ARC Advisory Group

kaspersky

THE STATE OF INDUSTRIAL CYBERSECURITY IN THE ERA OF DIGITALIZATION

September 2020

By Thomas Menze

Contents

Introduction 3

Key Findings 4

How the pandemic impacted cybersecurity 4
Cybersecurity maturity model in the age of digitalization 4
Key ICS cybersecurity drivers 5
Gaps during cybersecurity implementation 5
Typical ICS cyberthreat challenges in 2020 5

Survey Results 6

COVID-19 impact: Home office working increased the number of external network scans 6
COVID-19 impact: How it will change security posture 7
Network segmentation and endpoint protection on their own are no longer sufficient 8
The current security workload will keep you busy 9
The real security budget decision-makers 11
Typical ICS cyberthreat challenges in 2020 12
Which departments are driving cybersecurity projects in ICS? 13
New cybersecurity threats result from digitalization initiatives 15
Gaps during implementation of cybersecurity measures 16
Environmental and gender-specific situations in cybersecurity teams 18

Conclusions and recommendations 21

Appendix 23

Survey Methodology 23
About ARC Advisory Group 25
About Kaspersky 26

Introduction

This year was a special survey year. With the coronavirus pandemic and the subsequent industry lockdowns, industrial cybersecurity methods were exposed to new challenges. With the help of the survey results, we have worked out the impact the pandemic has had on existing cybersecurity methods. An important trend is the ongoing digitalization of the industry. For many industrial companies, the key question is: 'How must the cybersecurity maturity model be adapted to provide effective protection in the digital age?' Another major topic was: 'ICS cybersecurity drivers & threat challenges' during the pandemic.

In contrast to IT security approaches for conventional IT networks, industrial control systems (ICS) and their automation components were never considered to be a potential security risk in the past. This attitude has changed in recent years. In the past, the causes of anomalies in ICS were often due to user errors or defective hardware and software.

Today, however, cyberattacks on ICS environments are no longer fiction but reality. According to Gartner[1], 100% of large enterprises plan to report annually on cybersecurity risks to their boards of directors in 2020 (versus 40% in 2019).

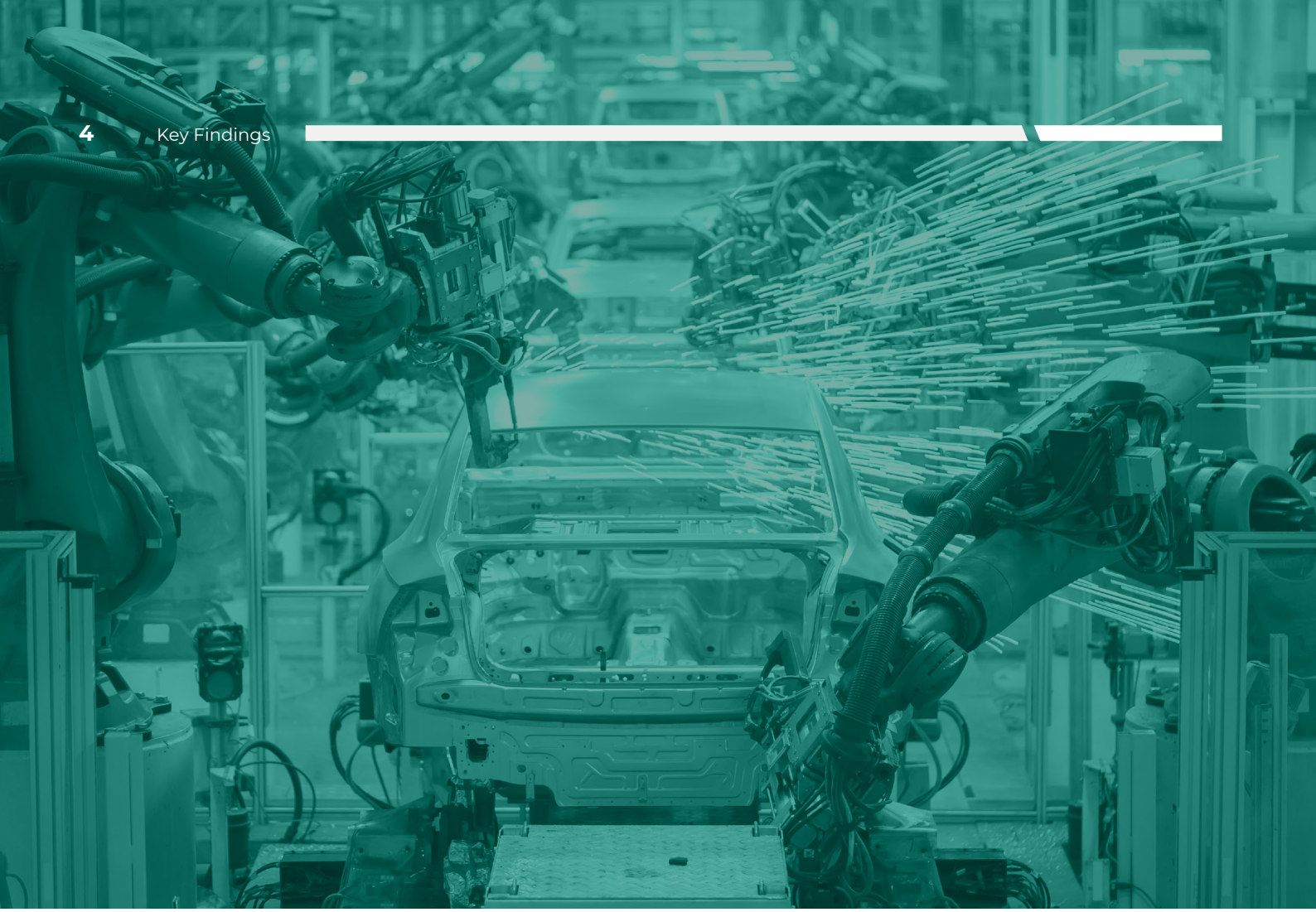
In the age of digitalization, ICS are connected to more and more components that, in turn, are connected directly to the internet. This makes it possible to communicate via the internet with automation systems, for example, in intelligent buildings, pipelines, or autonomous mobility.

In contrast to corporate networks that manage data, ICS manage physical processes. Physical assets can be manipulated or even destroyed by cyberattacks. Criminal organizations are now exploiting these possibilities as a business model. Users must protect themselves with new, modern security methods to detect attacks and initiate countermeasures.

This report explores the results of the survey and is a follow-on to previous ARC and Kaspersky surveys on ICS cybersecurity. More than 330 industrial companies and organizations[2] across the globe were surveyed online, and 10 industry representatives were interviewed at trade fairs and ARC forums worldwide. The majority of responses came from companies in Europe, North America, Latin America, Asia, and the Middle East.

1 https://www.gartner.com/en/information-technology/insights/cybersecurity

2 Survey respondents and interviewees work in a variety of roles in critical infrastructure, such as energy and water, as well as in process industries, including oil, gas and chemicals, and in manufacturing. About a quarter of the respondents work in ICS system integration, another 20% are responsible for the strategic management of ICS systems. This means that almost half of the respondents are responsible for the selection and configuration of ICS systems. The answers and assessments in this survey are therefore from professionals who are responsible for future ICS deployment strategies.



Key Findings

How the pandemic impacted cybersecurity

Many companies have changed the way they operate as a result of the pandemic, with 53% of respondents confirming that they have been operating with a remote workforce. This became a stress test for cybersecurity processes. As a result, 14% of organizations said they revised their cybersecurity concepts, and only seven percent stated that their cybersecurity strategy was sufficient during the pandemic. The increase in the number of remote workers drove up the number of OT network scan attempts during the pandemic. The result was that companies recognized the need to supplement cybersecurity procedures during exceptional situations.

Cybersecurity maturity model in the age of digitalization

Many companies expect certain benefits from digitization, such as improved efficiency. This is certainly possible, but interconnected digital devices influence the OT topology, so well-known ICS cybersecurity maturity models must be upgraded. 55% of respondents confirmed that their OT networks are checked for security issues at least once a year or more often. This suggests that the important principles for basic cybersecurity protection are in place. Furthermore, 44% stated that they work daily on cybersecurity initiatives for digital transformation.

Key ICS cybersecurity drivers

In many companies today, the deployment of cybersecurity budgets is decided in interdisciplinary teams. The reason for this is the complexity of ICS. The best way to find suitable protection measures is to consult experts from different fields. These include experts from IT, ICS, safety and production. 67% of respondents confirmed that such a team has more and more influence on cybersecurity decision-making.

Gaps during cybersecurity implementation

In the age of digitalization, communication inside OT networks often changes. It is therefore advisable to review security gaps in an OT network regularly. In particular, if a security vulnerability is discovered, why is the gap closed with a time delay, and are there regional differences? The most frequently mentioned reasons why a vulnerability cannot be closed quickly are undesired production stoppages (34%), approvals taking too long (31%) and too many decision-makers involved (23%).

Companies should appoint a responsible person to ensure that the identified security vulnerabilities are eliminated in a timely manner. These vulnerabilities represent a great risk and make it easy for attackers to manipulate.

Typical ICS cyberthreat challenges in 2020

As is the case every year, accidents caused by hazardous substances and deaths (32%) are globally recognized as the biggest challenges for ICS cybersecurity. For example, fatal accidents can happen in a company if safety systems are manipulated or switched off by cyberattackers. Naturally, these must be avoided at all cost. The points mentioned after are surprising: ‘damage of service quality’ and ‘loss of confidential information’, together with ‘mitigation costs’ are also seen as major challenges. This is different compared to last year’s survey, in which ‘mitigation costs’ played a subordinate role. This could be explained by the fact that incident mitigation now requires special, and sometimes external, expensive resources. At the same time, management is increasingly demanding more up-to-date cybersecurity as it becomes clearer how often companies are attacked, what a cyberattack can cost, and the effect of any resulting negative press.

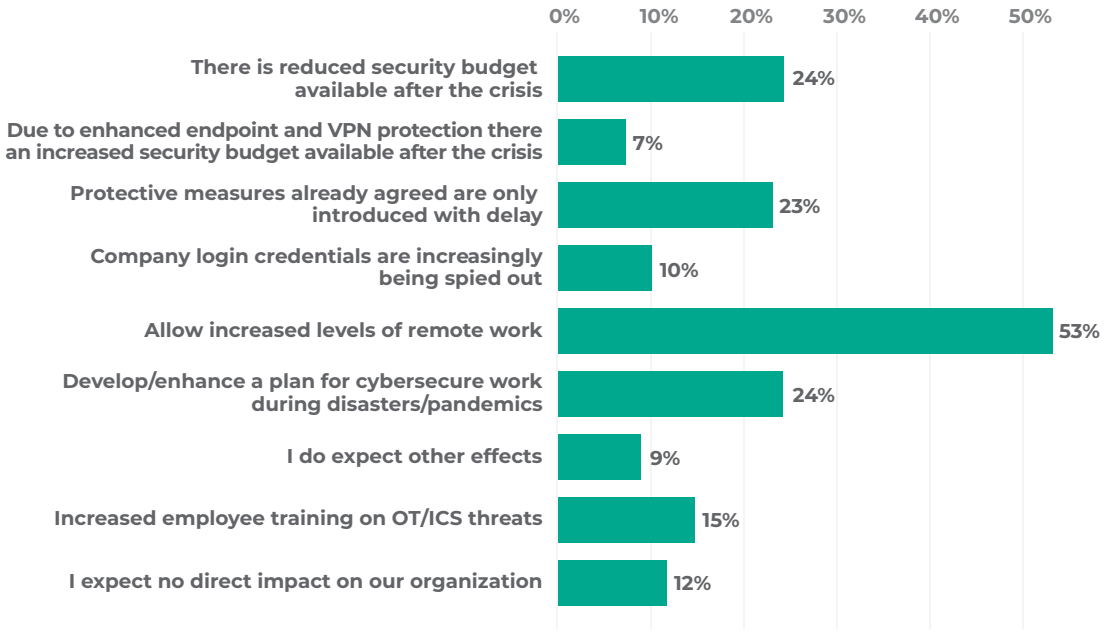
Survey Results

COVID-19 impact: Home office working increased the number of external network scans

Due to the coronavirus pandemic, many jobs were moved to home offices. In fact, 53% of respondents confirm that the pandemic has caused a shift to staff members working from home. Administrators who scanned their ICS networks for anomalies observed a new class of unwanted network scans from employees in home offices who connected to the production network via a VPN, using personal devices. The reason for these anomalies may be that some employers did not provide corporate devices for remote working quickly enough. Also, for some employees, working from home can be more convenient using their own desktop PC with keyboard, monitor and printer connected. This endpoint, the home office computer, typically has lower security standards than corporate networks, and companies have observed that these computers have been used to perform unwanted scanning attempts of production networks. This trend was observed worldwide.

Another interesting result is that only 24% of respondents confirmed that internal security processes needed to be revised during the pandemic. Similarly, only 15% suggested that employees received special security training for working from home during the pandemic. This suggests that a large majority of respondents saw no need to change security processes, nor provide additional employee training during the pandemic.

Which aspects of cybersecurity initiatives might the coronavirus pandemic influence in your organization?



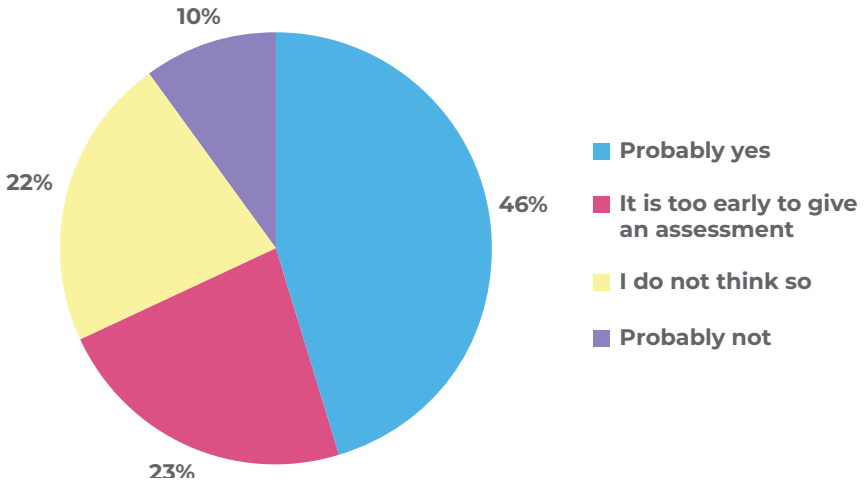
Q10 – Global pandemic influences. 606 answers from 337 participants. “Prefer not to answer” (PNA) excluded.

Recommendation: Companies should prepare for a change in working conditions during a lockdown. Company-owned devices should be used to access corporate networks so that the connecting device is managed by the organization's security team. If employees use their own computer, the use of virtual machines can improve security posture. The virtual desktop infrastructure (VDI) maintains a controlled environment and limits vulnerability to the company network by private equipment. To detect unauthorized access to the OT network early on, methods such as dual authentication can also be used.

COVID-19 impact: How it will change security posture

The current pandemic has influenced many cybersecurity projects. Only 32% of interviewees stated that the security processes in their companies are not influenced very much or not at all.

In your view, will the current coronavirus pandemic change the OT cybersecurity priorities in your organization?



Q9 – Global coronavirus impact on OT cybersecurity. 336 answers from 337 participants[3].

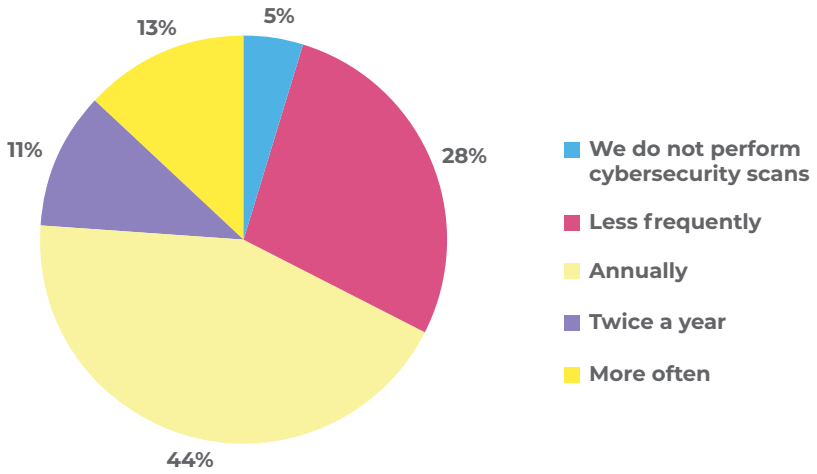
The pandemic is having the greatest impact in home office workplaces and situations where employees use their own devices to connect to the ICS network. Employees should be frequently trained and PC technology must be deployed to meet required security standards for extreme situations. Cybercriminals exploit fear surrounding coronavirus to carry out cyberattacks via phishing attacks, malware, and cyberattacks against remote maintenance infrastructures. According to Kaspersky research[4], the number of phishing and cyberattacks related to coronavirus since March went up.

3 Here and further: the number of answers is lower than the number of participants because some of them skipped the question
4 https://securelist.com/spam-and-phishing-in-q1-2020/97091/

Network segmentation and endpoint protection on their own are no longer sufficient

In the 2019 survey, 24% of participants answered that they would not conduct a 'security assessment on OT networks'. This year, only five percent of respondents stated that they are not going to conduct security assessments on their OT networks. Obviously, security assessments are now carried out more frequently to detect security gaps at an early stage.

How often does your company carry out a cybersecurity scan (security assessment) in the OT network?



Q23 – Global network assessments. 261 answers from 337 participants. "Don't know" (DK) excluded.

There are approximately 10 billion IoT devices currently connected to the internet[5]. Even if not all of these devices are used in industry, protective measures are still needed. Yet it is unlikely that every IoT device will be equipped with endpoint protection. Other effective security methods are required to detect attacks or anomalies in OT networks in advance. The point is to detect a change in communication behavior to prevent damage.

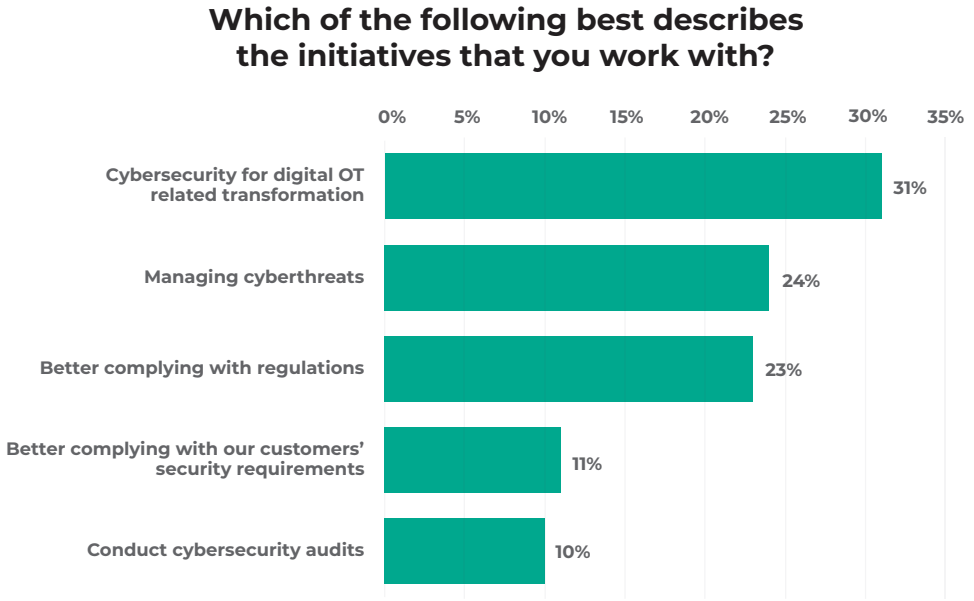
Recommendation: When a company develops an IoT strategy, the security aspect must be considered from the very beginning. Due to the large number of new communication channels, it is not practical to monitor every device. Instead, a better solution is to monitor communication behavior for anomalies.

5 https://iot-analytics.com/state-of-the-IoT-update-q1-q2-2018-number-of-IoT-devices-now-7b

The current security workload will keep you busy

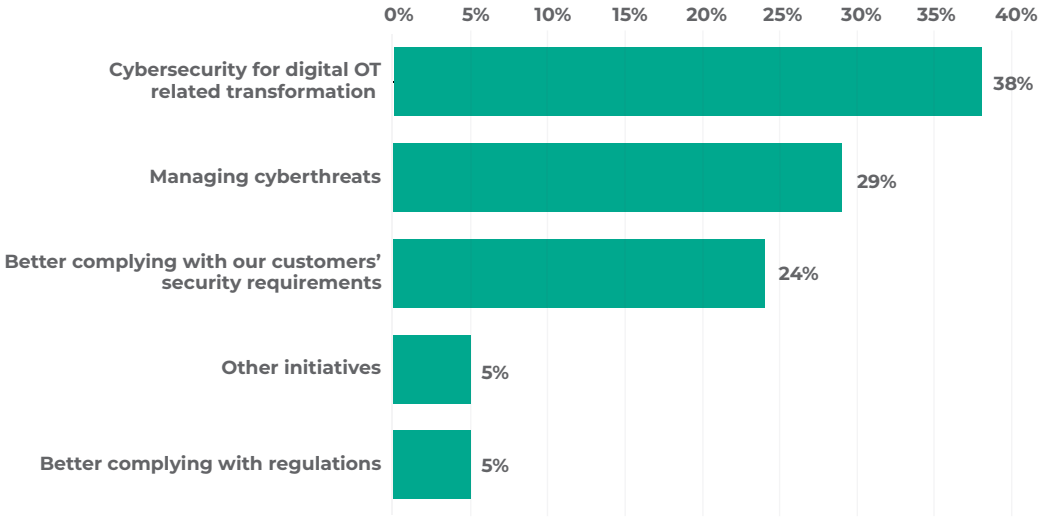
Globally, more than 44% of respondents are preparing their companies for digitalization. In the 2019 survey, 31% of respondents stated that their main task was to prepare for digital transformation and associated cybersecurity requirements. This trend is growing strongly globally, but there are differences when we look at the regional data. In Europe, 23% of respondents are working to comply with local regulations, while in Latin America 29% are working to close security gaps in OT networks. It is likely that these different priorities result from regional trends and policies. If policies need to be complied with in one region, that is the priority. If there are many OT vulnerabilities, then the priority for that respective region is different.

Q7 – Global initiatives that you work with. 335 answers from 337 participants



Q7 – European initiatives that you work with. 123 answers from 124 participants.

Which of the following best describes the initiatives that you work with?



Q7 – LatAm initiatives that you work with. 26 answers from 27 participants.

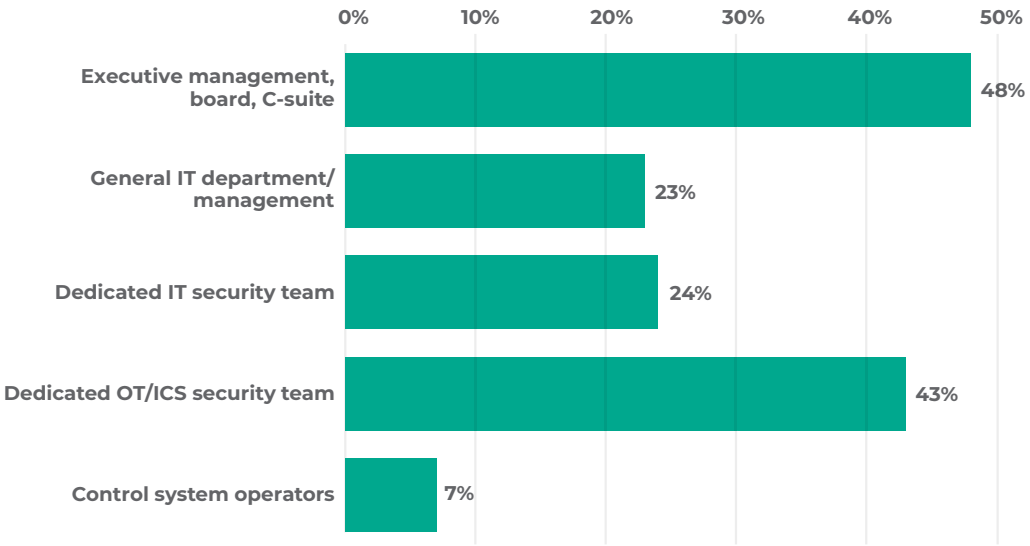
The real security budget decision-makers

> Often the budget for the introduction of security software (e.g. anomaly detection) is not the limiting factor, but rather the qualifications of OT operators. Often the correct use and interpretation of security software is not well known to OT operators.
>
> **Power Generation Industry**

From a legal point of view, boards of directors or managing directors decide how budgets are allocated. In practical terms, security teams are becoming increasingly important to make interdisciplinary decisions about necessary security measures and preferred suppliers. The term 'Team' in this context means experienced representatives from OT communication and ICS areas that jointly assess the risk situation and determine appropriate cybersecurity measures through interdisciplinary cooperation and decision-making.

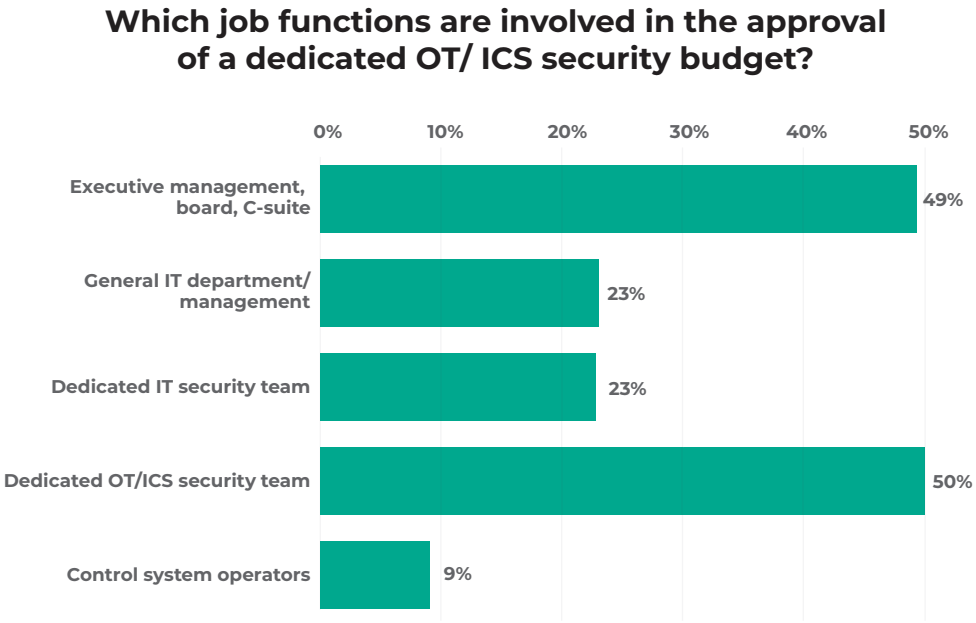
The trend towards team budget decisions is most prevalent in Europe, where team decision-making was chosen by 50% of respondents.

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



Q15 – Global approval of security budgets. 506 answers from 337 participants. DK excluded.

In last year's survey, 26% of respondents indicated that the 'General IT department/ management' is involved in the approval of security budgets. In this year's results, 23% responded that the IT department is responsible for OT/ICS budgets globally. This shows that the IT-security experience is also appreciated in the OT-security area. Obviously, one does not want to reinvent the wheel here, but rather to build on IT experiences.



Q15 - European approval of security budget. 187 answers from 124 participants. DK excluded.

Typical ICS cyberthreat challenges in 2020

As is the case every year, the most important challenge for industrial cybersecurity given by respondents is to protect employees from injury or death. The next three ranked responses are more interesting.

The second, third and fourth responses are roughly equal in size and together they make up 83% of the total. These challenges include damage to product/service quality (28%), loss of proprietary or confidential information (28%), and cost of incident response and mitigation (27%).

This year, the effects after an attack and the resulting costs were especially important. In 2019 the situation was different. In that survey, the cost of incident response and loss of customer confidence were deemed to be rather unimportant (only 5%). It's clear that a new perception is emerging. Due to the increasing sophistication of cyberattacks against industry assets[6], the effects are more noticeable. In addition, operational units now regularly report[7] to the board of directors so that the effects after a cyber-incident can be better analyzed.

Q8 – Global cybersecurity related challenges. 758 answers from 337 participants. PNA excluded.

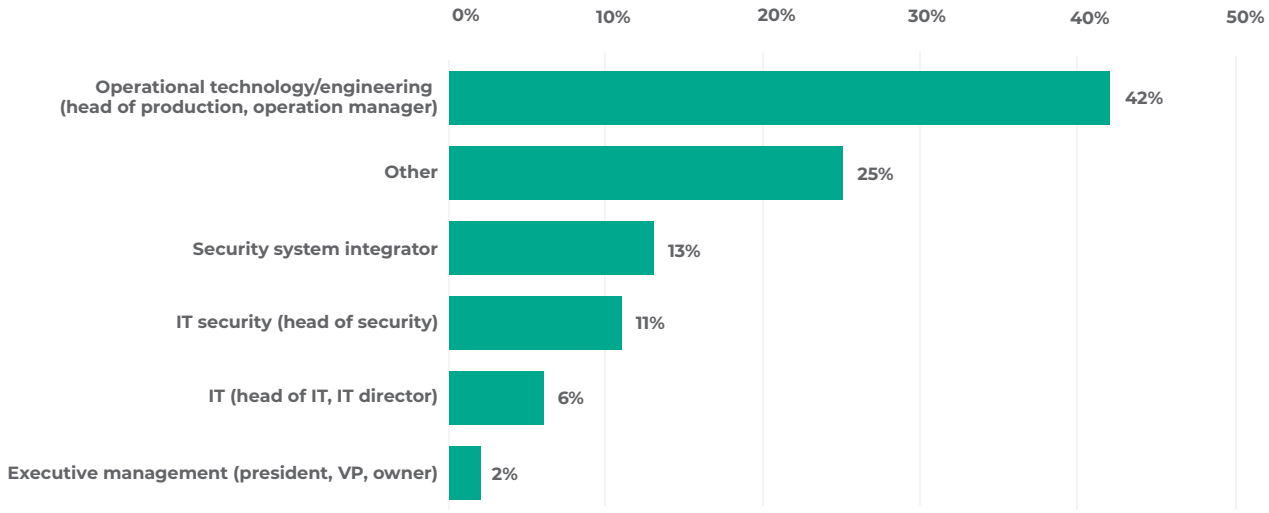
Which departments are driving cybersecurity projects in ICS?

Maintaining ICS integrity requires a thorough understanding of the communication standards used among all the various ICS components to maintain safe and efficient operations. In this cyber-physical layer, it can be difficult to spot communications errors, cybersecurity threats, and network health problems. The symptoms are obvious: sluggish human-machine interface (HMI) updates, unexplained shutdowns, and precarious failures of ICS components. A robust and healthy OT network is key to preventing these failures.

To summarize, cybersecurity planning is a complex task. It is often difficult to manage without interdisciplinary knowledge. The drivers for an increased level of OT security are the operational departments.

6 https://ics-cert.kaspersky.com/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-2019-report-at-a-glance
7 https://www.gartner.com/en/information-technology/insights/cybersecurity

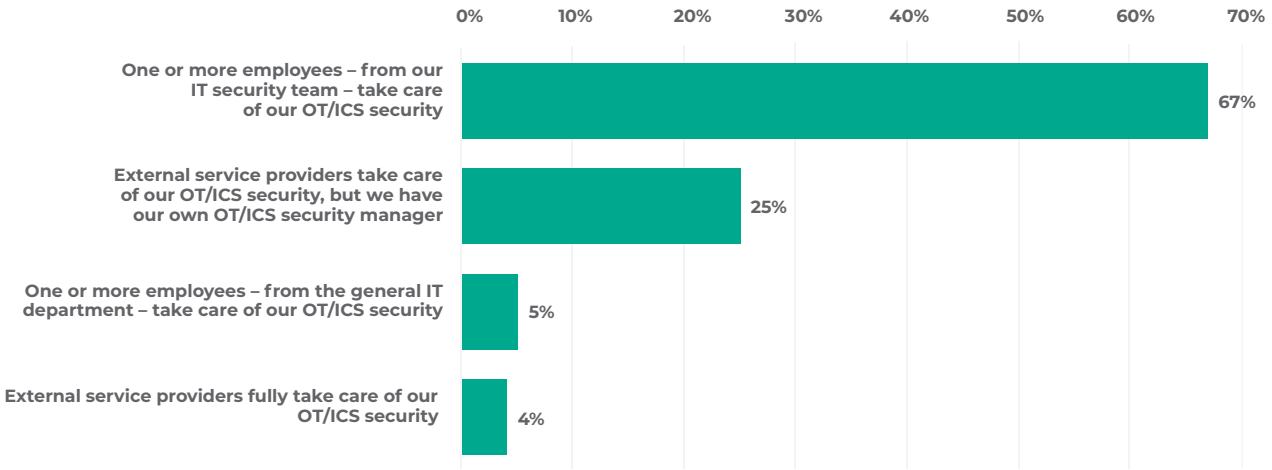
Which of the following best describes your department?



Q6 - Global participants' departments. 324 answers from 337 participants.

When we elaborated further and asked which team was best at engineering an OT cybersecurity solution, 67% of the answers named IT security. Nevertheless, even with this question, required interdisciplinary knowledge is evident as 25% of the respondents said that external consultants are also used.

According to your practical experience, what would be the best team to coordinate the OT/ICS security initiatives in your organization?



Q13 – Global team to coordinate OT security. 337 answers from 337 participants.

New cybersecurity threats result from digitalization initiatives

> ICS security suppliers often claim to know what users will require in the future. The users know their production processes best and can decide which security solutions are helpful. Users do not use security solutions, just because they are cool software.
>
> **Oil & Gas Industry**

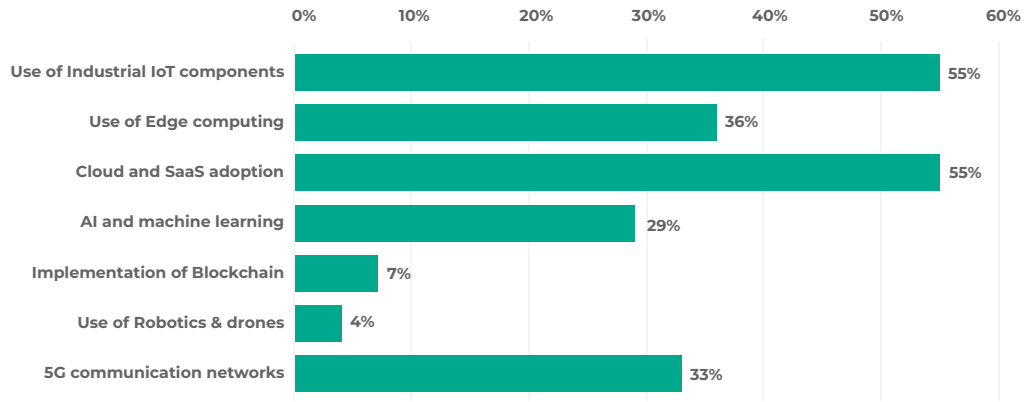
Which digital technologies do respondents expect to impact their traditional automation technology? It was not surprising that 55% of those surveyed indicated methods such as cloud and edge computing along with OT components being connected to the internet. The reason why cloud and edge computing are often mentioned is probably psychological[8]. While cloud computing has already proven its reliability in many other application areas, the industry currently still has security concerns about using cloud data or applications.

6 https://ieeexplore.ieee.org/abstract/document/6023923

The evaluation of new cybersecurity methods for the secure use of IoT technology is also reflected in the qualitative survey responses. Many stated that their companies have basic cybersecurity protection installed that protects classic, deterministic automation. Proceeding sequentially through the future, cybersecurity technologies ensure that the integrity of each digital technology is sustained. Every cybersecurity technique has an associated set of people, processes and technologies that are required to accomplish its goals.

Interestingly, the new 5G communication networks are classified as less critical than IoT components, which may be because a high level of embedded security is already implemented in this new connectivity standard.

From your practical experience, which technical trends have the strongest impact on OT/ICS cybersecurity? Please select up to 3 options



Q26 – Global digital trends impact OT cybersecurity. 756 answers from 337 participants. PNA excluded.

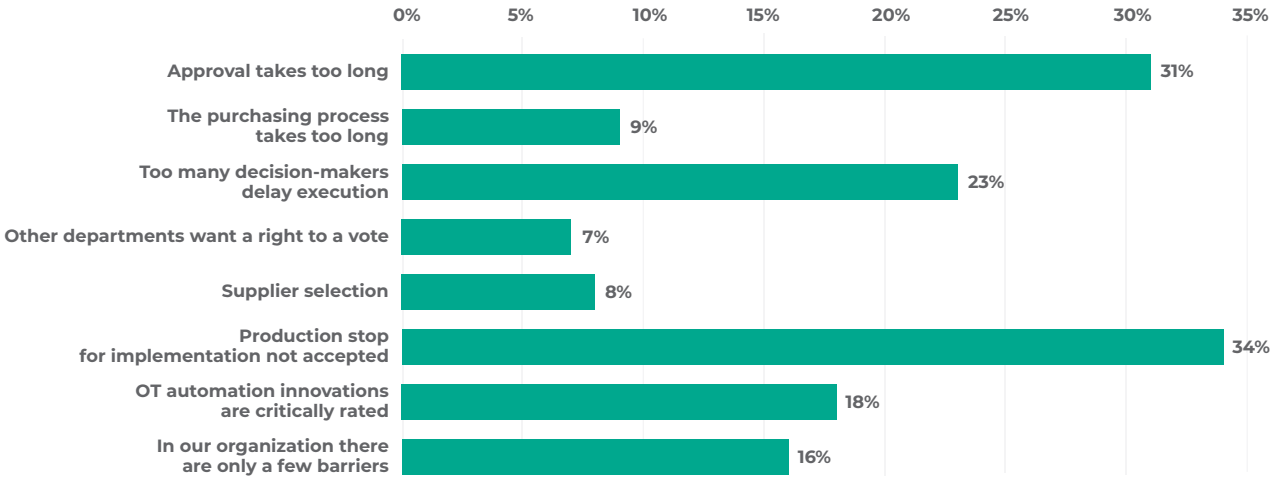
Gaps during implementation of cybersecurity measures

> Get the security basics in place before you implement the latest, greatest, newest technology or solution. Make sure you can sustain the security basics and you will derive value out of it.
>
> **Chemical Industry**

Organizational risks and cybersecurity gaps will always be present in modern companies. Experts agree that identifying and taking action to solve preventable vulnerabilities is a real opportunity to strengthen corporate defenses. This question is intended to clarify, after a vulnerability has been detected in the OT network, what the reasons may be for a delay in mitigating this vulnerability.

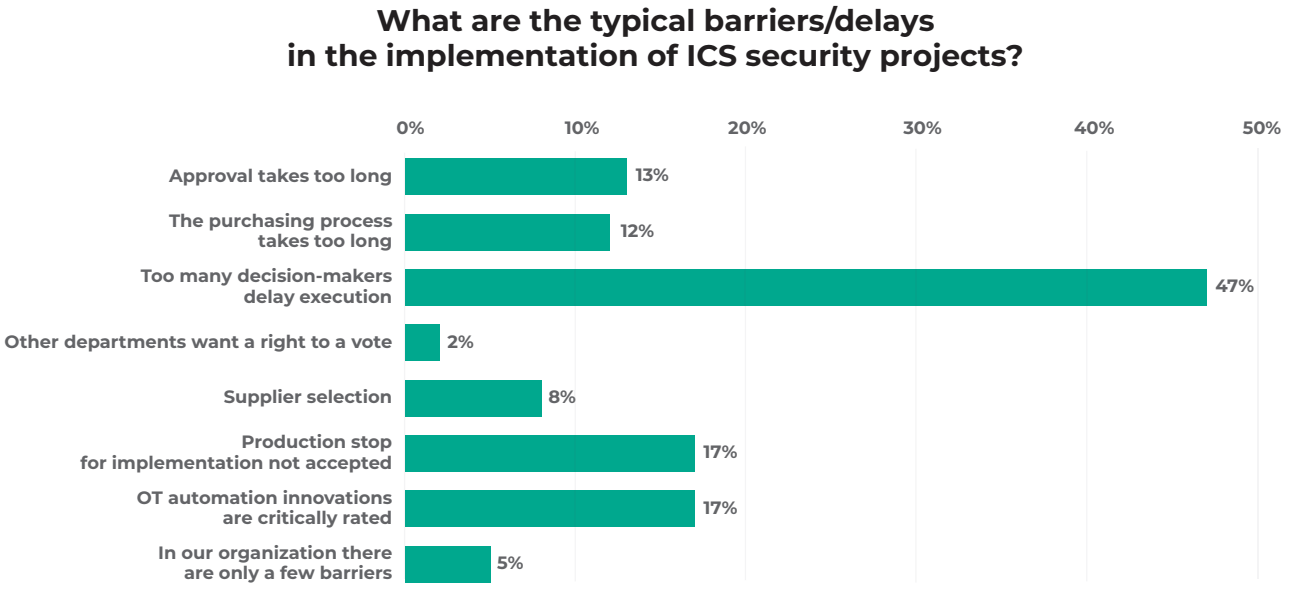
Filling these cybersecurity gaps has become a top-level concern in recent years, gaining more attention from decision-makers. A third of the participants globally ranked long approval periods (31%) and inability to stop production process (34%) as reasons for these gaps. Only 16% of respondents indicated that there are few hurdles in their company that delay the implementation of security measures.

What are the typical barriers/delays in the implementation of ICS security projects?



Q17 – Global implementation delays. 534 answers from 337 participants. PNA excluded.

But locally, there may be other reasons why the introduction of ICS measures may be delayed. In Asia, the large number of decision-makers involved in ICS implementation was frequently cited by most of the respondents as a reason for delays.

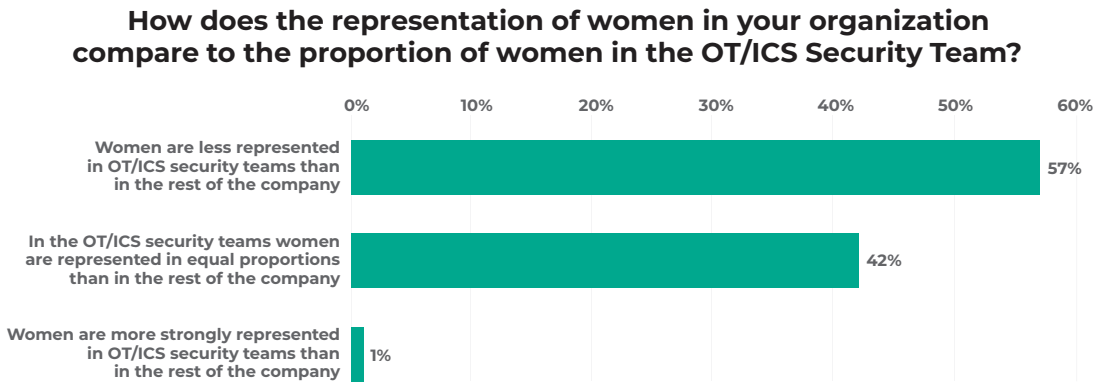


Q17 – Asia implementation delays. 72 answers from 337 participants. PNA excluded.

Globally operating companies must find a solution to resolve these delays. A detected security flaw can pose a similar risk to a zero-day exploit. Necessary security measures must be installed as soon as possible. Internationally, valid ISO or IEC guidelines can help to standardize methods and increase the speed of execution.

Environmental and gender-specific situations in cybersecurity teams

In technical jobs, gender equality is not always a given. This also applies to the current survey results. 57% of the respondents state that women are underrepresented in the cybersecurity teams in their companies.



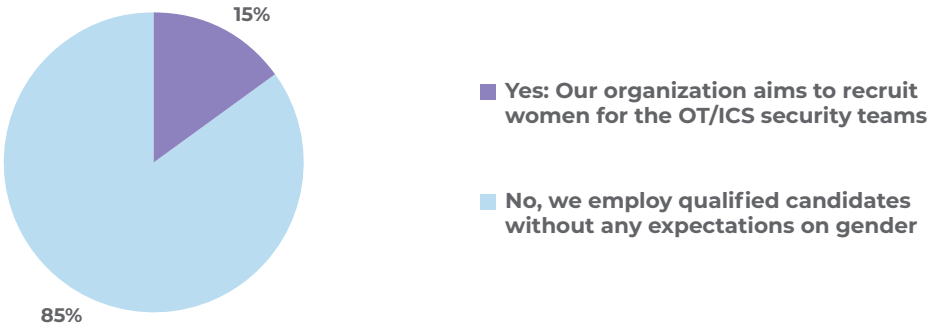
Q31 – Global women in ICS teams. 322 answers from 337 participants. DK excluded.

A report by Accenture[9] explores the barriers and challenges. 'Powering Economic Growth: Attracting More Young Women into Science and Technology' states that "women are vastly under-represented in science and technology-based careers that will drive digitalization". The statistics across the European Union also reflect this, with just seven percent of technical roles being filled by women.

According to Accenture's research, negative stereotypes around women in technology sadly continue to persist. Women still believe that technical education is for 'male' careers and this is the biggest reason why young men are more likely to choose this path versus young women.

This situation is reflected in the chart below. Only 15% of surveyed participants confirm that they expect the quota of women in cybersecurity teams to increase in the future.

Has your organization taken/is planning to take any steps to improve the representation of women in OT/ICS security teams?



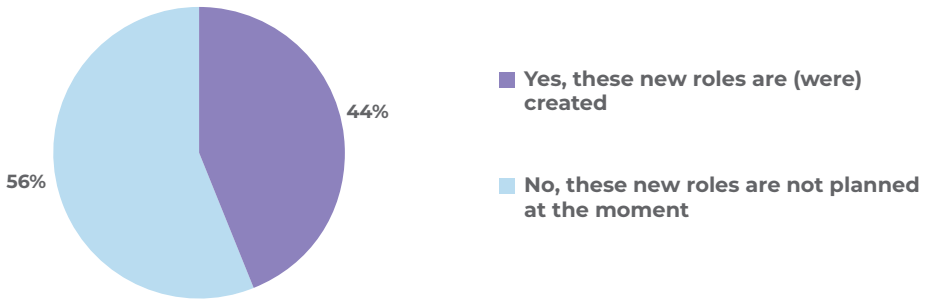
Q32 – Global improve representation of women. 333 answers from 337 participants. DK excluded.

9 https://www.accenture.com/ie-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_16/Accenture-Continuing-Power-Economic-Growth-Stem.pdf

When asked whether an environmental related role (e.g. Chief Sustainable Officer, CSO) has been created in their companies, 44% said this was the case.

The increase in demand for CSOs reflects a significant evolution in corporate sustainability. By and large, this is no longer about 'greenwashing' but instead about being a good corporate citizen. Sustainability is now incorporated into companies' core missions and signatories of the United Nations' Principles for Responsible Investment represent more than half of the world's institutional assets.

Will new environment-related roles (e.g. Chief Sustainability Officers) be introduced in your organization?



Q33 – Global CSO roles are introduced. 323 answers from 337 participants. DK excluded.

During the qualitative discussion, companies stated that under control of the CSO, they redesigned processes to handle customer and employee data as well as business partner information. Obviously the CSO manages personal data protection, but it remains crucial for companies to safeguard other business-related information to prevent damage to its competitive position in its market, as well as its brand and reputation. Cybersecurity is a vital part of data protection and with CSOs' help, the importance of cybersecurity will be elevated in companies.

Conclusions and recommendations

This year, various influences put increased pressure on industrial cybersecurity measures. A notable one-off influence was the COVID-19 pandemic, which affected the way companies work. A longer and ongoing process that is impacting industrial cybersecurity is the use of digital methods to increase efficiency in companies. Both influences, especially on cybersecurity measures, have already been explained in many sections of this report. But how should industrial cybersecurity measures be further developed so that protection objectives and safeguarding can be achieved in the future?

Cybersecurity maturity model

ARC has developed a model that supports the holistic development of the future industrial cybersecurity standard. This model provides a framework for strategically developing the benefits of cybersecurity technologies for risk reduction in industrial processes.

The underlying cybersecurity structure showed the need to align people, processes and technologies to ensure that the required security level is achieved.

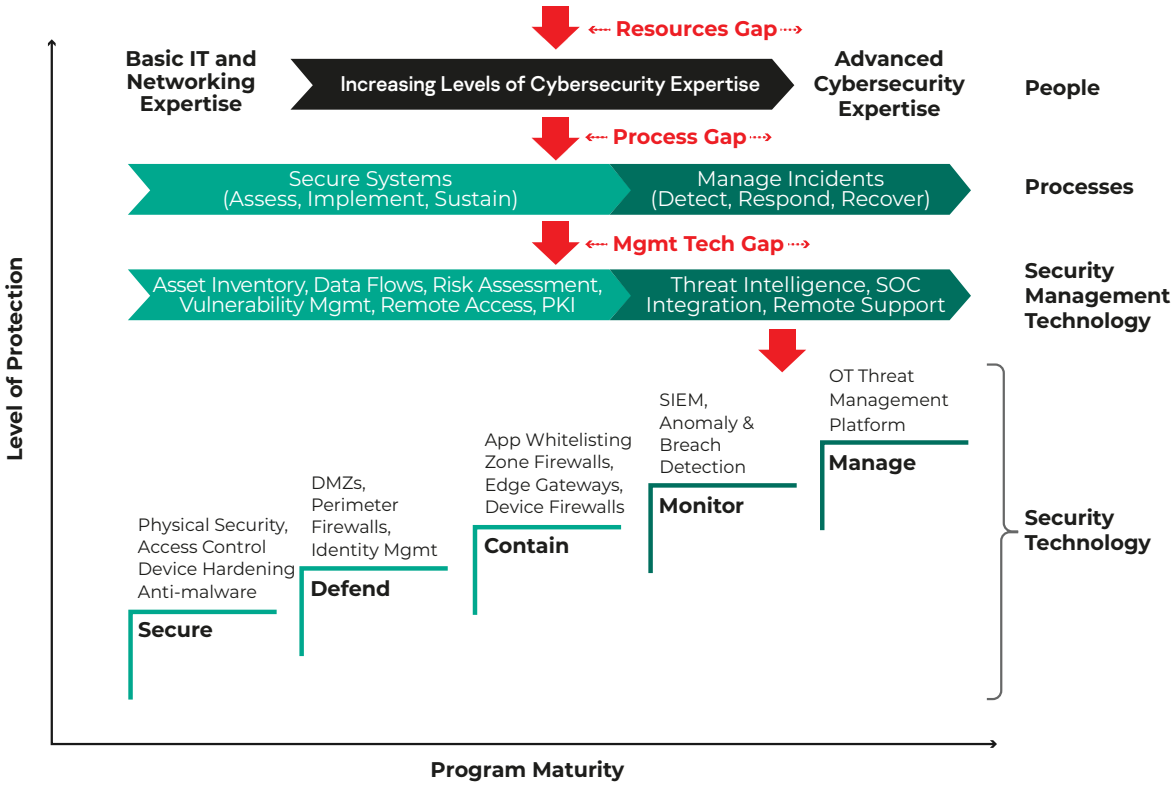
Industrial cybersecurity has changed significantly in recent years. Sophisticated attacks have increased the demand for better visibility of the cyber-risks that impact control systems. The integration of IT and OT cybersecurity programs has highlighted the need for increased system access by remote support teams. Digital transformation programs require new approaches to ensure the secure deployment of a variety of new, potentially unsafe devices within plant boundaries. The Industrial Cybersecurity Maturity Model provides the additional information managers need to manage industrial cybersecurity strategies in this new reality.

This cybersecurity model for evolving technologies and architectures goes beyond the recommendations of standards and guidelines by incorporating new OT technologies, such as edge gateways, new practices such as PKI and new strategies, including the integration of IT and OT cybersecurity programs. Efficiency gains are driving companies to adopt these developments despite a lack of industry guidelines. We have incorporated these developments into the model to help cybersecurity teams better assess and prepare for these developments. ARC's cybersecurity analysts regularly update this industrial OT cybersecurity maturity model. We have incorporated new technologies and practices used within industrial cybersecurity. In summary, this ARC model provides a practical tool for planning cybersecurity investments.

The model helps companies evaluate technology solutions and suppliers to assess how well they cover the focus points in the model. Regular ARC information on the state of industrial cybersecurity is used to identify critical resource and technology gaps that industrial companies need to close. In the current version of this model, end users can use the Industrial/OT cybersecurity maturity model to evaluate their cybersecurity programs and justify necessary investments to top management.

10 https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model

The model highlights the need to balance the discrepancy between technology investment and human resources, and is also often used by cyber-professionals to discuss a false sense of security after managers have approved technology investments. All technology investments require active management to maintain the required level of cybersecurity protection.



Anomaly detection as one of key practical measures against ICS threats

Today's production networks have a topology comparable to classic IT networks and increasingly use IT protocols. These protocols are not only referred to as intelligent control units, but sensors, and actuators are also increasingly using them to communicate. The number of these components results in these networks becoming more complex. Industrial network elements are connected via switches; firewalls and other monitoring solutions are used to secure segment interfaces and network connections. In this context, monitoring is the protocoling and analysis of the data and data streams occurring in the network, and is mainly used to detect anomalies that influence the automation processes.

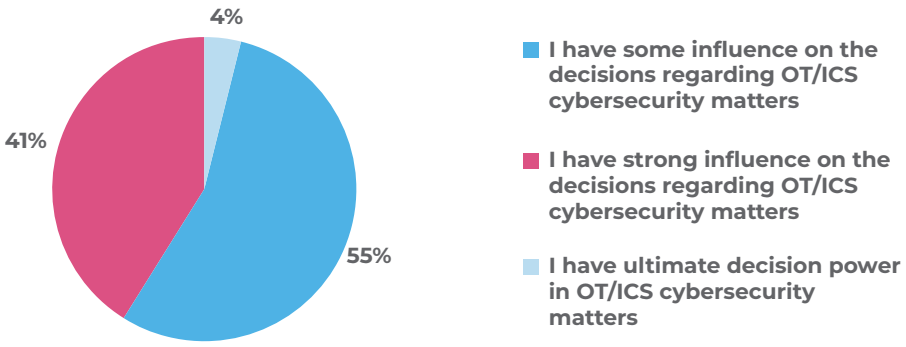
Anomalies are unexpected deviations from the normal rules, i.e. deviations from 'normal operating conditions'. These usually occur in the event of an error. However, they can also be an indication of an attack or manipulation within a production network. This is especially true when events occur for the first time, processes behave differently, or devices communicate with each other that have not done so before. It means that previously unknown attack patterns can also be detected by evaluating anomalies. Anomaly detection is therefore a suitable method of generating cyber-warnings and, if necessary, enabling more effective forensics. Anomaly detection is one of the basic methods of detecting cyberattacks.

Appendix

Survey Methodology

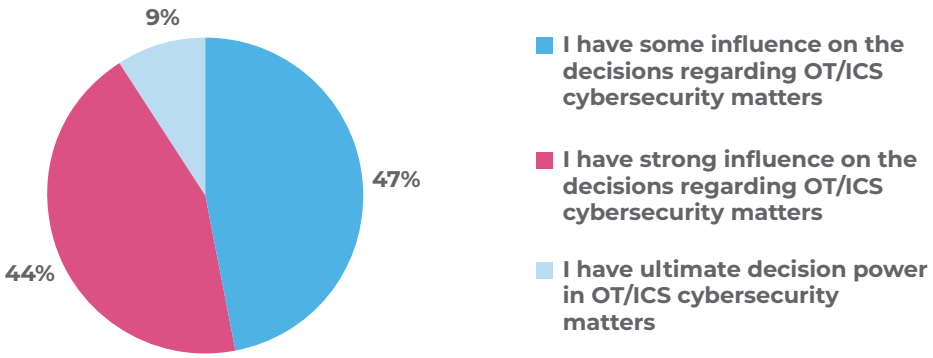
All respondents are involved in the decision-making and selection of cybersecurity solutions. Globally, more than 45% of the respondents have a strong or ultimate influence in the selection of cybersecurity solutions. In North America, more than 50% of the respondents have a direct influence on the choice of the cybersecurity solution.

Which of the following apply to your current role?



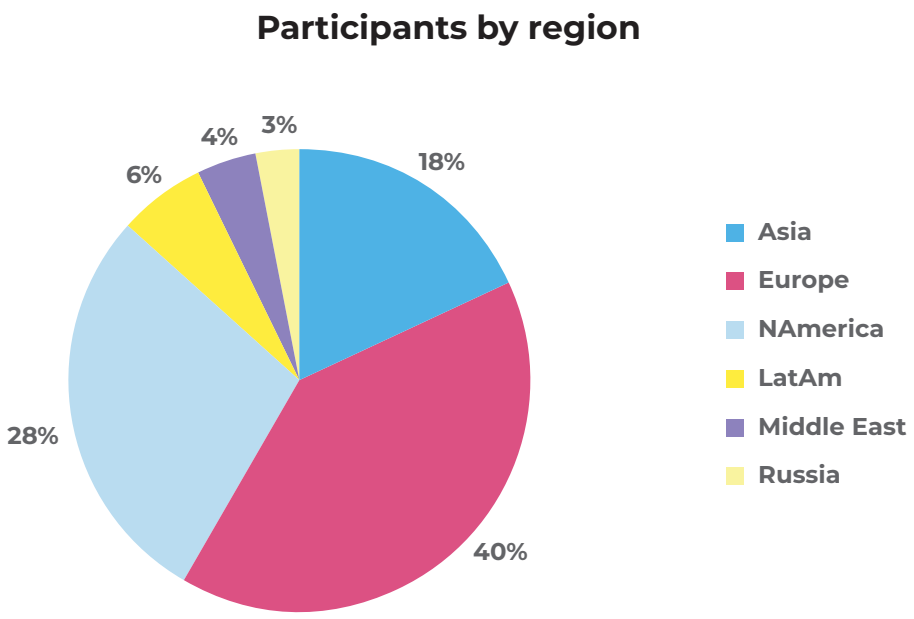
Q4 - Global current influence. 337 answers from 337 participants.

Which of the following apply to your current role?



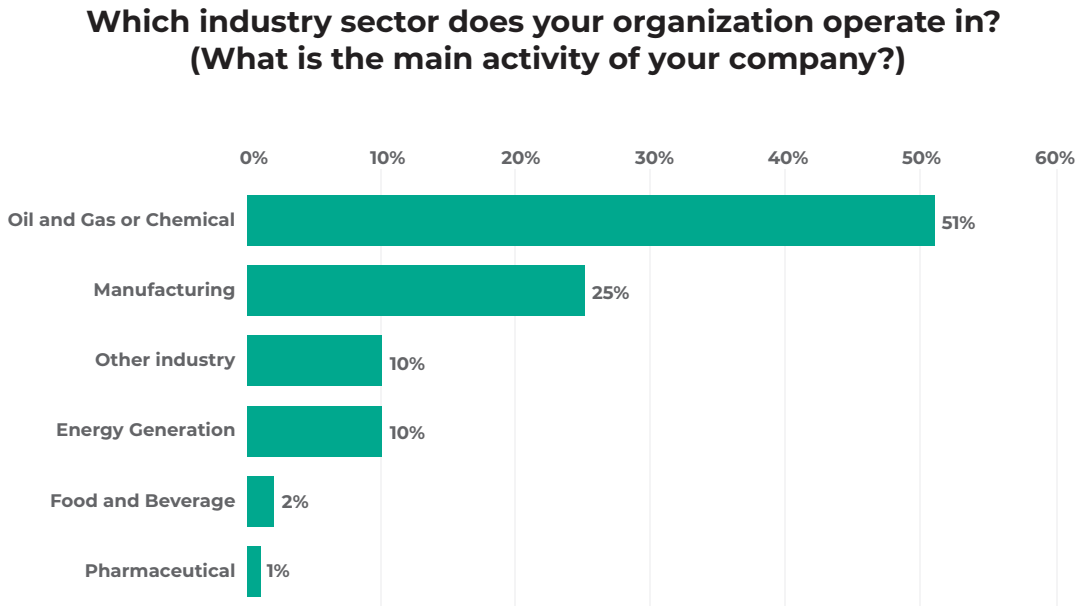
Q4 – North America current influence. 84 answers from 84 participants.

This survey was conducted globally on behalf of Kaspersky as a follow-on to previous ARC and Kaspersky surveys on ICS cybersecurity. 330 industrial companies were surveyed online, and 10 industry representatives were interviewed personally at trade fairs and ARC forums worldwide, covering Europe, North America, Latin America, Asia, and Middle East.



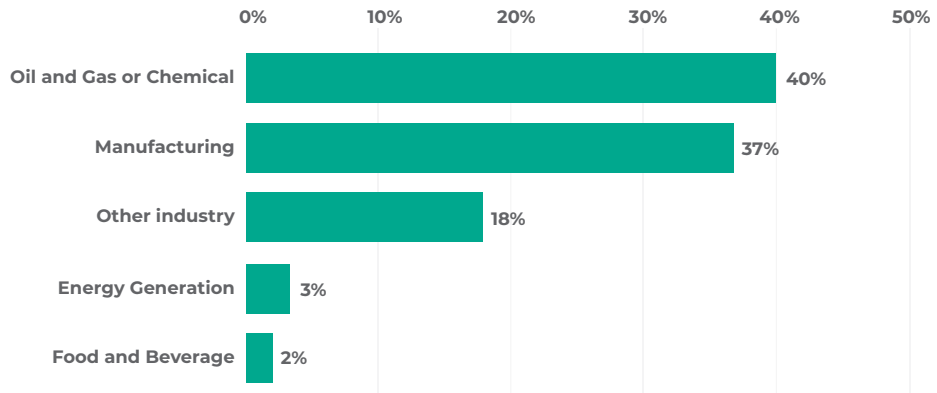
Q0 – Global survey participants. 337 answers from 337 participants.

Half of the industries surveyed worldwide originate from oil, gas and chemical industries. This ratio is only different in Asia, where 40% belong to the oil & gas sector and 37% to the manufacturing sector.



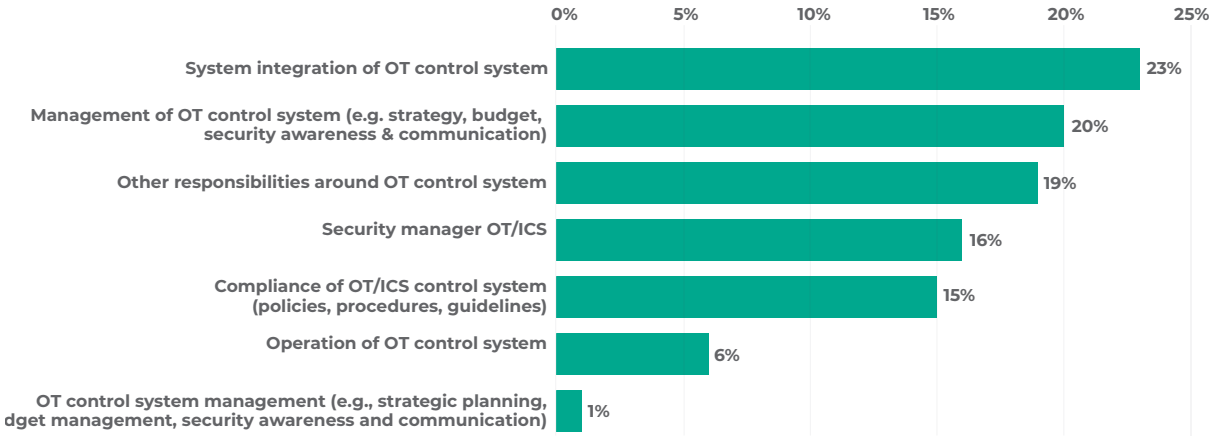
Q1 – Global Industries participating in the survey. 337 answers from 337 participants.

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



Q1 - Asia Industries participating in the survey. 60 answers from 60 participants.

What are your responsibilities around Operating Technology (OT) control systems? Which of the following applies?



Q3 - Global OT responsibilities. 336 answers from 337 respondents.

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 Düsseldorf, 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 250,000 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