The 7 Keys To Improving OT Security Outcomes

Kaspersky ICS Security Survey 2022

kaspersky BRING ON THE FUTURE

Contents

Introduction 3

About the research 4

Key takeaways 5

The current state of OT security 6

The importance of considering ESG 9

Introducing the 7 keys to improved industrial security outcomes 11

1. Having a well-resourced and appropriately skilled OT security team 12
2. Ability to master the internal 'politics' of industrial security management 14
3. Having a strategy for managing legacy infrastructure 17
4. Implementing solutions that are specifically designed for ICS environments 20
5. Having a strategy for IT/OT convergence, including IoT 22
6. Being quick to respond when incidents occur 24
7. Taking staff training and compliance seriously 26

Embedding industrial security best practices 28

About Kaspersky Industrial CyberSecurity 29

Appendix 30

Introduction

Organizations operating production facilities and critical infrastructure have been through a challenging few years. The COVID-19 pandemic revealed the extent to which many aspects of society are highly dependent on the uninterrupted operation of industrial processes. While often unseen, these operators are crucial in ensuring that life continues as normally as possible.

As we emerge from COVID, companies in these sectors have since been dealing with an aftermath of disrupted supply chains, a push towards more digitally driven efficiency gains and the need to consider how their operations can become more sustainable.

To realize these ambitions, industrial organizations also need to pay attention to cybersecurity matters. Just as the pandemic has highlighted the pivotal role played by these firms in the economy at large, this has unfortunately also demonstrated that they are attractive targets for criminals and other actors that wish to cause disruption.

Data collected by Kaspersky[1] suggests that attacks on industrial control systems (ICS) increased markedly over the course of 2021 compared with the previous year. Among other statistics, there has been:

- A **45%** relative increase in the incidence of **spyware on computers used for ICS purposes** compared with early 2020.
- A **43%** relative increase (vs. 2020) in instances of **malicious scripts and phishing pages** being blocked on devices running industrial systems.
- A **doubling** in the discovery of **cryptocurrency miners** on computers in ICS networks since the first half of 2020.

Given this apparent acceleration in activity, the topic of ICS security is one that warrants further investigation. This report takes a deeper look at the cybersecurity risks affecting organizations that use operational technology (OT)[2]. We start our investigation by reviewing the current 'state of OT security', covering subjects such as the scale of threats faced and the consequences. We then turn to considering what can be learned from those organizations that have been successful in avoiding major problems. As part of our analysis, we identify 7 factors that are consistently linked with better industrial security outcomes – all of which should be focus areas for operators in these markets.

1 https://ics-cert.kaspersky.com/publications/reports/2022/03/03/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2021/

2 For the purposes of survey recruitment, operational technology (OT) includes those using: Industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Distributed control systems (DCS), Process control systems (PCS), Building automation / management systems (BMS, BAS, BCS) or any other OT systems judged appropriate.

About the research

The report's findings are based on survey research with relevant operators of industrial infrastructure: 306 structured online interviews were completed by OT security decision-makers across 17 countries, spanning North America, Latin America, Europe, the Middle East, Africa, Asia-Pacific and Russia. All organizations had 1,000 or more employees. The individuals interviewed all had hands-on experience with industrial security matters – both operationally and in terms of decisions around which security solutions are used. Because of this requirement, most respondents were in specialist technology management or leadership roles.

The balance of responses received across industry groupings was as follows:

Industry grouping	% of survey responses
Critical manufacturing (metals, machinery, high-tech, transportation)	32%
Oil & Gas, Chemicals and Energy	14%
Commercial facilities (real estate, construction & retail)	13%
Consumer goods manufacturing (food, pharmaceuticals etc.)	12%
IT, telecoms and system integrators	11%
Transportation & logistics	8%
Others	10%

This structured (quantitative) fieldwork phase took place from 4th January 2022 to 3rd February 2022. Following the structured survey, we also conducted in-depth discussions with 10 respondents to understand more about their perspectives on current ICS security challenges and how they were planning to mitigate these issues. This feedback is also incorporated throughout the report.

This study builds on similar research conducted by Kaspersky in 2020. Where relevant, data from this prior research is also included in our findings.

Key takeaways

- The **number of security events affecting OT/ICS infrastructure is increasing sharply**, with 50% of organizations seeing an increase in incidents compared with 2019. This is especially concerning considering that the **estimated total financial costs of industrial infrastructure cybersecurity attacks are 59% higher than the average** for other large businesses.

- About 30% of organizations experience significantly more severe outcomes from operational technology security issues than others: These companies see 4 times as many incidents and suffer financial costs that are twice as large. Added to this, **these 'most affected' companies are more likely to see these cyber risks manifest in terms of physical risk, such as injury or death** (5 times more likely than the 'least affected' firms) and **environmental damage** (2.5 times more likely). Unfortunately, there has been little progress among industrial firms in specifically addressing these environmental, social and governance (ESG) impacts compared with a similar study conducted 2 years ago.

- Our research finds **7 areas of organizational behavior and capability that are significantly linked with these more severe security outcomes**:

  1. Having a well-resourced and appropriately skilled OT security team
  2. The ability to master the internal 'politics' of industrial security management
  3. Having a strategy for managing legacy infrastructure
  4. Implementing security solutions that are specifically designed for ICS environments
  5. Having a strategy for IT/OT convergence, including IoT
  6. Being quick to respond when incidents occur
  7. Taking staff training and compliance seriously

- When comparing different types of industrial and critical infrastructure operators, we find 3 areas in which the largest gaps in behavior and capability are most consistently found:

  - **Having a strategy for managing legacy ICS infrastructure:** Poor visibility of vulnerable infrastructure is identified as a problem by almost half (43%) of those suffering the most severe consequences from incidents. Moreover, the most affected firms identify that 31% of their endpoints in OT networks are unpatched, with 1 in 5 (20%) being 'unpatchable'.

  - **Having a strategy for IT/OT convergence, including IoT:** Organizations see the increased use of cloud technologies and Industrial Internet of Things (IIoT) components in their operational environments as among the top things impacting OT security. Compared with the least impacted, the 'most affected' firms are around 4 times more likely to suffer security incidents that target IoT cloud services, IoT sensors and IoT networking devices. This suggests that convergence and integration with IT environments may have been mismanaged in terms of security.

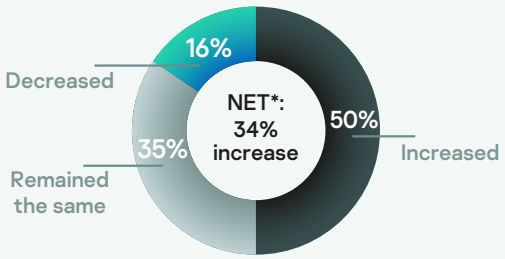
  - **Taking staff training and compliance seriously:** 68% of firms surveyed identified that they had experienced at least one incident involving a breach of staff compliance with security policies. Problems relating to IT security policy violations are over twice as common among the 'most affected' firms. Unfortunately, a third of firms (33%) reported that they do not yet implement OT/ICS-specific security awareness programs for their teams.

The current state of OT security: Real world experiences for industrial organizations in 2022

Although there is no shortage of macro-level data and threat intelligence on the cybersecurity challenges facing those with industrial automation systems, what are the individual, 'on the ground' experiences of those in charge of such matters? Overall, our survey finds a challenging and intensifying environment: Figure 1 (below) shows that half of organizations (50%) have seen an increase in security incidents affecting their cyber-physical systems since 2019. By contrast, fewer than 1 in 5 (16%) report a decrease inthe scale of threats:

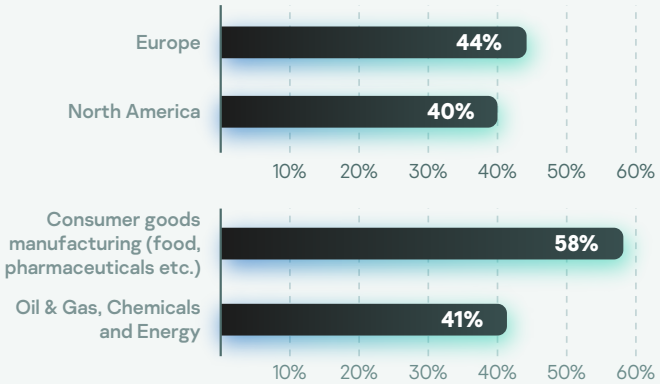
1

Change in security incidents in OT/ICS infrastructure since the end of 2019



* The "NET" score is calculated by subtracting the proportion of firms seeing a decrease in threats from the proportion reporting a decrease.

Regions and sectors seeing largest NET* increases in incidents

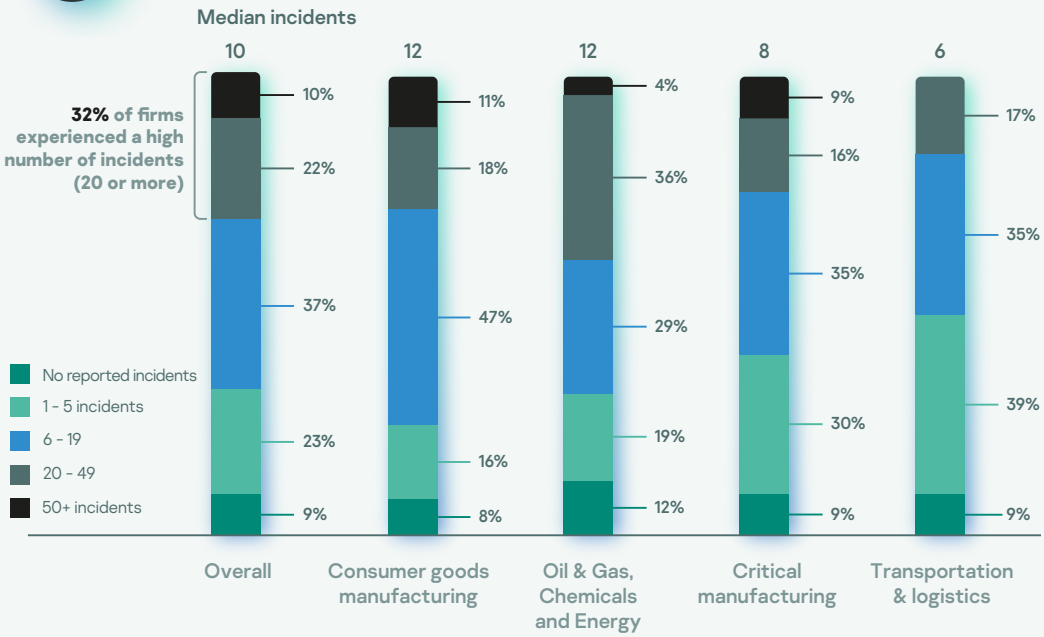


Taken across all organizations with ICS infrastructure, this results in the balance (or 'net' score) towards there being a perceived increase in the threat landscape affecting industrial companies. Organizations in Europe, North America, consumer goods manufacturing, oil & gas, energy and chemicals industries were especially likely to be negatively affected by a rise in incidents.

Our study also discovers that 91% of our survey participants have experienced at least one security issue within their operational technology environments in the last 12 months. Figure 2 (below) shows that the median average number of incidents impacting organizations in our sample was 10 in the past year, with almost a third (32%) of firms withstanding a high number of events (20 or more). Concerningly, the industries that, once again, tended to be most affected were those in nationally critical industries, such as food and energy production:

2

Total number of security incidents experienced (across all incident types, last 12 months)



On average, companies in the research identified 5.7 different types of incidents that they had been directly affected by in the past 12 months. The specific types of attacks that were reported most by our industrial respondents included:

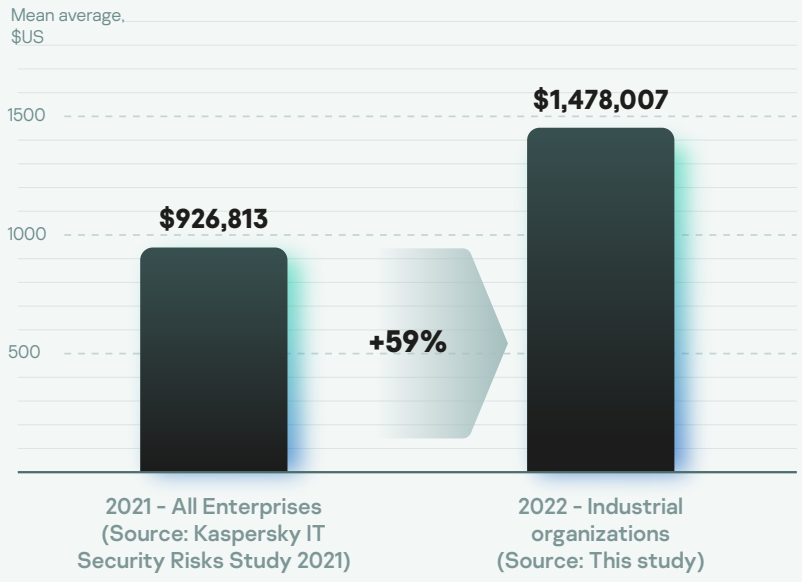
1. IT security policy violations by staff (44% reported at least one incident)
2. Malware infections (41%)
3. Inappropriate IT resource use by employees (36%)

Although some of the threats faced are familiar foes (such as malware, insider threats and policy violations), in the comments accompanying the survey responses we found that recent attacks now tend to be characterized by a marked increase in sophistication, not just frequency and volume. For instance, the use of obfuscatory techniques in incidents where malware was a vector was mentioned several times over. As one respondent recounted to us:

> **"In many cases, we are seeing the same types of threats that we have seen before – repeating themselves and trying again. We had an increase of about 200 percent during COVID lockdowns. Although we still see classic 'phishing' and 'spam' techniques, the attacks have grown in sophistication and intelligence. That requires us to sharpen our strategies to address them."**
>
> **– Automotive manufacturer, Latin America**

Considering the pivotal importance of these nationally critical industries and the sheer number and sophistication of the attacks they face, the financial implications of an incident are similarly elevated. When compared to other large organizations, firms operating OT/ICS infrastructure report total financial costs of security incidents that are 59% higher (see Figure 3).

3 Estimated total financial costs from OT/ICS attacks compared with the average for all Enterprise* businesses



* Enterprises defined as organizations with 1000 or more employees.

Allied with the above, more industrial companies feel that the costs of incidents have increased (vs. decreased) when compared to the end of 2019: 32% of organizations see the financial damage as having increased compared to 2 years ago, compared with 22% perceiving a decrease. 46% think the costs of an incident are at the same (usually high) level as before. This perception of a rise in the costs of incidents was especially high in North America and in the consumer goods manufacturing sector. It is easy to see how during the COVID-19 pandemic, manufacturers of essentials such as food and pharmaceuticals will have been particularly targeted.

These struggles are, of course, only the tip of the iceberg. Since we can reasonably assume that many companies will have been reluctant to disclose the full scale of the challenges they face, this suggests an acute issue that requires close and careful management.

What is also clear from this review of the 'state of OT security' is the range of severities of experience that survey respondents relayed. When taken across all the outcomes we have just reviewed, we are able to sort organizations into three groups: The 'most affected', the 'least affected' and those in the middle. When we review the security outcomes of these groups (see Figure 4), we see these disparities very transparently:

4 Segmentation of survey respondents by severity of ICS security outcomes

	Number of breach incidents	% Perceiving incidents as increasing	Costs of breaches
Most affected | 30%	40	85%	$2.8m
Middle third | 34%	16	46%	$1.3m
Least affected | 36%	8	14%	$304k

Severity assessed by analysing number of breach incidents, change overall in breach incidents over time, costs of breaches, perceived change in cost of incidents and performance for detection, prevention, response and remediation of incidents.

To take a few examples of the differences, the number of breach incidents among those 'most affected' is 4 times higher than average, and the costs of breaches are twice as large. By contrast, the 36% of firms that are the 'least affected' see considerably lower financial impacts.

Further consequences of being in the 'most affected' group – the importance of considering ESG[3]

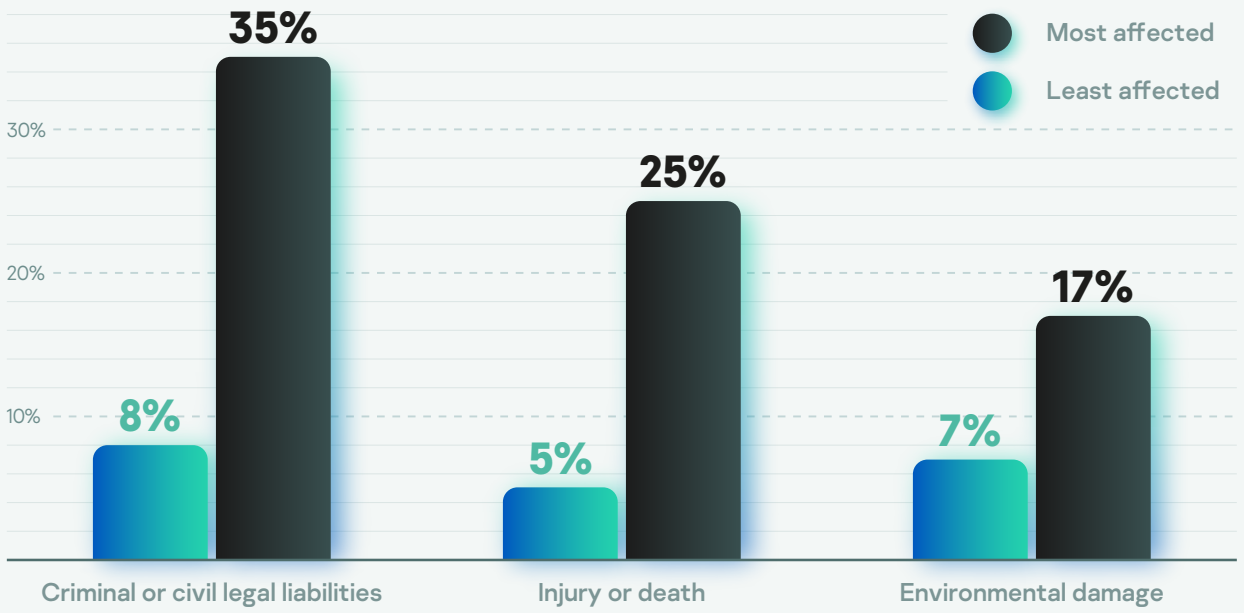
Aside from negative financial outcomes, our research also identifies some of the potential human and environmental costs of industrial organizations that are 'most affected' by incidents targeting their operational technology infrastructure.

To investigate this, we analyzed the consequences of OT/ICS security intrusions reported to us by survey respondents. These consequences ranged from intangible effects, such as damage to brand, customer confidence and commercial opportunities, through to physical impacts, such as damage to production equipment. Critically, we found that the 'most affected' organizations tended to be significantly and disproportionately impacted by human and environmental impacts. This included, for instance, death or injury caused to employees and others from compromised cyber-physical systems, and the potential for environmental damage resulting from such events (shown in Figure 5, below). Linked with this are the criminal or civil legal liabilities that may then also ensue:

5

Consequences of OT/ICS intrusions / breaches

Selected issues where difference between most and least affected firms is greatest

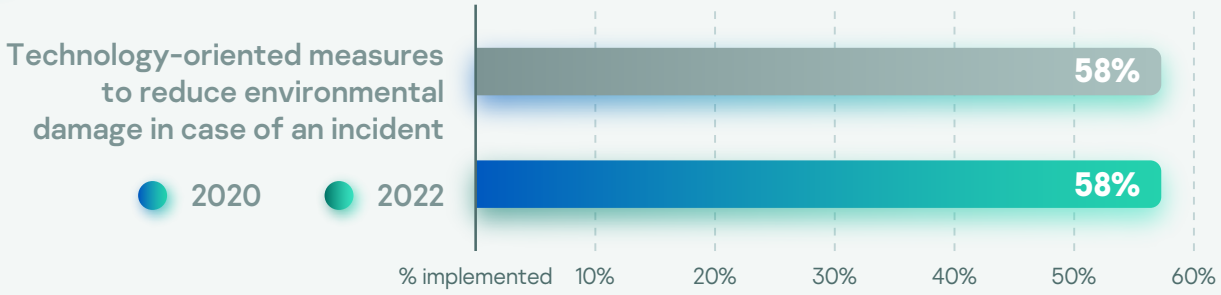


Because of the nature of cyber-physical risks, these sorts of consequences bring into sharp focus the interplay between the cybersecurity of industrial infrastructure and 'ESG' (or Environmental, Social and Governance) initiatives that many corporate entities are currently focusing on. A cyber-attack on, say, a safety-critical power station or oil and gas installation has the capacity to have knock-on impacts that touch all components of ESG.

[3] Environmental, social and governance (ESG) refers to a collection of corporate performance evaluation criteria that assess the robustness of a company's governance mechanisms and its ability to effectively manage its environmental and social impacts. (Gartner: https://www.gartner.com/en/finance/glossary/environmental-social-and-governance-esg-)

If we focus specifically on the environmental and social effects of cybersecurity incidents, we would expect to see increased attention to this within industrial firms. Unfortunately, there is no clear evidence of this when we compare our results to previous research conducted for Kaspersky in 2020: Only 58% of organizations surveyed now report implementing technology-oriented measures that would reduce environmental damage in the event of an incident (see Figure 6), a figure that has not increased over the past two years:

6 Implementation of sustainable development measures



Quite aside from technical measures to mitigate the impacts from cyber-attacks on industrial facilities, organizations also need to put in place appropriate, foundational governance measures. Again, we find concerning deficiencies on this, most notably the fact that:

- **36%** of organizations surveyed **do not yet have a dedicated ESG framework** or standard in place
- **38%** of firms **do not have a dedicated role or director responsible** for environment or health and safety matters

What else can we learn from the 'most affected' vs. 'least affected' organizations? Introducing the 7 keys to improved industrial security outcomes

Our deep dive into the consequences of those organizations most and least impacted by industrial security incidents can also be extended to the behaviors and organizational characteristics that these firms exhibit.

When analyzing all the questions asked in our survey, we find 7 clear themes that align strongly with organizations that are most successful in avoiding the worst outcomes. These 7 keys to improved industrial security outcomes are:

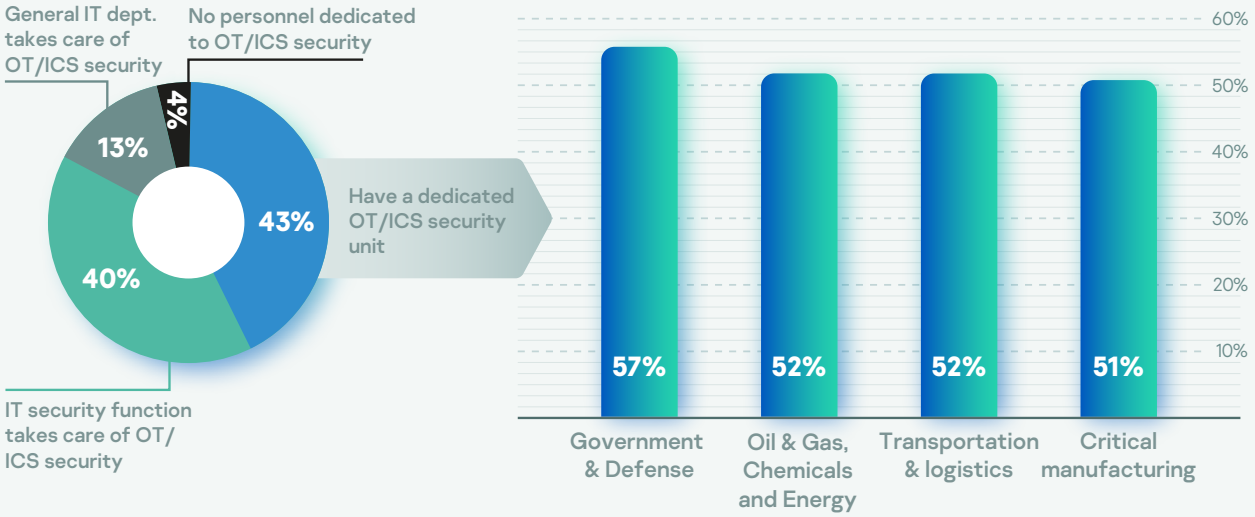
In the sections that follow in this white paper, we investigate each of these keys to success in greater detail.

1 Having a well-resourced and appropriately skilled OT security team

The first of the success factors that we identified is the extent to which production-focused and critical industries are adequately resourced in terms of their operational technology security teams.

Before we examine the factors that contribute towards better security outcomes, it is worth initially reflecting upon the extent to which industrial companies even have dedicated, specialist resource for industrial control systems security. What we find is that at present, fewer than half (43%) of organizations with OT/ICS infrastructure have such teams (see Figure 8). Instead, it is common for organizations to give this task to their IT security department or their general IT department. Given the unique, and often esoteric, challenges involved in securing operational technology systems, it is unsurprising that many companies face the sorts of difficulties identified earlier in this report.

8 Management of OT/ICS security overall and in selected industries



Furthermore, even in the most sensitive of critical industries (such as defense, oil & gas, chemicals and energy and transport and logistics), a significant proportion only have IT or IT security generalists taking charge.

Irrespective of how ICS security is organized in these firms, we also find clear evidence that resourcing for industrial security is especially challenging right now:

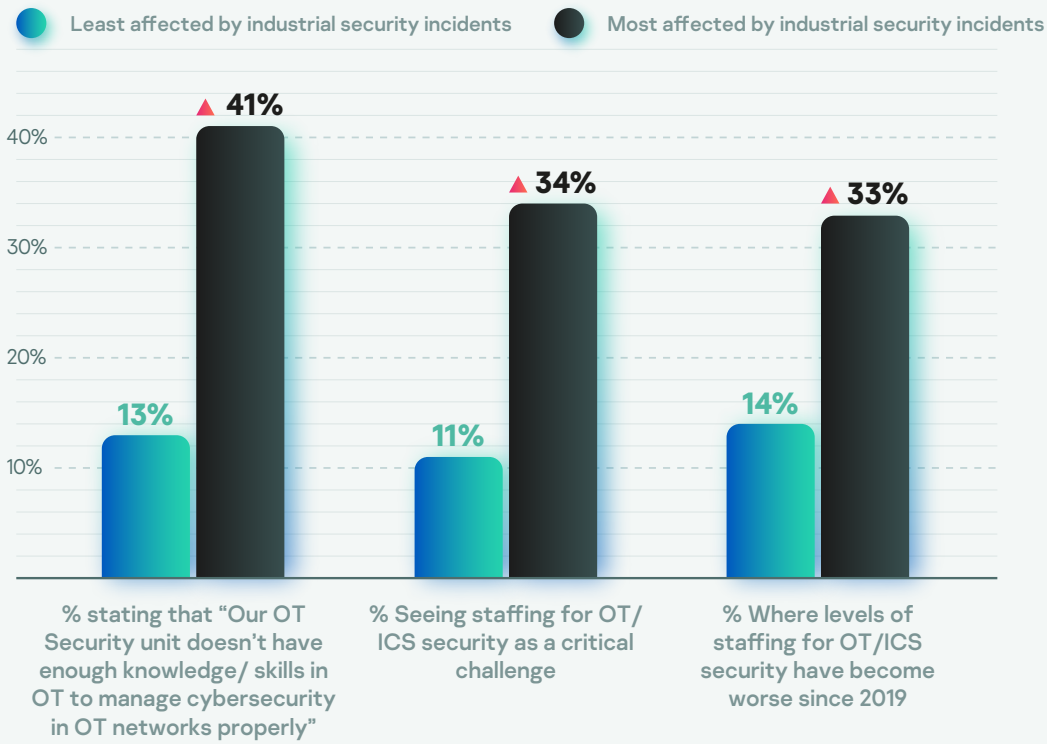
- **66%** of survey respondents **perceive significant OT security staffing challenges**, such as specialists being overloaded with work, high staff turnover and an inability to get access to qualified personnel.
- Among all the areas in which an organization may be under-resourced for ICS security investment, **staffing (specifically low headcount)** is the most common problem, with **55%** of those with under-financing issues mentioning this challenge specifically.
- For around 1 in 5 organizations **(19%)**, these problems are felt to be highly critical to the extent that they may be **directly contributing to security issues**.

In some of the open-ended feedback received within the interviews we conducted with decision-makers, several drew attention to a mismatch between the scarcity of the skills being sought and the relatively low salaries being offered:

> **"There is a good supply of security interns, but the job description is not consistent with the requirements and salaries on offer. Just look at the job descriptions asking for CISSP, SANS, CEH and CompTIA for a salary that doesn't match."**
>
> **– Retail bank, Latin America**

Organizations that have superior OT security outcomes are distinguished from the most affected on several factors relating to their ICS security teams (see Figure 9). The most impacted companies are significantly more likely to lack the knowledge of how to effectively manage cybersecurity in OT networks, are more prone to identifying ICS security staffing as a critical (i.e., security-endangering) challenge and are much likely to see the situation as having become worse since 2019.

9



Given the relative difficulty of recruiting appropriately skilled industrial security specialists into their teams, our research finds that many organizations are looking to specialist external partners for help:

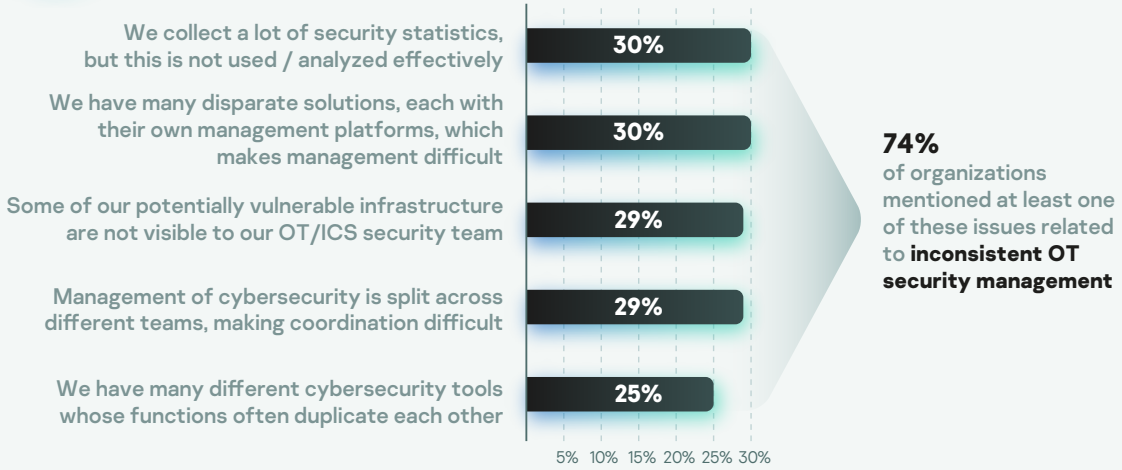
- **95%** rely on **external service providers (such as MSPs and MSSPs)** in some way to help manage their ICS/OT environments.
- This need for specialized support in firms with operational technology appears **far higher than for other large organizations** – While 95% of firms interviewed in this study use external partners in some way, this compares with only 42% of other enterprises (those with 1,000 or more employees) doing so in other Kaspersky research[4].
- We can expect this reliance on external service providers to accelerate even further: **58%** of those using MSPs or MSSPs stated that they had **started to rely more on these external providers** when compared with 2019.

4 Kaspersky IT Security Risks Study 2021 is a global survey of IT business decision makers. A total of 4,303 interviews from businesses with more than 50 employees were conducted across 31 countries in May-June 2021.

2 Ability to master the internal 'politics' of industrial security management

The previous section shows that there are many pressures being placed on those managing OT security. Ideally, industrial security issues would be managed by a dedicated ICS security unit, not least because this should allow for a more coherent and expert approach to such challenges. Further to this, our research finds several areas in which inconsistent and sub-optimal approaches to industrial security management are apparent (see Figure 10):

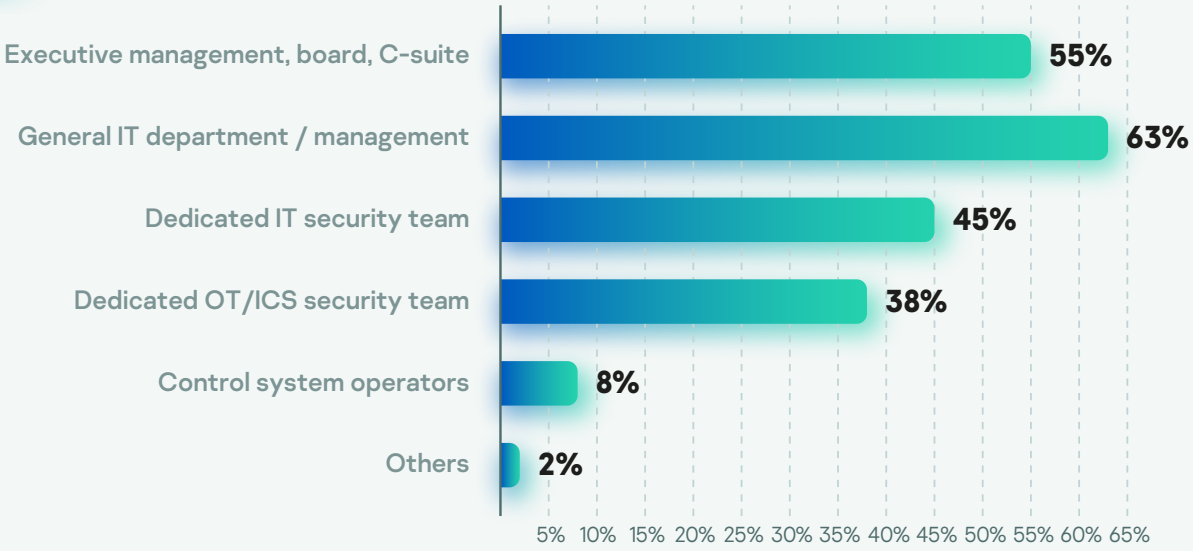
10 Selected pain points and risks relating to OT/ICS security management



Some of these inconsistencies concern having disparate (and/or duplicated) tools and processes, while other issues relate to a lack of coordination between teams due to splits between IT and OT security.

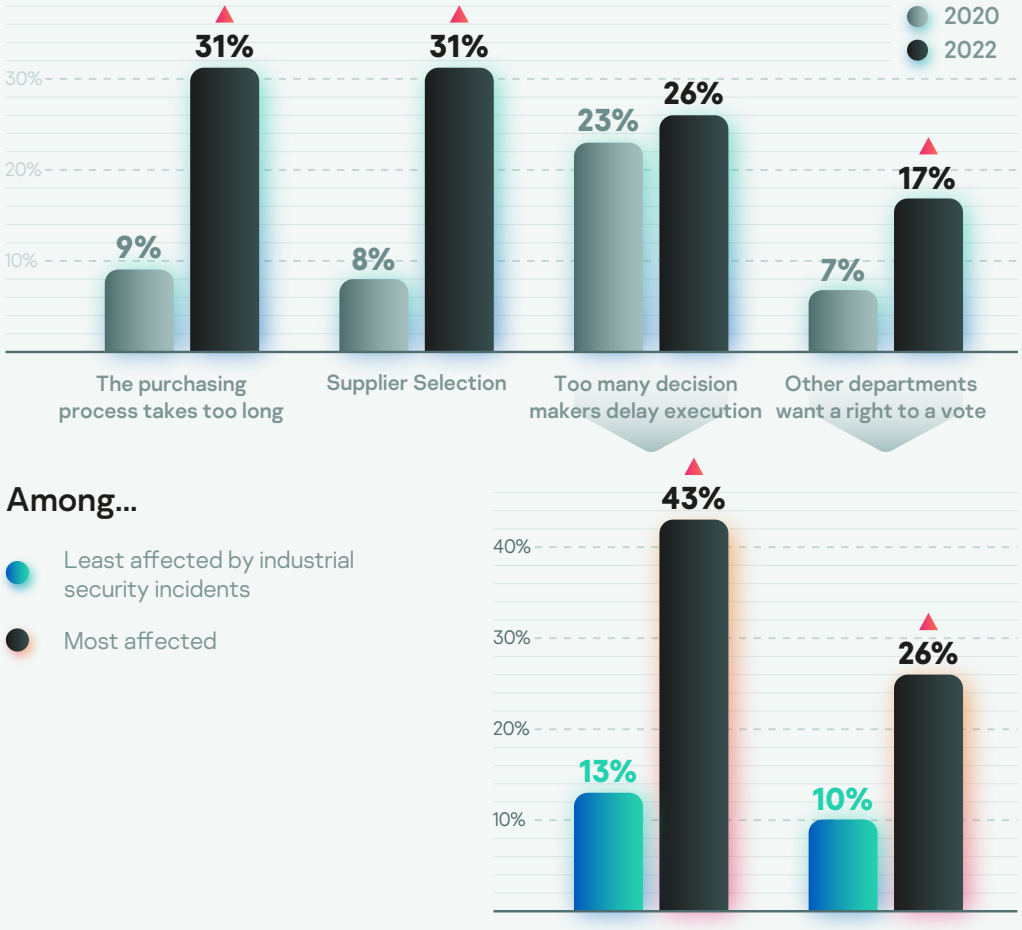
We also find clear evidence of this 'cross-over' in responsibilities when it comes to the approval of OT/ICS security projects and budgets. Figure 11 (below) shows the heavy degree of influence that executive management, IT departments and IT security teams have in approving plans for ICS security initiatives. Because many firms do not have dedicated industrial security teams, those that are the closest to the operational technology concerned (OT security teams and control system operators) are much less often driving decisions for the security solutions that protect these environments.

11 Functions involved in the approval of OT/ICS security projects and budgets



When we track the results of this year's ICS security survey with one conducted in 2020 by Kaspersky, there are signals that these inter-departmental tensions are rising. Compared with 2020, significantly higher proportions of organizations now report delays and barriers to the implementation of industrial security projects caused by different departments wanting to have a 'casting vote' (see Figure 12, below). It is also notable that decision-makers in the IT security function were especially likely to identify this as an issue, suggesting possible tensions with OT and automation specialists. This seems to then lead to an elongation of the purchasing process, and difficulties with supplier selection.

12 Delays / barriers to the implementation of OT/ICS security projects



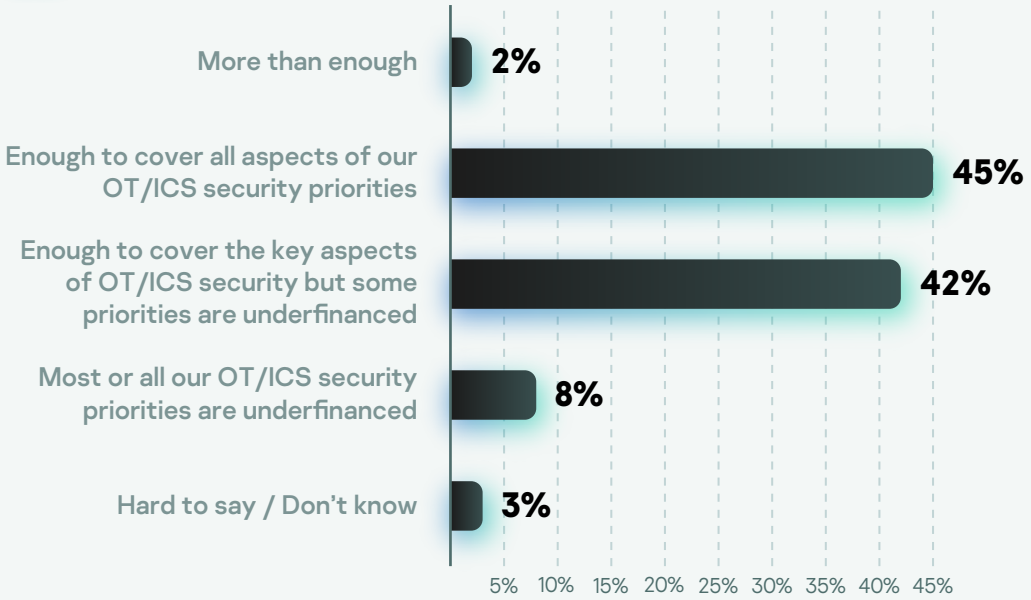
This lack of coordination and agreement between departments is not only stressful and inconvenient, but there is also evidence that it is linked with undesirable cybersecurity outcomes. The most affected organizations are several times more likely to identify this 'too many cooks' issue in decision-making when compared to the least impacted (see also Figure 12).

These tensions extend beyond a lack of coordination between technology, security and leadership teams. In follow-up conversations with the survey respondents, we found some signs that getting 'buy-in' from those at the plant level can also be particularly challenging, especially when introducing new security technology or working practices:

> **"Culturally [for] the plant operators or managers this sort of [security] technology is new and unexpected and does stuff they'd never thought needed to be done. From a cultural point of view there was quite a pushback as in 'why we are investing this much cash to do something we don't really need?'"**
>
> **– Manufacturer, Europe**

What this quote also reveals is that budgets are inevitably a considerable source of the friction between teams, especially when resources are limited. Figure 13 (below) shows that fewer than half (47%) of organizations with ICS/OT infrastructure see their current level of investment in securing these environments as adequate (that is, without some areas being underfinanced).

13 Perceived adequacy of OT/ICS security spending



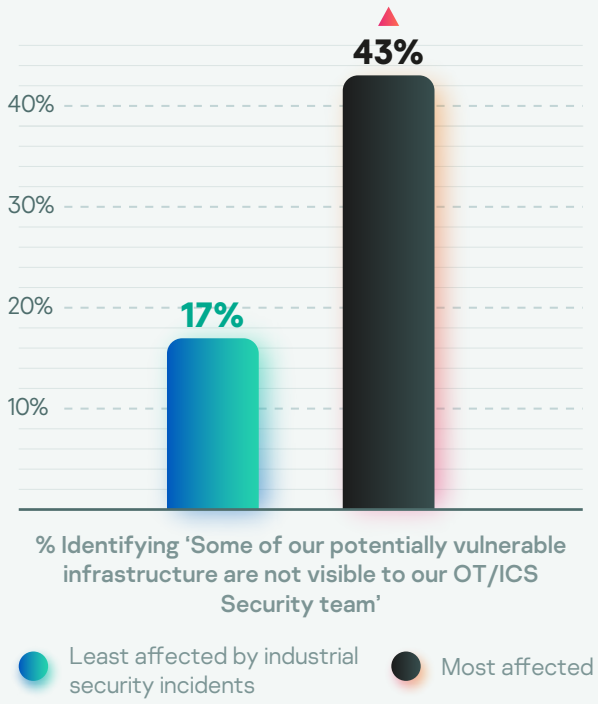
Added to this general picture, when we focus particularly upon those organizations that are 'most affected' by industrial security incidents, we find that a significantly higher proportion (60%) report not saving enough budget to cover all their OT security priorities.

3 Having a strategy for managing legacy infrastructure

Operational technology environments are filled with equipment that predates modern approaches to networking, systems management, and security. However, as industrial organizations become increasingly 'digital', separating OT networks from the rest of the enterprise and relying on 'security by obscurity' becomes less and less sustainable. Nonetheless, there is still a need for firms to effectively manage the array of legacy networking, programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) and other OT systems that many organizations maintain.

The starting point in this process is establishing a base level of visibility of all the nodes, networking devices and other objects active within the OT network. Figure 14 shows clearly that visibility of ICS infrastructure is an area in which the 'most affected' firms face more considerable challenges than those that are not so impacted:

14 Infrastructure visibility as a pain point / risk for OT/ICS security management

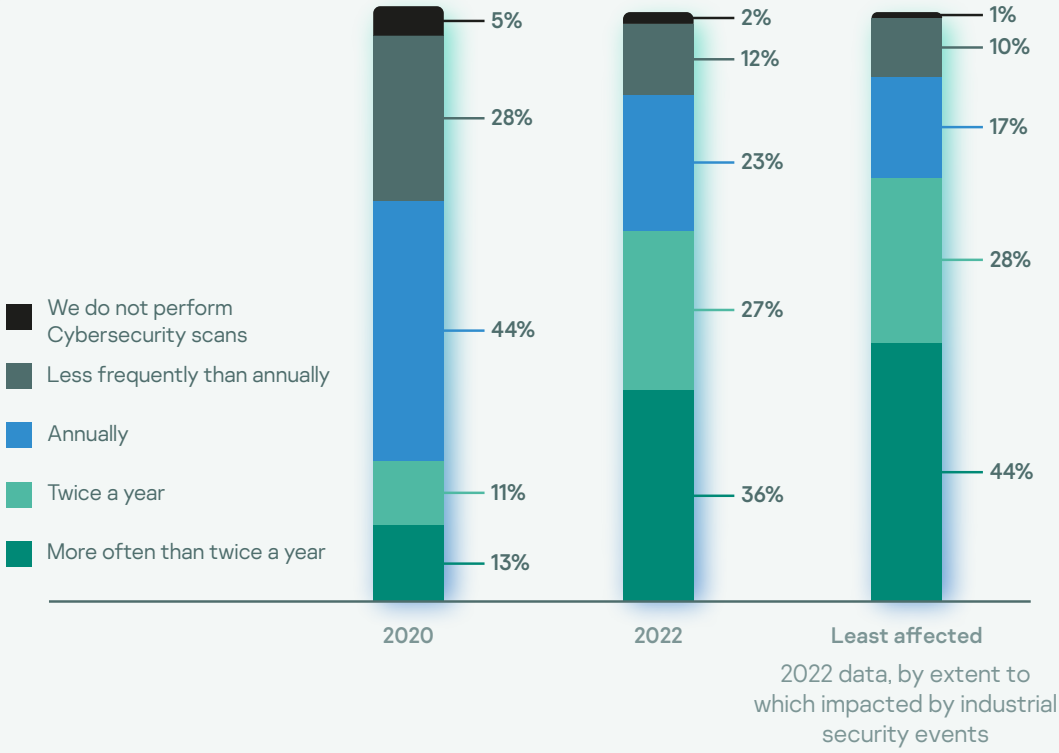


Several of our research respondents spontaneously identified the challenge of visibility in open-ended comments during the survey, including the following decision-maker in the utilities industry:

> **"Visibility [is an unsolved challenge]. Being able to see and understand the challenge of non-standard communications [protocols] and the ability to interrogate and see everything on the OT estate. Without sufficient visibility, asset management and protection cannot truly be achieved."**
>
> **– Utilities and Energy, Europe**

One of the ways in which industrial organizations can seek to get ahead of this challenge is through regular scanning of their networks – not just for the objects within them, but also for the existence of critical vulnerabilities. Encouragingly, data from this year's survey shows broad improvement on this metric compared with 2 years ago: 63% of organizations now conduct cyber security scans of OT networks at least twice a year, compared with just 24% in 2020 (see Figure 15, below):

15 Frequency of cyber security scans (security assessments) in OT networks



A rigorous process of asset discovery is also important in countering a threat inherent to all legacy technology – that of unpatched infrastructure. Industrial companies that are among the 'most impacted' by security incidents were 2.9 times more likely to identify the challenge of having 'a lot of infrastructure that we are unable to patch' when compared with the least impacted in our research sample.

This issue appears to be very clearly linked with outcomes when we also consider that the most affected firms were 6.3 times more likely than the least impacted to have suffered 'zero-day' exploits in their operational technology environments – that is, attacks that exploit vulnerabilities in outmoded software, firmware and other systems.

Unpatched and 'un-patchable' infrastructure was present in nearly all of the organizations we interviewed. Among survey participants that were able to provide a response:

- **92%** of firms reported at least **some unpatched endpoints**.
- **87%** had at least some nodes that were **unable to be patched**.

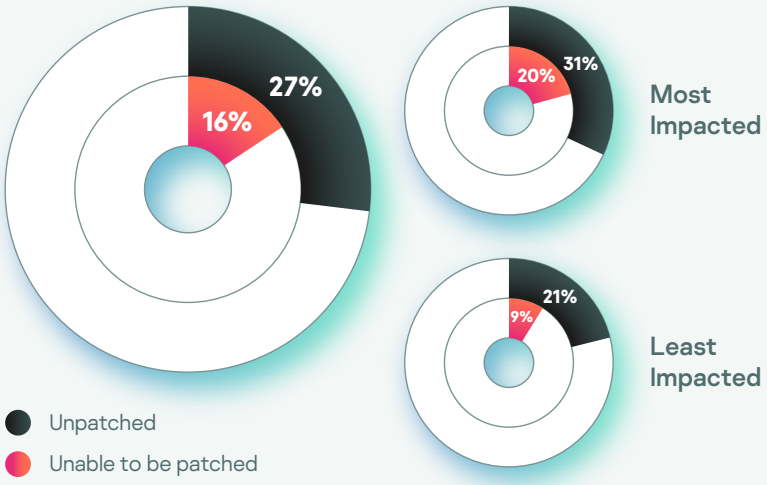
Added to this, there was also considerable uncertainty about the true scale of the issue: 30% of those responding were unable to provide even a broad estimate of the proportion of infrastructure that is either unpatched or unable to be patched in their ICS networks.

For those that were able to provide an answer, Figure 16 shows that over a quarter (27%) of all endpoints are currently unpatched in OT networks, with around 1 in 6 (16%) of all devices being unable to be patched. Once again, there are clear – and significant – differences between the most and least affected organizations on this measure. The least impacted firms have been especially effective in minimizing the proportion of their operational technology estate that is exposed to such issues (see also Figure 16)

16

Proportion of all endpoints that are unpatched and unable to be patched in the OT network

(Mean average of all endpoints)



However, eliminating these problems may be easier said than done: In the open-ended comments, we found repeated misgivings about the degree of security support provided by automation vendors:

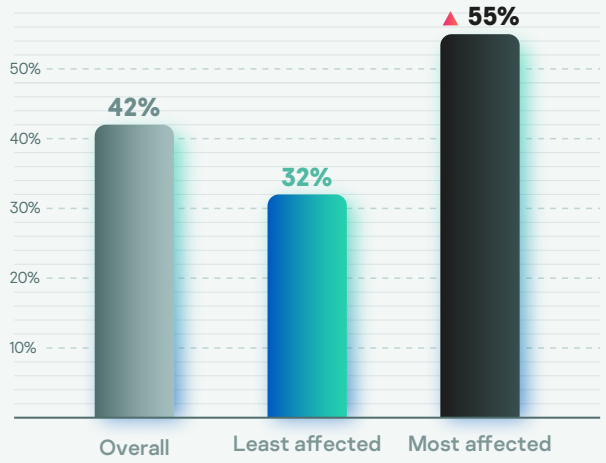
> **"Our largest issue with our OT and ICS is the equipment we own is that it isn't upgradable beyond the current level. The manufacturers don't offer any type of upgrade to our current systems. We are stuck on outdated platforms that are and remain vulnerable"**
>
> **– High tech manufacturing, North America**

4 Implementing solutions that are specifically designed for ICS environments

The challenge of legacy infrastructure explored in the previous section also lays bare an essential problem with how many firms approach ICS security – that the security solutions that many are using are not designed to account for the idiosyncrasies of operational technology.

In our survey we asked about the extent to which organizations felt they had any inadequacies or areas of industrial security that were under-financed. Overall, over 4 in 10 organizations (42%) confess to having areas that are not adequately resourced in terms of having ICS-specific security software, security assessments and/or staffing. Once again, this figure is significantly higher for the industrial firms most affected by cybersecurity incidents (see Figure 17).

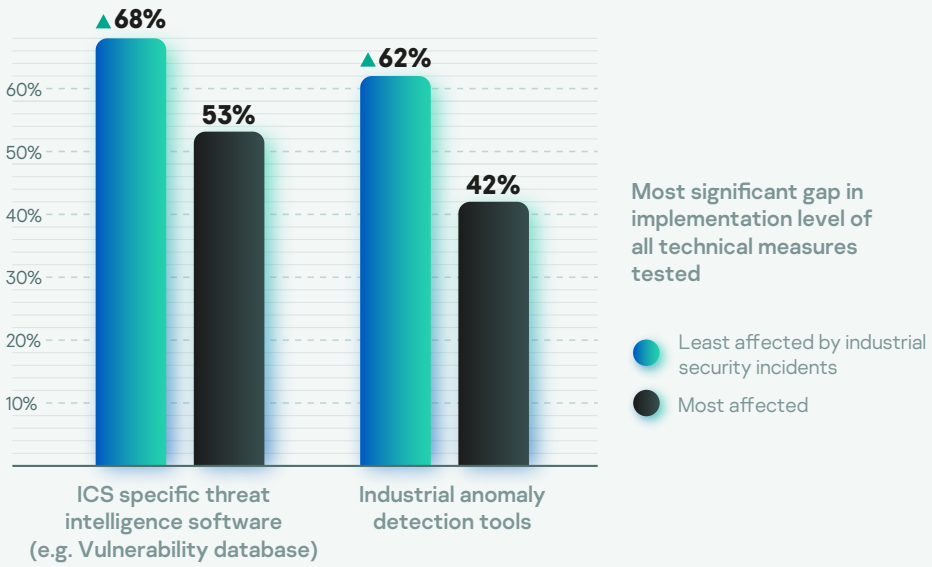
17 % perceiving inadequacies / underfunding of OT/ICS security software, security assessments and/or staffing



What, therefore, are the technologies that appear to be most effective in thwarting and mitigating security incidents in operational environments? Figure 18 (below) shows that 2 specific measures (out of 18 asked about in our survey) are significantly more likely to be implemented by those firms that are more successful in avoiding the most severe outcomes. What is notable about both of these measures is that they are technologies that are specifically-intended for industrial environments:

18 Implementation levels of selected ICS/OT technology measures

% implementing in each group. Those with the most statistically significant gap between the 'most affected' and 'least affected' are shown.



When implementing security solutions in operational technology environments, it is vital that organizations strike an appropriate balance between security and ensuring that production can continue unimpeded. Our survey findings revealed that:

- 40% of survey respondents stated that their current security tools were not compatible with their automation systems. This figure was even higher among the 'most affected' at 49% identifying this as a barrier.
- 38% of organizations can clearly recall cases where cybersecurity systems have **affected / interrupted** their operations
- Where this type of interruption occurs, almost **1 in 3 (30%)** of these firms resorted to turning off security systems when these conflicts arose

Given these challenges, it is important that the solutions used in industrial networks are designed specifically for those contexts. At the same time, the benefits of ICS-specific security technologies must also be made clear to those at the plant level. In follow-up conversations with research participants, one respondent identified this issue of 'translating the benefits' as being key:

> **"What are the benefits [of the security technology] to the plant manager, how does it improve quality and reduce waste and bring consistency? ...I'm not a plant manager, these are my guys trying to translate technology and outcomes from a technology point of view into raw manufacturing is quite difficult."**
>
> **– Manufacturer, Europe**

5 Having a strategy for IT/OT convergence, including IoT

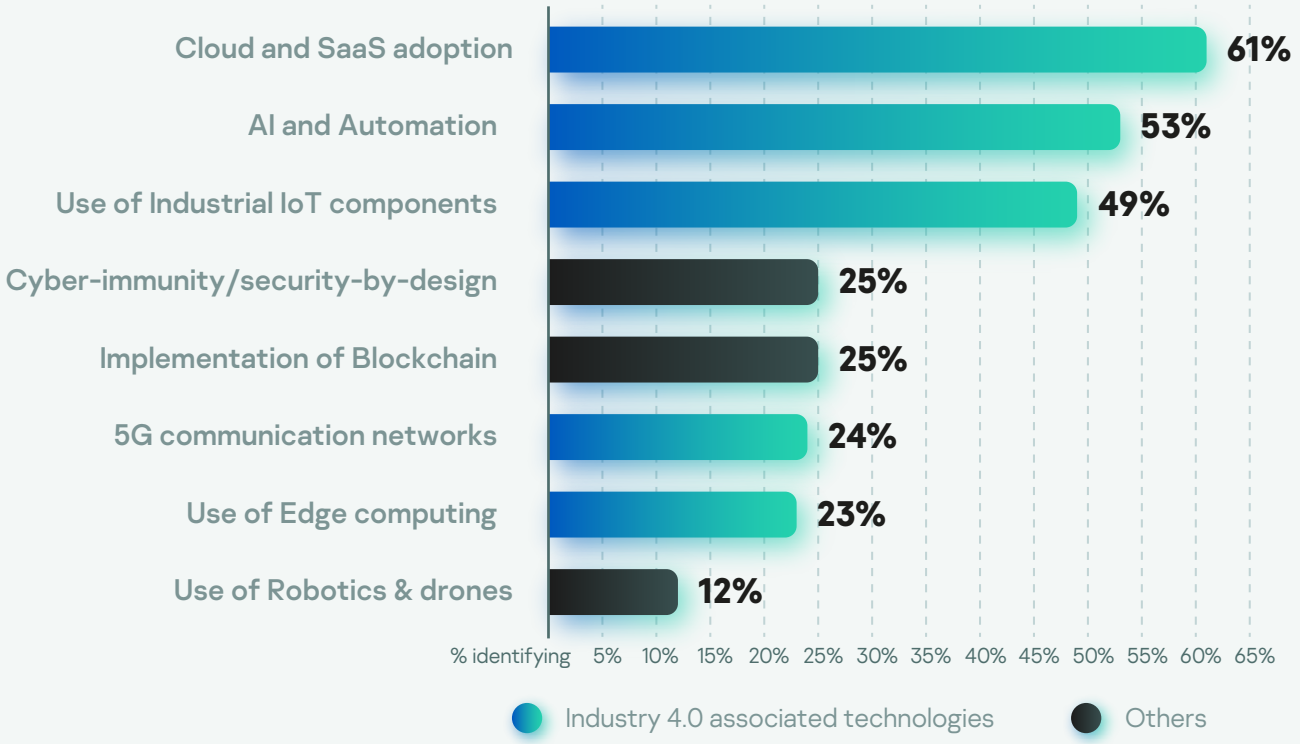
While industrial organizations need to have a clear approach for managing the considerable amount of legacy operational technology in their midst, they must also keep one eye on the future. Increasing digital transformation of production environments, and a push towards 'Industry 4.0' mean that increased convergence and integration between IT and OT environments will be necessary. In open-ended comments and during further discussions with respondents, this challenge was cited repeatedly, with a lack of coordination, confusion and inefficiency being potential issues if this is not mastered:

> The inefficiency of our employees working in an environment which has a combination of Information Technology and Operational Technology – it confuses the employees working in such an environment; they are not able to deal with data security threats properly.
>
> -IT / Integrator, APAC

> The biggest unsolved security challenge is the convergence of Information technology with Operational Technology – it increases security threats and IT personnel don't have much idea about how to handle them in a merged environment.
>
> – Manufacturer, APAC

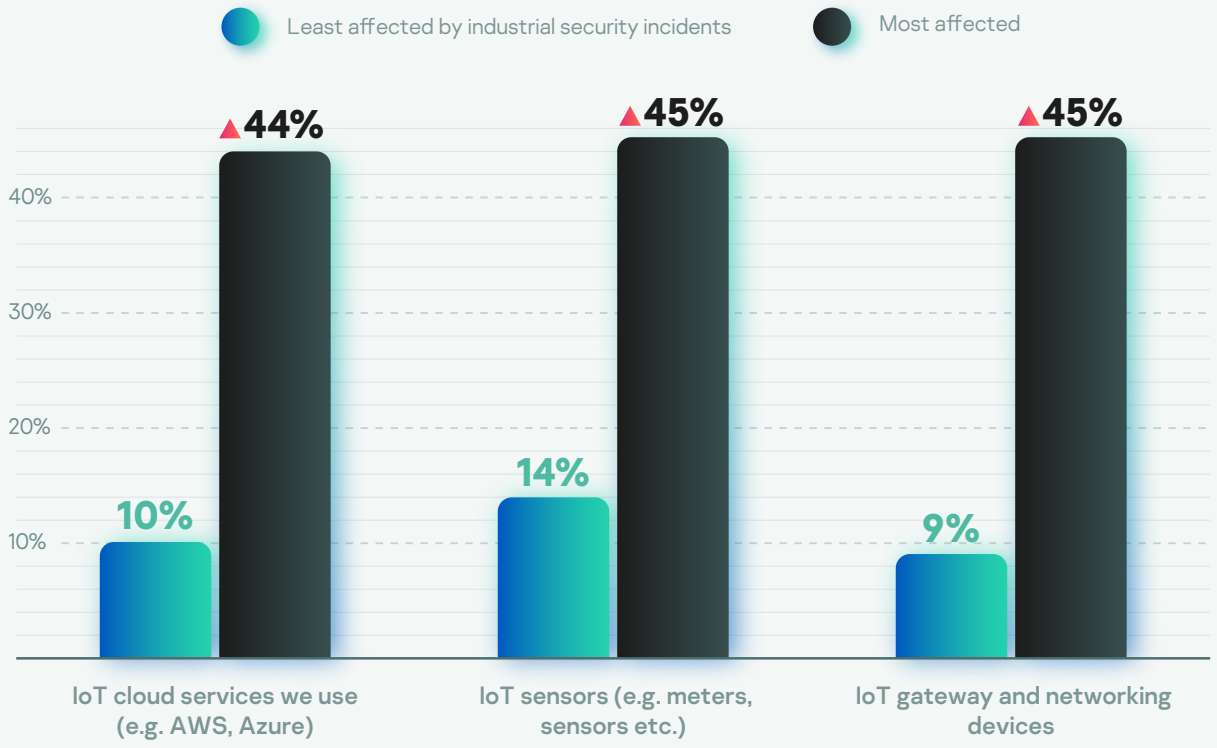
When looking at some of the issues that are having the strongest impact on OT/ICS cybersecurity, respondents identified several key technologies associated with Industry 4.0 as being drivers of this (see Figure 19, below), including the adoption of cloud-hosted systems, edge computing, 5G communications and the use of Industrial Internet of Things (IIoT) components:

19 Technical trends having an impact on OT/ICS security



If we deep-dive into the topic of IoT components specifically, Figure 20 (below) shows that when compared with the least impacted, the 'most affected' organizations were between 3 and 5 times more likely to have experienced a cybersecurity attack involving IoT public cloud services, IoT sensors and/or IoT gateways.

20 % of organizations experiencing attacks impacting the following types of IoT infrastructure



Ensuring a smooth and secure journey to IoT adoption is clearly challenging, and links back to success factor #2 which we identified earlier – that of being able to achieve greater internal harmonization between IT and OT teams. Part of this harmonization may also entail having a more coordinated series of security tools that bridges both worlds. As one respondent relayed to us:

> **"I believe we can be much more efficient and harmonize these [security] solutions: Instead of having 10 solutions solving similar problems, we have to eliminate this overlap in solutions and harmonize, probably go to three."**
>
> **– Consumer Goods Manufacturer, Europe**

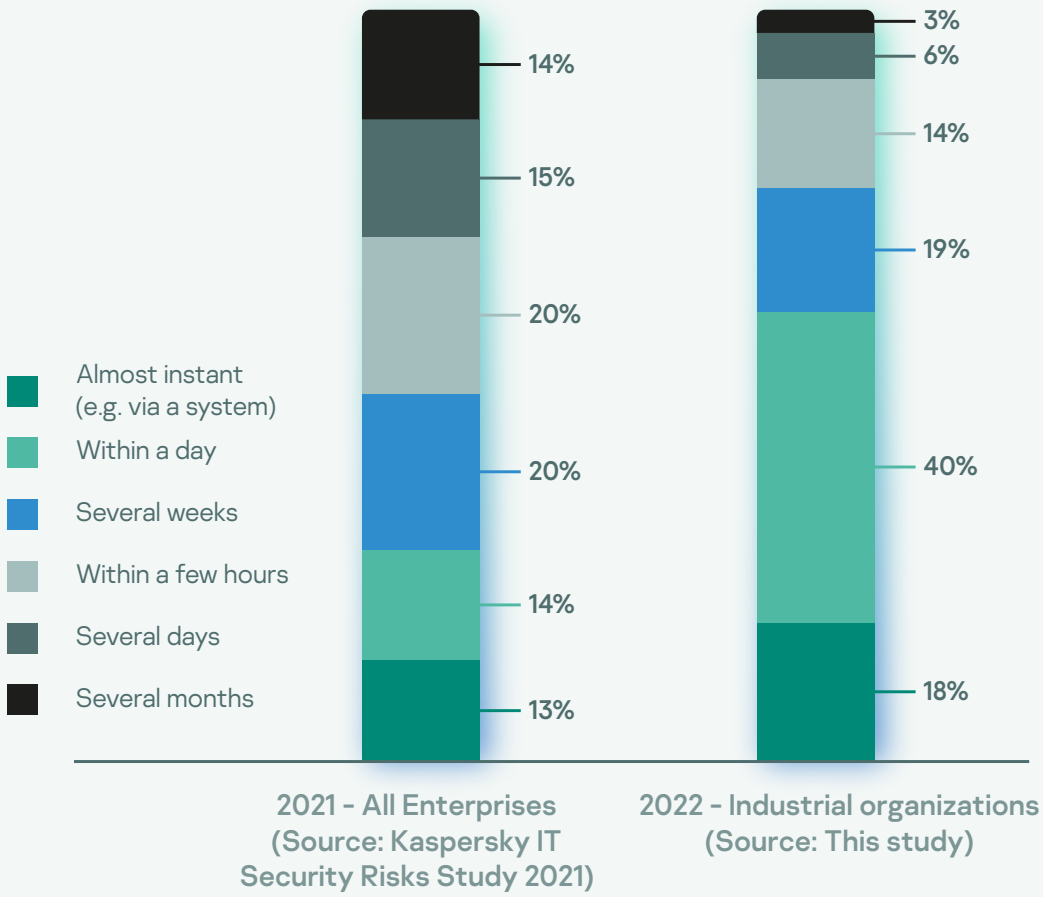
6 Being quick to respond when incidents occur

For all the preventative measures that an industrial organization may implement, security incidents in OT systems will, unfortunately, remain an inevitability. When cybersecurity events do occur, it is vital that these are detected, responded to, and remediated as quickly as possible.

Detection is the first component of this process: What is encouraging from our research is that companies with industrial and operational infrastructure are generally quicker than other large organizations at discovering incidents when they happen. Figure 21 shows that over half (58%) of firms are able to detect the threats that they are aware of within just a few hours. This compares favorably with other large enterprises surveyed in separate Kaspersky research, where only 27% were able to detect within this period.

21 Time taken to first detect incidents

Based on longest incident taken to detect

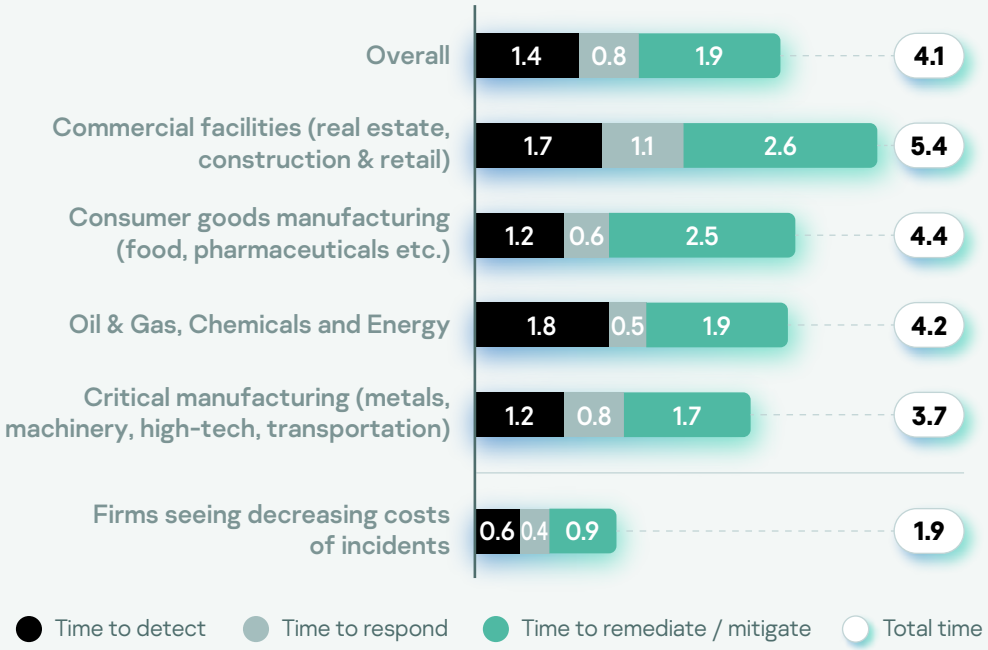


Beyond this initial detection period, we also asked about the time it took, on average, for organizations to respond and remediate / mitigate the issue. Figure 22 (below) shows that all stages of managing a 'typical' security incident take a combined average of just over 4 days to fully resolve. This total is broadly consistent across many industries, albeit organizations in the commercial facilities sector (responsible for building automation systems, among others) are somewhat slower to respond than others:

22

Average time taken to detect, respond, remediate an average incident

Figures are days



The bar at the bottom of Figure 22 is also notable – Organizations that are succeeding the most at limiting and reducing the cost of industrial security incidents are those that have significantly quicker incident resolution. When it comes to OT security, it seems, time is money.

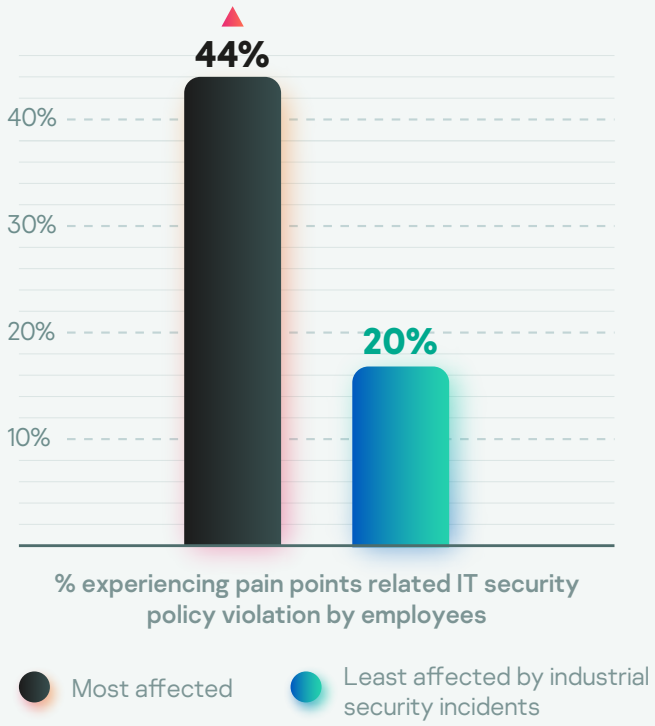
7 Taking staff training and compliance seriously

Our final key to success concerns the importance of embedding the correct, security-conscious behaviors within industrial companies and operators of critical infrastructure. 68% of organizations identified that they had experienced at least one incident that involved a breach of staff compliance, including:

- IT **security policy violations** (44% of companies reported)
- **Inappropriate IT resource use** by employees (36%)
- In more serious cases, **deliberate sabotage / industrial espionage** (16%)

Among all the challenges faced, policy violations by staff were significantly higher in companies that have seen the most severe security outcomes. Figure 23 (below) shows this difference very clearly:

23 Pain points and risks experienced relating to OT/ICS security management

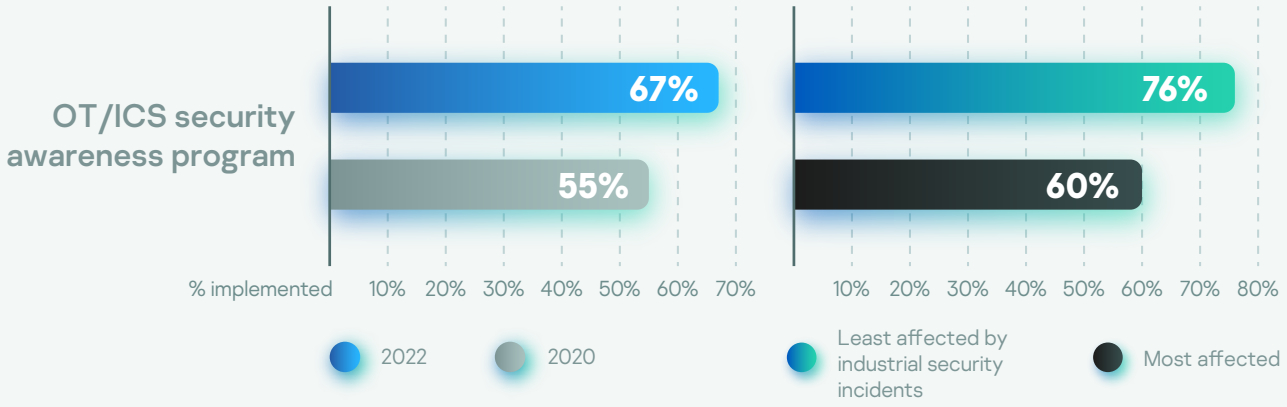


Ensuring that all levels of the organization exhibit strong 'security hygiene' is important in any large organization, but especially in companies where the knock-on impacts of a breach can be wide-reaching and result in severe physical harm. One transport operator recounted the following cautionary note:

> **It's bad enough to see a yellow sticky note with your username and password attached to an office computer. But what if there's one of those notes on a computer that, if hacked, can dump a hundred-ton object moving at 100 km/h into another large object moving at the same speed in the opposite direction?**
>
> **– Transportation & Logistics, Latin America**

In terms of acting on this problem, companies appear to be making reasonable progress. Compared to 2020, more firms now implement OT/ICS-specific security awareness programs, with up to 67% of firms embedding such measures in 2022 (Figure 24). On the contrary, of course, this also means that almost a third of organizations are failing to implement these essential courses:

24 Implementation level of OT/ICS security awareness programs



The impact of these programs on outcomes – along with all the other areas of best practice identified in this report – are clear: companies experiencing less severe ICS security outcomes are significantly more likely to implement awareness training (see also Figure 24).

Embedding industrial security best practices

In this report, we have seen that there are 7 clear themes for OT security that align with the extent and severity of incidents that occur. We can think of these 7 factors as a basis for the steps that any firms wishing to improve their industrial security posture should seek to follow.

When we review the performance of different industry sectors that operate industrial automation and control systems or other cyber-physical infrastructure, we see that there are certain success factors where more ground needs to be made up then others. In the table below (Figure 25), we summarize vertical-level differences from survey respondents, highlighting the top 3 ranked areas for improvement on which each industry sector should concentrate. This analysis is based on identifying where the greatest gap in capability or behavior exists for those that have been particularly affected by incidents in each sector.

25 Top priorites for improvement (based on the largest gap in performance for each industry vertical)

7 keys to improved industrial security outcomes	Industry vertical: Oil & Gas, Chemicals & Energy	Critical manufacturing (metals, machinery, high-tech, transportation)	Consumer goods manu-facturing (food, pharma etc.)	Commercial facilities (real estate, construction etc.)	Transport & logistics	IT & telecoms	Others
1 Having a well-resourced and appropriately skilled OT security team	1					2	
2 Ability to master the internal 'politics' of managing industrial security					1		3
3 Having a strategy for managing legacy infrastructure	3	3	3		2		
4 Implementing solutions that are specifically designed for ICS environments				3		3	2
5 Having a strategy for IT/OT convergence, including IoT	2	1	1	2			
6 Being quick to respond when incidents occur		2		1			
7 Taking staff training and compliance seriously			2		3	1	1

Numbers shown are the rank order of each priority area, based on the size of the gap (1 = Highest priority and largest gap; 2 = second highest; 3 = third highest)

Of course, these analyses are generalizations at the industry level. In practice, individual organizations will have markedly different levels of maturity and knowledge in each domain. Accordingly, cyber– and industrial security leaders should conduct their own in-depth audits to challenge their degree of preparedness for future challenges to come.

About Kaspersky Industrial CyberSecurity

Kaspersky Industrial Cybersecurity delivers a platform of natively integrated products and services designed specifically to protect the operational technology layers of industrial enterprises, without impacting on continuity or consistency of processes. Protected layers and elements include: SCADA servers, HMIs, PLCs, network connections and engineering work stations. The innovation and integrity of Kaspersky's approach to OT, ICS and IoT cybersecurity is centred around its ability to 'ground' enterprise best practices within the realities of industrial settings:

- the ability to provide EDR functionality starting with Windows XP
- IoC-based discovery on workstations
- active polling
- attack spread path visualization for root-cause analysis of critical incidents
- machine learning for anomaly detection
- protection of cyber-physical systems and technological process
- automated SCADA vulnerability assessment
- compliance audits.

Building an XDR solution with Kaspersky means customers can see the whole picture, resist attacks on all their assets, manage products from different vendors from a single console, respond more quickly to incidents, and reduce downtime.

Kaspersky maintains a high level of expertise in industrial cybersecurity, supported by Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT). It is a global project launched by Kaspersky in 2016 to coordinate the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the Industrial Internet of Things.

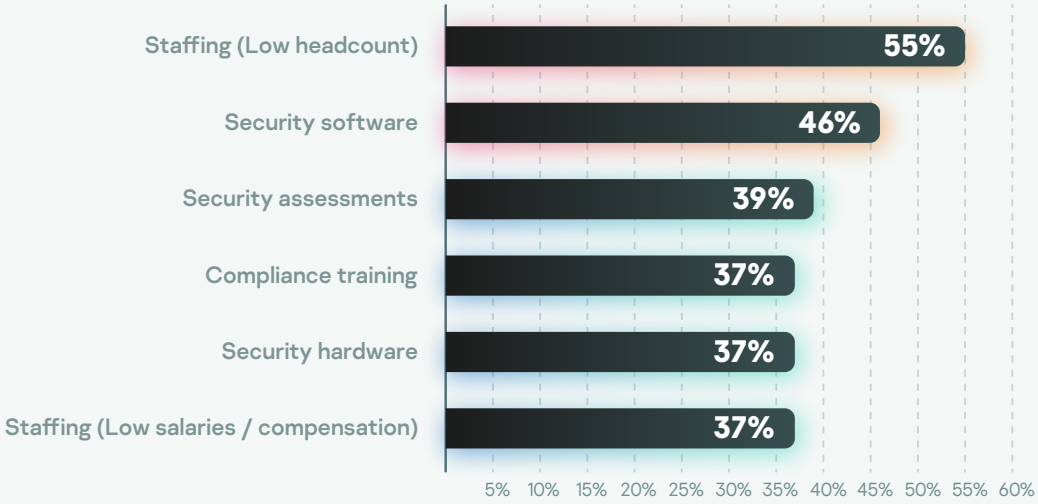
Learn more at:
ics.kaspersky.com

Contact us:
ics@kaspersky.com

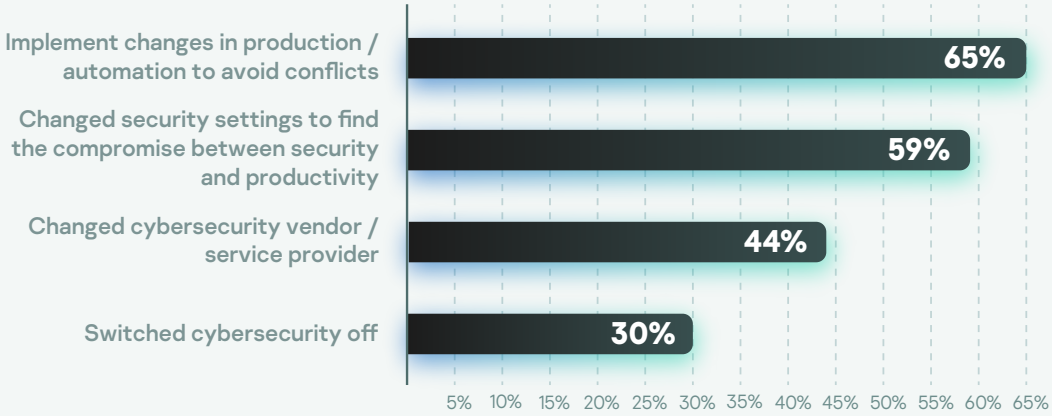
Follow us:
twitter.com/KasperskyICS

Appendix

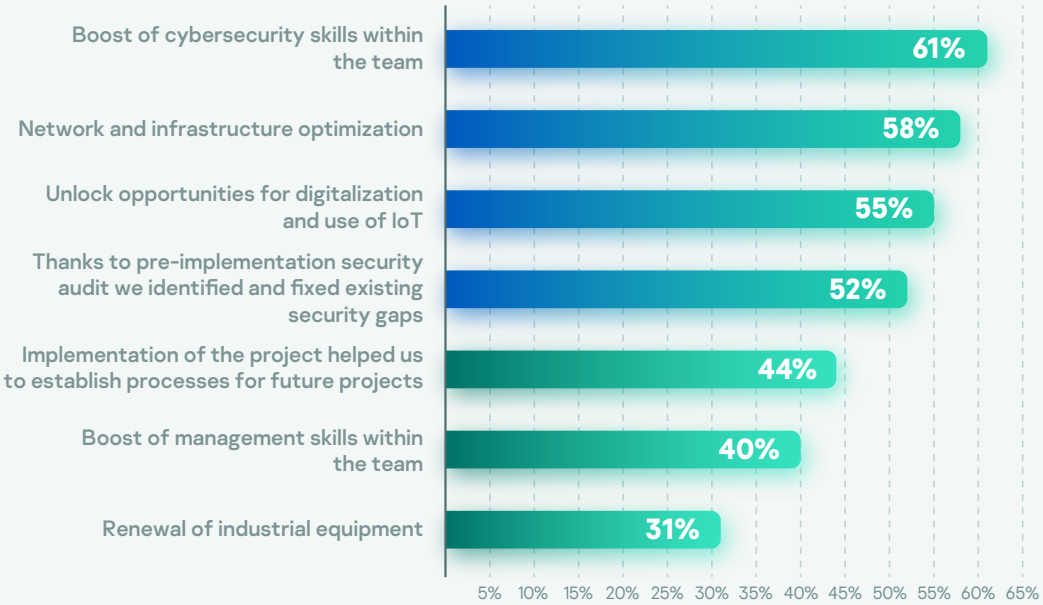
Areas of OT/ICS security considered to be under-resourced
(% of those mentioning potential under-financing issues)



Actions taken due to cybersecurity systems interrupting operations
(% of those reporting interruption to production / automation systems)

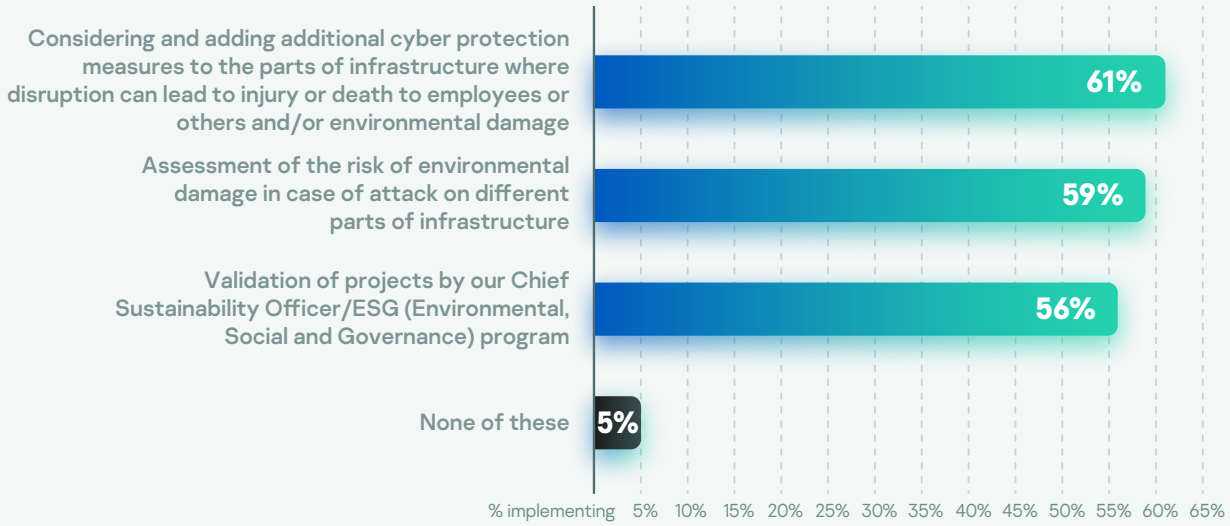


Positive side effects from OT/ICS security project implementation



Consequences of OT security intrusions / breaches tending to occur in respondent's company / industry

Implementation levels of measures to manage environmental risks associated with security incidents



www.kaspersky.com

© 2022 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.