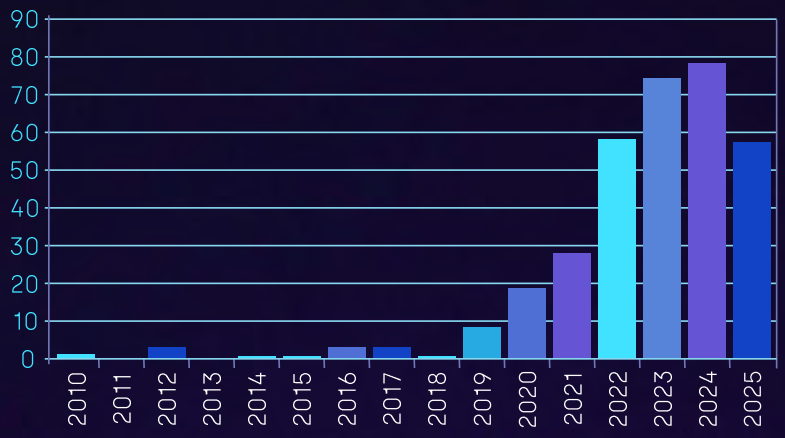


Figure 1: Breaches with physical consequences (2010-2025)

As is evident in the figure, cyber breaches with physical consequences increased markedly at the turn of the decade. The single biggest reason for the step function change was ransomware. *Figure (2)* shows that the single type of adversary responsible for a clear majority of attacks in the years 2019-2024 is ransomware criminal groups. It is also the conclusion of the research team that in the years 2022-2025, the majority of "Unknown" incidents are also ransomware, because:

- Hacktivists generally mean to make a point with the victim and with the public, and so generally make public claims about their attacks, successful or not. No such claims were made for attacks in the "Unknown" category.
- Nation state attacks are still comparatively infrequent.
- For most "Unknown" attacks, there are no details in the public record contradicting the ransomware theory.

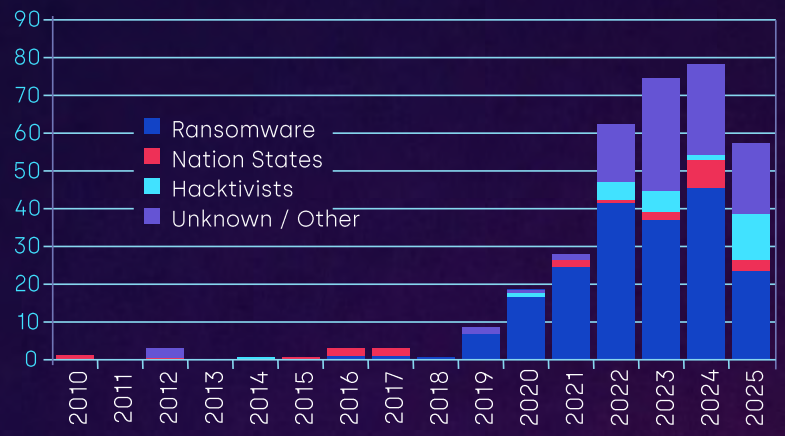


Figure 2: Attack distribution by threat actor

It is therefore reasonable to conclude the distribution of attack types in the "Unknown" category is similar to the distribution of known attacks, the majority of which are ransomware.

In the remainder of this report, we dive deeper into these numbers, looking at what they mean for industrial defenses.

> A clear majority of cyber attacks with physical consequences are the result of ransomware criminal groups

Summary: Attacks that meet our inclusion criteria are down 25% in 2025 over 2024. Most of these breaches, as in previous years, are ransomware. It is reasonable to expect that even most of the "unknown" threat actor attacks are ransomware. That said, hacktivist and nation-state attacks that deliberately bring about physical consequences increased in 2025 over 2024, despite the overall breach reduction.

Nation States & Hacktivists

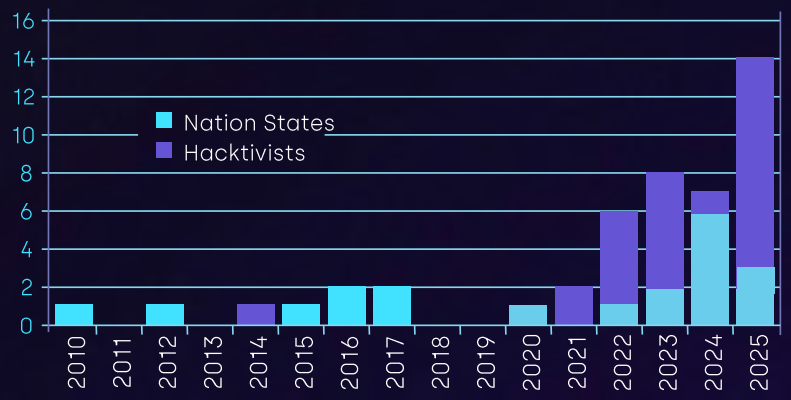


Figure 3: Nation-state and hacktivist attacks

Nation-state and hacktivist attacks **doubled** in 2025.

Nation-state and hacktivist attacks doubled in 2025 over 2024, with 5 of the 14 attacks clearly linked to the kinetic conflict which is the Russian invasion of Ukraine. This report tracks hacktivists and nation states together, because unlike many ransomware criminals, both hacktivists and nation states deliberately try to bring about physical consequences. In addition, distinguishing between hacktivists and nation states has become difficult. In principle:

Hacktivists – are amateurs. Hacktivists are not paid to carry out attacks, nor do they profit financially from such attacks. Hacktivists thus generally have no money to buy, nor the organization nor infrastructure needed build their own sophisticated attack tools, and again, have no organization that can coordinate the efforts of large numbers of attackers.

Nation States – are professional attackers, employed by armies, intelligence agencies and other government agencies. These adversaries generally have the money to buy powerful tools, have development teams able to create their own powerful attack tools, and have a strict organizational structure able to coordinate the activities of large numbers of attackers.

These distinctions have blurred in recent years. Increasingly, hacktivist groups with limited organizations or budgets have at least the blessing, if not other support from nation states, when those hacktivists act to support nation-state goals and objectives in a physical / kinetic conflict.

Significant breaches by hacktivists and nation states in 2025 included:

- **Iran's air defenses** – an American military cyber attack prevented Iran from launching surface-to-air missiles when American warplanes entered Iranian airspace, as part of a mission to bomb nuclear weapons development sites.
- **Russia's Mercury / VetIS / Saturn systems** – for tracking the movement of animal products for human consumption were twice crippled by DDoS attacks. Some Russian meat-packing plants that needed these raw products could switch to manual / printed certificate processing to continue receiving meat products, but other plants had automated their operations to the degree that a manual fall-back was impossible. Processing animal products stopped at many Russian plants for the multi-day duration of the attack.
- **Drones** – could not be converted by the Russian military from consumer firmware to military firmware for use in the invasion of Ukraine for several days because a Ukrainian cyber attack impaired the computers used to reprogram the drones at over 400 military sites.
- **MSC Antonia** – a container ship, ran aground in the Red Sea due to nation-state GPS jamming.

Two lesser incidents targeted infrastructure – a Norwegian dam was mis-operated for a period of hours, and a small Polish hydro power plant suffered a short outage, both apparently "low tech" attacks tied to Internet-exposed industrial automation.

A serious near miss occurred on December 29, 2025. A coordinated Russian nation-state attack targeted Polish Distributed Energy Resources (DER) including wind and solar sites. See the Section *Polish Energy Sector Attack*.

As significant as these developments currently seem, defenders are cautioned that reality is certainly worse than these appearances. Even nation-state militaries, intelligence agencies and other highly capable adversaries routinely take measures to control costs. When an attacker uses a costly, sophisticated attack capability, such as a zero-day or a new, powerful attack tool, that attack "ages" quickly. Defenders develop security updates and patch the zero days, develop anti-virus signatures and models to recognize and quarantine the new attack tools and patterns, rendering the sophisticated, expensive attack rapidly less effective over time. Thus, when a nation-state-backed team is given an attack objective, we should expect that team to employ the cheapest, simplest tools and techniques that will accomplish the mission objective. In short, it is reasonable to expect that nation-state adversaries have materially greater capabilities available to them than have been revealed in public thus far.

> Nation states can be cost conscious, using as little of their attack capabilities as needed to achieve a specific mission objective – be confident they have materially greater capabilities in reserve than they have yet revealed in public.

Recommendation (1): When nation-state attacks on a facility are credible threats, from nation-state-backed hacktivists to more sophisticated and well-resourced adversaries, defenders should include a large margin for error in the strength of defensive capabilities, because nation states are almost certainly more capable than their historic attacks indicate.

Despite a reputation for unlimited capability, powerful tools for addressing even nation-state threats are emerging. The Section *Defensive Developments* describes approaches to cybersecurity that are effective at eliminating entire threat vectors, even for very capable and sophisticated adversaries.

Summary: Nation-state and hacktivist attacks that caused physical consequences doubled in 2025. Victims included Iranian air defense, Russian civilian infrastructure, Russian military infrastructure, as well as shipping infrastructure. Given that nation-state adversaries try to be efficient, we should expect them to use the least capable, least costly attack tools in their arsenal that will achieve each mission objective. Recommendation summary:

1. Defenders should include a large margin for error when estimating nation-state adversary attack capabilities.

Geographies and Industries

Historically, the USA, Germany and Canada have rotated through the "top 3" victim geographies. In part this is due to these regions and economies being heavily automated and comparatively wealthy, thus hosting more targets and more lucrative targets for ransomware attacks. In part it is due to these nations serving as head offices of industrial businesses – when cyber attacks target multiple geographies, this report records the impacted geography as the country hosting the head office for the affected business.

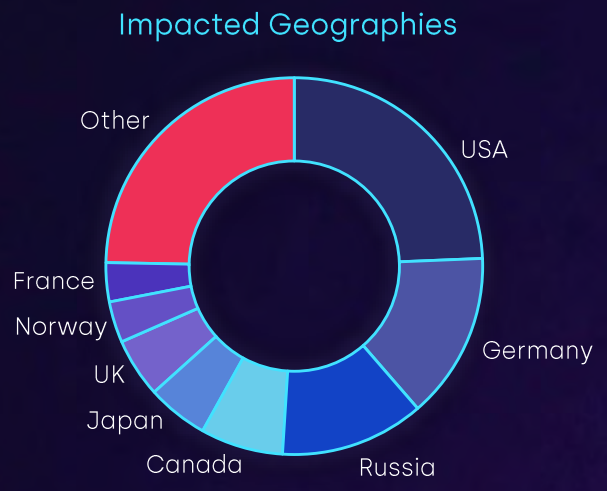


Figure 4: Impacted Geographies

In 2025, the USA and Germany were #1 and #2 targets, which is not surprising. This year, for the first time however, Russia placed in the top three, primarily due to Ukrainian nation-state and hacktivist attacks.

The "other" category in the figure is important as well – "other" includes all the nations that suffered only a single industrial outage in the public record in 2025. In total, 21 nations are represented in the data set, both developed / heavily industrialized nations, and poorer nations.

Essentially every automated industrial operation can be a target of cyber-sabotage attacks that impair physical operations.

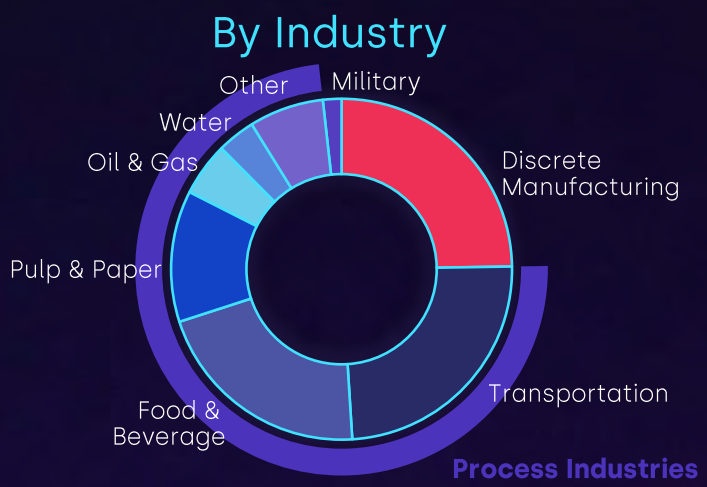


Figure 5: Impacted Industries

In *Figure (5)* we see that in 2025, discrete manufacturing and transportation were tied for the most-affected industries. In a sense however, this is a misnomer. We define:

- **Discrete manufacturing** – assembling small widgets into larger products, such as automobiles and laptop computers, and
- **Process industries** – production processes where at some point in its lifecycle, the product can be modeled as a fluid, such as oil refining, water treatment, and – stretching the point somewhat – electricity distribution and printing (turning large continuous sheets of paper into books and magazines).

All automated industrial operations in all geographies are potential targets and should deploy defensive measures proportional to credible threats and credible consequences.

Transportation is widely considered a process industry as well, because in a real sense what we "put into the pipeline," such as people boarding a train or aircraft, had better "come out of the pipeline" on the other end, or we have a serious problem.

That discrete manufacturing tied for first place is a somewhat misleading, because discrete manufacturing is no more one industry than is process manufacturing. We produce large trucks very differently than we produce shoes or plastic children's toys. All the process industries in the figure added together are a much larger set of victims than the discrete manufacturing fraction.

Critical infrastructures were impacted as well, for a total of 7 breaches (12%) across Oil & Gas, Water & Wastewater, Electric Power and Metals & Mining. This is in addition to the 14 breaches (25%) in transportation, many of which counted as critical infrastructure outages, including a ship running aground, hundreds of flights cancelled or delayed, and thousands of trucks idled for days.

Recommendation (2): All automated industrial operations in all geographies are potential targets and should deploy defensive measures proportional to credible threats and credible consequences.

Summary: The top three victim geographies in 2025 were USA, Germany and Russia – the latter primarily due to Ukrainian hacktivist and nation-state attacks. The single biggest industry vertical was discrete manufacturing. Critical infrastructures breached with physical consequences included Oil & Gas, Water Systems, Power, Metals & Mining, and Pharmaceutical Manufacturing. Recommendations summary:

2. All geographies and industries are at risk and should deploy reasonable defenses to prevent credible consequences.

How Operations Were Impacted

In past years, this report documented how cyber attacks affected physical operations. In 2025, as *Figure (6)* illustrates, 65% of public incident reports did not provide enough detail to conclude how the cyber attack impaired physical operations. Historically, there were four ways cyber attacks caused physical consequences:

- **OT compromise** – the cyber attack compromised, mis-operated, rendered inoperable or otherwise impaired OT / industrial automation cyber assets,
- **Abundance of caution** – safety-critical physical operations were shut down as a preventive measure, because the victim organization did not trust operating those assets while a cyber attack was in progress, even if there was not (yet) evidence of the attack propagating into industrial automation equipment,
- **IT dependencies** – one or more compromised IT computers or services were essential to physical operations, and those assets were impaired by a cyber attack on IT systems, or
- **Supply chain** – an operation – most often in manufacturing – had to shut down, because a cyber attack impaired the supply of critical components, or the attack shut down so many of the operation's customers that production could not continue until customer demand returned.

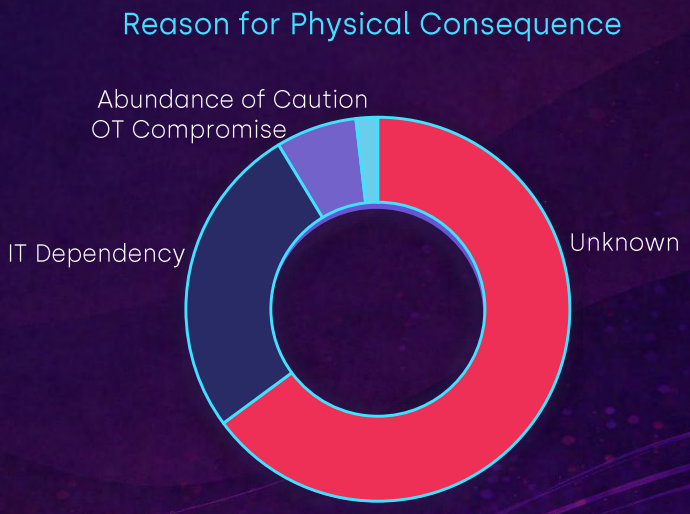


Figure 6: How cyber attacks impacted physical operations

There are four ways ransomware affects physical operations: direct compromise of OT automation, "abundance of caution" shutdowns, OT dependencies on IT systems crippled in an IT ransomware attack, and external supply chain dependencies – where ransomware shuts down a key supplier, or key customer of an industrial operation.

Historically, the breakdown between these causes of physical outages was roughly 30% / 30% / 30% / 10%, but the available data from 2025 is neither detailed nor comprehensive enough to draw useful conclusions about trends as to how attacks are affecting physical operations.

The majority of public reports of industrial breaches in 2025 described little more than the minimum required by Security and Exchange Commission 8-K or comparable filings: victim's name, attack date, whether the attack was "material" or not, whether "operations" were affected, and whether there was confidential information stolen. Often the reports did not contain enough detail to determine even whether affected "operations" were business operations or physical / manufacturing / production operations, much less how those physical effects came about, what was the initial attack vector, nor how the attack propagated within the victim's networks.

As a result, the research team has stopped tracking and reporting on the reason the cyber attack caused the physical consequence – the data is simply not available for 2025.

Recommendation (3): To prevent cyber-sabotage attack information from entering OT networks, strengthen the security at network connections – see Section *Defensive Developments*. To prevent "abundance of caution" shutdowns, increase the strength of security at the IT/OT interface to be confident of operating safety-critical physical processes even when IT networks are dealing with a sophisticated compromise. To prevent "dependency" shutdowns, understand and address OT dependencies on IT systems and services in cybersecurity planning. For examples, see *Engineering-Grade OT Security – A manager's guide*.

Summary: Incident reports are becoming much less detailed on average. It is no longer feasible to report on how cyber attacks caused physical consequences – the details are not available in the public record. Historically, physical consequences were caused by "abundance of caution" shutdowns, OT dependencies on IT systems, direct OT equipment compromise, and supply chain effects. Recommendation summary:

3. Increase OT security program strength to avoid OT targeting and "abundance of caution" shutdowns, and analyze and plan for OT dependencies on IT systems.

Noteworthy Incidents & Near Misses

2025 saw a wide variety of kinds of attacks and impacts. In this section we summarize incidents that teach important lessons.

Jaguar / LandRover – What appears to be ransomware shut down JLR UK factories for over a month. The company reported direct costs of recovery at USD $258M. Total losses for the company are estimated at roughly USD $1B, with a total impact on the UK economy, including Jaguar's suppliers, at USD $2.5B. The next-most-costly incident before JLR was the NotPetya attack that impaired many targets and for which Maerk Pharmaceutical won USD $1.4B from their insurer, Zurich.

The Jaguar / LandRover incident was the most expensive physical consequence of a cyber attack in 2025 (USD $2.5B), comparable to the NotPetya impact on Maerk Pharmaceutical in 2017 (USD $1.4B) and the Stuxnet attack on Iran's nuclear weapons program in 2010 (USD $2-3B)

Recommendation (4): It is reasonable to expect that JLR executives are wishing they had deployed a stronger security program to (a) prevent this kind of consequence, or (b) dramatically speed up recovery from this kind of attack, or (c) both of the aforementioned. Cyber attacks can be very expensive. Owners and operators should deploy very strong security programs when the cost of outages can be unacceptable.

Collins Aerospace – Ransomware crippled the Collins Aerospace vMUSE system that many airports use at check-in counters and gates used by multiple airlines. The attack is said to have encrypted over 1000 computers. The outage caused flights to be cancelled and delayed for as much as 16 days at some airports.

Recommendation (5): Highly distributed and cloud-based systems are highly vulnerable, so much so that the compromise of such systems should be seen as inevitable. When important operations depend on these exposed, distributed systems, especially systems owned or managed by another vendor (ie: supply chain risk), it is important to demand evidence of a rapid recovery capability or have practiced procedures in place for manual fallbacks to assure continued physical operations, even if those fall-backs somewhat increase costs.

United Natural Foods – A cyber attack widely thought to be ransomware impaired order processing and distribution by the food wholesaler for 30,000 retailers. The company is estimated to have lost USD $400M in sales, spent $25M in incident mitigation costs and lost $160M overall due to the event, reporting a net loss of over $50M on the quarter. This, again, is an example of a very expensive breach.

Ships ran aground – The containership MSC Antonia ran aground in the Red Sea, and the bulker Meghna Princess ran up on rocks near the Russian port of Ust-Luga (occurred in 2024 but was disclosed in 2025) – both groundings due to position system spoofing.

Recommendation (6): GPS and other position system jamming is commonplace in conflict zones, including Russian waters adjoining Europe, throughout Ukraine, and throughout the Red Sea and surrounding areas. Vessels, aircraft and others navigating these areas should be aware that positioning information is often deliberately inaccurate and should have compensating measures and practiced fall-backs in place.

More generally, when industrial / physical operations rely on external inputs, we must anticipate the failure or spoofing of those inputs. For example – again in the maritime space – a 15-year-old hacker gained access to an Italian system that establishes routes for ships in the Mediterranean Sea, changed a number of ships' courses, and took those ships off course, with some of the ships being oil tankers.

Hacktivists – opened floodgates at a dam in Norway and stopped production at a small hydro-power plant in Poland, both by accessing Internet-exposed elements of the respective control systems.

Recommendation (7): Anyone with Internet-exposed elements of their control systems should sever those connections immediately, on an emergency basis.

Summary: The Jaguar / LandRover breach is one of the top 3 most consequential breaches in all OT security history. The Collins Aerospace breach is an example of physical operations depending on very vulnerable designs. The United Natural Foods breach was also very expensive. Ships ran aground because of GPS jamming and spoofing. Hacktivists interfered with small dams and power plants from Internet-exposed OT equipment. Recommendation summary:

4. When credible consequences are very expensive, deploy very strong OT security programs.
5. For highly vulnerable systems, such as cloud-based or highly distributed systems, design for rapid recovery and to control consequences.
6. Anticipate GPS spoofing and jamming in conflict zones and more generally, design systems to be deeply suspicious of external inputs – all such inputs are more likely to be compromised than internal data sources and services.
7. Disconnect all OT assets from the Internet – do this on an emergency basis.

Polish Energy Sector Attack

The Polish CERT reports that in December 2025, Russian attackers broke into over 30 small Polish wind and solar generators. The attack also impacted control equipment in an un-named private manufacturing business and a combined heat and power (CHP) plant supplying heat to nearly a half million customers in Poland. The result was a near miss and was not counted in this report's statistics. Power continued to be generated and heat continued to flow, but the attackers erased the firmware in an undisclosed number of automation devices, rendering the devices permanently unbootable.

> Russia's attack on Polish distributed generation was a near miss – power continued to flow uninterrupted – but demonstrated that critical infrastructures are in scope for Russia-backed nation-state attacks.

The attackers gained access to the networks in the months that preceded the attack on the generators and used that access on December 29, 2025. In post-attack forensics, it was determined that at the time of the Dec 29 attack, the attackers had administrative privileges on the firewalls deployed at each of the affected sites. The attackers used the privileges they had acquired to attack monitoring and control equipment at each of the DER sites. The attack affected many kinds of devices:

- **Hitachi RTU560** – loaded corrupted firmware, sending these devices into a reboot loop,
- **Mikronika RTUs** – logged into the underlying Linux operating system and attempted to remove all files in the Linux filesystem, causing the failure of the devices,

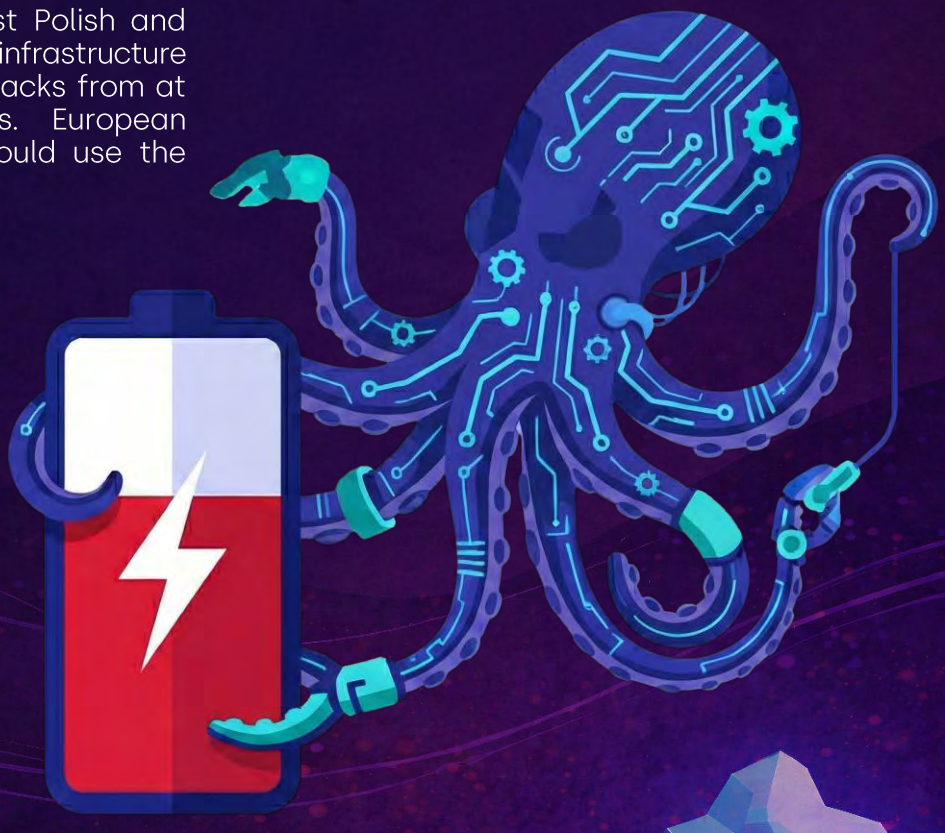
- **Hitachi Relion 650 Protection and Control Relays** – logged into the devices via a default FTP account and deleted essential files, preventing the device from restarting,
- **Mikronika HMI Computers** – logged into these Windows computers via RDP and ran a "wiper" program to first corrupt non-operating-system files and in a second pass, delete all files that could be deleted.
- **Moxa NPort 6xxx Serial Device Servers** – logged into the devices with default credentials, reset them to factory default, changed the password, and set the device IP address to an unreachable value.

The attack is noteworthy in several respects. This was an attack on Polish critical infrastructure, even if the infrastructure was on the small side. The Polish CERT concluded that the sum of generation at all 30 generation sites was not large enough to have an impact on the Polish power grid, even if all the sites' power generation were taken down simultaneously. None the less, this was an attack on industrial automation in the Polish electric sector. There is also evidence the adversaries had a presence in the Polish power networks for some months before the attack was triggered.

Recommendation (8): At least Polish and more likely all European critical infrastructure is in scope for nation-state attacks from at least Russian threat actors. European critical infrastructure sites should use the Polish CERT's report to search their own networks for evidence of a Russian adversary's long-term presence, and should adopt the most recent, most powerful innovations in OT cybersecurity to bolster those sites' defenses – see the section *Defensive Developments* below.

The attack is noteworthy in a third respect – industrial firmware was corrupted and erased, and devices were sent into reboot loops. The CERT's report does not indicate whether the industrial equipment was rendered permanently unbootable / "bricked," or if there still existed a way to restore good firmware to the devices somehow. The risk of "bricking" industrial devices is real.

If an attack "bricks" the majority of a certain model of PLC's or other automation equipment at a site, can replacement equipment still be purchased from reliable sources, or must the site carry out an emergency upgrade, with associated development, testing, certification and deployment costs?



Many industrial operations use devices that are so old, the manufacturer is no longer able to produce the devices, nor sell them. Most industrial sites, as a result, have a modest supply of spare devices in stock, to replace units that fail in the course of normal use. If most or all of one kind of old device in an industrial operation is bricked, there will not be enough spares in the organization to replace the failed devices, and few other reliable sources of spares. Such attacks risk rendering industrial sites inoperable until engineering teams can carry out emergency upgrades: upgrading programming, configuring, testing and commissioning modern replacements for the bricked equipment. This risks weeks or months of downtime for production operations, not mere hours or days.

Recommendation (9): All owners and operators of industrial facilities that use control equipment for which like-for-like replacements can no longer be purchased should take action to address the risk of large-scale device "bricking." Either upgrade automation to use only still-supported, easily replaced equipment, or deploy defenses strong enough defeat with a high degree of confidence all credible threats and attacks able to bring about large-scale "bricking."

Summary: The Polish DER attack was a near miss – the lights stayed on. That said, some kinds of automation equipment were most likely bricked in the attack, necessitating their replacement. Recommendations summary:

8. At least European critical infrastructure sites should use the Polish CERT's report and the most recent advice for deterministic defenses to bolster their defenses.
9. Owners and operators should anticipate attacks that brick large fractions of their out-of-sale equipment – such attacks risk months-long downtime due to emergency upgrades.

Broader Attack Trends

Ransomware attacks more generally showed signs of leveling off or decreasing in 2025. While there are no comprehensive or authoritative repositories of all cyber attacks nor all ransomware attacks in 2025, there are data points that suggest a levelling off.

Figure (7) for example illustrates reports to the FBI of ransomware attacks from victims in their jurisdiction. The 2025 data has not yet been published, but it is clear the number of reported ransomware attacks can vary upwards or downwards in a given year.

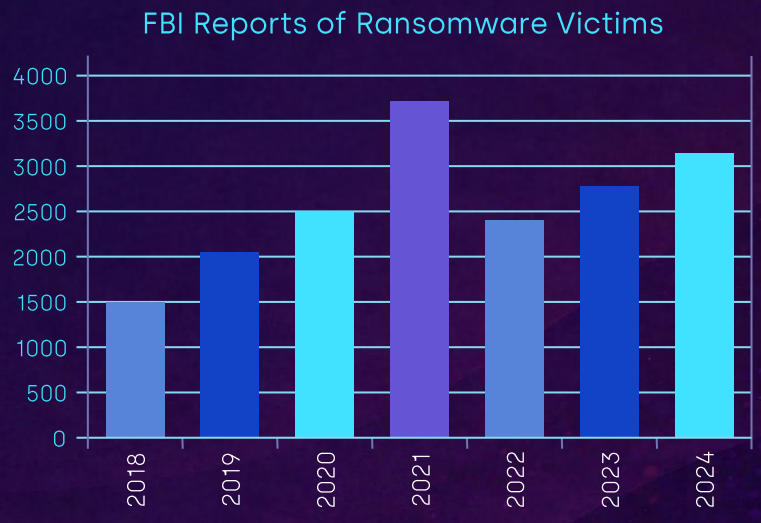


Figure 7: Ransomware attacks reported to the FBI

The NCC Group tracks alleged ransomware attacks that ransomware criminals themselves publish. The group's November 2025 data in *Figure (8)* shows ransomware attacks were mostly flat from 2024 through 2025. While ransomware and other criminals often over-state their prowess, their impact and their victims, it is worth considering that in aggregate, this unreliable over-statement is flat year over year, even if individual allegations are suspect.

Outside of the OT domain, there is evidence of a leveling-off in 2025 of ransomware attacks and encrypting ransomware attacks.

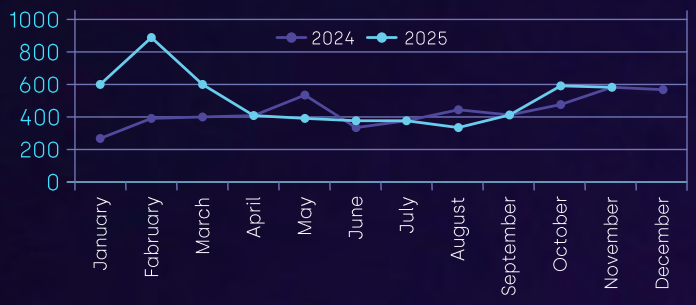


Figure 8: Criminal-reported alleged ransomware attacks (NCC Group)

The German BSI also publishes data about cyber attacks – Germany requires critical infrastructures to report all attacks that *could* impact critical infrastructures, including for example information-stealing attacks, such as an attack that steals all of a power utility's employees' personal data. Adding up the German data for industries this report tracks, we get *Figure (9)*. The data for each indicated year includes reports from June or July of the previous year, to May or June of the indicated year. As is evident in the figure, mandatory incident reports increased by 40% and 52% in 2023 and 2024, respectively, but increased by only 6% in the year ending half-way through 2025.

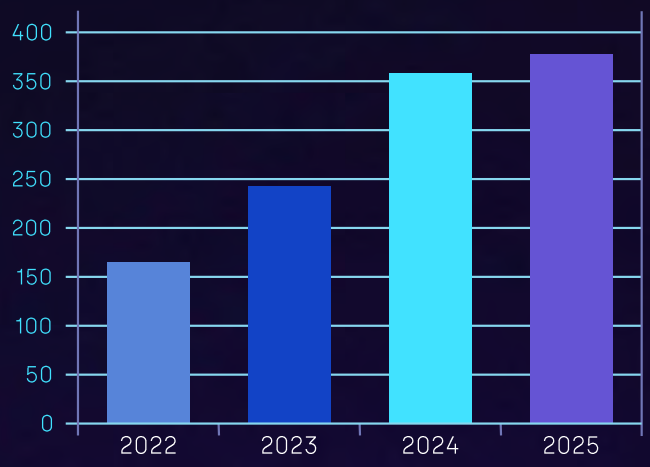


Figure 9: BSI KRITIS incident report counts in industries we track

Other data points include Coalition insurance reporting a 3% reduction in ransomware claims in 2024 over 2023, and Cyber Resilience insurance reporting a 53% reduction in cyber claims in 2025 H1 over 2024 H1. The Microsoft Digital Defense Report 2025 does not report how total ransomware attacks in their data set changed year over year, but the report does show that from July 1, 2024 through June 30, 2025 ransomware attacks reaching the encryption stage increased only 7%, compared to a 102% increase in the preceding 12 months.

That ransomware attacks overall appear to be flat or declining in 2025, with encrypting ransomware attacks mostly flat, is a significant development. All ransomware attacks on IT networks risk triggering "abundance of caution" OT shutdowns, and encrypting attacks can either directly impair OT systems, or impair IT systems essential to continuous OT operations.

Summary: FBI, BSI and other data suggests that ransomware attacks, and to an extent other attacks on critical infrastructure, increased less in 2025 than was the trend in previous years. Encrypting ransomware attacks also increased very little. This may be a proximate cause of reduced attacks with physical consequences in 2025.

Analysis – Where Did the Attacks Go?

Given the hyperbole that is commonplace in the media, vendor threat reports and sometimes even in government threat reports, most readers expect the number of OT breaches with physical consequences to increase steadily. In this section we look at what happened in 2025 – why were fewer breaches reported than in 2024?

Hypothesis: Fewer ransomware attacks mean fewer breaches.

In the section "Broader Attack Trends" above, there are strong indications ransomware attacks overall plateaued or even dropped in 2025 over 2024. Microsoft data also indicates encrypting ransomware attacks plateaued. Reasons for this effect include:

- Ransomware criminals no longer universally encrypt their victims' systems – a material fraction of those criminals now merely steal data and extort ransoms for promises of not disclosing the data,
- The global ransomware ecosystem re-organized mid-2025 as a major provider closed down and other criminal groups competed to take the place of that provider, and
- There is some evidence that C2 take-downs, sanctions and prosecution of ransomware criminals is somewhat reducing the population of ransomware criminals, because of concern over being apprehended.

A somewhat clearer picture of ransomware trends should emerge in the months ahead, as additional data sets are analyzed and documented.

Recommendation (10): Disarray in the ransomware criminal ecosystem is likely to stabilize in 2026 and beyond. The fraction of criminal groups encrypting data is also likely to stabilize. Improved law enforcement is a deterrent but given the persistent increases in ransomware attacks in the last half decade, it is reasonable to expect that a consistent enforcement posture will consistently deter a reasonably constant fraction of would-be criminals. All these factors suggest that in the absence of any other change, ransomware activity will again start to increase at near-historic 30-60% per annum rates in 2026-2027. Teams defending industrial operations should not rely on a prolonged decline in cyber threat activity, nor a prolonged decline in breaches with physical consequences.

> The reasons for ransomware attacks leveling out in 2025 reduce attacks by constant percentages. In the absence of new reasons emerging or percentages changing, ransomware attacks are expected to resume increasing in 2026-2027.

Hypothesis: Fewer attacks are being reported in public

Given steadily increasing legal mandates to report cyber incidents, one might expect that a steadily greater fraction of all incidents is reported to the public. There are some concerns that this is not the case:

- Regulations requiring reports to government authorities, such as NERC, KRITIS and other NIS2-inspired regulations, assure reporting organizations of anonymity – essentially none of these regulatory reports become public knowledge.
- It is reasonable to believe high-profile prosecutions and fines for organizations disclosing incorrect information to the public is causing legal teams to advise disclosing only the minimum. The minimum in most jurisdictions is any information that might cause a reasonable investor to buy, sell or assign a value to shares. Incidents that do not meet this threshold do not need to be reported and increasingly appear not to be reported to authorities nor to the press.

- There are few legal mandates for public incident disclosures in authoritarian regimes, nor in kinetic conflict zones. It is reasonable to expect governments in these regions to order victims to deny they were targets of a cyber attack.

On the other hand, this report tracks breaches with physical consequences. Significant physical consequences are harder to hide than stolen information or encrypted IT systems, no matter what governments or legal teams order. If the lights go out, for example, people notice, and very likely the press notices.

"Back of the envelope calculations" suggest there are not huge numbers of incidents being withheld. For example, in the recent SANS State of ICS/OT Security 2025 survey, 330 respondents indicated that 22% had suffered a "security incident" in the preceding 12 months, and 15% of those resulted in an "engineering system degradation or outage" (10 respondents / incidents). These ten incidents were due to all causes, including insider error, such as an insider inadvertently doing something on a computer in violation of company policy. This is a small number, and even this small number includes kinds of events and industries that are out of scope for this report.

Furthermore, our research team interacts routinely with many experts and incident responders in OT security. There is no hint from that community that there is a material world-wide conspiracy that is effectively covering up "huge" numbers of incidents with material physical consequences.

> Conspiracy theories postulating "huge" numbers of unreported high-physical-consequence attacks are not credible.

Thus, there are no reasonable grounds to believe there is a large body of unreported incidents in 2025 with material physical consequences. It is reasonable to believe the numbers in this report are somewhat understated – cyber attacks with minor physical effects might be successfully covered up by victim organizations, but attacks with material physical consequences are much more difficult to hide. The sky is not falling.

Recommendation (11): Despite the decline in OT consequences, the 2025 data set includes consequences that are material. Owners and operators should continue anticipate cyber attacks that are able to bring about significant consequences.

Hypothesis: Defenses are becoming more capable.

It is reasonable to believe that, given the constant exhortations from governments and others, industrial enterprises are on average and at least to some degree increasing the strength of their defenses over time. There are few objective measures of the average strength of OT cybersecurity, world-wide, however. While of this year's incidents betray woefully inadequate defenses – hacktivists exploiting Internet-facing OT infrastructure and Internet-facing IT infrastructure which is essential to physical operations, there are also a small number of breaches impacting what should have been heavily-defended OT infrastructures, such as the Jaguar / LandRover breach, and the attack that shut down Venezuelan oil terminals for several days.

In addition, stronger defenses only mean fewer breaches *when attack volume and sophistication remain constant.* Attack volume was addressed earlier in this section – it appears to be mostly constant. As to attack sophistication, while there are few objective measures of the capabilities of all the world's adversaries, there are some indications that attack sophistication is holding constant.

For example, Google/Mandiant data in *Figure (10)* shows the number of zero-day vulnerabilities exploited in the wild is largely constant since the turn of the decade. Zero-day exploits are used by the most sophisticated of threat actors, including high-end ransomware toolkits and nation-state adversaries. The number of exploited zero-days suggests the sophistication of high-end attacks is more constant than not.

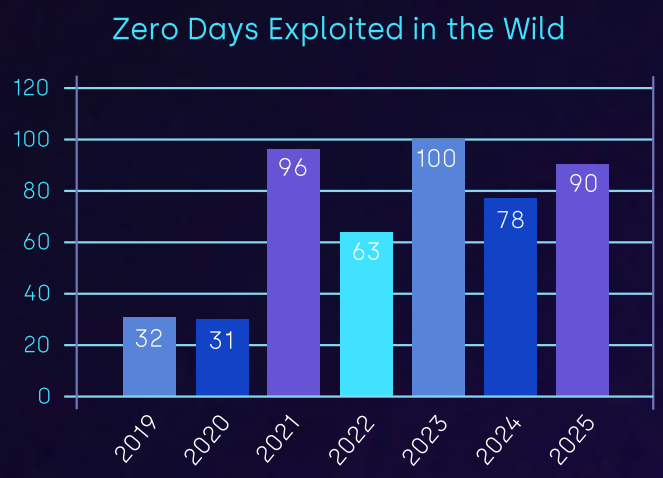


Figure 10: Zero-day vulnerabilities exploited in the wild (Google / Mandiant)

Furthermore, no new ICS-capable attack tools were disclosed in 2025. While the Dragos report on the Russian attack on Polish energy infrastructure identified the Russian ELECTRUM group as the adversary, and this group has produced new ICS-specific malware in the past, it did not do so for the attack on Poland.

> Both attacker and defender tools and techniques continue to improve incrementally.

Artificial intelligence-based (AI-based) attacks were again in the news in 2025. Artificial Intelligence is being used by both attackers and defenders. For example:

- Large language models (LLMs) are used to speed up development of effective phishing emails, and software development models are used to speed development of attack tools.
- AIs are starting to be used to automate attacks. For example, Promptlock data exfiltration malware appears to be a proof-of-concept still under development. The malware includes functions for automatically generating new attack code to evade anti-virus, deciding which data to exfiltrate, and (not yet active) encrypting valuable targets. Another example: Anthropic reported detecting and defeating a Chinese exfiltration attack campaign that used Anthropic's Claud Code AI to automate an attack campaign. Anthropic estimates the AI carried out 80-90% of the attack steps, with humans providing strategic oversight of the campaign.
- On the other hand, security product vendors also use LLMs to develop marketing messages to encourage prospects to deploy stronger defenses and use software development models to speed up the development of defensive tools.
- AIs are also built into more and more security products, especially intrusion detection and automatic intrusion prevention products.

There is no compelling evidence that this year's reduction in breaches is due to materially improved cyber defenses. Current indications in the public record are that both offensive and defensive designs and technologies, AI-based and otherwise, continue to improve incrementally. In the absence of a disruptive new criminal business model, new offensive or defensive technology, or other dramatic development, this incremental improvement seems likely to continue in the medium term, with material OT breach frequency tracking overall global cyber attack frequencies as those attacks increase.

Recommendation (12): All defenders should plan for incrementally more sophisticated cyber attacks in the near future.

While, to date there are no public report of truly independent AI-automated attacks specifically targeting industrial automation, there is concern that if a truly AI-driven autonomous attack were designed and released inside OT networks, it would have an advantage over truly AI-driven autonomous defenses, at least in change-controlled environments. Engineering teams are legitimately unwilling to deploy automatic intrusion prevention systems, much less AI-driven systems, because of the risk of those systems misdiagnosing legitimate activity and acting to impair safety-critical or reliability-critical functions. Autonomous AI attacks have no such compunctions.

Recommendation (13): AI-based attacks are an emerging threat that bears tracking. A shift by attackers to highly automated, highly targeted, higher-volume and higher-success-rate AI-based attacks on critical infrastructure could trigger a new step-function increase in OT breaches, similar to the step that occurred in the 2019-2021 timeframe. OT defenders are advised to continue improving defenses, for example by implementing the latest insights and approaches in Section *Defensive Developments* in anticipation of the next innovation in attack techniques and technologies, most likely involving AI.

Summary: Ransomware attacks appear to have plateaued or marginally declined in 2025 due to fewer criminals using encryption tactics, disarray in the ransomware criminal economy, and increased success in law enforcement efforts. These effects are expected to stabilize, resulting in a resumed increase in OT breaches with physical consequences due to ransomware in 2026-2027. Concerns about lawsuits are likely reducing the reporting of the lowest-consequence OT events and limiting the amount of detail available in the public record for other events. It is not however, reasonable to believe that there is a large body of material events going unreported.

While defenses should be somewhat more capable on average in 2025 than they were in 2024, there is evidence in the public record that attacker capabilities are also increasing incrementally, even taking current offensive and defensive AI usage into account. In the future however, fully automated AI attacks are more credible than fully automated AI defenses in change-controlled automation systems. The emergence of fully automated AI attacks targeting OT risks triggering another step-change in breach counts, analogous to the ransomware step change that occurred at the turn of the decade. Recommendation summary:

10. Teams defending industrial operations should not rely on a prolonged decline in cyber threat activity, nor a prolonged decline in breaches with physical consequences.
11. The decline in OT breaches is real. Despite the decline however, the 2025 data set includes consequences that are significant. Owners and operators should continue anticipate cyber attacks that are able to bring about material consequences.
12. Defenders should plan for incrementally more sophisticated cyber attacks in the near future.
13. Since autonomous AI attacks on OT automation confers an advantage on defenders that cannot be matched by autonomous AI defenses in change-controlled environments, defenders should closely track the development of autonomous attack capabilities and invest in deterministic defenses.

Defensive Developments

Tools, techniques and perspectives for defending industrial control systems continue to evolve as well. In the sections below, we sample highlights of 2025, and one highlight of very early 2026.

CIE Engineered Controls Database

The Cyber-Informed Engineering (CIE) body of knowledge is the most important innovation in 20 years for OT Security. Idaho National Laboratory is assembling the body of knowledge with funding from the US Department of Energy (US DoE). CIE is focused resilience by design: ensuring that even if cyber protections fail, physical systems remain safe, reliable and capable of recovery.

The latest development in CIE is the CIE Controls Database – a database of technologies and design patterns that can be applied to address specific threats and needs, in a wide spectrum of industries. For example, the database sorts controls into seven categories:

- **Physical logic mechanisms** – such as electro-mechanical relief valves and governors, physically prevent unsafe operations.
- **Redundant designs** – such as circuit breakers that incorporate both electrical and mechanical elements, so the failure of one does not eliminate protection.
- **Physical constraints and material properties** – such as plugs that melt when a vessel temperature becomes too high.
- **Digital engineered controls** – digital designs that maintain process stability even in the face of compromised, failed or inconsistent inputs.
- **Passive physical dynamics** – such as flywheels and hydraulic accumulators that physically buffer unsafe variations in physical processes.
- **One-way enforcement and irreversible actions** – such as (physical) ratchets or (digital) unidirectional gateways that make "backwards" flows of materials, movement or data physically impossible.
- **Fail-safe defaults** – such as spring-loaded brakes that engage when pneumatic pressure or power is lost, return processes to safe states in emergencies.

This is the first time anyone has collected into a single body of knowledge this many and this varied a set of engineering-grade controls for addressing cyber threats. Many of these controls are in a real sense "unhackable." Overpressure relief valves, for example, contain no CPU's nor software and thus carry out their safety-preserving functions independent of the sophistication of any advanced ransomware or nation-state-grade cyber assault.

> Many tools and techniques in the CIE body of knowledge are in a real sense "unhackable" – they carry out their protective functions reliably, even in the face of the most sophisticated-imaginable nation-state-grade cyber assaults.

Recommendation (14): OT security teams should adopt CIE, track the emerging body of knowledge as it grows and develops, and join the CIE Community of Practice to contribute actively to the development of the methodology.

Summary: The CIE Controls Database documents engineering-grade tools and techniques for addressing cyber risk – many of them in a real sense "unhackable." Recommendation summary:

14. Use CIE, use the techniques in the new database, and contribute experience and expertise to the emerging CIE body of knowledge.

Secure Connectivity Principles

The UK National Cyber Security Center (UK NCSC) along with nine international partners published *Secure connectivity principles for Operational Technology (OT)* in January of 2026. The 33-page document is focused on securing networks and connectivity, rather than securing endpoints.

The focus on connectivity is refreshing – too much first-generation-style OT security advice positions network segmentation as a compensating measure rather than a primary protective measure. Such advice ignores 50-year-old cybersecurity theory:

- Bell / Lapadula – showed that to prevent *espionage* – theft of valuable information – we must prevent lower-security actors reading from higher-security sources, and prevent high-security actors from writing to low-security sources, while
- Biba – showed that to prevent *sabotage* – mis-operation of important assets, we must prevent lower-security actors *writing* to high-security operations and prevent actors in high-security operations from *reading* potentially compromised information from low-security sources.

> Controlling the flow of attack information is essential to preventing cyber-sabotage and is not a "compensating measure."

In other words, to prevent sabotage, which is the most important cybersecurity goal at most industrial operations, we must prevent the movement of attack information into those operations from less trustworthy sources, such as from the Internet, or from Internet-exposed IT networks. Controlling the flow of information, particularly but not exclusively online / networked information, is a primary security goal, not a secondary compensating measure.

> The new UK NCSC et al. advice recommends hardware-enforced unidirectional protections – protections that, when deployed correctly, even nation-state adversaries struggle to overcome.

The new advice from the UK NCSC et al highlights this. The advice contains much that is unique – that has never been said before in any government's OT security guidelines nor recommendations. Very briefly, the document explores eight principles:

1. **Balance the risks and opportunities** – *a conventional discussion of risk management*
2. **Limit the exposure of your connectivity** – *when we must connect automation assets to IT computers, or worse to the Internet, **keep the affected OT assets patched**, scan regularly for Internet-exposed IP addresses and services, and be paranoid about wireless communications. While none of the individual pieces of advice are new, some of the combinations are new and unusually useful.*
3. **Centralise and standardise network connections** – *minimise our external connectivity and ideally route it all through a central facility for intrusion detection and active management of rules, vulnerabilities, actionable intel, etc.*
4. **Use standardised and secure protocols** – *use encryption and authentication inside our ICS as much as is practical, and always encrypt and authenticate communications across IT, Internet and other external networks.*

5. **Harden your OT boundary** – *lots of good advice for the important IT / OT consequence boundary, including hardware-enforced unidirectional communications, hardware-enforced remote access and military-grade cross-domain solutions for vetting information entering OT networks.*
6. **Limit the impact of compromise** – *some older advice coupled with a newer discussion of options for micro-segmentation to control lateral movement / pivoting attacks.*
7. **Ensure all connectivity is logged and monitored** – *the usual advice to monitor network traffic, especially remote access from IT networks and the Internet, with new advice for "break glass" emergency connections.*
8. **Establish an isolation plan** – *talks about different kinds of site and/or subsystem emergency isolation / islanding approaches, including a brand-new discussion of the business value of hardware-enforced unidirectional communications as part of the emergency islanding plan.*

Again, the document is a refreshing new look at network segmentation options, with some all-new advice, and a perspective that recognizes the importance of controlling and managing connectivity as a primary protective measure for physical operations.

Recommendation (15): Defensive teams should review and adopt the new OT connectivity guidelines, recognizing that controlling the flow of attack information to prevent cyber-sabotage is a primary goal of OT security programs, not a compensating measure.

Summary: The new multi-agency advice on OT connectivity highlights the importance of controlling the flow of attacks through connections into and out of OT networks. The advice is ground-breaking in some respects, including recommending hardware-based unidirectional protections, cross domain systems, "browse down" policies for engineering workstations and other innovations. Recommendation summary:

15. Review and adopt the new connectivity guidelines.

Looking Forward

For 50 years, industry has deployed automation systems to increase productivity and reduce production costs. All modern automation uses computers, all computers use software, all software has defects, and some of those defects are cyber vulnerabilities. Thus, for 50 years, we have deployed more and more *targets for cyber attacks*. In addition, data in motion is the lifeblood of modern automation, all cyber-sabotage is by definition attack information, and all information flows can encode attacks. Thus, for 50 years, we have deployed more and more *opportunities to attack* the ever-increasing number of targets. Neither of these trends is reversing in the next 25 years.

> It is not reasonable for workers at industrial sites to increasingly fear for their lives as their workplace becomes increasingly automated, increasing both cyber targets and cyber attack vectors. To protect workers, we must deploy deterministic "unhackable" defenses, in addition to software / cybersecurity defenses.

The majority of today's OT networks are protected from cyber attacks exclusively by software protections, and software fails predictably. If a given exploit can take advantage of a vulnerability, launching that exploit against the vulnerable target *always* produces the same result. Modelling this kind of design failure as a probability is a mistake – in engineering safety terms, cyber attacks most often represent design failures rather than random equipment failures or human error.

The CIE initiative, the latest UK NCSC guidance, CISA secure remote access guidance, and many others recognize the intrinsic limitations of software protections and recommend deterministic, hardware-enforced protections.

It is not reasonable for workers at industrial sites to increasingly fear for their lives as their workplace becomes increasingly automated and thus increasingly vulnerable. We need to start deploying "unhackable" deterministic defenses, in addition to software / cybersecurity defenses.

To this end, key questions defenders should ask going forward include:

- **Detecting, responding to and recovering from attacks** all take time, during which time adversaries have control of some or all of our industrial automation systems. What is an acceptable amount of time for adversaries to control or operate safety-critical, critical infrastructure, or otherwise important or valuable physical processes?
- **What credible cyber attacks and credible consequences are not defeated** with a high degree of confidence by the current defensive posture, and are those credible consequences acceptable?
- **Is it reasonable to protect industrial operations with only software,** given the attack capabilities it is reasonable to attribute to credible threats, including the track record of zero-day software exploits?

Critical infrastructures especially, anyone for whom a nation-state-grade attack is a credible threat, and enterprises whose worst credible consequences are very expensive should all consider deterministic, hardware-enforced defenses including hardware-enforced remote access, in addition to conventional software defenses.

Appendix A – 2025 Data Set

Date	Victim	Region	Industry	Attacker Type	Consequence	Summary	References
2025-01-19	Many	Mediter-ranean Sea	Transport	Hacktivist	Several ships, including oil tankers, diverted off course in the Mediterranean Sea	A 15-year-old logged into a portal that controls the routes of oil tankers and transport ships in the Mediterranean Sea, changing some routes. The teenager was referred to youth justice in Italy.	icsstrive.com corriere.it
2025-02-03	Lee Enterprises	USA	Pulp & Paper	Ransomware	More than 79 print newspapers cancelled, delayed or forced to print smaller versions for over 10 days	Qilin ransomware criminals attacked a large newspaper printer	icsstrive.com pressfreedomtracker.us cybersecuritydive.com
2025-02-07	CPI	UK	Pulp & Paper	Ransomware	Production at 8 factories shut down for over 12 days. Customers reported delays in printing their books as long as 18 days after the initial attack.	Cyber attack hits CPI printing - UK's largest book printer	icsstrive.com thebookseller.com reddit.com
2025-02-09	Sault Tribe	USA	Oil & Gas	Ransomware	Gas stations & other facilities closed for 2 weeks	Ransomware attack on IT impacted numerous computer and phone systems	icsstrive.com myupnow.com therecord.media
2025-02-11	Alf DaFrè	Italy	Discrete Mfg	Ransomware	Two factories shut down and 350 people laid off for 8 days	Ransomware encrypted equipment on the IT network. Initially it was thought that enough info was cached in production to continue operating up to 36 hours, suggesting OT was not breached.	icsstrive.com decripto.org comparitech.com
2025-02-22	Ganong	Canada	Food & Beverage	Ransomware	Operations at St. Stephen facility were affected temporarily	Very few details released	icsstrive.com fipa.bc.ca
2025-02-25	Stürmer Maschinen	Germany	Transport	Ransomware	Deliveries delayed - not specified how long	Lynx ransomware group compromised the machine wholesaler	icsstrive.com csoonline.com
2025-03-01	National Presto Industries	USA	Discrete Mfg	Ransomware	Temporarily impacted shipping and receiving and some manufacturing processes.	Few details. A ransomware group later took credit for the attack. The company says temporary work-arounds were put in place for critical processes.	icsstrive.com securityweek.com
2025-03-02	Adval Tech	Switzerland	Discrete Mfg	Ransomware	"Production losses could occur at various locations"	Few details released, but criminal charges against a ransomware group were filed	icsstrive.com cybermaterial.com inside-it.ch
2025-03-07	Crystal D	USA	Discrete Mfg	Unknown	Approximately 3% of orders delayed during a multi-day production shutdown	A cyber attack on the crystal awards and gifts manufacturer shut down order processing and production for a number of days	icsstrive.com asicentral.com
2025-03-16	Astral Foods	South Africa	Food & Beverage	Unknown	Chicken processing plants shut down for one week	Company issued a profit warning due to costs and revenue delays from cleaning up after cyber attack	icsstrive.com therecord.media
2025-03-23	Kuala Lumpur Inter-national Airport	Malaysia	Transport	Unknown	Airport displays, check-in and baggage handling became inoperable for 1-2 days, leading to flight delays	Few details were released. Authorities initially denied impacts on flights, but reports from travellers contradicted these denials.	icsstrive.com jobstore.com

Date	Victim	Region	Industry	Attacker Type	Consequence	Summary	References
2025-03-26	Lukoil	Russia	Oil & Gas	Unknown	Partial halt in fuel distribution to gas stations & other consumers for several days	Few details beyond that workers were told not to log in to their accounts after an unusual error message showed on many computers	icsstrive.com newsukraine.bc.ua united24media.com
2025-03-27	Platon	Russia	Transport	Hacktivist	Over one thousand trucks could not move	DDOS attack crippled Platon system that provides drivers with destinations and route maps	icsstrive.com obozrevatel.com
2025-03-28	Instituto de Pesquisas Energéticas e Nucleares (IPEN/CNEN)	Brazil	Pharma-ceuticals	Unknown	Production of radioisotopes used in medicine stopped for 13 days	Few details beyond that the plant was scheduled to restart Mar 31, with resumed shipments of medicine expected Apr 10	icsstrive.com gov.br
2025-04-06	Sensata	USA	Discrete Mfg	Ransomware	Temporarily impacted Sensata's operations, including shipping, receiving, and manufacturing production.	No details released beyond 8-K statement	icsstrive.com cloudfront.net
2025-04-07	Lake Risevatnet Dam	Norway	Water & Wastewater	Hacktivist	Water flows at 497 l/s above normal for 4 hours	Exploited a weak password on a web-accessible control panel. No risk to public - river capacity is 20,000 l/s	icsstrive.com hackread.com
2025-04-19	City in Silicon Valley	USA	Transport	Hacktivist	Incorrect messages coming out of handicap-accessible pedestrian crossing buttons	"Hackers" accessed crossing button control systems - most likely using Bluetooth and a default password - and substituted "funny" / political recordings	icsstrive.com theregister.com
2025-04-27	Masimo Corporation	USA	Discrete Mfg	Unknown	Some factories working at reduced capacity	Few details disclosed beyond 8-K filing	icsstrive.com sec.gov hipaajournal.com
2025-05-14	Nucor Corporation	USA	Metals & Mining	Unknown	Halted certain production operations at various locations.	No details released beyond 8-K statement	icsstrive.com cloudfront.net
2025-05-14	Peter Green Chilled Logistics	UK	Transport	Ransomware	Customer shipments could not be processed for up to 5 days	Ransomware disrupted new order processing and some existing orders	icsstrive.com therecord.media
2025-05-15	Pole Star Global	Saudi Arabia	Transport	Nation State	Containership MSC Antonia ran aground in Red Sea	GPS spoofing is widespread in the region, usually attributed to Houti rebels, Iran and / or Israel. The ship ran aground because its AIS system was confused by spoofed GPS data	icsstrive.com gcaptain.com
2025-05-16	Arla Foods	Germany	Food & Beverage	Unknown	Uphal Germany plant halted & reduced production for 6 days	Few details beyond that a cyber attack impacted at least IT systems leading to a shutdown + delayed or cancelled orders	icsstrive.com food.com yahoo.com
2025-05-19	Fasana	Germany	Pulp & Paper	Ransomware	Factory employing 240 people shut down for 3 weeks, business declared bankruptcy	Napkin manufacturer hit by ransomware was forced to declare bankruptcy after factory was shut down for 3 weeks.	icsstrive.com securityaffairs.com
2025-05-23	Wellteam	Germany	Pulp & Paper	Unknown	Three factories stopped production for about one week	Cardboard manufacturer hit by cyber attack	icsstrive.com security.de csoonline.com
2025-05-27	Mediehuset Altaposten	Norway	Pulp & Paper	Ransomware	Unable to print one edition of newspaper	Ransomware impacted business systems & print edition of newspaper. Online editions were still available	icsstrive.com altaposten.no

Date	Victim	Region	Industry	Attacker Type	Consequence	Summary	References
2025-06-05	United Natural Foods	USA	Food & Beverage	Unknown	Unable to fulfill wholesale food orders for 10 days. Retailers like Whole Foods suffered supply shortages	The company reports approximately $400M in lost sales, $25M in incident mitigation costs, for a net / profit loss of $50-60M. A cyber attack took down IT systems resulting in an inability to take orders to deliver foods.	icsstrive.com youtube.com cpomagazine.com
2025-06-10	Roularta Media Group	Belgium	Pulp & Paper	Unknown	Printing stopped for 1 day	DDoS attack took down one printing facility + business systems	icsstrive.com cybermaterial.com
2025-06-11	Dairy Farmers of America	USA	Food & Beverage	Ransomware	Multiple plants were unable to receive or process milk for a short period	Ransomware hit the milk processor, stealing information and leading to a shutdown of some IT systems	icsstrive.com farms.com
2025-06-15	Siloking	Germany	Discrete Mfg	Ransomware	Production stopped for 5 days	Production was able to resume in "emergency mode" after 5 days	icsstrive.com csoonline.com agrartechnikonline.de
2025-06-18	Federal State Information System for Veterinary Surveillance	Russia	Food & Beverage	Hacktivist	Meat, dairy, egg and other animal-based products could not be delivered to processing plants nor consumers for several hours, some perishable goods discarded as a result	"IT Army of Ukraine" took credit for a DDoS attack halted access to Russia's Mercury system for certifying human-consumable animal products. Producers were encouraged to switch to manual processing, but not all processors had procedures that could accept paper certificates anymore.	icsstrive.com bitdefender.com therecord.media
2025-06-22	Iranian nuclear program	Iran	Military	Nation State	Prevented Iran from launching surface-to-air missiles at American warplanes that had entered Iranian airspace.	The US military bombed Iranian nuclear weapons development sites, and "digitally disrupted" Iranian air missile defense systems. Few other details are released at this writing.	therecord.media
2025-06-24	Heim & Haus	Germany	Discrete Mfg	Unknown	Production and shipments stopped for one week	Building supply manufacturer was hit by a "cyber attack" that impaired production & order processing	icsstrive.com heimhaus.de comborncity.com
2025-06-30	Hero	Spain	Food & Beverage	Unknown	Production and logistics operation stopped for "several" days	A cyber attack shut down one plant in Spain	icsstrive.com democrata.es
2025-07-03	Ingram Micro	USA	Transport	Ransomware	Shipments were delayed and new orders could not be processed	Wholesaler suffered ransomware attack that affected order processing and other systems	icsstrive.com blackfog.com
2025-07-04	Русские Хакеры – Фронту / Gaskar Group / RH	Russia	Discrete Mfg	Nation State	Russian army could not configure ~500 new drones / day for several days	RH produces and distributes commercial drone firmware hacked / modified for Russian military use. The attack impaired servers & terminals used to install the modified firmware at ~400 sites, not the firmware itself.	icsstrive.com tufts.edu
2025-07-09	Wibaie à Cholet	France	Discrete Mfg	Ransomware	Shut down factory with 600 employees for 10 days	Qilin ransomware shut down the window & door manufacturer	icsstrive.com france.fr france.fr
2025-07-16	NovaBev	Russia	Food & Beverage	Ransomware	Customer shipments delayed 2 days	NovaBev announced that ransomware had hit its IT network delaying shipments but not affecting production.	icsstrive.com scmagazineuk.com
2025-07-20	Colabor Foods	Canada	Food & Beverage	Unknown	Suspended food & other shipments up to 2 weeks	A cyber attack on the food & other goods wholesaler disrupted order processing and impaired ability to ship product	icsstrive.com colabor.com lapresse.ca reddit.com

Date	Victim	Region	Industry	Attacker Type	Consequence	Summary	References
2025-07-28	Aeroflot	Russia	Transport	Hacktivist	50 flights cancelled and 10 delayed	"Silent Crow" pro-Ukrainian hackers claim to have erased 7,000 IT servers	icsstrive.com reuters.com
2025-08-14	Nigeria Customs Service	Nigeria	Transport	Unknown	Delays clearing imported containers and increased demurrage charges for shippers for storing containers during customs clearance operations.	An attack on the ICT platform of Nigeria customs service delayed cargo clearance operations.	icsstrive.com maritimecybersecurity.nl vanguardngr.com
2025-08-19	Tczew Hydro Plant	Poland	Electric Power	Hacktivist	Shut down power production at a small hydro power plant	Attackers gained control of an HMI - not clear if it was main HMI or engineering tool - and changed settings causing turbine and generator to stop.	icsstrive.com cybernews.com
2025-08-31	Jaguar / LandRover	UK	Discrete Mfg	Ransomware	All plants shut down for up to 5 weeks and full production did not resume until mid-November. Reported $900B direct losses with up to $2.5B estimated losses for the entire UK economy.	Social engineering & phishing stole credentials to compromise IT network. With SAP shut down, everything stopped - could not auto-order parts, etc. Attributed to "Scattered Lapsus" ransomware group.	icsstrive.com bbc.com hackers4u.com
2025-09-02	Bridgestone	Japan	Process Mfg	Unknown	All NA & SA plants shut down for 16 days	Few details beyond that a cyber attack shut down operations at NA & Latin American plants	icsstrive.com industrialcyber.co cyberpress.org
2025-09-16	Data I/O	USA	Discrete Mfg	Unknown	Shipping, receiving, manufacturing, production and other functions down for 3 weeks	Attackers accessed the firm via a vulnerability in a third-party firewall service provider.	icsstrive.com sec.gov yahoo.com
2025-09-19	Collins Aerospace	USA	Transport	Ransomware	Flights delayed and cancelled in several European airports for 10-16 days	Ransomware crippled vMUSE check-in and boarding software	icsstrive.com bbc.com airport.de
2025-09-24	Refresco	Germany	Food & Beverage	Unknown	German production reduced or shut down at least two days	A cyber attack shut down at least German plants of the beverage bottler	icsstrive.com lebensmittelzeitung.net
2025-09-30	Asahi Group Holdings	Japan	Food & Beverage	Ransomware	Most of 30 plants shut down for a week. Shipments only at 10% of normal a month after the incident	Asahi recovery was slowed by large numbers of very old systems - both IT and OT - left over from years of acquisitions.	icsstrive.com securityweek.com japantimes.co.jp
2025-10-14	Kelowna Airport	Canada	Transport	Hacktivist	Two flights were delayed by several hours	Hacktivists compromised PA systems in a number of Canadian and US airports with political messages praising Hamas. Only one airport reported associated flight delays.	icsstrive.com ctvnews.ca
2025-10-22	Rossel-khoznadzor	Russia	Food & Beverage	Hacktivist	Food shipments halted for one day	"IT Army of Ukraine" took credit for a DDoS attack halted VetIS (Mercury) and Saturn tracking systems used to register the movement of animal products	icsstrive.com securityaffairs.com beyondmachines.net
2025-10-29	Unspecified Canadian Water Utility	Canada	Water & Wastewater	Hacktivist	"Degraded service" for the community	Canadian government alert does not give details, but states a cyber attack tampered with water pressures resulting in degraded service	icsstrive.com cyber.gc.ca

Date	Victim	Region	Industry	Attacker Type	Consequence	Summary	References
2025-10-31	Tein Inc.	Japan	Discrete Mfg	Ransomware	Factory in Japan shut down for one day, Chinese factory shut down for one week	The automotive suspension manufacturer reported two factory outages due to ransomware but noted that backlogs would be cleared by using overtime and holiday work. The "Warlock" ransomware group claimed credit for the attack.	icsstrive.com tein.co.jp linkedin.com
2025-11-28	Gerd Bär GmbH	Germany	Discrete Mfg	Ransomware	2 factories shut down for 7 days	Criminals encrypted parts of the IT environment. An announcement 7 days later indicated that "production is back up and running". Few other details were released.	icsstrive.com cargolift.com
2025-11-30	Aras Kargo	Turkey	Transport	Unknown	All parcel pick-up and delivery were halted for one day	Aras Kargo's press release said that there were short-term delays and service interruptions. Independent press reported a complete cessation of pick-ups and deliveries for roughly one day.	icsstrive.com araskargo.com.tr
2025-12-14	PDVSA	Venezuela	Oil & Gas	Ransomware	Stopped loading oil on to tankers at 10+ ports	The state-run oil firm detected a ransomware attack days earlier, but the AV software it used to try to fix the problem "affected" its entire administrative system. By Dec 17 ports had started making manual records of deliveries to avoid a longer suspension of exports.	icsstrive.com marinelink.com
2025-12-19	Evergreen Printing Company	USA	Pup & Paper	Ransomware	Suspended printing operations for 4+ days	Customers of Evergreen Printing Company in Belmawr, NJ reported that the company had suspended printing because of a ransomware attack. There is no record of a public statement by the company about the attack.	icsstrive.com theretrospect.com dysruptionhub.com
2025-12-22	La Poste	France	Transport	Hacktivist	Home delivery of parcels was disrupted for 4 days	Pro-Russian group Noname057 claimed credit for a DDOS attack that affected deliveries. Deliveries were slowed because of an impaired parcel tracking capability.	icsstrive.com therecord.media lapostegroupe.com

Appendix B – Sources

The authors thank and acknowledge the many incident repositories and reports we searched to find the incidents reported in the 2025 data set.

ICS STRIVE	https://icsstrive.com
CERT-EU	https://cow-prod-www-v3.azurewebsites.net/publications/threat-intelligence/2025
Checkpoint	https://research.checkpoint.com/2025/
Cloudian	https://cloudian.com/ransomware-attack-list-and-alerts/
Cybercrime Magazine	https://cybersecurityventures.com/ransomware-report
CyberEvents Global Cyber Threat Landscape	https://cybereventsdatabase.org/dashboard
Cyber Security Incident Database	https://www.csidb.net/
DysruptionHub	https://dysruptionhub.com
European Repository of Cyber Incidents	https://eurepoc.eu
KonBriefing	https://konbriefing.com/en-topics/cyber-attacks.html
Security & Exchange Commission	https://www.sec.gov/edgar/search/
NHL Stenden University of Applied Sciences, MCAD Maritime Cyber Attack Database	https://maritimecybersecurity.nl/listview
TI Safe	https://hub.tisafe.com/base-de-dados/

Published March 2026