ARC Advisory Group

kaspersky

THE STATE OF INDUSTRIAL CYBERSECURITY

July 2019

By Thomas Menze

CONTENTS

Survey Methodology **4**

Key Findings **5**

Survey Results **7**

- Priorities in Daily Business 7
- OT/ICS Risks 7
- ICS Cybersecurity Organizational Approach 9
- External Factors Affecting ICS Cybersecurity 11
- Attacks and Incidents 13
- What's Next? Future Strategy 17
- Future OT/ICS Cybersecurity Measures 20

Conclusions **21**

Appendix **24**

- Survey Methodology 24
- About ARC Advisory Group 26
- About Kaspersky 27

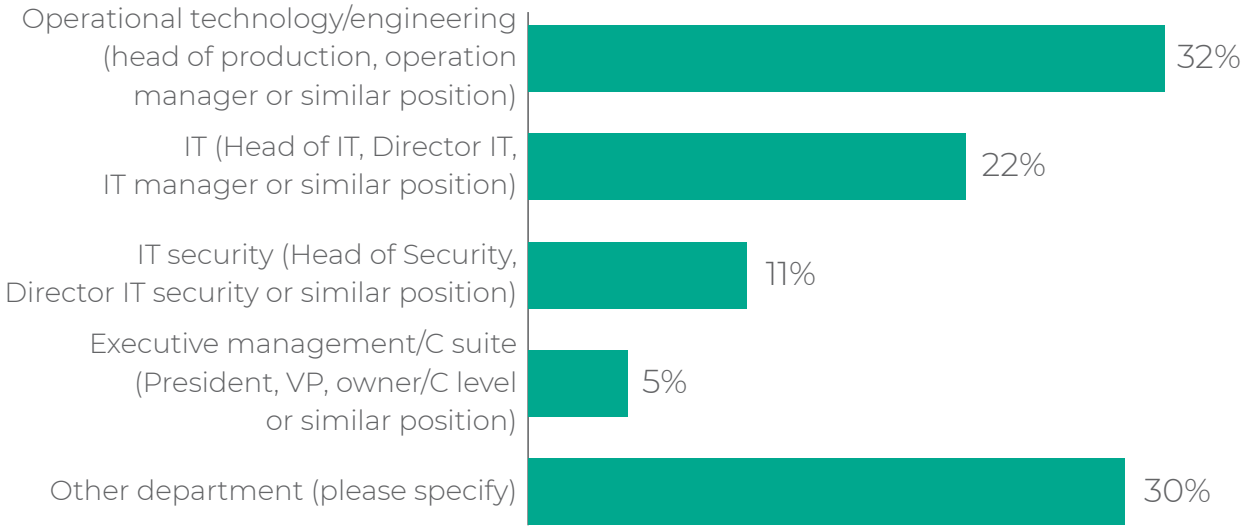
SURVEY METHODOLOGY

In spring 2019, ARC Advisory Group conducted a survey on the state of cybersecurity of Industrial Control Systems (ICS), as well as the priorities, concerns and challenges it brings for industrial organizations. The objective of the research was to understand the measures and processes involved in the prevention of cyber-incidents in industry.

This report explores the results of the survey and is a follow-on to previous ARC and Kaspersky surveys on ICS cybersecurity. 282 industrial companies and organizations across the globe were surveyed online, and 20 industry representatives were interviewed at trade fairs and ARC forums worldwide. The majority of responses came from companies in Europe, America and Asia.

Survey respondents and interviewees work in a variety of roles in critical infrastructure; such as energy and water supply, as well as in process industries, including oil, gas and chemicals.

Which of the following best describes the department that you work in?



About 40% of companies surveyed stated that they have not experienced any cyber-incidents within the last 12 months

KEY FINDINGS

1. Of the companies surveyed, more than 80% stated that operational technology (OT) cybersecurity is a high priority. However, only 31% have implemented an incident response program, while 37% said that such a process will be implemented within the next 12 months. This is a worrying situation because without a clear response plan, it is likely that the aftermath of a cyberattack could be mishandled. To ensure industrial companies put the appropriate measures in place, IEC 62443 describes procedures for handling a cyberattack which should be implemented as soon as possible.

2. More than half (52%) of the surveyed companies are aware of the need to provide more resources for OT/ICS cybersecurity. Depending on the criticality of the company, a wide range of budget sizes are allocated to OT automation. This results in a highly diverse range of security protection measures and opportunities to invest in more resources, such as systems and staff (ICS experts). Whilst the budget often allows for investment on endpoint protection or OT audits, a lack of experts remains a problem for the industry and resources are not being allocated to solve it.

3. How a company approaches cybersecurity often reflects their view of the entire industry. When talking to companies with well-defined OT/ICS cybersecurity processes, they believe that other organizations also have well-defined processes. In contrast, companies without clearly defined security processes believe that the entire industry needs to catch-up on how it approaches cybersecurity.

4. Four-in-ten (41%) companies surveyed stated that they have not experienced any cyber-incidents within the last 12 months, which is lower than the 51% recorded in 2018. While this appears to be a negative development, it is possible these companies simply were unable to identify all incidents in 2018. The higher use of intrusion detection solutions today may expose more cyber incidents than were visible in the past. Instead, it is more likely that they employ little or no anomaly detection to detect dangerous or suspicious network traffic.

5. Around 70% of companies surveyed consider an attack on their OT/ICS infrastructure likely. Despite this, many have yet to define their own approach to implementing OT/ICS cybersecurity.

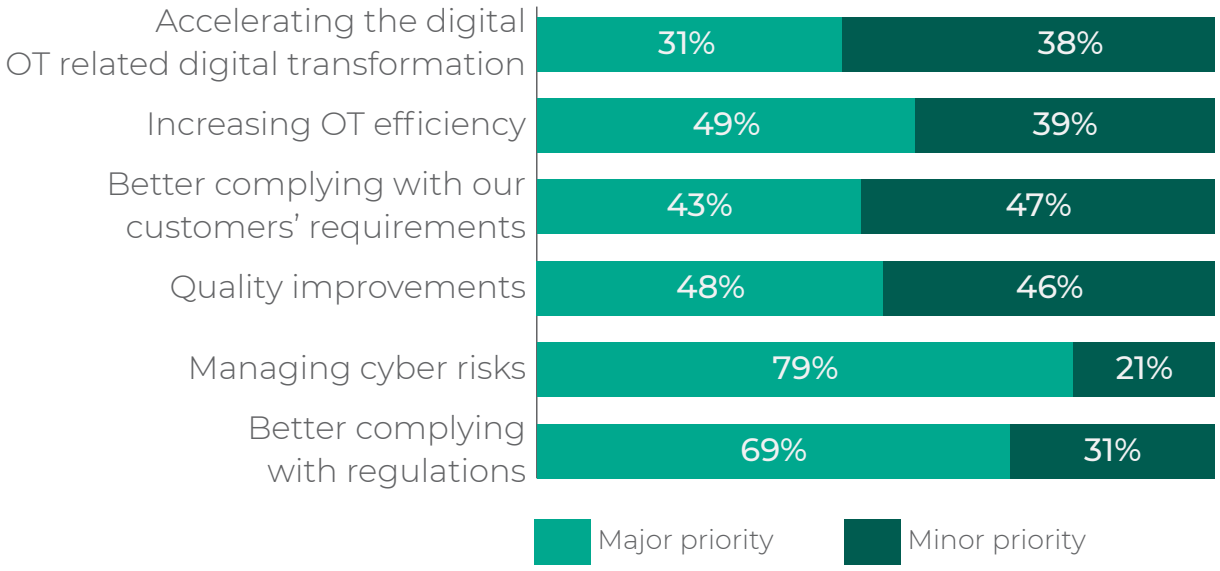
6. In many cases, a company's own workers pose a security threat. Unintentional actions by employees can lead to the disruption of OT/ICS automation. This is partly due to a lack of awareness, especially regarding new digital OT automation systems. Of the companies surveyed, nearly half (48%) indicate plans to invest more in training. Ongoing rather than one-off training, is an important security measure.

SURVEY RESULTS

Priorities in Daily Business

More than 80% companies surveyed consider OT cyber defense measures to be very important. More than half are currently working to carry out their digital transformation, to comply with regulatory guidelines and to meet customer requirements.

Which of the following initiatives will be a major, minor or no priority for your organization over the next 12 months?

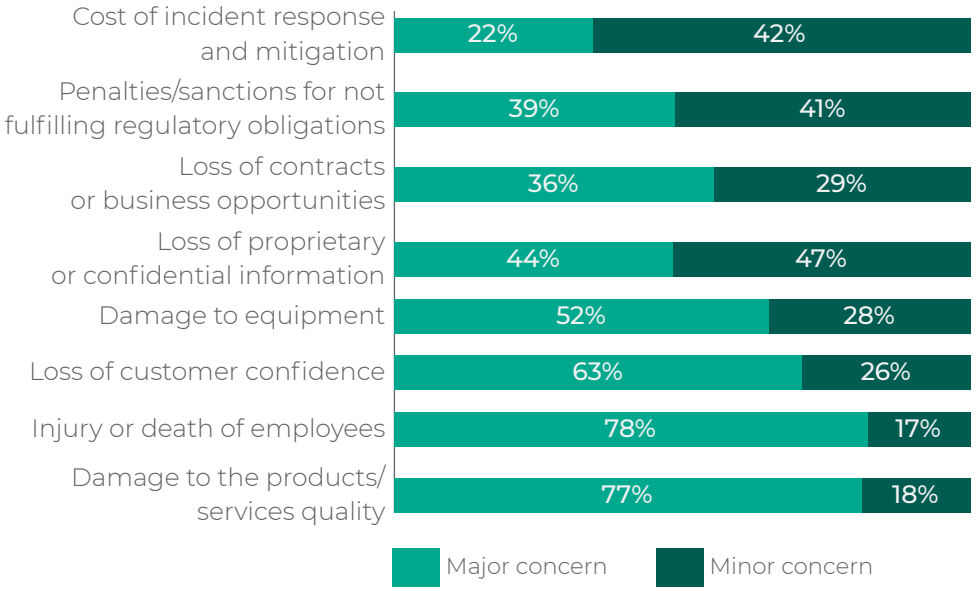


> In many discussions with managers of industrial enterprises, I hear that their own workers pose a threat. Unintentionally, employees may cause errors in the configuration, or during the operation, of the ICS. This situation can only be amended through awareness training,
>
> **Thomas Menze**,
> Senior Consultant, ARC

OT/ICS Risks

When asked to rank their concerns around an ICS cybersecurity incident, respondents primarily cited the health and safety of their employees (78%), as well as possible damage to the quality of their products or services (77%) as major worries, should the worst happen. The loss of customer confidence (63%) and possible damage to equipment (52%) were also rated as significant concerns.

Which of the following aspects will be a major, minor or no concern for your company in case of an ICS cybersecurity incident/breach?



> When we talk about ICS cybersecurity, many think about issues like anti-virus software, endpoint protection and other technical protection measures. However, we should also remember to make regular ICS backups. In addition, a defined process is needed to restore these backups.
>
> **An Energy Distributor**

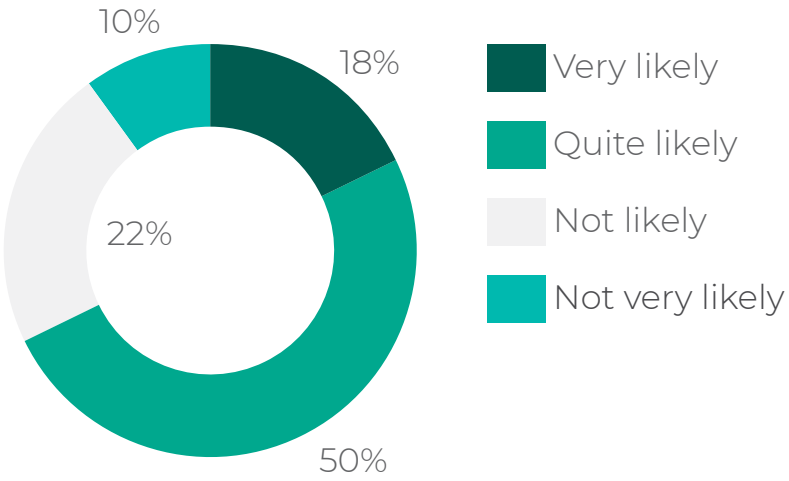
In-depth interviews with those in the industry show an increased awareness of the need for OT/ICS security. Respondents tell us that internal security training and the implementation of standards and regulations have become more frequent. More than half (59%) of interviewees named health and safety, and damage to production equipment as their highest priority behind adopting OT/ICS cybersecurity.

To understand how secure they are, 67% of the companies surveyed carry out regular cybersecurity assessments. In general, companies strive to prevent cyber-incidents and minimize their impact, as this is more cost-effective than re-commissioning systems following a successful cyberattack. More than two-thirds (70%) said they expect to receive higher budgets for security audits and incident response in the future. Thanks to the availability of the IEC 62443 international industrial security standard, companies can now implement best practices, using standardized methodology to audit and verify their industrial networks.

ICS Cybersecurity Organizational Approach

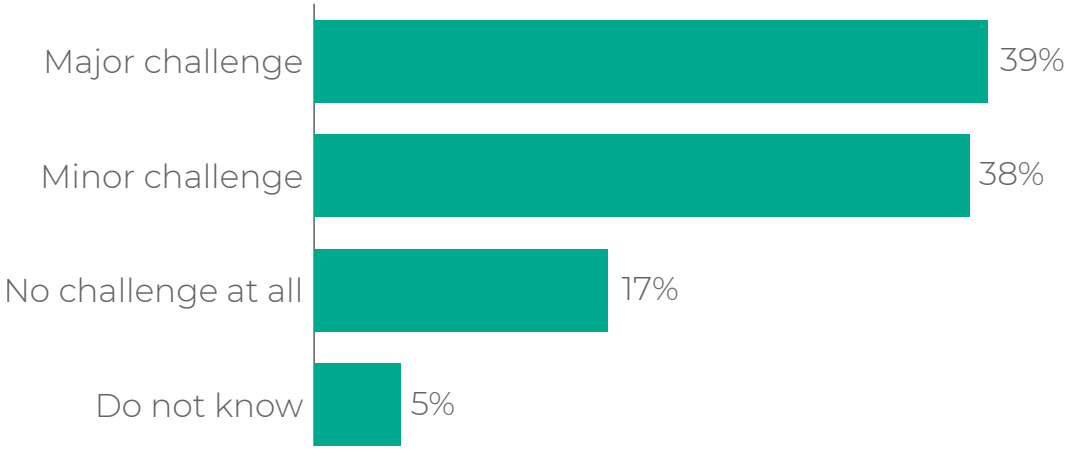
When self-assessing their OT/ICS security risks, more than 60% of companies surveyed consider themselves likely to become the target of an attack. But what are the potential sources of cyber-attacks and why is this risk growing?

How likely is your organization to become the target of a cybersecurity incident involving ICS or industrial control network?



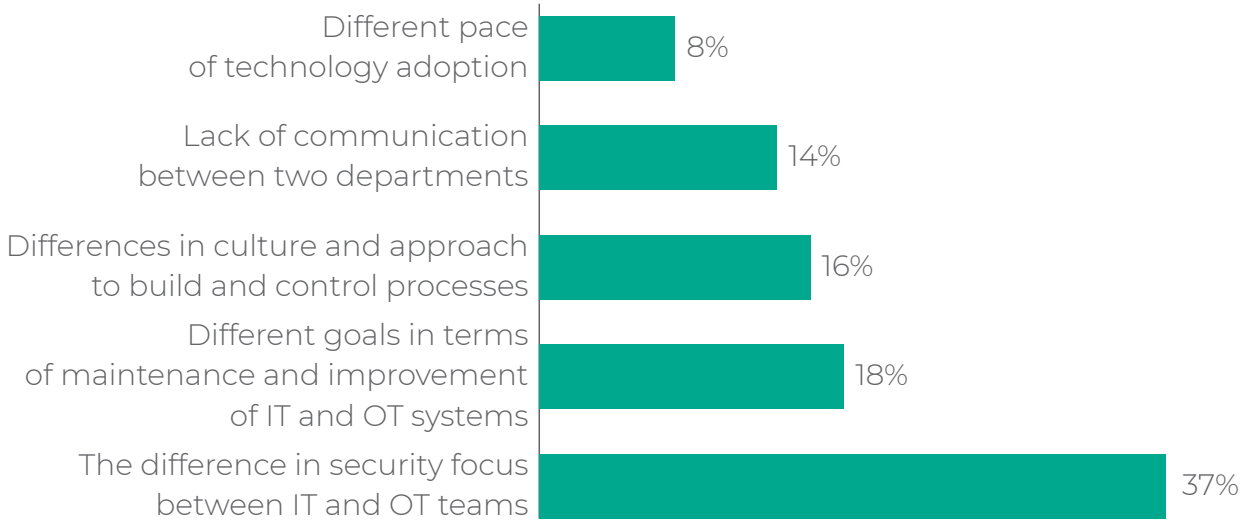
Many companies today feel threatened by malicious software. As digitalization increases the number of internet connections, the likelihood of being attacked grows – a fact that unsettles many plant operators.

Is increasing interconnectedness with corporate/enterprise IT a major, minor or no challenge related to managing your organization's OT/ICS cybersecurity?



Nearly 80% of companies surveyed regard the growing interconnectedness of OT and IT as a challenge. This is a result of the digitalization of OT, especially of industrial networks, which can expose industrial systems and devices that might not be adequately protected to cyberthreats. IT and OT teams often have different security priorities, and different goals for maintenance and improvement of their systems. In addition, cultural differences and the lack of communication between departments can exacerbate the problem.

You said that you see challenges to increasing cooperation between OT/ICS cybersecurity and corporate/enterprise IT. In your opinion, what are the main obstacles for this?

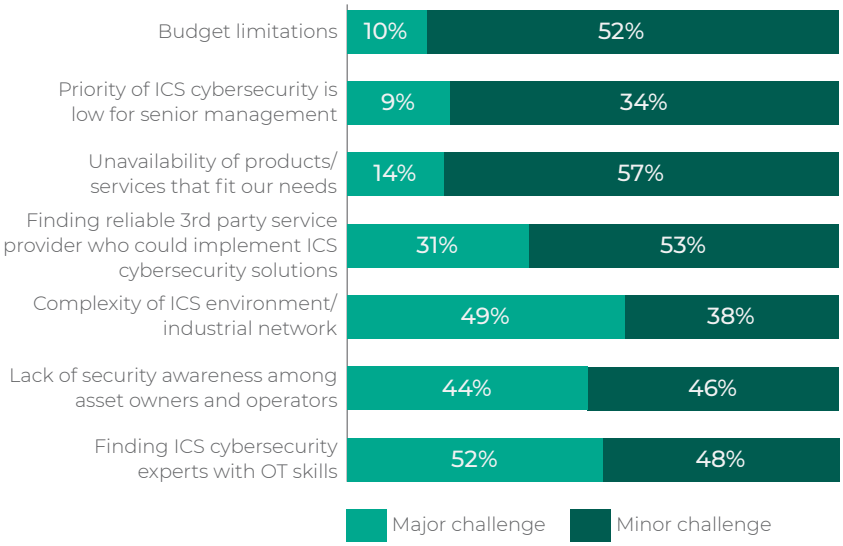


Cybersecurity Awareness

In personal interviews conducted for this study, a new challenge for OT/ICS cybersecurity emerged: the human factor. Many security managers have noticed that six to nine months after a successful security awareness training course, employees fall back into their old, dangerous patterns of behavior. To counter this phenomenon, companies should hold security awareness training courses on a regular basis.

The survey also showed that it is not easy to find ICS cybersecurity experts who have adequate OT knowledge. Facilities are threatened by the fact that there are too few ICS security experts. In addition, it is not easy to fall back on external service providers as there are too few available on the market.

Which of the following aspects will be a major, minor or no concern for your company in case of an ICS cybersecurity incident/breach?



> ICS cybersecurity is often seen as a project that is completed on a target date. Then all protection measures are tested and installed. This assumption is wrong because the protective measures must be tested again and again depending on the threat situation.
>
> **Russian production company**

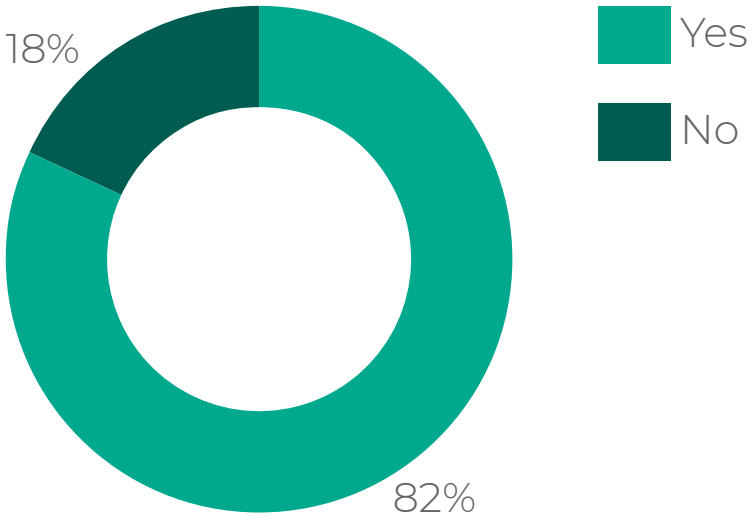
Comparing these results with the 2018 survey, it is clear that industrial companies are still not able to find enough suitable experts for adopting and managing ICS cybersecurity. This applies to employees as well as external security experts. To counteract this situation, new training opportunities should be created to make skilled personnel available. Otherwise, the situation will continue to worsen.

External Factors Affecting ICS Cybersecurity

For industrial companies in general, and especially for those involved in critical infrastructure, observing cybersecurity directives is imperative. Failure to do so can result in companies being accused of serious negligence. Even if failing to adhere to such regulation does not compromise security, this can still result in bad press and damage a company's public image.

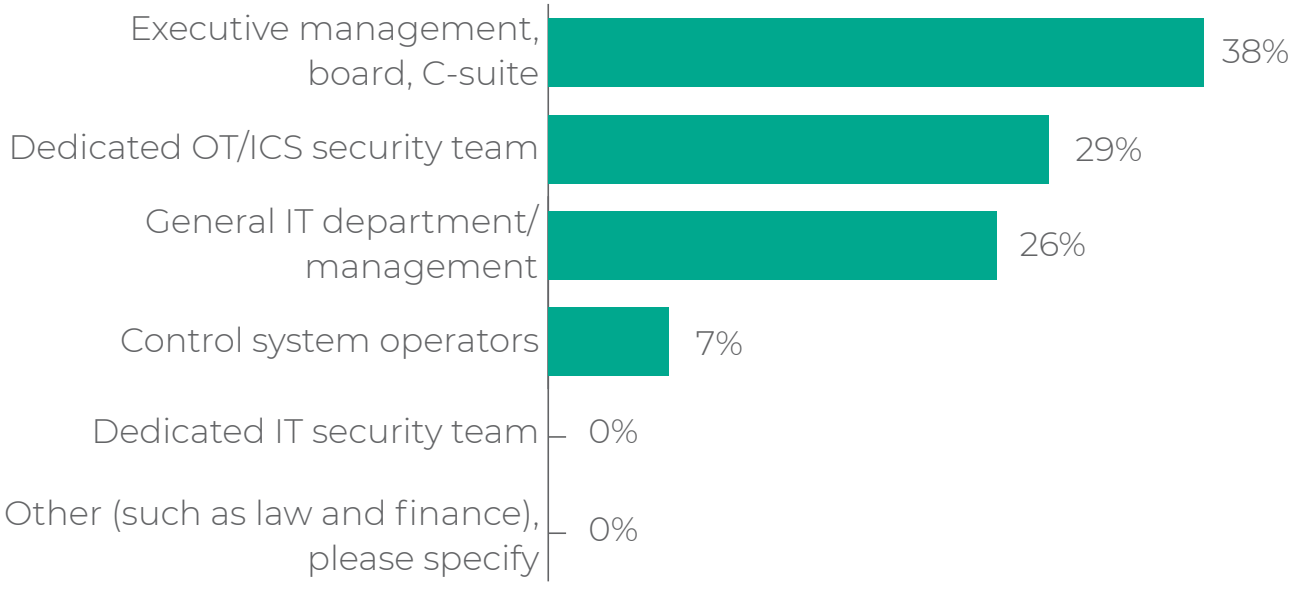
In the 2018 survey, only a quarter (23%) of companies reported compliance with mandatory directives. At that time, few companies besides those involved in critical infrastructure were obliged to follow binding directives. A lack of finances and available experts hindered the implementation of best practices or company-own standards. In 2018, awareness grew about IEC 62443, the directive that regulates IT security between the automation supplier, system integrator and end user. This standard provides companies with the tools to define their own cybersecurity processes.

Does your organization have an approved and documented OT/ICS cybersecurity policy/program?



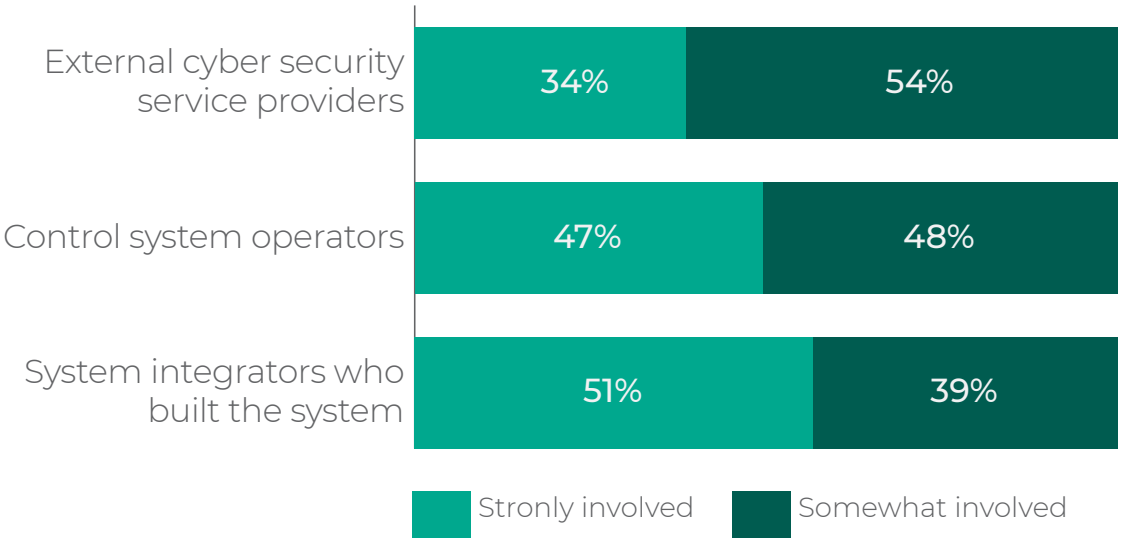
More than 80% of respondents stated that they have developed their own written OT/ICS cybersecurity standard. In 2018, this was only true for about 60% (62%) of the companies surveyed. Since then, customer compliance with IEC 62443 has grown.

Which of the job functions are involved in approval of a dedicated OT/ ICS security budget?



In most cases, internal teams with different roles and abilities are formed to drive the implementation of OT/ICS cybersecurity activities. Due to the lack of in-house experts, this work is often carried out with external system integrators or service providers. This type of teamwork or cooperation is recommended by IEC 62443.

Which of the following groups/players are strongly, somewhat or not involved when it comes to managing your organization's cybersecurity of ICS?



The objective of these security activities is to ensure compliance with regulations and policies, and to demonstrate to customers that companies are following a cybersecurity standard that ensures consistent quality of finished goods without any impact from cyber-incidents. This is considered a priority by respondents for the next 12 months.

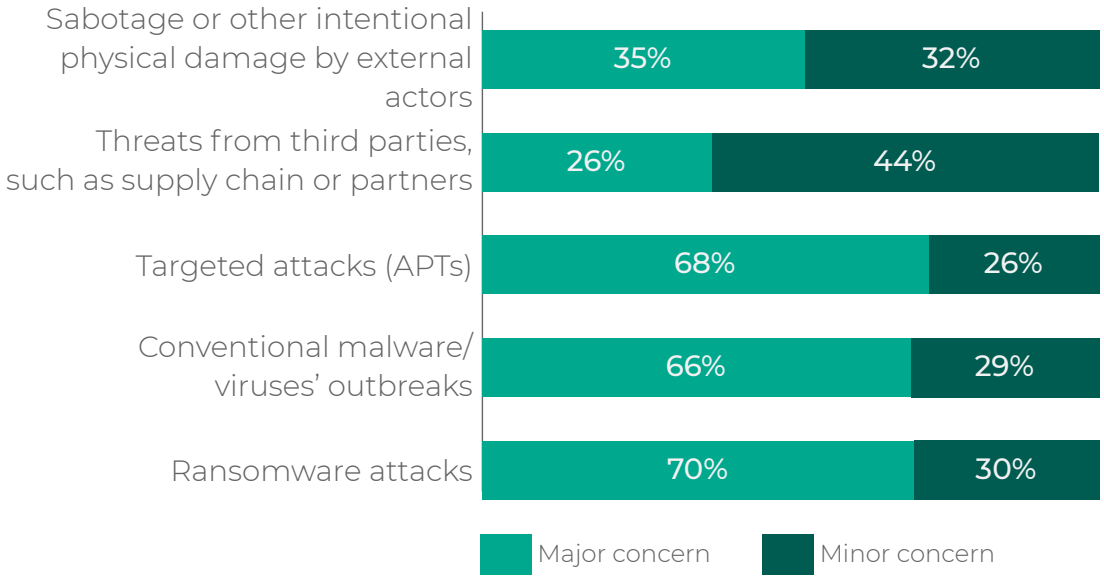
Attacks and Incidents

When analyzing the number of attacks or incidents that companies have experienced, it is worth noting that a subset of respondents still do not know the number of incidents they have experienced.

About 40% of companies surveyed stated that they have not experienced any cyber-incidents within the last 12 months, which is lower than the 51% recorded last year. While this appears to be a negative development, it is possible these companies simply were unable to identify all incidents in 2018. The higher use of intrusion detection solutions today may expose more cyber-incidents than were visible in the past.

Taking a closer look at the incidents that have occurred, ransomware attacks were cited as the greatest concern. In the 2018 survey, the greatest concern was malware or viruses. Advanced persistent threats (APTs) were recognized as the third greatest concern. The nature of cyberattacks are changing from undirected attacks to targeted attacks that expose companies to 'loss of control' or 'manipulation of control'.

Which of the following security incidents are a major, minor or no concern for your control system?

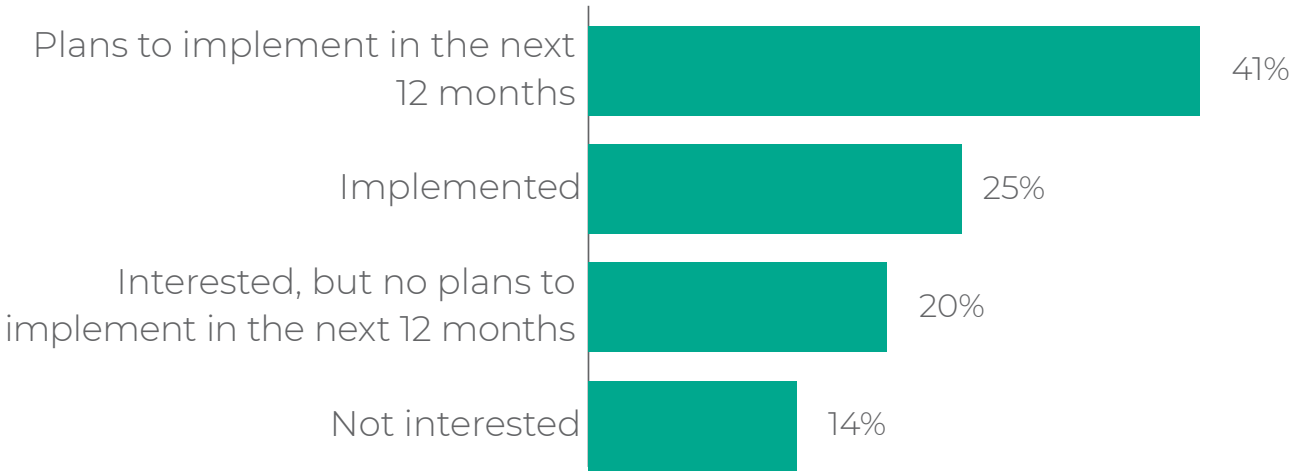


> Many companies overestimate their installed security measures. Just because no cyber-incidents have been observed over a long period of time does not mean that none have taken place. Perhaps the attacks are just not detected.
>
> **Oil & Gas Company**

With the increasing digitalization of OT/ICS environments, conventional malware attacks in the OT/ICS area cannot be ignored. Although more and more targeted attacks on companies are being observed, the danger from classic malware attacks is still present. For example, in 2019, a metallurgy company had to shut down for a week after a ransomware attack. According to the company's financial report, costs for the system backup and production downtime amounted to more than €50 million.

As the number of gateways to the internet grows due to digitalization, these may become conduits for viruses. A quarter of companies (25%) surveyed already use digital services in connection with OT/ICS automation, and another 40% plan to use digital services within the next 12 months. For this reason, protection against targeted and untargeted attacks has to be balanced with the need to provide data access to digital service providers.

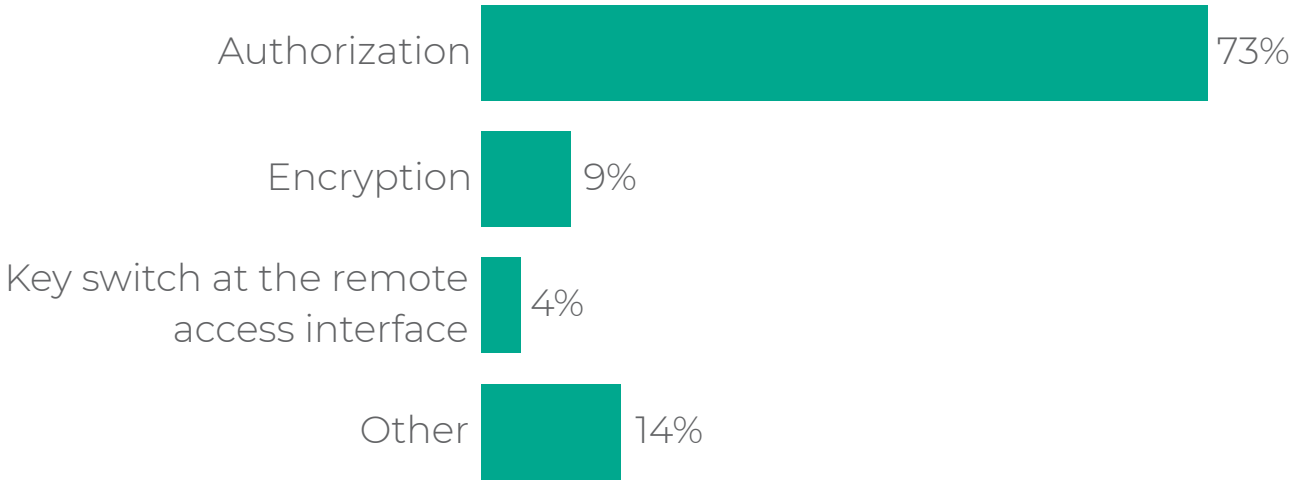
Is your company well prepared to use cloud services, such as pre-significant maintenance, data analysis or digital twins?



Almost 70% of respondents need to establish remote access to systems and equipment. Typically, this is intended to enable services for condition-based monitoring, real-time quality control, and monitoring of overall equipment effectiveness (OEE).

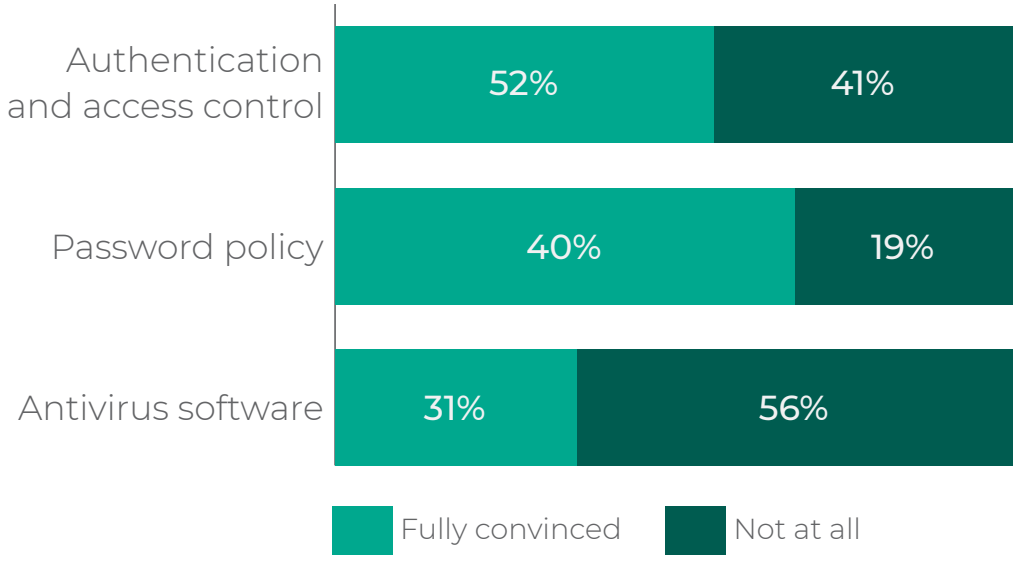
Digitalization means that systems and equipment are interconnected, so these connections must be secured by authentication and encryption. It remains to be seen whether these security methods are enough to protect networked OT/ICS systems effectively.

How do you ensure that remote access is secure?



When companies were asked whether or not they feel that these protective measures provide good security, more than 60% answered positively. Companies were most confident regarding their authentication and access control. In contrast, companies are not convinced that a simple password without dual authentication protection is sufficient to secure remote access.

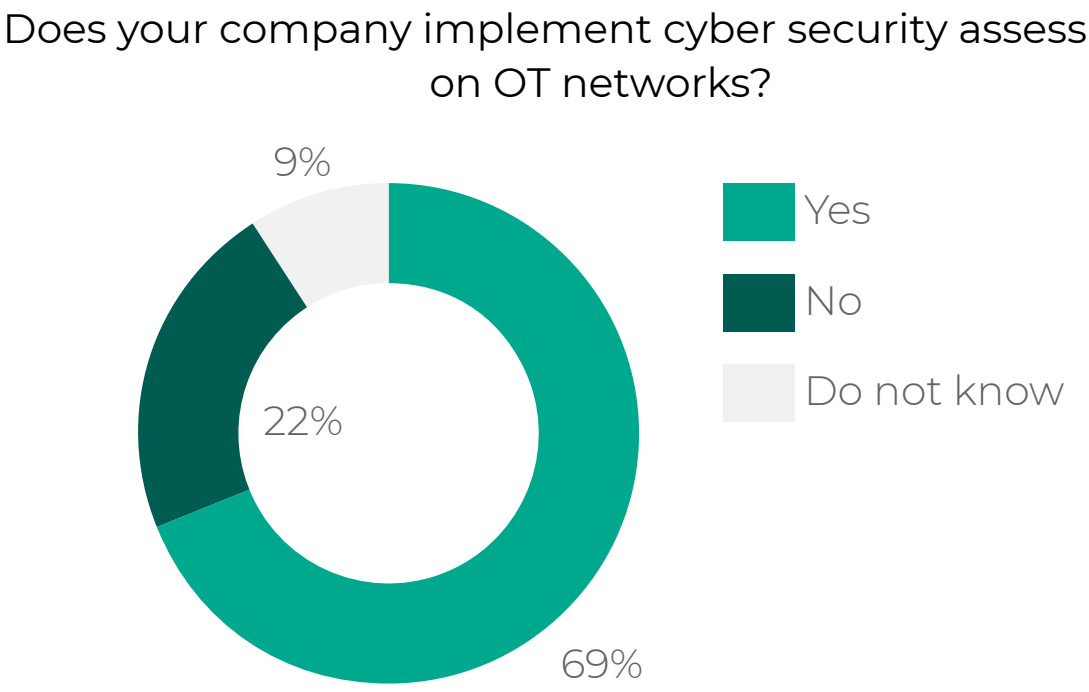
How convinced are you that the following basic protective measures are effective?



What's Next? Future Strategy

To address current and future OT/ICS cybersecurity challenges, companies must adjust their strategies, including decisions about personnel, budget and required technologies.

When it comes to securing the existing OT/ICS cybersecurity installation, an important question is whether companies are regularly reviewing the security of their automation systems. Nearly 70% said that they do.



When asked how OT/ICS cybersecurity budgets will be used in the future, interviewees reported on average a 10-15% increase for operator awareness training, endpoint protection, and OT/ICS security audits.

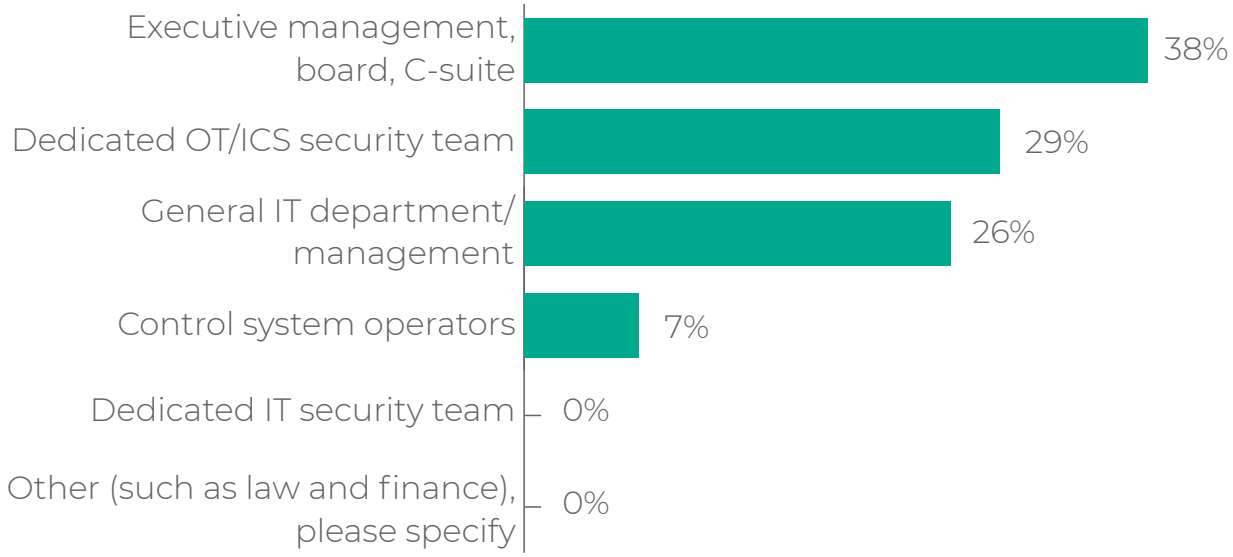
If digital services will be used increasingly in the future, then operators must be trained to deal with potential threats stemming from more connectivity. This is especially true when working with third party contractors who support OT networks.

Regarding security risks, the systems must be audited more thoroughly, which in turn offers justification for larger budgets.

According to the 2018 survey, cybersecurity solutions and training budgets were already growing, so industry digitalization apparently has little effect on the allocation of OT/ICS security budgets.

The decision of how much budget to allocate is, of course, up to management, but budget requirements are often pre-planned in internal task forces. Yet in many companies internal OT security teams make their own decisions regarding budgets, similar to IT departments. Those who we spoke to ruled out an inadequate budget as a reason for having failing to adopt adequate cybersecurity protection, so a lack of funds cannot be the main reason for insufficient OT/ICS cybersecurity.

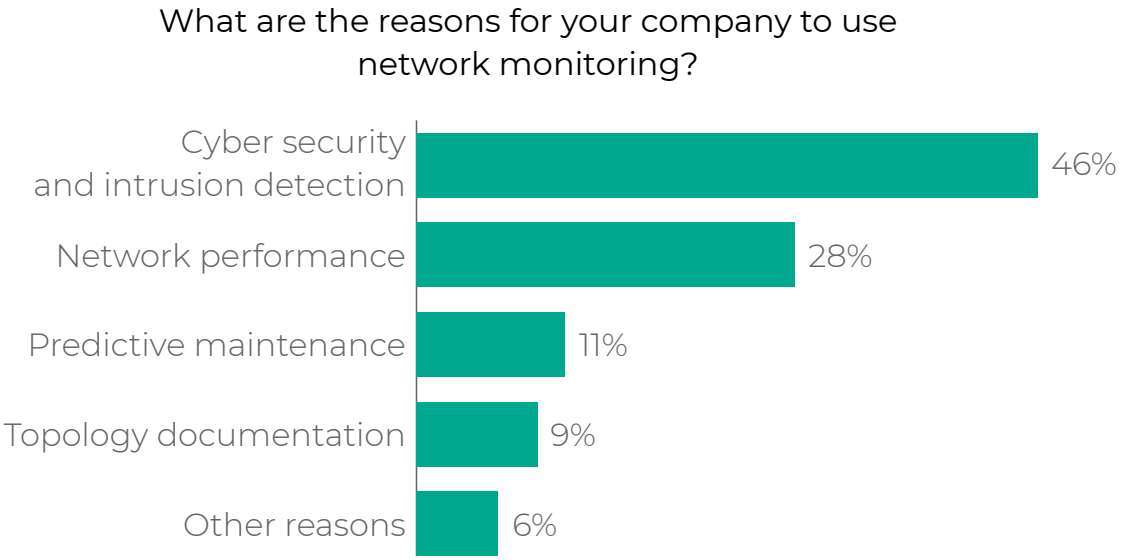
Which of the job functions are involved in approval of a dedicated OT/ ICS security budget?



In addition to having a general IT and OT/ICS cybersecurity strategy, several initiatives are vital to a successful OT/ICS cybersecurity approach.

In the 2018 survey, participants rated ICS security training as important. Training programs such as 'Incident Response Program', 'Security Awareness Program' and 'Security Compliance Program' ideally should be carried out before introducing ICS cybersecurity processes.. In the current survey, respondents questioned the effectiveness of such training programs. In practice, it is often the case that employees are trained but over time return to old, insecure patterns of behavior. Training should be ongoing to ensure theory is put into practice and knowledge retained and updated in line with the current threat landscape.

When it comes to implementing specific technologies, companies are favoring those that offer additional IT/OT security in light of increased network usage. These include technologies such as intrusion detection and network performance monitoring.



Future OT/ICS Cybersecurity Measures

With the landscape continually evolving, we wanted to understand how companies are planning for the future and what OT/ICS cybersecurity measures they are considering to put in place for the next 12 months.

> With increasing OT digitalization, the OT/ICS cybersecurity situation will become even more complicated. Current OT cybersecurity protection measures will probably no longer be adequate.
>
> **Metallurgy, Russia**

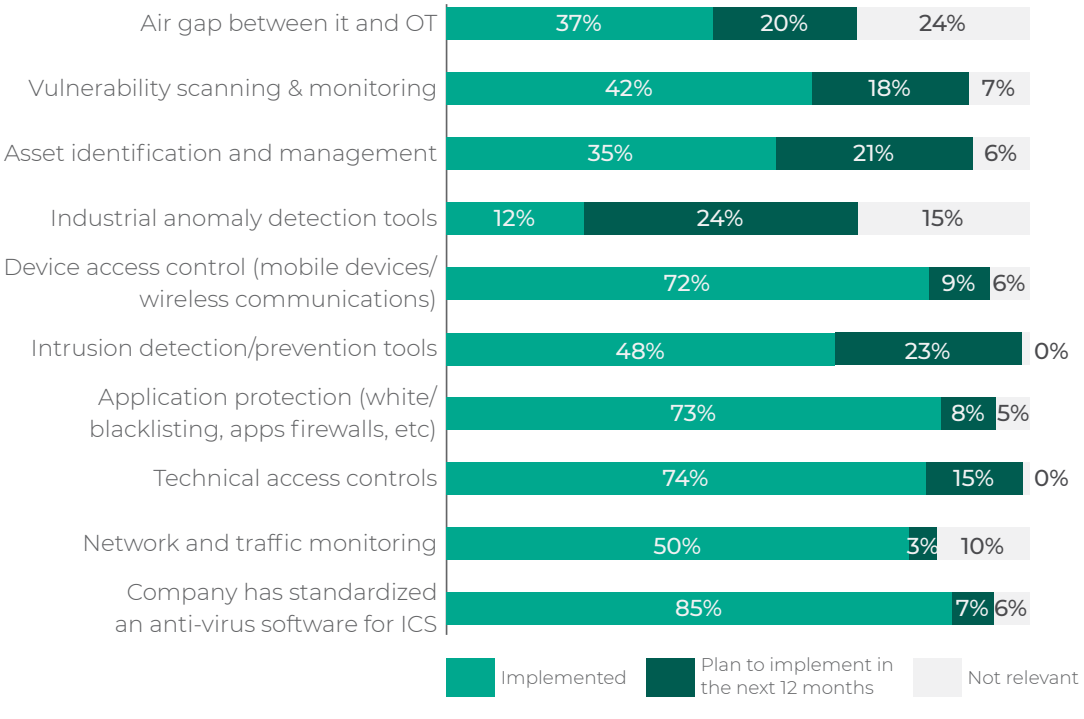
Technology-Oriented Measures

Technical measures planned in 2018 have now been implemented, including: the deployment of anti-virus software, access control for ICS workstations and access control for wireless devices.

So the question remains: which technical measures are planned for the next 12 months? Responses include technologies that offer an additional level of IT security within the framework of more secure OT networks. The most frequent solutions are OT network intrusion detection, industrial anomaly detection and OT network vulnerability scans.

Even though these technologies are commonly used in IT cybersecurity, they are still used much less frequently in OT/ICS cybersecurity. Yet, an early adopter trend is emerging.

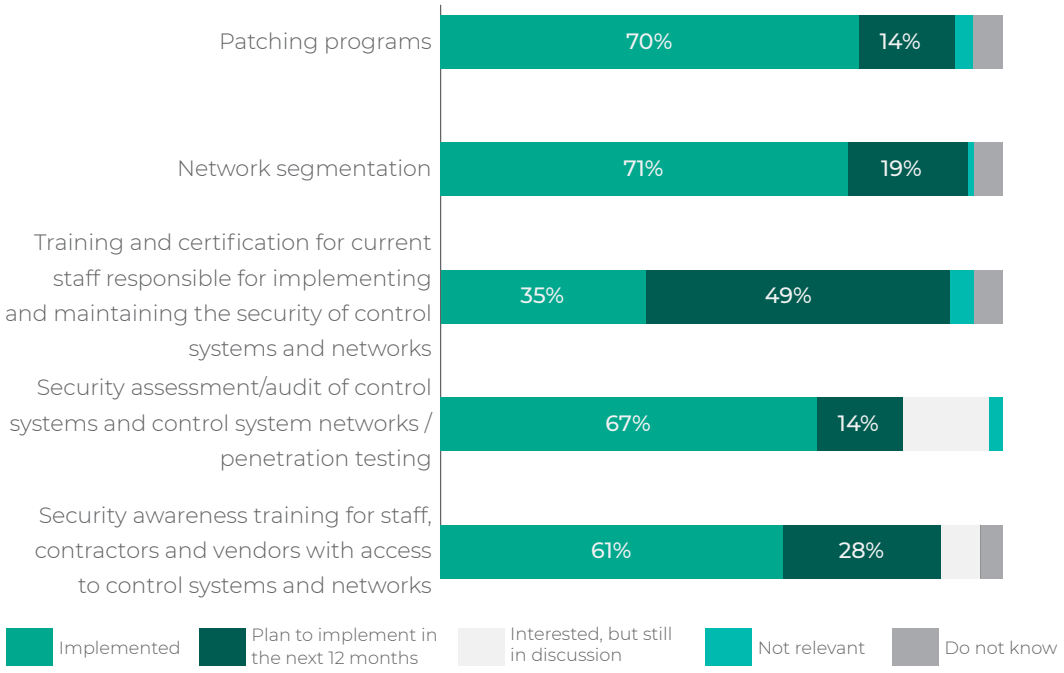
Does your organization have any of the following technology-oriented measures already implemented, is it planned within the next 12 months, is it of interest but still in discussion, or not relevant?



Process-Oriented Measures

When it comes to processes, safety awareness training for employees and subcontractors is standard today and is conducted by most companies surveyed. The same applies to effective network segmentation or patch management of automation components.

Does your organization have any of the following process-oriented measures already implemented, is it planned?



CONCLUSIONS

To keep up with the evolving nature of threats aimed at industrial organizations and the consequences of such attacks, it is clear that companies need to up their game. This includes offering advanced OT/ICS cybersecurity training courses, including the configuration and maintenance of OT security components or a process to introduce advanced patch management.

2019 will be the year of digitalization in OT automation. Companies will use digital methods to further improve their competitiveness, but this will also bring risks for the business. Although the consequences for OT/ICS cybersecurity are difficult to predict, these are likely outcomes:

- OT automation brings increased connections to the internet
- OT networks are becoming more sophisticated
- There are still not enough OT/ICS cybersecurity experts available on the market
- The number of attacks on OT automation will likely continue to increase
- Compliance with best practices and cybersecurity standards, such as IEC 62443, will become more important

> It is remarkable that companies with well-defined OT/ICS cybersecurity processes think that this is true for their entire industry. In contrast, companies without a clear definition of security processes believe that the industry needs to catch-up.
>
> **Dmitry Feshin,**
> ARC Russia and CIS

For this reason, new cybersecurity solutions must be increasingly implemented. Network performance measurement and anomaly detection should be added to the traditional cybersecurity 'defense-in-depth' concept. As a result of OT audits, new cybersecurity solutions should be added to harden the systems. Then, the effectiveness of these new cybersecurity solutions must be checked in the next audit. ARC recommends coordinating and maintaining protection through a central Security Operation Center (SOC).

The additional cybersecurity benefits of threat detection and response solutions are clear, but many companies already have more cybersecurity technology than they can manage. It is important to ensure that these solutions have features that deliver an immediate ROI, which can help users justify investments. For example, adding or linking additional, non-cybersecurity information to the results of asset discovery scans can help controls engineers avoid the tedious work of integrating various information sources.

ARC strongly recommends that companies develop their own cybersecurity strategy. This strategy should define the company's security level, as described in IEC 62443. The effectiveness of the cybersecurity strategy must then be verified in periodic audits. If the threat situation changes or other deviations are found in an audit, this strategy must be adapted accordingly. Staff should be taught how to conduct company specific ICS Cybersecurity Audits. ARC recommends coordinating and maintaining ICS protection through a central Security Operation Center (SOC).

Extending Solution Depth

Industrial control systems are known for their complex collections of specialized equipment of various vintages that are sourced from multiple vendors and communicate via a variety of industrial protocols. Solutions that secure all these control system assets would help manufacturers deal with the problem of integrated legacy OT equipment in modern IT architectures. Threat detection and response solution providers should include extensions of device coverage in product development plans and roadmaps.

Broadening Solution Capabilities

While important, detection of potential compromises only addresses one aspect of the problems that end users need to solve. Investigation and remediation of suspicious situations is equally important, and end users see value in solutions that include such support. According to the survey, 24% of respondents plan to introduce 'Industrial Anomaly Detection Tools' within the next 12 months, due to suspicious network communication being detected.

SOCs might prefer integration with popular SIEMs, but many companies rely upon plant personnel for initial investigation and blocking of suspicious behavior. These people often prefer a solution where all actions can be performed through a single platform. Integration of breach and anomaly alerts with operator alarm systems and compliance reporting tools (internal and NERC CIP)

When companies were asked whether or not they feel that these protective measures provide good security, more than 60% answered positively

are other capabilities that end users value. In the survey, 69% of respondents stated that they regularly perform a 'cybersecurity assessment on the OT network'. This is done with the company's own staff and should also detect and avoid suspicious network communication.

SOC Application Integration

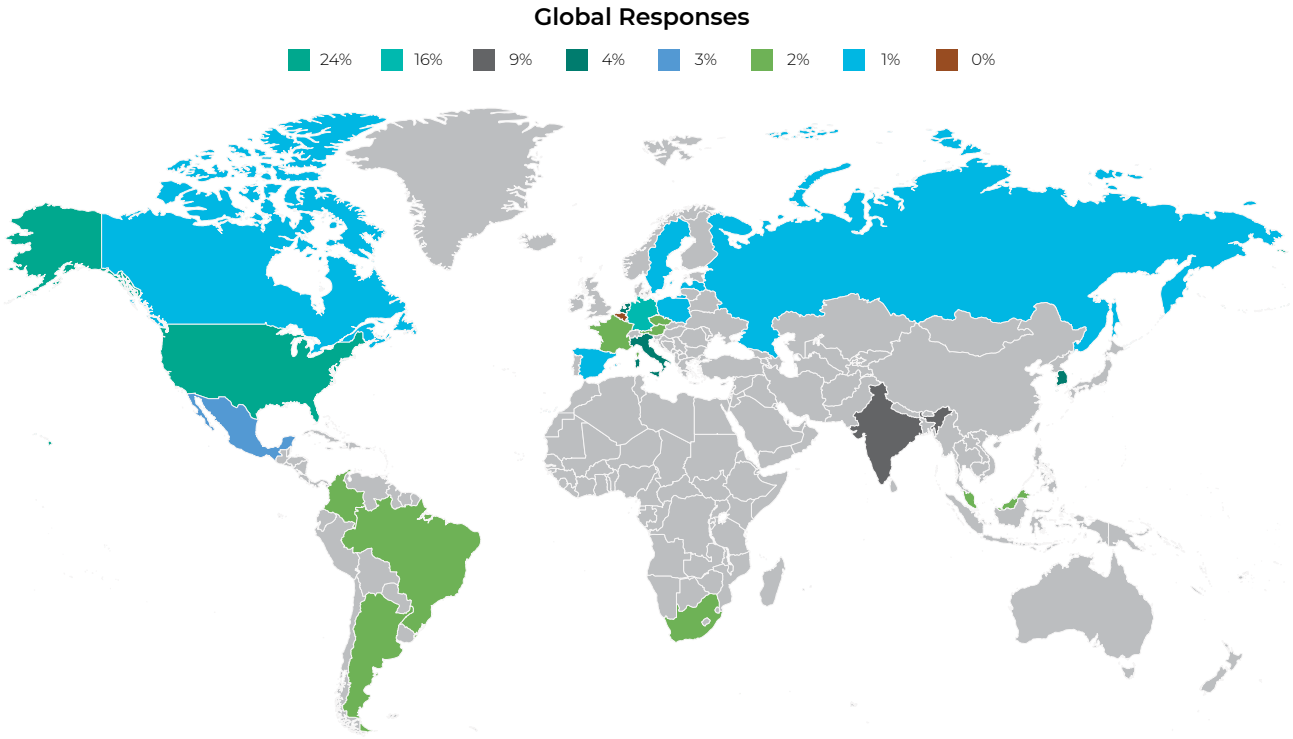
Industrial companies are increasingly moving towards integrated IT-OT cybersecurity strategies. CISOs and CIOs who are responsible for security across all of a company's cyber assets recognize the importance of addressing their OT security visibility gaps. They also see industrial/OT threat detection and response solutions as a means of gaining this insight. Survey respondents reported that budgets for security audit and anomaly and breach detection are growing by more than 50%. This is an indication that IT-OT cybersecurity strategies are growing closer together.

ARC recommends working with SOC to constantly monitor the threat landscape. Appropriate recommendations for protection can only be made when the SOC knows the threat situation. Here it makes sense to work closely with a security software provider that is aware of current threats. When threats are reported to the SOC, it can take appropriate measures that help the end user achieve a higher level of ICS cybersecurity protection.

APPENDIX

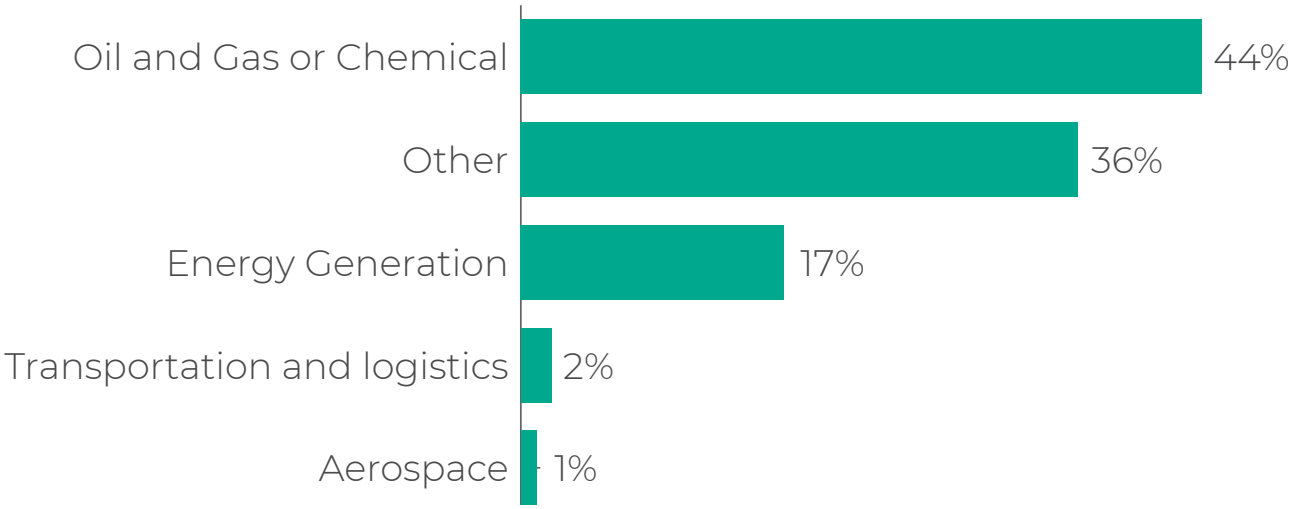
Survey Methodology

This survey was conducted on behalf of Kaspersky as a follow-on to previous ARC and Kaspersky surveys on ICS cybersecurity. 282 industrial companies were surveyed online, and 20 industry representatives were interviewed personally at trade fairs and ARC forums worldwide, covering Europe, North America, Latin America, the Middle East, and APAC.

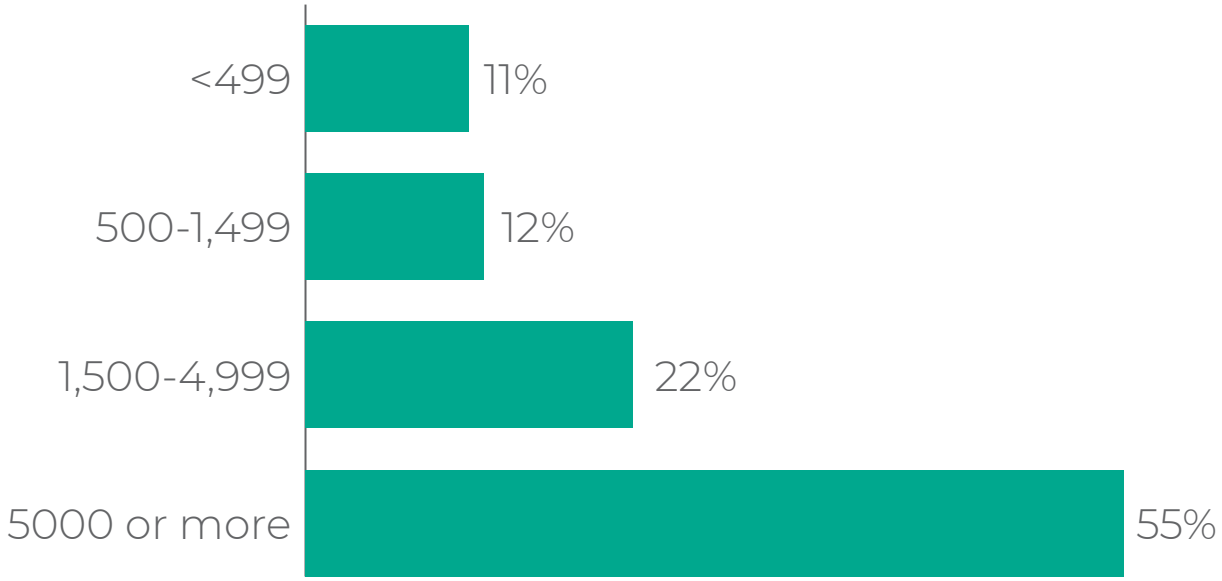


Survey respondents and interviewees work in a variety of functions in critical infrastructure, such as energy and water supply, as well as in process industries, such as oil and gas and chemicals.

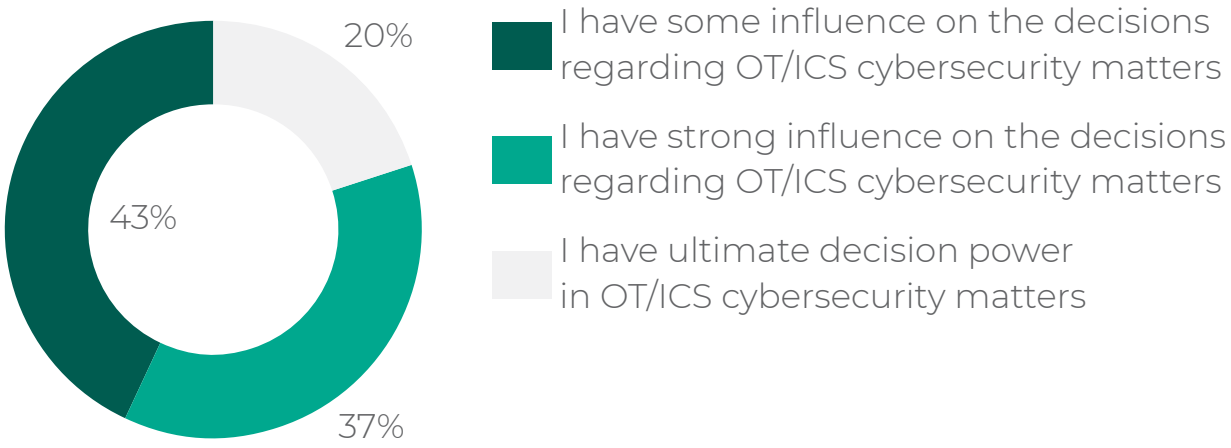
Which industry sector does your organization operate in?
(What is the main activity of your company?)



How many employees working for your company in total?



Do you have ultimate decision power
in OT control systems matters?
Or do you have strong or some, limited influence
in this decision-making process?



About ARC Advisory Group

Founded in 1986, ARC Advisory Group is the leading technology research and advisory firm for industry and infrastructure. ARC stands apart due to our in-depth coverage of both information technologies (IT) and operational technologies (OT) and associated business trends.

Our analysts and consultants have the industry knowledge and the first-hand experience to help our clients find the best answers to the complex business issues facing organizations today. We provide technology supplier clients with strategic market research, and help technology end user clients develop appropriate adoption strategies and evaluate and select the best technology solutions for their needs.

You can take advantage of ARC's extensive ongoing research plus the experience of our staff members through our Advisory Services. ARC's Advisory Services are specifically designed for executives responsible for developing strategies and directions for their organizations. For membership information, please call or write us or visit our website at www.arcweb.com.

ARC Advisory Group GmbH & Co. KG,
Stadttor 1, 40219 Dusseldorf, Germany

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997.

Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at **www.kaspersky.com**.

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.

Kaspersky Industrial CyberSecurity is a dedicated portfolio of products and services designed to protect operational technology layers and elements of industrial enterprises – including SCADA servers, HMIs, engineering workstations, PLCs, network connections – without impacting on operational continuity and consistency of industrial processes. Kaspersky Industrial CyberSecurity provides a holistic approach to industrial cybersecurity: from industrial endpoint protection and industrial network monitoring to training programs and expert services.

Learn more at: **https://ics.kaspersky.com**
Contact us: **ics@kaspersky.com**
Follow us: **https://twitter.com/KasperskyICS**

ARC Advisory Group GmbH & Co. KG,
Stadttor 1, 40219 Dusseldorf,
Germany