

Ransomware Resilience in Operational Technology (OT) Environments- Threat Landscape, Defense Architectures, and Recovery Strategies for Critical Industrial Infrastructure

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India.

Abstract - Ransomware is no longer just in the office, it's now on the factory floor. In 2025, approximately 3,300 industrial organisations around the world were targeted by ransomware almost twice as many as in 2024 and the number of criminal groups targeting industrial firms increased by nearly 50 per cent. This article breaks down, in simple terms, what operational technology (OT) is, why it has become a prime target for extortion and what it takes to be resilient against ransomware in an environment where computers control physical processes like power generation, water treatment and manufacturing lines. This article summarizes the incident data that is publicly available, the government advice, the international standards and industry survey results published from 2021 to 2026. It outlines the practical defensive strategies such as network segmentation, asset inventory, passive monitoring, tested offline backups and engineering led recovery planning, and explores the economics of the criminal business model and the defensive investment case. It also highlights areas that are lacking, such as inadequate separation of office and plant networks, inadequate monitoring coverage, and the standard practice of defining OT events as IT events. The target audience are engineers, plant operators, businessmen, policy makers, students, and the public at large, who rely on the industrial infrastructure, that is, all of us.

Keywords: Operational technology, Ransomware, Industrial control systems, Critical infrastructure, Cyber resilience, Network segmentation, Incident response, IT/OT convergence.

1. INTRODUCTION

If it's a hospital billing office that's hit by ransomware, then the bills are not paid. Physical things stop occurring when it hits a water treatment plant, refinery, or an auto assembly line pumps cease, valves don't open, production lines go silent. It is that difference that is the topic of this article.

Operational technology (OT), typically abbreviated, is the term used to describe all the hardware and software used to monitor and control physical processes. It is used to control programmable logic controllers on factory floors, to monitor supervisory control and data acquisition systems in utilities, to manage building systems in hospitals and to run human-machine interfaces that operators monitor 24 hours a day. These systems were built decades ago for reliability and safety not against organised crime. Many will last for 15-30 years before needing replacement. Many continue to use software that hasn't been updated for years because it is not possible to put them offline for patching during production or, in some cases, public service.

Most of these systems were isolated for most of their history. Plants had their own networks which were physically isolated from office networks, and an intruder who gained access to a company's e-mail server had no route to its turbines. Much of that protection has now been lost. Companies linked their

facilities to networks and the Internet for monitoring, prediction and efficiency, and this linkage hacriminalsdoors for the criminals to use routinely. This is known as IT/OT convergence and is one of the security challenges of this decade.

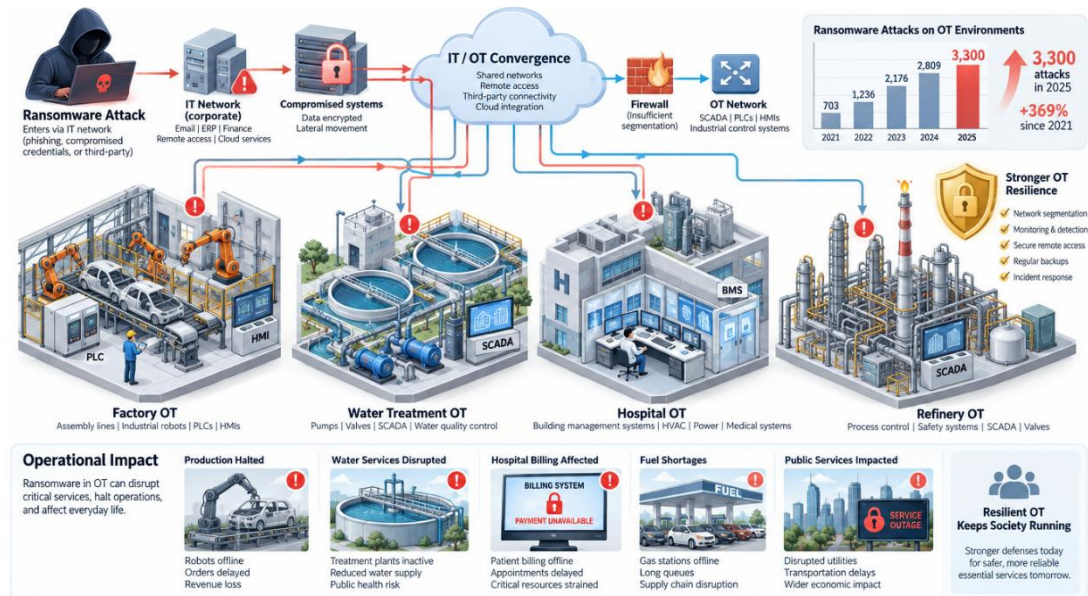


Fig -1: IT/OT Convergence

It's no longer a matter of speculation the magnitude of the issue is now undeniable. A report in February 2026 on the state of industrial cyber threats reported that in 2025, there were around 3,300 industrial organisations that suffered ransomware attacks, an increase from the 1,693 industrial organisations attacked in 2024, and 119 different ransomware groups that targeted industrial organisations, up 49 percent from 2024. More than two-thirds of these attacks went into manufacturing. The average ransomware demand against manufacturers was estimated to be around 1.16 million US dollars in 2025, more than double the previous year, and another global study revealed that an average ransomware attack against OT cost 4.56 million US dollars. Each of these numbers represents a true story of workers being sent home, deliveries being missed and, in some of the worst cases, communities being deprived of fuel, food processing and healthcare.

The most famous case is that of the attack on a large fuel pipeline operator in the United States in 2021. The ransomware was not used on the pipeline's control systems but was used to encrypt the company's billing servers. But the operator turned off the pipeline as a precaution and in days motorists throughout the eastern United States were lining up for gas. The lesson was squirmish and it's still relevant. An industrial plant can be paralysed without any controllers being infected, as modern plants cannot function when the business systems operate in breakdown. This article outlines the meaning of resilience in this context, how it is created, its cost and its returns, and where the gaps are. It is written for engineers and executives, but also for the general reader, since the systems in question provide water, power, food, medicine, and transport which daily life depends on.

2. UNDERSTANDING OPERATIONAL TECHNOLOGY AND WHY IT BECAME A TARGET

2.1 What OT Actually Is

Operational technology is defined as any computerized system responsible for sensing and or altering the physical world. A programmable logic controller (PLC) is programmed to read the sensor values and switch the motors and valves based on the sensor values. Supervisory control and data acquisition (SCADA) system collects data from hundreds of such controllers and displays them to the human operators. The software for programming the controllers is on engineering workstations, while years of process data are stored on historians. These systems collectively operate power plants, water and wastewater treatment facilities, oil and gas plants, railways, ports, food processing plants, pharmaceutical manufacturing, and almost all the discrete manufacturing.

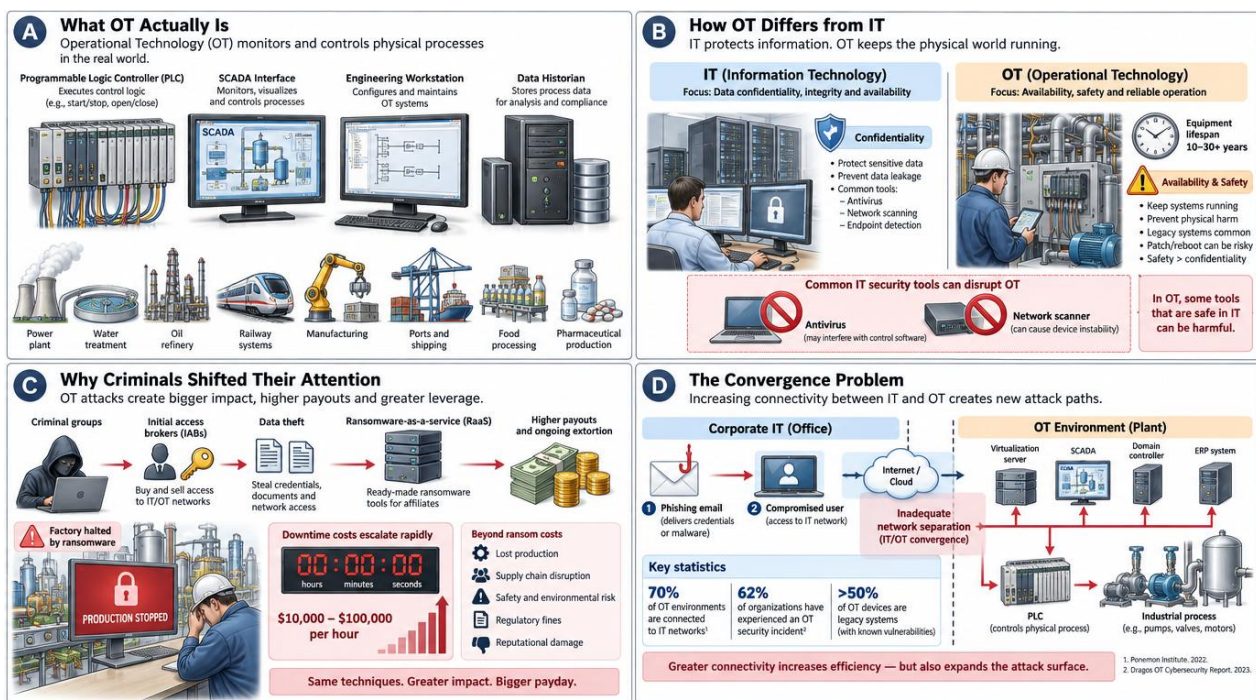


Fig -2: Operation Technology and Cybersecurity

2.2 How OT Differs from IT

The priorities are turned upside down. Confidentiality of data is typically a top priority in office IT. Availability and safety are the first priorities in OT it must continue to operate, and it cannot injure people. This inversion is in the real world. An IT administrator can reboot a server at midnight, an OT engineer can't reboot a controller that is controlling a chemical reaction. While IT equipment is regularly changed every 3-5 years, OT equipment can last for decades. The IT security tools, for example agent-based anti-virus or aggressive network scanning, can crash into sensitive industrial devices, and that's why OT security requires its own methods.

2.3 Why Criminals Shifted Their Attention

Ransomware is a business and the operators follow leverage. A retailer that loses their database suffers, but a manufacturer that loses their production line haemorrhages money by the hour. The cost of unplanned downtime on a highly automated assembly line is estimated to be in millions of dollars per hour, and a 2026 survey of manufacturers revealed that almost 60% estimated damages more than one

million US dollars per cyber incident, with the average downtime exceeding 15 hours. Those who are under such pressure pay quicker and pay more. The criminal ecosystem has industrialised as well initial access brokers sell footholds into corporate networks, ransomware-as-a-service operations lease malware to affiliates and double extortion combines data theft with encryption, blackmailing even victims with adequate backups with the threat of stolen engineering drawings and customer data.

2.4 The Convergence Problem

Fewer than ever ransomware attacks start within the plant. Phishing email, stolen password, or unpatched internet facing device on the corporate side is typically the first link in the typical chain. The attacker then proceeds to move laterally to systems that the plant relies on the virtualization servers running SCADA software, the domain controllers that are used to logon operators, or the enterprise resource planning system that instructs the plant on what to make. 81 percent of the industrial sites surveyed in 2026 had inadequate separation between IT networks and OT networks and compromised remote access credentials were identified in 73 percent of incidents surveyed. In most organisations the space between office and plant is open.

3. THE OBJECTIVE OF THIS ARTICLE

3.1 Primary Aim

The main goal is to be aware of being aware with substance. There is a lot more attention on data breaches and privacy in the public discourse around ransomware, with the industrial aspect which involves physical safety and continuity of essential services not getting as much attention beyond the specialist community. This article aims to fill that gap by providing the non-specialist reader with a realistic sense of the threat and the practitioner with a framework of what resilience entails, based on public and credible sources and not on marketing.

3.2 What the Article Deliberately Avoids

There are three options that determine the text. First, there are no vendor, product or company names mentioned since the principles of OT resilience are applicable to any vendor and awareness writing doesn't carry the same weight when it is also an advertisement. Incidents are outlined by sector, geography, and year, instead. Second, the article does not go into technical detail that is only of interest to specialists such as protocol level analysis but rather provides explanations that can be acted on by a plant manager, a policy maker or an engineering student. Third, all figures are taken from published reports and surveys and in the event of any discrepancies between the numbers reported from different sources, the discrepancy is reported, rather than smoothed out.

3.3 Who Should Read It and Why

A single map will be available for engineers and OT operators to see defensive practice and the evidence supporting it. In terms a board understands, the economic case downtime costs, insurance dynamics and regulatory exposure is presented to business leaders. The link between plant security and the national economy will be understood by public officials. This will serve as an orientation for students and early career professionals in a field that has a high need for workers and great opportunities. The general reader will find an answer to a reasonable question, Why should someone who has never seen a PLC care about industrial cybersecurity. It's a conclusion that is reached throughout the article that the fallout of failure falls on the public first, in the form of fuel queues, empty shelves, cancelled medical procedures and disrupted pay cheques.

4. METHODOLOGY

4.1 Sources and Selection

The article more specifically answers five questions. So, how does ransomware get in and cause disruption to industrial operations. What are the technologies and practices that can be shown to mitigate that risk. How much do they cost and what do they yield for one company and for a nation's economy. What are the needs according to the current standards and laws. But where is research and practice still lacking. The gap analysis at the end is not an add-on it's as important to the reader to know what is not solved as it is to know what works.

4.2 How Figures Were Treated

The figures in this box are not consistent from source to source as different organisations count in different ways. The leak-site counting method excludes those who pay quietly, while the incident response method over-represents larger companies who can afford to hire somebody to help. If a figure is mentioned in this article, the type of source is indicated and the period. In cases where there are conflicting numbers, such as the manufacturing sector attacks, which had been cited as increasing between 46 and 64 percent year over year in 2025 in different reports, the range is indicated instead of a single number. The author did not make any statistics or estimates in this article.

4.3 Analytical Approach

It is a qualitative, not original measurement. Description of incidents in various reports were compared to determine if there were common paths of attack, and recommendations from standards organizations, government guidance, and post-incident analysis were categorized into the three functional layers that are used later in this article prevention (architecture), detection (visibility), and recovery (preparation). The layering is organized according to the structure of existing national and international frameworks such as the five functions of the national cybersecurity framework (identify, protect, detect, respond, recover), tailored to the needs of the industrial sector.

4.4 Limitations

There are three caveats that need to be noted. First, because all data is public, state sponsored intrusions and incidents that go unreported are not reflected in the data, researchers even point out that many OT incidents are also classified as IT incidents and thus do not show up in OT statistics. Second, this is a rapidly changing field and the figures presented here are for 2025 and early 2026 and are therefore not static. Third, none of the defensive measures mentioned here have been tested by the author, effectiveness is based on the assessments and surveys cited and is qualified as such.

5. HOW RANSOMWARE DISRUPTS INDUSTRIAL OPERATIONS

5.1 The Two Pathways to Shutdown

Digging into incidents in 2025 and 2026 reveals that ransomware can cause plant disruptions in two paths, with the latter being much more prevalent. In the first case, the malware encrypts enterprise systems, virtualization servers or engineering workstations and operations cease due to the real need of these systems or because the operator takes a precautionary approach. The second, and less common, path is for attackers to directly target OT assets, like human-machine interfaces, with ransomware. In 2026, a quarterly analysis of ransomware attacks against industrial organisations found that 1,140 organisations were attacked during one quarter, with the majority of the impacts being on the loss of enterprise and virtualization infrastructure and not necessarily on the control systems. This distinction is

important for defence the plant is not only the controllers, it is ordinary business systems around it that need to be protected.

5.2 The Virtualization Chokepoint

A pattern should be highlighted. Many operators have converged their SCADA servers, historians, and engineering tools to virtual machines on shared hypervisor infrastructure. Criminals figured this out and now attack hypervisors on purpose, as it's possible to encrypt dozens of systems at once. At that time, the physical equipment can continue to operate on the last instructions, but the operators can no longer view or control the physical equipment, thus requiring a manual shutdown for safety reasons. The production stoppages were repeatedly identified as being the result of encrypted virtualization infrastructure as a proximate cause in post incident reviews in 2025 and 2026.

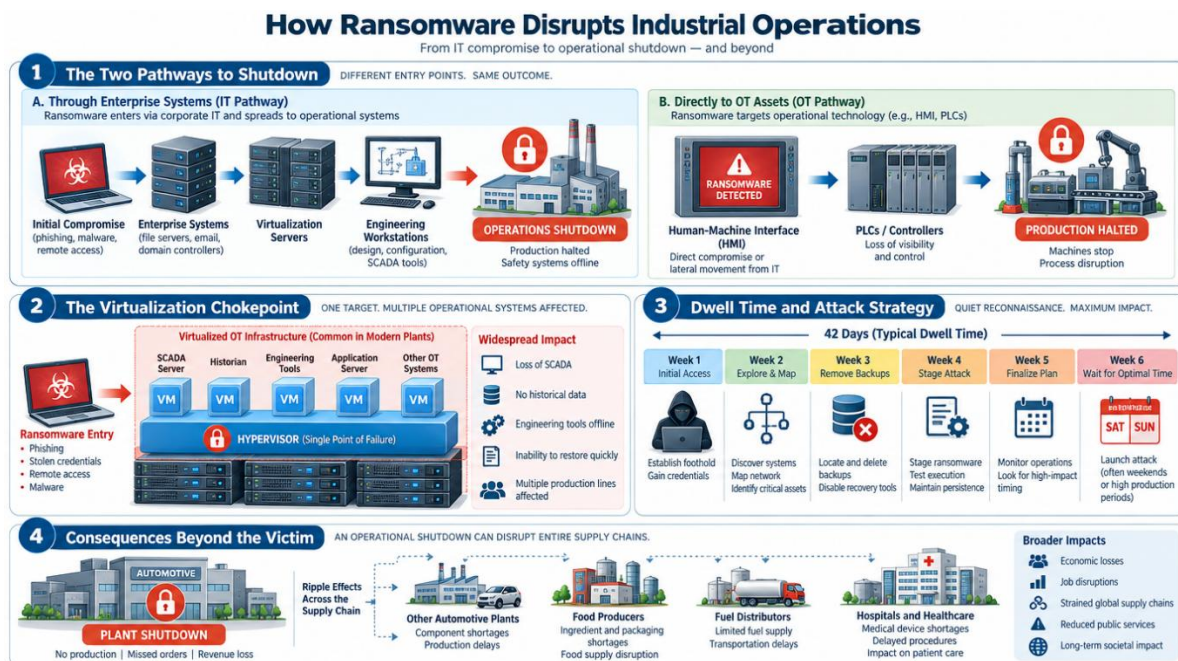


Fig -3: How Ransomware Disrupts Industrial Operations

5.3 Dwell Time and What It Means

Attackers will not hit as soon as they've gained access. An average dwell time of 42 days was observed for ransomware actors within OT-connected environments prior to the start of an encryption attack, the industry analysis for 2025 revealed. Those weeks, the intruders explore the network, find backups to remove, and select the most opportune time to strike, typically a weekend or busy production time. Six weeks is a long time, and this is the best case for monitoring an organization that can see something unusual in that time period can get rid of the intruder before any encryption is done.

5.4 Consequences Beyond the Victim

Industrial ransomware is spreading outwards. In 2025, a major automotive company in the United Kingdom was attacked, bringing the production lines to a standstill for weeks and depriving hundreds of companies in the supply chain of orders, which led to government intervention to save jobs in the supply chain. Disruption has been passed down the stream to the public by food producers, fuel distributors, and hospital networks. That's why this topic should not be limited to writing for trade journals but should be

part of public awareness writing often the party who was hit the hardest is not the party who was attacked.

6. THE CURRENT THREAT PICTURE IN NUMBERS

6.1 Victim Counts and Growth

The overall pattern of independent sources is the same. The annual industrial threat review, published in February 2026, showed that there were approximately 3,300 industrial ransomware victims in 2025 compared to 1,693 in 2024, and 119 active criminal groups compared to 80 the previous year. Another study of the last 12 months of March 2025 found that industrial organisations were hit by a total of 2,073 ransomware attacks, representing almost 30 percent of all ransomware attacks in each of the 12 months. Documented manufacturing incidents for 2025 rose 56 percent YOY to 1,466, based on sector-focused research. The discrepancies in the counts are due to differences in the ways the counts are made, but there is no credible source that indicates that the problem is getting smaller.

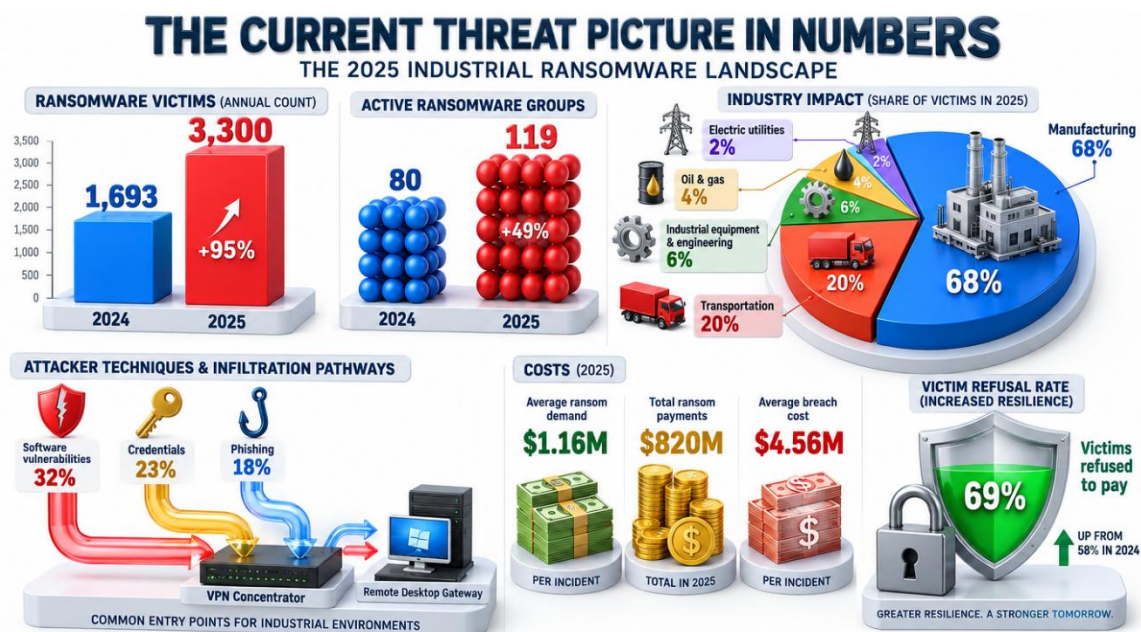


Fig -4: The Current Threat Picture in Numbers

6.2 Which Sectors Bear the Weight

By far the most targeted industry is manufacturing, with over two thirds of industrial victims in 2025, by one count. These are followed by transportation, industrial equipment & engineering, oil & gas, and electric utilities. From the criminal perspective, it makes sense to focus on manufacturing because of the high cost of downtime, the complex supply chain, the aging systems and, in the past, less investment in security than in regulated utilities.

6.3 How Attackers Get In

The top three exploited software vulnerabilities identified through the surveys in 2025 were around 32 percent, 23 percent, and 18 percent for software vulnerabilities, compromised credentials, and phishing, respectively. The vulnerability route should be a priority as in theory it is preventable a large study in 2026

found that only around a quarter of the vulnerabilities on the list of known exploited vulnerabilities in the United States government's list of vulnerabilities were fully remediated in more than 13,000 organisations studied. Most of the exploited devices are perimeter devices, such as VPN concentrators and remote desktop gateways, which are precisely the devices that are used to connect industrial sites to the outside world.

6.4 The Cost Ledger

In 2025, a global breach cost study revealed that 15 per cent of the organisations surveyed had experienced incidents that impacted their OT environment with an average cost of 4.56 million US dollars, which is higher than the global average for all breaches. The average ransom demand for manufacturers has increased by approximately 100% in 2025 to approximately 1.16 million US dollars. At the same time, global tracked ransom payments dropped by roughly 8% to approximately 820 million U.S. dollars in 2025, while some 69% of victims refused to pay, indicating that resilience investment has an impact on victim behavior despite the increase in attacks. However, refusal to pay is only possible with recovery prearranged this is addressed in the sections that follow.

7. BUILDING RESILIENCE, PART ONE ARCHITECTURE AND PREVENTION

7.1 Knowing What You Own

The first step to resilience is an inventory and it is not as simple as it sounds. Over decades of time, acquisitions, contractor installations, and undocumented changes have resulted in industrial sites that have equipment accumulated. Controllers, remote access boxes, and even whole network segments are discovered on a regular basis as part of security assessments. Everything else depends on having an accurate inventory of assets, including all devices, software versions, network attachments, and their function in the process, which is maintained continuously. Modern inventory tools do this passively, by listening to traffic on the network, not probing devices, since doing so can cause fragile industrial devices to crash.

7.2 Segmentation Rebuilding the Walls

Plant and office networks can no longer be physically isolated, so the next best thing is to have a very strict segmentation. The reference model that is widely adopted throughout the industry has a hierarchy of systems, from the bottom field devices to the top enterprise systems and a buffer zone between plant and office, which is known as an industrial demilitarised zone. The data that needs to be passed between the two passes through tightly controlled relay servers in that zone, such that no office system ever talks to a controller. Only the necessary protocols and directions are allowed between segments by firewalls. Data diodes are hardware devices that physically prevent data from flowing in either direction, which is useful in situations where data must flow one way only, such as from a safety system to a monitoring dashboard, where an attack from the dashboard to the safety system is not possible. The lack of IT/OT segmentation is one of the well-established designs that the 2026 assessment found only 81 percent of the sites examined had poor IT/OT segmentation.

7.3 Controlling Remote Access

Almost three quarters of industrial incidents investigated included compromised VPN and jump-host credentials, making remote access the No. 1 door to secure. The specific aspects of good practice are use multi-factor authentication for all remote sessions into the OT environment do not connect directly to plant systems from the remote session only enable remote sessions for the duration of a specific task

and limit remote sessions to the specific systems needed to complete the task. Access from vendors and contractors should be treated with the same care as access from employees, as they were a part of most manufacturing breaches analyzed in a big 2026 study.

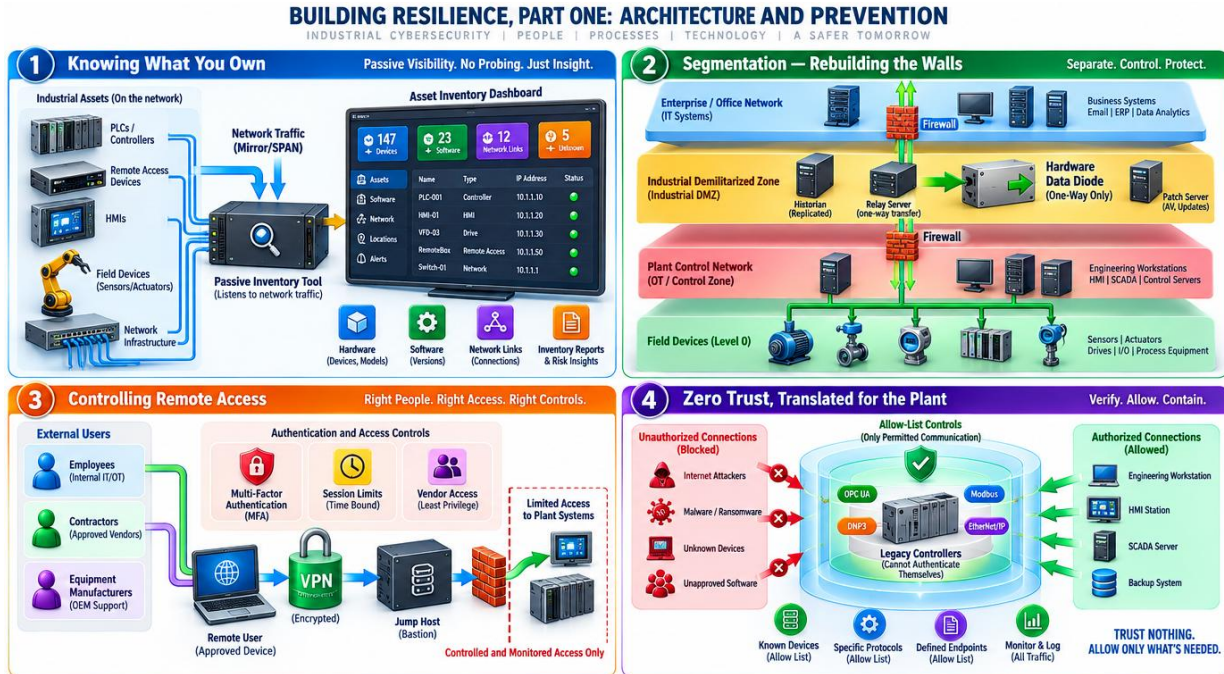


Fig -5: Building Resilience Part One Architecture and Prevention

7.4 Zero Trust, Translated for the Plant

With adaptation, zero-trust principles, in which users and devices are not trusted by default, no matter their location, also apply to OT. Legacy controllers are unable to authenticate themselves, and trust decisions are now delegated to the network surrounding them a strict allow-list of devices that can communicate, what protocols they can use, and which direction. The controller remains the same and the surrounding world becomes less innocent.

8. BUILDING RESILIENCE, PART TWO VISIBILITY AND DETECTION

8.1 Why Monitoring Is the Highest-Leverage Investment

Remember the average dwell time for 42 days. All those days are a chance to catch and outstand an intruder before encryption starts if an organisation can see its network. Here's the sobering 2026 assessment data Only 46 percent of the sites assessed were found to have adequate OT network monitoring in place and other industry analysis indicates that most OT networks are not effectively covered by detection and response. The other issue organisations without telemetry have following an incident is they are unable to reconstruct the incident as the network traffic was not recorded. This is always referred to as the difference between a 2 day and a 2 week recovery.

8.2 Passive Monitoring and Its Advantages

In OT, as in most other networks, the passive network monitoring method is used. A copy of the network traffic is sent to a sensor, and it is analysed without the sensor sending anything, thus avoiding the risk of

disturbing fragile devices. Since industrial networks are very repetitive, with the same devices sending the same messages on fixed cycles, any deviation is easily identified, such as the appearance of a new device, a workstation sending a command that it has never sent, or a controller being reprogrammed out of a maintenance window. Regularity makes industrial networks exceptionally suitable for anomaly detection.

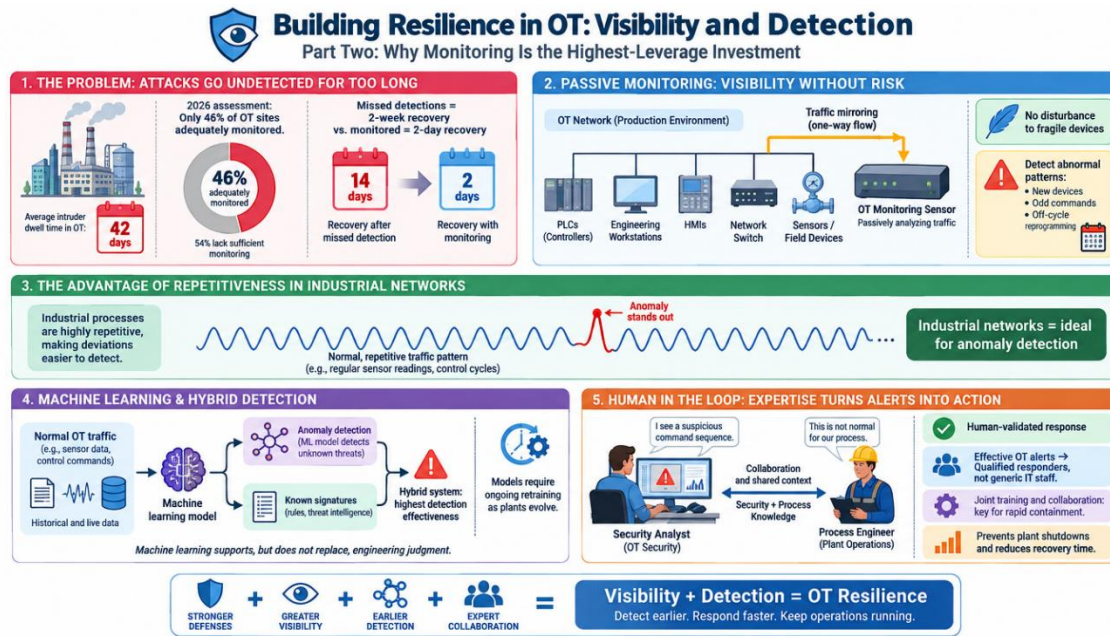


Fig -6: Building Resilience in OT Visibility and Detection

8.3 The Role of Machine Learning, Stated Carefully

Machine learning models have been increasingly used for anomaly detection and are trained on a site's normal traffic patterns. Published research up to 2025 shows that these techniques can identify new threats which signature-based systems fail to detect, and that hybrid systems, which combine learned baselines with known threat signatures are more effective than either approach alone. The same study is honest about its constraints as plants evolve, so do the models. Data for training the model to recognize industrial activity is hard to come by, and operators are loath to act on an alert that the system cannot explain. Machine learning is a helpful tool in the monitoring toolbox but should not be used as a replacement for engineering judgement and awareness writing should not be done to suggest otherwise.

8.4 Detection as a Human Activity

If there is no one who is competent to respond to the alert, it is not useful. Effective operators send OT alerts to responders who know how to respond, not just the network, as what is the right response to an anomaly on a live plant may be very different than the right response in an office. Security analysts and process engineers working together during training, as well as on call security analysts and process engineers, are common findings in post-incident reviews that differentiate a contained incident from a shutdown.

9. BUILDING RESILIENCE, PART THREE RECOVERY AND RESPONSE

9.1 Backups That Survive the Attack

Nowadays, the ransomware makers look for backups before they begin encrypting files, as a victim with backups won't pay. So, recovery is a matter of having backups which the attacker cannot access offline copies, physically separated from the network, or immutable storage, where data can only be written and not changed or deleted for a set period of time. Unlike office-based backups, which tend to overlook controller programs and configurations, human-machine interface (HMI) projects, and even the engineering software required to return them, the backup scope for OT must be broad. If a backup hasn't been tested with an actual restore, it's a hope, not a plan; disciplining yourself to schedule restores is part of the discipline.

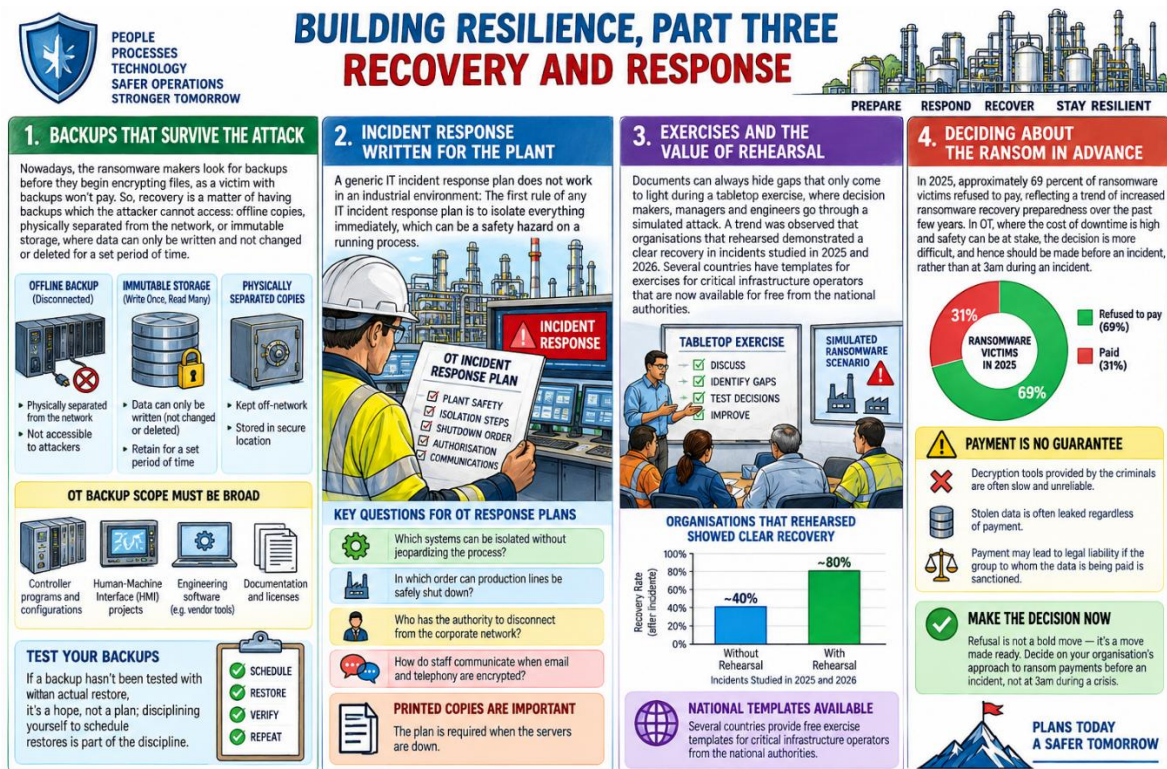


Fig -7: Building Resilience Part Three Recovery and Response

9.2 Incident Response Written for the Plant

A generic IT incident response plan does not work in an industrial environment: The first rule of any IT incident response plan is to isolate everything immediately, which can be a safety hazard on a running process. OT response plans address questions that don't have good answers in the middle of a crisis, such as which systems can be isolated without jeopardizing the process, in which order production lines can safely be shut down, who has the authority to disconnect from the corporate network, and how staff communicate when email and telephony are encrypted. Printed copies are important the plan is required when the servers are down.

9.3 Exercises and the Value of Rehearsal

Documents can always hide gaps that only come to light during a tabletop exercise, where decision makers, managers and engineers go through a simulated attack. A trend was observed that

organisations that rehearsed demonstrated a clear recovery in incidents studied in 2025 and 2026. Several countries have templates for exercises for critical infrastructure operators that are now available for free from the national authorities.

9.4 Deciding About the Ransom in Advance

In 2025, approximately 69 percent of ransomware victims refused to pay, reflecting a trend of increased ransomware recovery preparedness over the past few years. In OT, where the cost of downtime is high and safety can be at stake, the decision is more difficult, and hence should be made before an incident, rather than at 3am during an incident. Payment is no guaranteed decryption tools provided by the criminals are often slow and unreliable, stolen data is often leaked regardless of payment, and payment may lead to legal liability if the group to whom the data is being paid is sanctioned. Refusal is not a bold move it's a move made ready.

10. STANDARDS, REGULATION, AND THE LEGAL LANDSCAPE

10.1 The International Standard for Industrial Security

The IEC 62443 series of standards is the internationally recognised family of standards for industrial automation security. For general use, a good point it can make is the concept of a graduated security level commensurate with the threat that a system is likely to encounter, and a shared responsibility between the equipment manufacturer, system integrator, and plant owner. It does not require operators to strive for perfection in all places but does require them to divide their plants into zones, evaluate the impact of compromise to each zone, and provide protection in proportion to the risk. A 2026 extension of the series has been added to cover the security of connected sensors and edge devices, which is where plant equipment has progressed to be cloud connected.



Fig -8: Standards, Regulations and the Legal Landscape

10.2 Government Guidance

The national standards institute's guide to OT security, Special Publication 800-82 third edition is freely available and vendor neutral and covers the entire spectrum of measures detailed in this article in the U.S. National cyber centres in the United Kingdom, Canada, Australia and other countries release similar advisories and some centres provide joint alerts if a certain criminal campaign is targeting an industrial sector. These free documents represent the lowest cost option for smaller operators that don't have security personnel.

10.3 Regulation with Teeth

The European Union's NIS2 directive is a real move from doing the right thing to must do. The operators of essential and important services, which includes energy, water, transport, health, food production and manufacturing of critical products, will have to take measures to manage the risks, report significant events on a strict clock early warning within 24 hours, notification within 72 hours, final report within a month and be liable to fines of up to millions of euros or a percentage of global revenue. Significantly, the directive places cybersecurity risk oversight on the permanent agenda of management bodies, and places personal responsibility on the management bodies for the oversight. Similar laws for critical cyber systems exist in Canada and have been in place since the sector regulations, like the mandatory standards for North American electric utilities.

10.4 What Regulation Can and Cannot Do

Regulation sets the base level, and the base level had to be raised. It can't replace competence a compliant plant is not necessarily a resilient one, and post incident reviews include victims that had passed their audits. The fair reading of the evidence is that regulation is most effective as a forcing function it gets the budget and the attention; then it's a question of good engineering.

11. ECONOMICS THE CRIMINAL BUSINESS AND THE DEFENSIVE BUSINESS CASE

11.1 The Attacker's Economy

Ransomware against industry is a well-organized industry. Initial access brokers break into networks and sell access at least 14 million US dollars of earnings in 2025 were attributed to just this brokerage layer. Those who deploy ransomware are affiliates who pay a percentage of the ransom to ransomware-as-a-service operators who create the malware. Double extortion is the second way that ransomware operators can profit from stolen information. This is the reason for the proliferation of active groups no need to be technically deep to get into the business and the reason for the focus on industry downtime pressure yields the most rapid payments. To see the opponent as a market, not as a bunch of hackers, helps to explain the defence make the attacker's cost higher and the expected payout less until it is no longer worth their while.

11.2 What Defence Costs

According to one estimate, in 2026, the global OT security market was worth approximately 30.9 billion U.S. dollars and is projected to expand at a rate of 15 to 16 percent per year. The cost of the core measures, inventory, segmentation, monitoring, hardened remote access and tested backups are typically in hundreds of thousands to low millions of dollars and can be very different depending on the size and starting state of a single mid-sized plant and the number of years for implementation. This is not to minimise these real costs, but this article does not.

11.3 What Defence Returns

Those costs an average of 4.56 million US dollars in the cost of an average OT-touching incident an average of US dollars in millions lost due to downtime on automated lines nearly 60 percent of surveyed manufacturers reporting more than one million dollars per incident not including recovery costs, penalties for missed deliveries, and lost customers and an average manufacturing ransom demand of more than one million dollars, prior to recovery costs, penalties for missed deliveries, and lost customers. In these cases, a resilience programme can pay for itself many times over if it helps to prevent or limit one major incident. There are secondary returns, too insurers are now increasingly charging premiums and coverage on proven OT controls, some customers are even now auditing suppliers security before signing contracts, and the monitoring infrastructure put in place for security often has operational benefits, too, as it shows equipment faults and inefficiencies.



Fig -9: Economics The Criminal Business And the Defensive Business Case

11.4 An Honest Caveat

Security return on investment arguments are based on probabilities, not on certainties. Even if a plant is well defended, it can still be broken and even if it is not defended, it can be fortunate for years. Risk reduction at a justified price is the correct frame, and on present frequencies of incidents, with about 1 in 3 chances of significant industrial firms in the most targeted sectors being hit at, the justification has increased each year for 10 years.

12. BENEFITS FOR SOCIETY, NATIONAL ECONOMIES, AND DAILY LIFE

12.1 The Public's Unseen Stake

Most people will never even get a chance to come into a control room, and each one of us eats its product. When the fuel pipeline was shut down in 2021, the lack of fuel in the United States became apparent in just days, with filling stations along the eastern part of the country running dry. The same is true for an attack on a food and beverage manufacturer, or a hospital network's imaging system, or a port's logistics system in 2025. Thus, resilience to ransomware in OT is a public good in the true sense. The advantage of a water utility being able to withstand or recover from an attack in hours rather than weeks is that it applies to all taps served by the water utility.



Fig -10: OT Resilience to Ransomware

12.2 National Economic Stability

Industrial cyber incidents are small natural disasters at the national economy level in that they destroy output, disrupt supply chains, and have recovery costs. A large U.K. automotive manufacturer was closed in 2025, which resulted in hundreds of supplier companies being idle and led to state intervention to save jobs. In 2025–2026, academic modelling estimated that the potential losses from severe tail scenarios of cascading OT incidents are more than 300 billion US dollars, with most being from business interruption losses. Other less-publicized benefits of countries with resilient critical sectors include lower insurance costs for the systems, higher manufacturing investment attractiveness, and less coercion in times of geopolitical tension because several state sponsored entities have been observed pre-positioning within foreign critical infrastructure.

12.3 Jobs and the Coming Workforce

There's a known lack of individuals who understand both industrial processes and security, and that's a chance for the next generation. There are two groups of people that can pursue OT security careers OT professionals control and process engineers who will pick up security skills and security professionals who will learn how plants work. In many countries, universities and technical colleges have started to provide industrial cybersecurity courses and the market growth projections mentioned earlier suggest the need for at least another ten years. There are few areas of specialization which offer a young engineer the same security, utility, and scope as the field of engineering in medicine.

12.4 Everyday Improvements Nobody Notices

Maybe the best way to describe the benefit is to say that it is a lack of something, it's a lack of anything happening when resilience is doing its job. The lights remain on, the water continues to flow, the factory continues to ship on time and wages are paid. The only time people notice infrastructure is when they don't have it, that's why we need articles such as this one to remind people of the infrastructure.

13. WHAT THIS MEANS FOR ENGINEERS AND OT PRACTITIONERS

13.1 A Change in Professional Identity

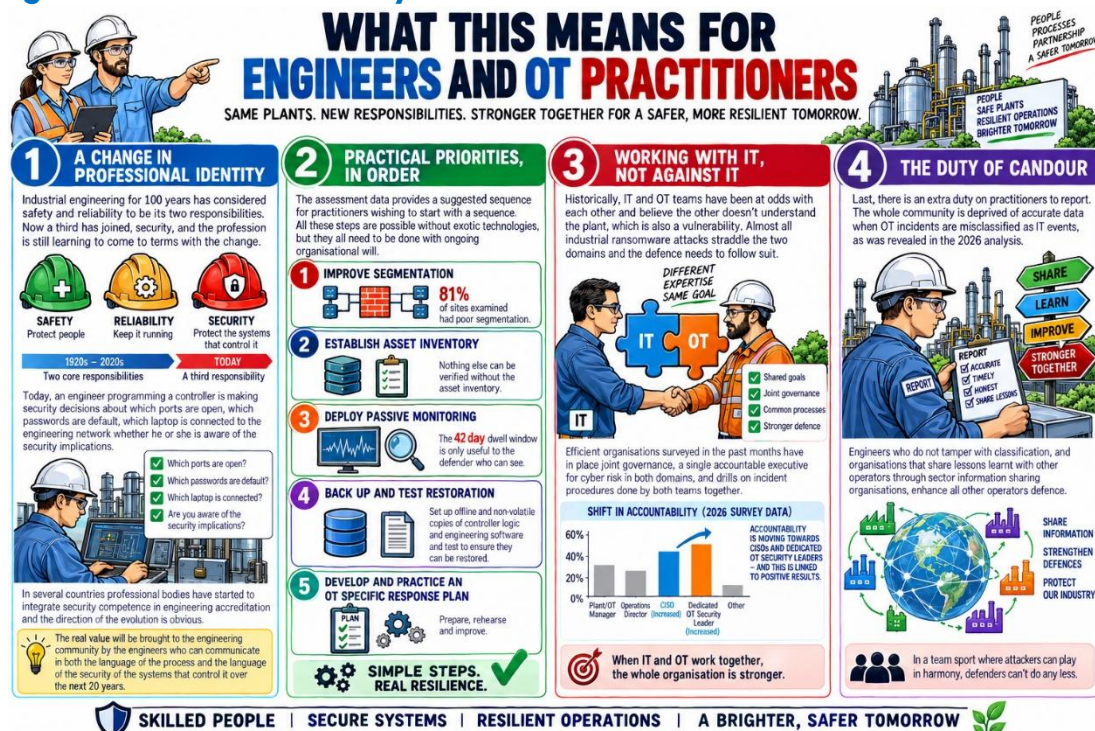


Fig -11: Engineers and OT Practitioners

Industrial engineering for 100 years has considered safety and reliability to be its two responsibilities. Now a third has joined, security, and the profession is still learning to come to terms with the change. Today, an engineer programming a controller is making security decisions about which ports are open, which passwords are default, which laptop is connected to the engineering network whether he or she is aware of the security implications. In several countries professional bodies have started to integrate security competence in engineering accreditation and the direction of the evolution is obvious. The real value will

be brought to the engineering community by the engineers who can communicate in both the language of the process and the language of the security of the systems that control it over the next 20 years.

13.2 Practical Priorities, In Order

The assessment data provides a suggested sequence for practitioners wishing to start with a sequence. The first money should be spent on good segmentation 81 percent of the sites examined had poor segmentation and compromised remote access in 73 percent of incidents. Second, establish the asset inventory, since there is nothing else that can be verified without the asset inventory. Third, using passive monitoring the 42 day dwell window is only useful to the defender who can see. Fourth, set up offline and non-volatile copies of controller logic and engineering software and test to ensure they can be restored. Fifth, develop and practice an OT specific response plan. All these steps are possible without exotic technologies, but they all need to be done with ongoing organisational will.

13.3 Working with IT, Not Against It

Historically, IT and OT teams have been at odds with each other and believe the other doesn't understand the plant, which is also a vulnerability. Almost all industrial ransomware attacks straddle the two domains and the defence needs to follow suit. Efficient organisations surveyed in the past months have in place joint governance, a single accountable executive for cyber risk in both domains, and drills on incident procedures done by both teams together. This evolution is reflected in the 2026 practitioner survey data, which reveals a shift in who is accountable for OT security, with accountability moving towards chief information security officers (CISOs) and dedicated OT security leaders, which is linked to positive results.

13.4 The Duty of Candour

Last, there is an extra duty on practitioners to report. The whole community is deprived of accurate data when OT incidents are misclassified as IT events, as was revealed in the 2026 analysis. Engineers who do not tamper with classification, and organisations that share lessons learnt with other operators through sector information sharing organisations, enhance all other operators defence. In a team sport where attackers can play in harmony, defenders can't do any less.

14. THE GAPS WHAT CURRENT PRACTICE AND RESEARCH HAVE NOT SOLVED

14.1 The Implementation Gap

It is not knowledge but execution that is the most outstanding difference. All the measures outlined in this article have been standard guidance for 10+ years, and the 2026 assessments reveal poor Segmentation in 81% of sites and only 46% of sites have adequate monitoring. The reasons are structural OT security budgets are competing with production investment, plants cannot easily halt for architectural surgery and equipment has a 30-year life and can't be replaced on a security schedule. Research on the actual nature of change in organisations and what makes some operators close the gap and some not, is light compared to research on technology and may be more important.

14.2 The Data Gap

There is lack of ground truth in OT security research. Under reporting, incidents are classified as IT events with insurers estimating tens of billions of dollars per year and the lack of labelled industrial attack data no operator can ethically generate attack traffic on a live plant all hinder the research of machine learning. Testbeds and digital twins are replaced to some extent but the difference between lab and refinery is yet to be bridged and published detection results should be viewed in this context.

14.3 The Legacy and Small-Operator Gap

Guidance and products focus on large operators, those with security teams. Current practice answers the question of what to do with such operators with a partial answer, a small municipal water utility or a family owned food processor is faced with the same criminal groups, but with much less resources. While the free government guidance is useful, there are no models in the sector that have been proven and are affordable to defend thousands of small essential facilities. The same goes for the deep legacy problem devices which can't be patched, can't be authenticated, can't be replaced for 20 years can be wrapped in compensating controls, but wrapping is mitigation, not cured.

14.5 The Measurement Gap

Rigorous answers to the question every board asks, how much safer each dollar make us are still elusive in the field. Security metrics are still mostly activity-based patches and alerts and are not about reduced risk. While outcome measurement is still in its infancy, investing will be based on judgment and fear, in varying degrees.

14.6 The Horizon Gap

Two developments will alter the problem quicker than standard bodies can move. By 2026, threat analysts reported that criminals were making strides in the quality of phishing and in targeting research and moving from opportunistic access to systematic mapping of physical control loops. In the meantime, the fast pace of distributed energy resource (DER) interconnection, battery storage, and cloud-connected devices is outpacing monitoring. In candour, the difference between the pace of change, and the pace of defence, is the difference that should worry readers the most.

15. CONCLUSION

The facts presented in this article suggest a conclusion that is dismal but not despairing. Uncomfortable because each of the trend lines is trending upwards the number of victims, which had almost doubled in 2025 to approximately 3,300 industrial organisations the number of criminal groups targeting industry, which had increased by 50% in 2025 and manufacturing, which has been the world's most attacked sector for several years. The criminal aspect of this game is well organised, well financed and patient, spending an average of six weeks in victim networks before striking. Not hopeless, as the defensive record has improved in step most victims are now rejecting paying, the total amount of ransom paid has decreased despite the number of attacks increasing, and the organisations that invested in segmentation, monitoring and rehearsed recovery have clearly suffered less and recovered faster than those that haven't.

Let's reiterate three findings. First, industrial ransomware is not a unique attack on controllers, but rather a standard attack on the office and virtualization systems that plants rely on, and the defence starts with the unsung basics. Segregated networks controlled remote access, patched perimeter devices, and honest inventories. Second, it is an execution, not an IQ, difference. What works has been published, standardised and in many jurisdictions are now required, what is not yet implemented because it is difficult, time consuming and expensive compared to production in terms of money and downtime windows. Third, the failure has public repercussions. The queues at petrol stations in 2021 and the idled supplier firms in 2025 were inflicted on those who played no part in the victims security decisions and that is the best case for the OT resilience being a matter of public policy and public awareness, not of private housekeeping.

If you're one of the readers who will act because of this article, the steps are obvious and designed to be modest. Know what you own, separate what you can, watch what you can't, prepare to recover, rehearse before you need to. The focus for policy makers is to back small essential operators that can't stand up for themselves on their own, and to ensure that essential operators report incidents honestly, so that everyone can benefit from improved data. It's an area of work that provides lasting, fulfilling projects for students and young engineers to protect systems that society would not be able to function without. Infrastructure only becomes a topic of discussion when it breaks. The true measure of success for all the foregoing is a silent one: uninterrupted flow of water, uninterrupted lines and a public that never knows how close the disruption came. That's silence that needs to be constructed, and, for the last two years, it will not construct itself.

REFERENCES

- [1] Axis Intelligence. (2026a, June 19). Ransomware Statistics 2026: Attacks, Costs & Trends - Complete Guide. <https://axis-intelligence.com/ransomware-statistics/>
- [2] Dragos OT Cybersecurity Report: Adversaries increase Real-World Impact, Map control loops across industrial infrastructure. (2026, February 17). <https://www.dragos.com/resources/press-release/dragos-2026-year-in-review-new-ot-threats-ransomware>
- [3] GASPAR POCA & PARTNER BTR CONSULTING. (2025). THREATS TO MISSION-CRITICAL INFRASTRUCTURES 2025 Outlook and 2026 priorities [Report]. <https://btrconsulting.com/wp-content/uploads/2026/08/BTR-OT-Report-2025-2026.pdf>
- [4] George, D. (2025). The Dual Shield: Cybersecurity insurance in an era of evolving digital threats. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.15428076>
- [5] George, D. (2026a). Architectural Convergence in Security Operations: a technical framework for AI-Augmented Threat Detection, Automated response, and Organizational cyber resilience. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.19986642>
- [6] George, D. (2026b). IEC 62443 Wireless Security: Deploying OT wireless controllers in industrial factory networks. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.19428491>
- [7] George, D. (2026c). Skills to level up Operational Technology (OT) Cybersecurity: A Quadrant-Based analysis of workforce capabilities, demand trajectories, and strategic development pathways. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.20433334>
- [8] George, D. (2026d). The Convergence of Intelligence and Infrastructure: A review of Emerging Technology Trends Reshaping Modern Operational Technology (OT) ecosystems. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.20353282>
- [9] George, D. (2026e). Large language model firewalls runtime safeguards for securing generative systems in enterprise deployment. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.21725826>
- [10] George, D., Dr.T.Baskar, & Dr.M.M.Karthikeyan. (2026). Driving Cybersecurity transformation through Managed Extended Detection and Response (MXDR): a framework for unified threat visibility and operational resilience. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.20341639>
- [11] Khalil, M. (2026, August 27). IoT Hacking statistics 2026: Threats, costs & regulations. DeepStrike. <https://deepstrike.io/blog/iot-hacking-statistics>
- [12] Mooney, L., & Alamri, A. H. (2026, August 10). Industrial Ransomware analysis for Q2 2026. <https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q2-2026>
- [13] Operational technology faces heightened cyber risk, with the industrials sector experiencing thousands of attacks per year, warns NCC Group. (n.d.). NCC Group. <https://www.nccgroup.com/newsroom/operational-technology-faces-heightened-cyber-risk-with-the-industrials-sector-experiencing-thousands-of-attacks-per-year-warns-ncc-group/>



- [14] OT security leaders take the helm as cyber resilience becomes a manufacturing performance driver. (2026, July 24). /. <https://www.kaspersky.com/about/press-releases/ot-security-leaders-take-the-helm-as-cyber-resilience-becomes-a-manufacturing-performance-driver>
- [15] Palmer, D. . (2026a, September 11). Significant rise in ransomware attacks targeting industrial operations. Infosecurity Magazine. <https://www.infosecurity-magazine.com/news/rise-in-ransomware-targeting/>
- [16] Sharma, D. a. K. (2026). AI-Powered Cybersecurity for OT and the IoT: A review of convergence, risk, and resilience in industrial environments. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.20156819>
- [17] Viorel, P. (2026, August 27). OT Cybersecurity for Manufacturers: 2026 Guide. IIoT World. <https://www.iiot-world.com/ics-security/ot-cybersecurity-manufacturing-2026/>
- [18] While OT security is maturing, risk is not slowing down | Fortinet blog. (2026a, June 9). Fortinet Blog. <https://www.fortinet.com/blog/operational-technology/while-ot-security-is-maturing-risk-is-not-slowing-down>