txOne networks

Legacy systems in European industrial environments: a cybersecurity review

Exploring the key cybersecurity challenges and trends impacting Europe's industrial organisations

Introduction

Operational technology (OT) plays a critical role in many industries—from utilities and manufacturing through to food and beverage, transportation, and automotive. Keeping OT systems safe is essential, as cyberattacks can have severe and wide-ranging impacts. Physical harm, operational disruptions, and equipment damage, and more can follow in their wake. However, securing OT environments isn't easy.

Often custom-built for specific tasks, many industrial OT assets are still reliant on Windows 7, XP, or other legacy systems. Designed with reliability and uptime—not cybersecurity—in mind, these "legacy" devices typically lack the security protections needed to withstand modern threats. And, with Microsoft ending support for Windows 10 in October 2025, even relatively modern assets could soon be at risk.

To understand how industrial organisations are stepping up to the challenge of protecting their OT systems, TXOne Networks commissioned an independent research agency to survey senior executives and decision makers from across Europe to learn more about their experiences—and challenges—with OT security.

Survey methodology

Undertaken in March 2025 on behalf of TXOne by iVOX, an independent research consultancy, an online survey was conducted with 550 senior professionals working for industrial organisations in France (100 respondents), Germany (100 respondents), Italy (100 respondents), Poland (50 respondents), Sweden (100 respondents), and the UK (100 respondents).

Responsible for their organisation's OT or Industrial Control System (ICS) cybersecurity posture, survey respondents included IT Managers (28%), OT/ICS Managers (17%), CIO/CTOs (17%), and Operations Directors (13%). All respondents were employed within mid-sized and large enterprise firms operating within a range of industry sectors.

Company size

Industry sector

Executive summary

The results of our survey shed light on some of the key concerns for OT security professionals, their attitudes towards dedicated OT cybersecurity solutions, and what's preventing them from implementing stronger controls. In a hurry? Then here are our headline findings.

Legacy systems still dominate in European OT/ICS environments

- Half the organisations we surveyed confirm that 50% of their OT environment is still reliant on legacy systems. For one-in-five, this share exceeds 75%.
- Compatibility issues (54%) and high replacement costs (45%) are the top reasons why industrial firms continue to depend on the outdated OT systems. However, this overreliance creates tangible cybersecurity risks.

Concerns about the operational and business impact of cyberattacks are high

- 40% of organisations say they experienced cyber incidents involving legacy OT systems in the previous 12 months.
- Top cybersecurity concerns relating to legacy OT systems include malware/virus infections (52%), unauthorised access (36%), lack of patches or security updates (34%), and ransomware (32%).

Organisations are caught between a rock and a hard place when it comes to protecting their legacy OT environments

- Organisations are holding back from implementing security measures in their OT environments, most commonly due to concerns over the impact on system performance (44%) and conflict with OT applications (42%).
- Ease of integration with existing infrastructures (50%) and zero operational disruption (49%) are a 'must have' when organisations assess which cybersecurity solutions to deploy.
- Most organisations believe that protecting legacy OT is as expensive as upgrading it—59% of respondents say it's the same or only a little more expensive to upgrade.

Despite the risks, just 50% of organisations have explored legacy-ready security solutions

- Of those that moved to protect their legacy systems, continuous monitoring (52%) and endpoint protection tools (51%) are the two most commonly deployed tools.
- The future looks safer. 62% of organisations say they intend to invest in cybersecurity solutions for their legacy systems and reduce their risk exposure.

The legacy technology challenge

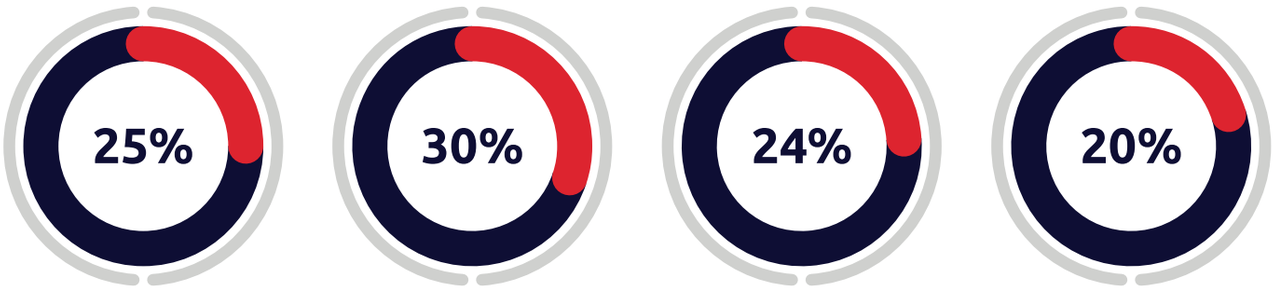
While the push for digital transformation has been underway for many years, we wanted to explore the extent to which legacy OT systems continue to be pivotal to the operations of European industrial firms.

In addition to understanding how much of the average OT environment is made up of legacy assets, we wanted to investigate why organisations continue to rely on these systems and the key challenges and issues this exposes them to.

Evaluating the tech stack: the enduring dominance of legacy systems

One of the key findings revealed by our study is the extent to which legacy systems in OT environments continue to play a critical role in European industrial organisations. 25% of organisations say that a quarter of their OT environment is reliant on legacy systems, with one-in-five stating that three-quarters or more of their environment still runs on legacy.

What percentage of your OT environment relies on legacy systems?



Less than 25% | **26-50%** | **51-75%** | **More than 75%**

Evaluating which countries are least reliant on outdated systems, organisations in Germany (38%), France (36%), and Sweden (28%) lead the way. On average, less than 25% of OT environments run on legacy systems in these countries. In other geographies, however, it's a different story. Around a third or more of organisations in Italy (38%) and the UK (30%) confirm that more than three-quarters of their OT systems are legacy-based.

Turning to individual industry sectors, pharmaceuticals and chemicals in particular stands out, with 42% of organisations saying that a sizeable portion (51-75%) of their OT environment runs on legacy.

Why legacy systems persist

Upgrading their OT environments to newer, more cyber resilient systems isn't a straightforward proposition for industrial organisations. Deeply embedded in their operations, the prospect of ripping out and replacing legacy systems comes with significant disruption and financial risk.

Compatibility with legacy equipment (54%) and the high cost associated with upgrading their estate (45%) are the most commonly cited reasons why industrial organisations are finding it difficult to transition to newer technologies.

For Italian organisations in particular, compatibility issues with legacy equipment are the top barrier to modernisation, cited by two thirds (66%). In Sweden, meanwhile, the downtime risks associated with upgrading is why half (51%) of organisations say they have no plans to change their current environment.

Top barriers to replacing legacy systems

Interestingly, a lack of vendor support for newer systems is proving the major sticking point for 20% of all European industrial organisations. This issue was notably top of mind for organisations in Poland (30%) and Germany (29%), as well as those operating in the energy (30%) and pharma/chemicals (29%) sectors.

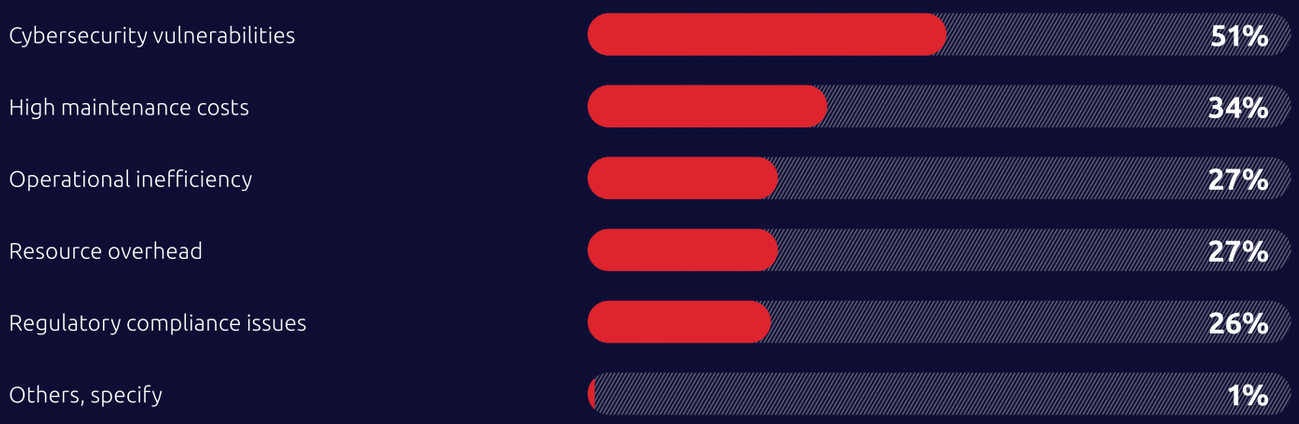
Untangling the legacy challenge

The continued dependence on outdated legacy software in their OT environments means industrial organisations are facing business challenges on multiple fronts.

Cybersecurity vulnerabilities were identified as the top risk by over half (51%) of all organisations surveyed. But the potential exposure of their operations to cyber threats isn't the only risk that legacy systems pose to industrial firms.

The high costs associated with maintaining outdated systems is another challenge, with more than a third (34%) of industrial firms citing it as an issue. Cost is a particular issue for organisations at the smaller end of the scale, with 40% of enterprises with 500-999 employees pointing to it as a barrier.

The legacy system business challenges



The key takeaways

A significant number of European OT environments are still heavily reliant on legacy software platforms. And, while these systems are vulnerable to cyberattacks, replacing these decades old systems isn't a straightforward proposition.

Deeply ingrained in day-to-day operations, the cost of replacing these systems goes beyond that of implementing new technology. Downtime risks and potential incompatibility issues are making it difficult for many organisations to upgrade.

Security and technology leaders in industrial firms are navigating a number of challenges caused by legacy. In addition to the potential exposure of OT systems to cyber risks, the ongoing cost of maintaining these outdated systems is soaring.

Understanding the cyber risks

Heavily reliant on legacy systems as they are, industrial leaders are understandably concerned about the cybersecurity risks their operations could be exposed to.

Wanting to understand if their legacy systems had already been targeted by cyber attackers—and which specific threats were creating the greatest cause for concern—we also wanted to learn which issues organisations come up against when trying to protect their legacy OT environments.

Cyberattacks: a clear and present danger

Almost half (43%) of European industrial organisations confirm they have experienced a cyber attack aimed at their legacy OT systems in the past year. The number of organisations that fell victim to those attacks varies considerably by geography, however. 60% of organisations in Poland and 59% of those in the UK report that their legacy OT systems had been attacked, compared to just 20% in France and 32% in Italy.

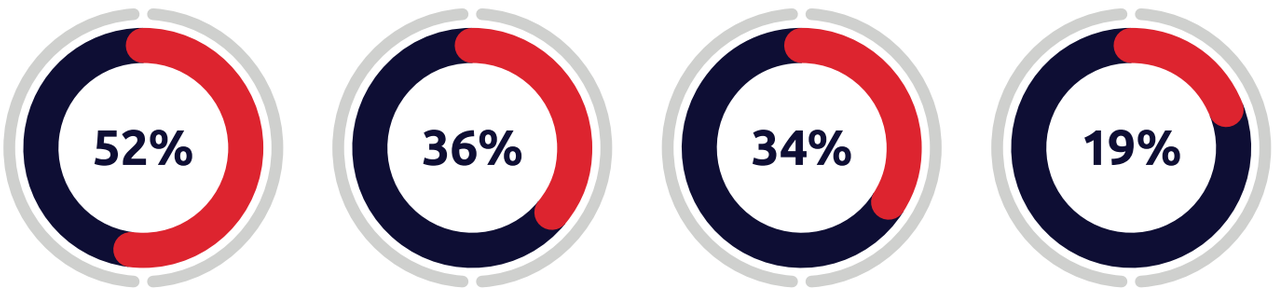
Looking at which sectors experienced the most incidents, those in the energy (54%), machine building (54%), and semiconductor (54%) industries were the most likely to report an attack against their systems. By contrast, just 24% of organisations in the utilities sector experienced an attack.

Legacy OT systems: the top cybersecurity concerns

Asked to state their top cybersecurity concerns in relation to legacy systems, malware and virus infections were identified as the key threat by 52% of industrial organisations. This issue appears to be a particular worry for French companies and organisations, with almost two-thirds (63%) stating their concerns here.

Unauthorised system access is seen as another key threat, with more than a third (36%) of industrial organisations calling it out, followed closely by ransomware attacks (32%).

The top cybersecurity concerns associated with legacy OT systems



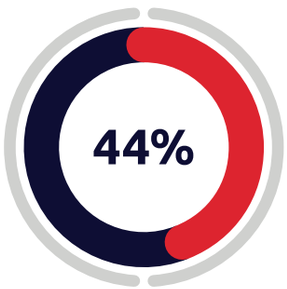
Implementing security measures: the key challenges

While they're highly aware of the risks that legacy systems pose, industrial organisations remain hesitant to implement cybersecurity measures in their OT environments.

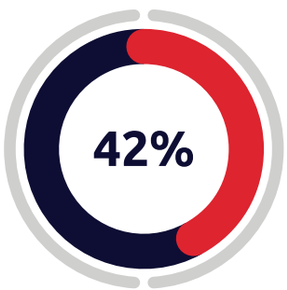
Worries around the potential impact on system performance is the prevailing concern here, as stated by 44% of respondents. Possible conflicts with existing OT applications was identified as another key inhibiting factor, meanwhile, noted as an issue by 42%. These aren't the only challenges that are preventing organisations from deploying cybersecurity measures in their OT environments, however.

Technical know-how is also a problem, with 13% suggesting that they don't have the expertise required to configure modern cybersecurity systems in OT environments. This is a particular challenge for Italian organisations, with more than double the average (28%) citing their concerns.

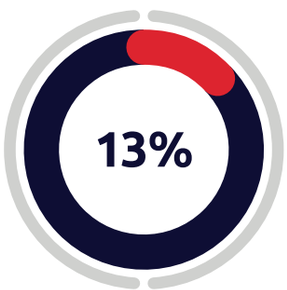
Implementing security measures: the top concerns



System performance impact



Conflict with OT applications



Don't know how to configure security policies

The key takeaways

Almost half of industrial organisations have experienced cyber attacks on their legacy OT systems in the past year.

While industrial firms are most worried about malware and viruses, they are also struggling with issues like patching and unauthorised access.

Respondents are also concerned that putting cybersecurity protection in place will cause disruptions. In addition to impacting the operational efficiency of their systems, industrial organisations are worried about the fallout created by potential conflicts with OT systems.

Protecting production

With so many organisations saying that protecting legacy OT is difficult to do, we wanted to understand the extent to which they'd explored dedicated security solutions capable of managing risk within legacy systems.

Specifically, we wanted to know what—if any—measures they've put in place to protect their systems, how likely they are to invest in a security solution, and the key considerations and factors that most influence the choice of solution they deploy.

Investing in cybersecurity: the progress to date

Despite the risks, the usage of security solutions within OT environments remains comparatively low. Continuous monitoring and endpoint security tools are the most popular measures by far, but even these are only used by around half of organisations (52% and 51% respectively).

Circumstances change by industry, too. Continuous monitoring is the tool most commonly applied in the energy sector (71%), for example, while endpoint protection is the predominant choice for 70% in the semiconductor industry. Network protection (64%), meanwhile, is most frequently used by pharma/chemicals firms, with virtual patching (50%) proving to be the solution of choice in food and beverage.

Top security measures already implemented

Future cybersecurity investment plans

While usage of legacy-capable OT security remains relatively low today, the growing threat against OT security does appear to be forcing many organisations to think again. 62% of professionals say that they are now “likely” to invest in those solutions in the future, for instance. Those aspirations are particularly acute within German (68%) and British (79%) firms.

Top factors influencing cybersecurity investment decisions

When choosing a legacy-capable OT security solution, organisations evaluate a range of different issues. Integration with existing infrastructure is the top priority, cited by 50%. Ease of implementation—something that respondents associate with “zero operational disruption”—comes a close second (49%).

Budgetary considerations are also important, with 47% of organisations saying that solutions must be cost-effective. 45% of respondents will only consider cybersecurity solutions that have a proven track record, meanwhile.

The top cybersecurity adoption priorities

Priorities change from industry to industry, too. Cost-effectiveness is the most significant factor for food and beverage (56%), manufacturing (56%) and semiconductor manufacturers. Integration with existing infrastructure is the top requirement for organisations in the utilities (54%) and transportation (44%) sectors, meanwhile.

Asked to evaluate which was more expensive—implementing a cybersecurity solution or upgrading their legacy systems—59% of industrial organisations stated the total cost of upgrading would prove more financially prohibitive.

That said, around a fifth (20%) believe that the costs associated with upgrading and implementing protection are broadly comparable. A further 17% felt that implementing protection would prove more expensive. This perception—while almost certainly incorrect—is no less damaging.

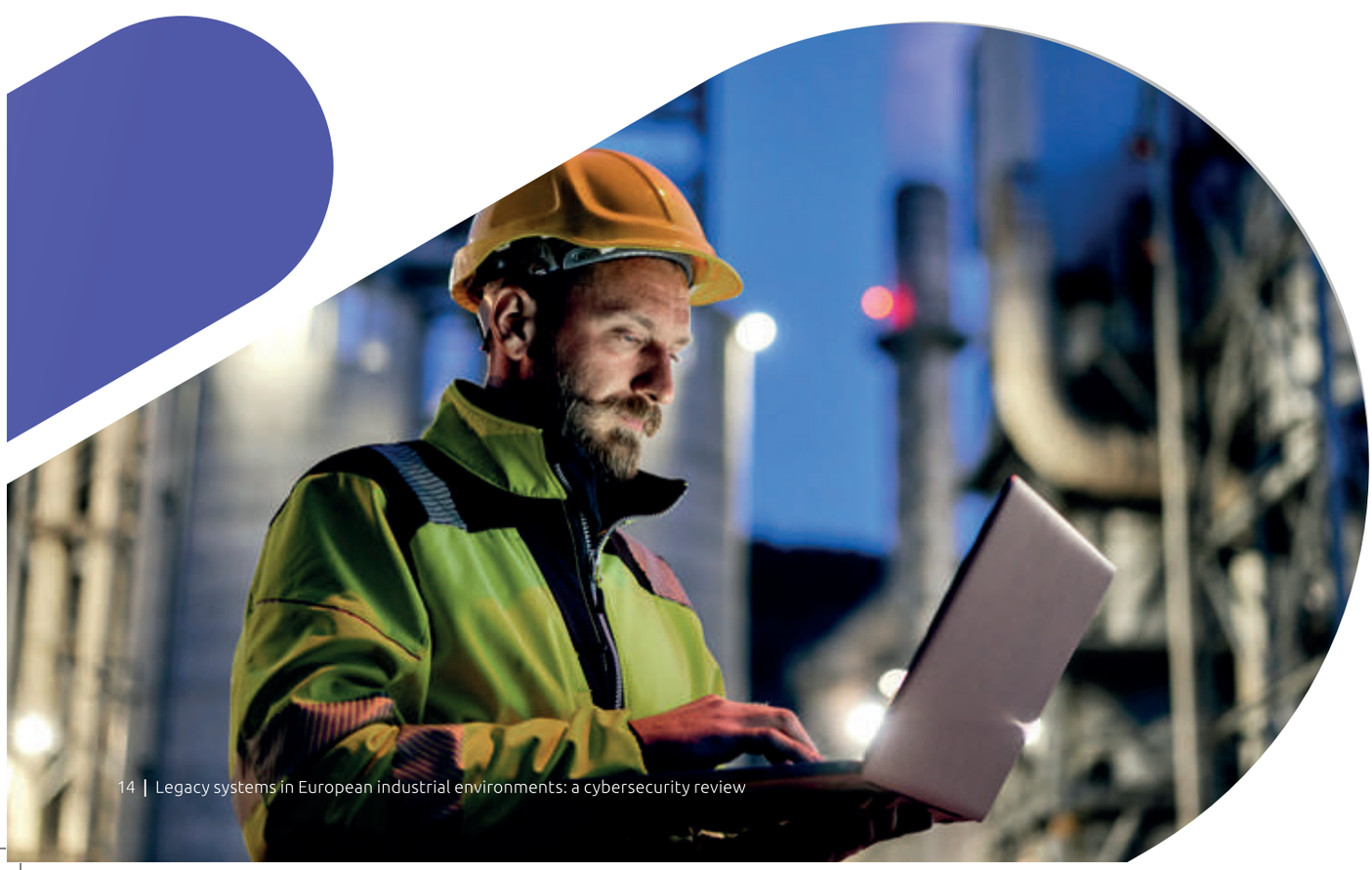
The key takeaways

Despite the risks, only a limited number of the organisations surveyed have explored legacy-ready security solutions.

That will change. 62% of organisations are considering adopting a dedicated cybersecurity solution for their legacy OT systems.

Given the constraints they operate under, industrial firms have clear requirements when it comes to the solutions they deploy—they need to integrate seamlessly, be non-disruptive, and cost-effective.

There's a misconception that protecting legacy OT is as expensive as upgrading it. Over a third (37%) of organisations believe it would cost the same, or more, to implement a dedicated security solution.



Legacy OT—a universal challenge

Controlling the physical processes that keep today's industries up and running, many of the OT systems in use today lack fundamental security protection, making them vulnerable to cyberattacks. Considering that so many organisations have suffered an attack on their systems in the past 12 months, this is undeniably troubling.

Dedicated OT protection exists—and many organisations are keen to secure their legacy systems against exploitation. But right now, few are actively exploring these solutions because of concerns around operational disruption and cost. These misconceptions should not—and cannot—get in the way of proactive risk mitigation.

Introducing TXOne Networks

More than 5,000 organisations around the world rely on us, a world-leader in OT security, to protect their operations. Easy to deploy and purpose built for operational environments, our solutions are designed to be as low impact and unintrusive as possible. But that's not all that makes us different.

Offering a solution that protects both legacy and modern OT and ICS systems, we ensure organisations are able to keep their high-value assets in use throughout their lifecycle —with no compromises or disruptions.

From intrusion prevention and firewalls for legacy OT assets, through to end-point protection, anti-malware/ ransomware protection, and threat detection, we make it easy for organisations to protect their legacy systems and secure their OT environments.

Find out more. Visit **www.txone.com**.

txOne networks

Stellar: endpoint security that puts your operations first

Balancing security and operational continuity can be difficult—particularly when it comes to legacy systems. That's why we created Stellar, our OT-native endpoint security solution.

Not only is Stellar capable of protecting assets running on Windows 2000, Windows XP, and other legacy systems, it does so in a low-impact, unintrusive way—helping you to manage risks while minimising disruption.

Find out what Stellar could do for you.
Download the datasheet here

txone.com