TREND STUDY

The State of Industrial Cybersecurity 2018

Authors:

Wolfgang Schwab, Principal Consultant
Mathieu Poujol, Head of Cybersecurity

June 2018

commissioned by

KASPERSKY lab

CXP Group

BARC · Ie CXP · PAC

CONTENTS

The State of Industrial Cybersecurity 2018

Wolfgang Schwab, Principal Consultant
Mathieu Poujol, Head of Cybersecurity

June 2018

INTRODUCTION – INDUSTRIAL CYBERSECURITY

As connectivity to the outside world grows, security is becoming one of the most important topics in industrial IT and Operational Technology (OT), i.e. the hardware and software used in the production area. Industrial cybersecurity developed into a board-level topic during 2017.

But what do user companies really want? What are their priorities, and what concerns and challenges do they face? What external and internal factors are impacting industrial cybersecurity? What strategies and measures are being employed, now and in the future?

The present trend study "The State of Industrial Cybersecurity 2018" seeks to answer all these questions. It was carried out by PAC on behalf of Kaspersky Lab and analyzes the status quo and future developments worldwide with regard to industrial cybersecurity. It is based on a CATI survey of 320 worldwide professionals with decision-making power on OT/ICS cybersecurity, as well as 12 expert interviews. This study is an annual study. The first one was carried out in 2017.

"Cybersecurity is grabbing a lot of attention at every level. But to deal with this problem we must do more. Cyber threats are a harsh reality of today's world, which we can't keep on ignoring. With most of the processes being handled remotely, there is always a chance of breach, of someone getting ahold of these processes and causing a lot of harm."

(Steel manufacturing, US)

KEY FINDINGS – TAKE-AWAYS

Over three quarters of the companies surveyed state that OT/ICS cybersecurity is a major priority

But if companies really attribute such a high level of importance to this topic, it would be essential to carry out the associated measures in a very stringent way. This seems not to be the case in all companies.

Over three quarters of the companies surveyed state that it is very likely or at least quite likely to become a target of a cybersecurity attack in the OT/ICS space

Despite this, only 23% are compliant with minimal mandatory industry or government guidance and regulations around cybersecurity of industrial control systems. On the other hand, the vast majority of the companies surveyed are increasing their OT/ICS cybersecurity investments or keeping them at least steady.

More than half of the companies did not experience any incident or breach in the past 12 months

Although this seems to be a good thing at first glance, the question is whether or not they would even have recognized it. Many companies do not detect or even track attacks! Moreover, since the companies surveyed have only just started digital transformation, it can be said that the attack surface will increase along with the level of digitalization.

For most companies that experienced OT/ICS cybersecurity incidents or breaches this had a relevant negative impact on their bottom line

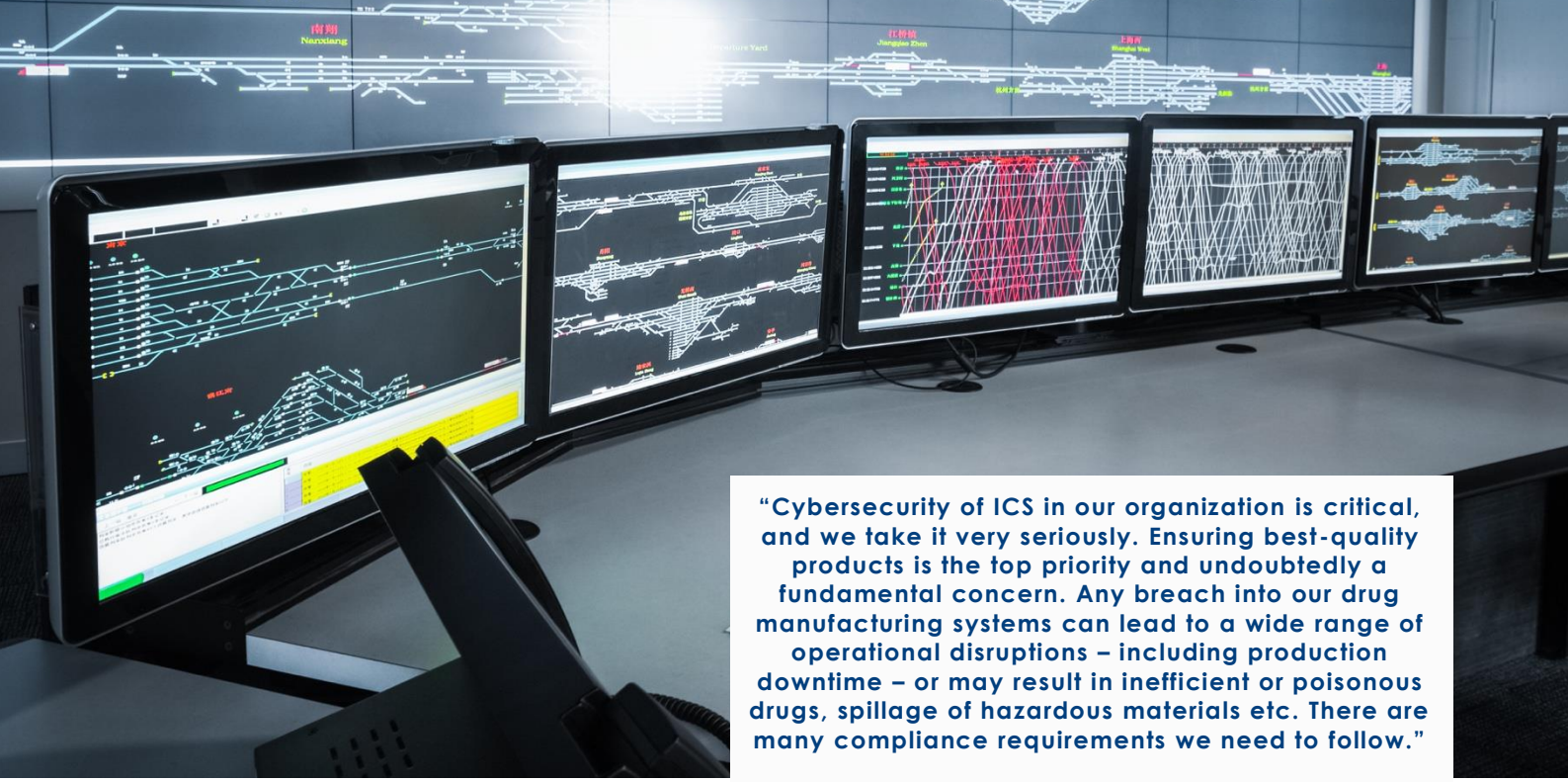
If incidents or breaches occur, they have a strong negative impact, usually regarding the company's bottom line; in the worst-case scenarios, the consequences could even mean casualties.

Low but increasing maturity

The maturity of ICS/OT cybersecurity remains low, e.g. the way OT/ICS security is organized, but the potential impacts and liabilities make it a priority; besides, the level of maturity is quickly rising, even if it is strongly limited by the lack of skills and collaboration.

Collaboration between IT and OT teams is critical

Collaboration is a critical factor for cybersecurity, even more so in OT/ICS cybersecurity. IT and OT people have different goals, processes, tools, and languages, but they must collaborate if they want to protect the OT/ICS space that is more and more blended with the IT space.



"Cybersecurity of ICS in our organization is critical, and we take it very seriously. Ensuring best-quality products is the top priority and undoubtedly a fundamental concern. Any breach into our drug manufacturing systems can lead to a wide range of operational disruptions – including production downtime – or may result in inefficient or poisonous drugs, spillage of hazardous materials etc. There are many compliance requirements we need to follow."

(Pharmaceuticals, US)

CYBERSECURITY IN AN INDUSTRIAL ENVIRONMENT: MANAGING RISKS AND COMPLIANCE ARE KEY

As digital transformation is spreading within the industrial environment, cybersecurity is becoming more and more important across the board. This section will look at the business priorities, the priorities of OT/ICS cybersecurity, OT/ICS cybersecurity business risks and concerns, and the challenges that lie in management of OT/ICS cybersecurity.

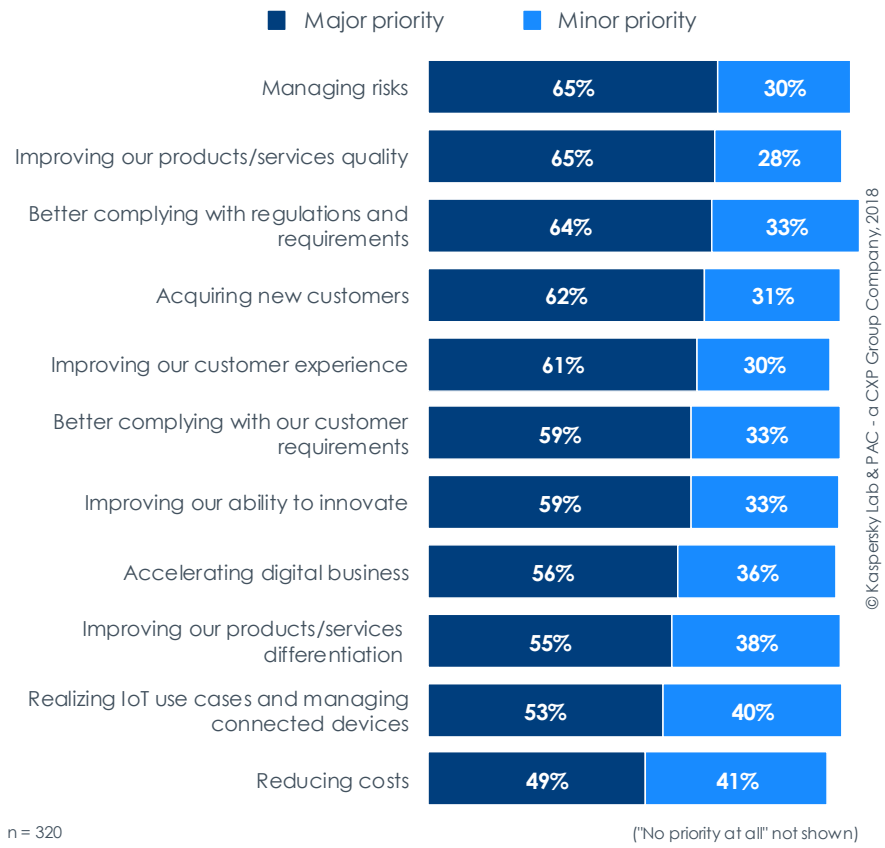
"Although it appears there are incremental improvements in several areas of addressing OT cybersecurity risk, it is discouraging to see that for the most part we still lack significant progress across the board when it comes to dedicating resources to these challenges. As we increase the level of automation in our critical infrastructures, we MUST take security issues seriously."

(Marty Edwards, Managing Director, Automation Federation, USA)

BUSINESS PRIORITIES

Basically, all surveyed business priorities have become even more pronounced at most companies, as we compare the 2017 survey results with the 2018 ones. The most important ones are still the management of risks, improving products/services quality, and better compliance with regulations and requirements. Especially customer-related items have seen a growth in prioritization, unlike cost reduction. In 2018, companies are not in defensive mode anymore; they want to grow, expand, and profit from digital transformation.

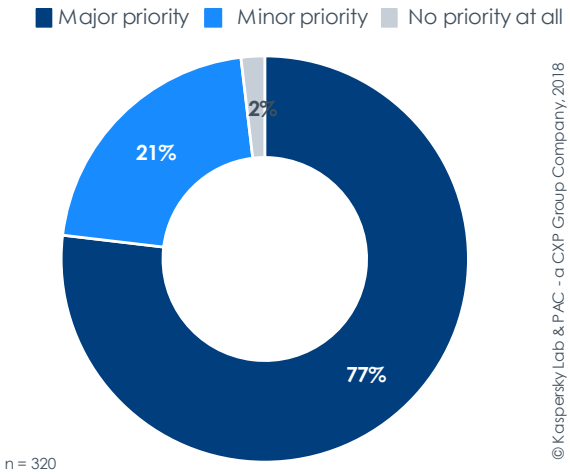
Which of the following initiatives will be a major, minor, or no priority for your organization over the next 12 months?



PRIORITY OF OT/ICS CYBERSECURITY

When it comes to prioritization of OT/ICS cybersecurity, we see that the vast majority of the companies see it as major priority. The risks are understood and therefore the ground for actions is laid out.

What level of priority is given to OT/ICS cybersecurity in your organization?



77%

of the companies surveyed rank cybersecurity as a major priority.

OT/ICS CYBERSECURITY BUSINESS RISKS AND CONCERNS

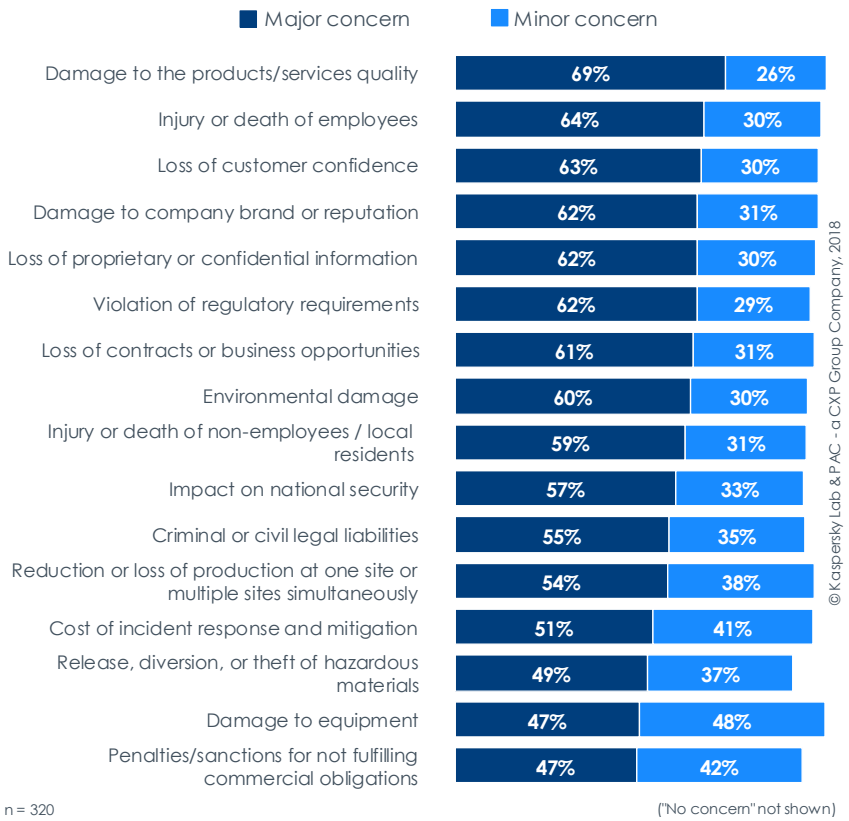
Looking at cybersecurity business risks and concerns in the OT/ICS space, we see that awareness levels have risen strongly. While in the 2017 survey, about one third of companies attributed concerns to the different items, in 2018 it is about two thirds attributing major concerns and almost one third attributing minor concerns.

The top concerns are damage to the products/services and injury or death of employees. Most companies also see a link between cyber damage and business success on different levels: an adverse effect on quality is directly linked to the loss of customer confidence, while the loss of business sensitive information is associated with a loss of contracts or business opportunities. In addition, most companies have concerns over a violation of regulations.

"ICS cybersecurity is attributed a lot of importance at all levels. But I would agree that there has been an awareness issue at lower levels because people there are not so much aware of the impact of a breach or cyber-attack."

(Energy and utility, US)

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

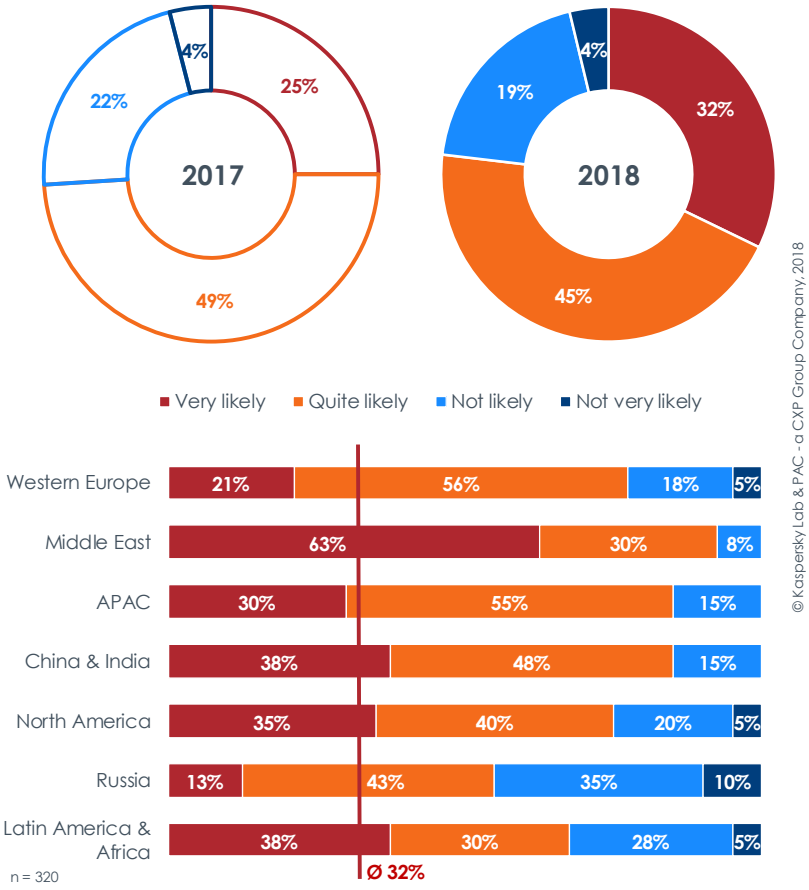


We can see that awareness of many items has risen considerably. Most of the items are now seen as a major concern by the majority of companies.

When comparing IT security and OT/ICS cybersecurity, a key aspect is that in the former damage is mostly confined to the IT space, thus remaining largely virtual, while in the OT/ICS space it could also be physical. This has a totally different impact on risk mitigation and on the liabilities enterprises could face.

To evaluate the actions needed in terms of cybersecurity in the OT/ICS space, it is not only important to know the concerns and the associated potential damage, but also the likelihood of an attack.

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



"There are a lot of changes right now. I can feel that many of the organizations across the Middle East are very much involved in risk assessment now. I noticed that there is a lot of demand and a lot of attention because of current attacks. It's a great challenge because we are connected globally through the Internet, so we are not really secure."

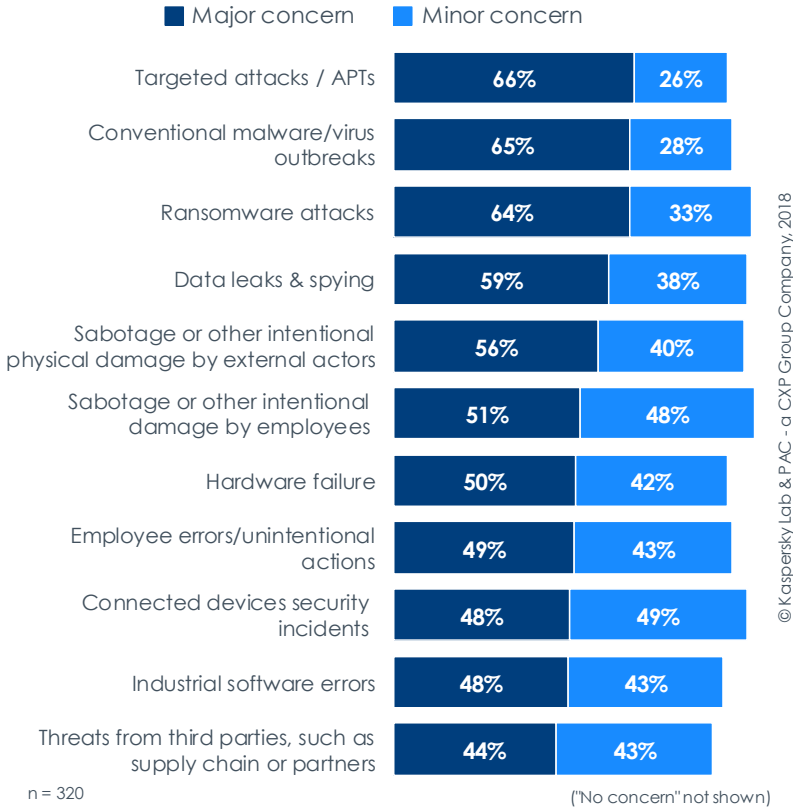
(Oil and gas industry, UAE)

The answers given indicate a rising likelihood of companies becoming a target of cyber-attacks in the OT/ICS space: 32% of the companies surveyed believe it very likely that they will be targeted, an increase of 7% on last year.

When it comes to the self-assessment of OT/ICS security risks, we see huge differences between the various regions surveyed. While 35% of Russian companies do not see themselves as targets and only 13% think it very likely that they will become a target, companies from the Middle East are much more alarmed – there, 63% of companies consider it very likely that they will become the target of a cyber-attack. This attitude does not come as a surprise since industrial companies in the Middle East have been victims of targeted ICS attacks in recent years, including the recent Triton case. This can also be seen as an indicator of market maturity, which is pretty low in Russia at the moment.

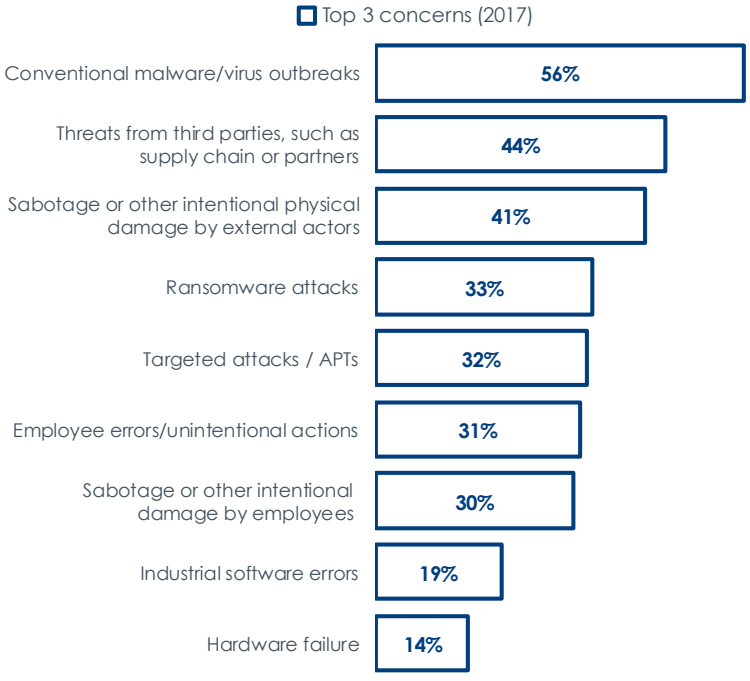
Even in the area of OT/ICS cybersecurity, traditional cyber threats are a major concern for the majority of the companies surveyed. 66% of the companies state that targeted attacks and APTs are a major concern – this is understandable given that in 2017 there were new rumors of cyber-physical attacks, including Triton and Industroyer. For conventional malware/virus outbreaks, this figure is 65%, while for ransomware attacks it is 64%. In 2017, there were lots of ransomware outbreaks, including cases inside industrial environments, which explains the high level of consensus regarding these as major concerns.

Which of the following security incidents are a major, minor, or no concern for your OT/ICS systems or industrial control network? (2018)



66%

of the companies surveyed say targeted attacks / APTs are a major concern.



"There is not 100% security. You're just trying to defend yourself, but threats always exist. Even if you don't have an Internet connection, there may be inside threats, as people from different regions and companies come for implementation processes, so it's impossible to take care of those things. So, we're always vulnerable to threat."

(Oil and gas industry, UAE)

What are the TOP 3 most concerning security incidents that you think might happen to your organization's OT/ICS or industrial control network? (2017)

Compared to last year's survey the increase in all segments shows a clear improvement in problem-awareness.

CHALLENGES TO MANAGING AN ORGANIZATION'S OT/ICS CYBERSECURITY – HIRING NEW TALENT IS ALMOST IMPOSSIBLE

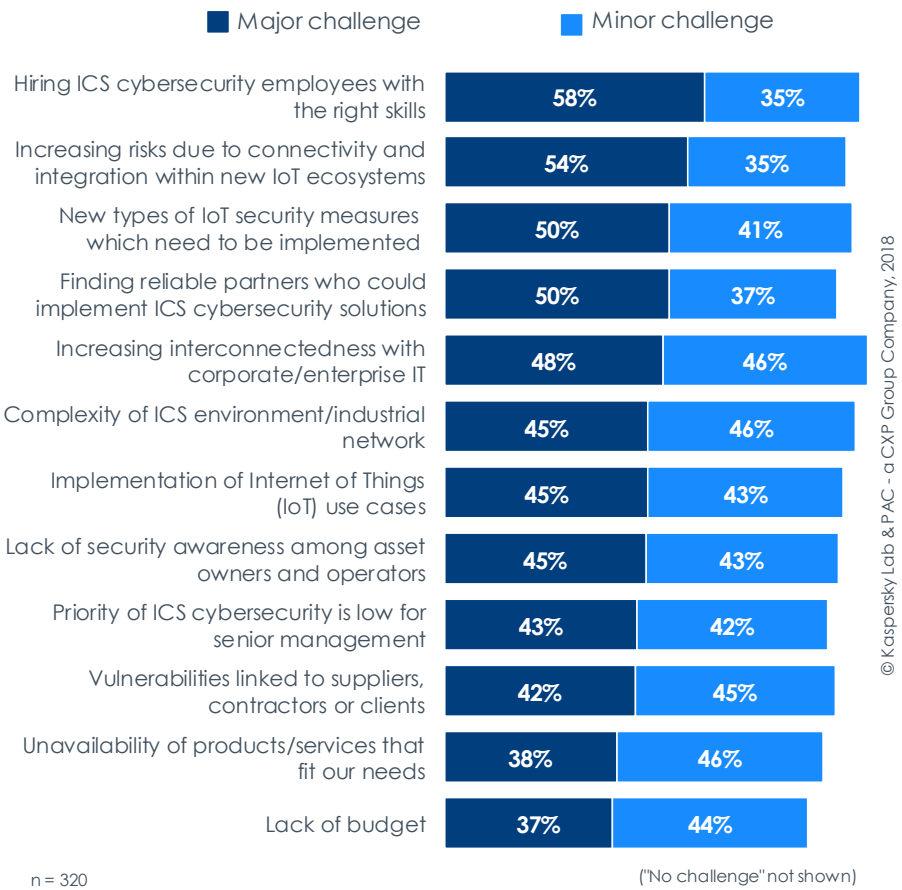
Our survey of the OT/ICS cybersecurity market revealed significant challenges in virtually all segments. 58% of the companies surveyed classify it as a major challenge to hire ICS cybersecurity employees with the right skills, a global issue in cybersecurity. This aspect is even more critical given that companies need to integrate their OT/ICS with their IT systems and IoT ecosystems, meaning they are opening up these systems to the outside (non-internal ICS/OT) world.

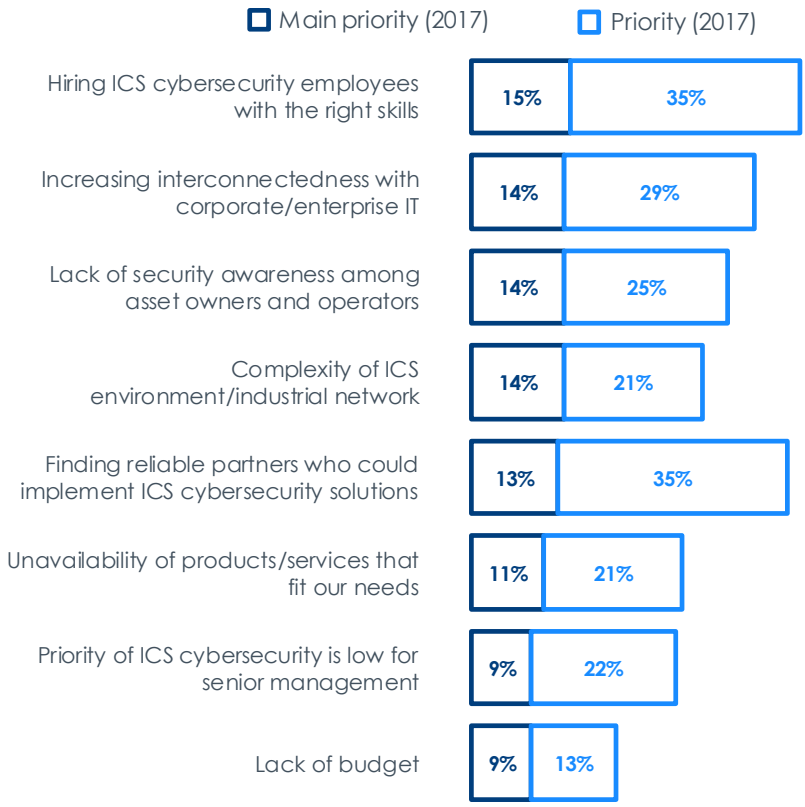
Another major challenge for 50% of the companies surveyed is finding suitable partners and service providers to implement ICS solutions. Given that the market for talent is exhausted, this is especially critical; if hiring and using external services is not possible, companies' options are strongly limited.

"First of all, a company has to set up some kind of security framework. There are a lot of resources with IT skills, but they don't have any experience in terms of the actual security processes. This is in fact a difficult combination to find, which poses a lot of challenges."

(Oil and gas industry, UAE)

Which of the following is a major, minor, or no challenge related to managing your organization's OT/ICS cybersecurity? (2018)





"We have an in-house team that takes care of ICS cybersecurity. It is challenging to hire a cybersecurity professional, because there are very few and you should have a specific type of cybersecurity professional. There are software professionals who do a lot of penetration testing and reverse engineering."

(Energy and utility, US)

What are the top 3 challenges related to managing an organization's OT/ICS cybersecurity? (2017)

Interestingly, the aspect of budget is only a major challenge for 37% of the companies surveyed, and thus least challenging in terms of cybersecurity management. However, when looking at the importance of cybersecurity for digital transformation and the rise of regulations in an environment where hiring and using managed services is problematic or even impossible in some regions, this is hardly surprising.

EXTERNAL FACTORS IMPACTING INDUSTRIAL CYBERSECURITY: REPORTING TO REGULATORY BODIES IS MORE OFTEN OBEYED THAN REAL COMPLIANCE

ROLE OF COMPLIANCE AND REGULATIONS

In most areas of business, compliance with industry or governmental guidance or regulations is a must-have for companies as they are often audited and investigated.

But only 23% of the companies surveyed say they are compliant with mandatory industry or governmental guidance or regulations. In 2017, this result was at a similarly low level, so we see no real improvement in this area.

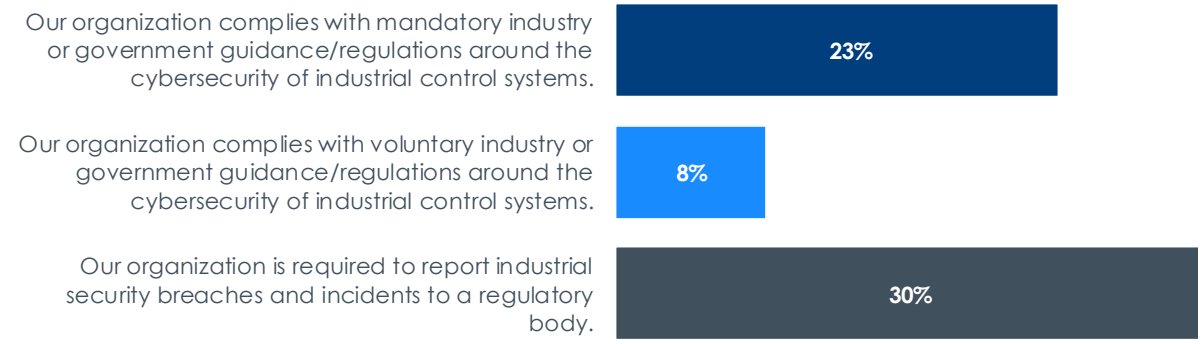
Only 23%

of the companies surveyed state that they are compliant with mandatory industry or governmental guidance or regulations.

Compliance with voluntary industry or government guidance or regulations has seen a strong decline compared to last year, for which there are three reasons:

1. Mandatory cybersecurity regulations such as the NIS Directive are given priority, and as they are expensive to implement, they are eating up all the budget and time of the companies surveyed.
2. In times of internal and external skills shortages, voluntary tasks are the first to be skipped.
3. A lot of guidance and regulations evolve quickly and as such are difficult to follow in full, i.e. being compliant in 2017 does not necessarily mean being so in 2018 as well; no resources are available for additional actions.

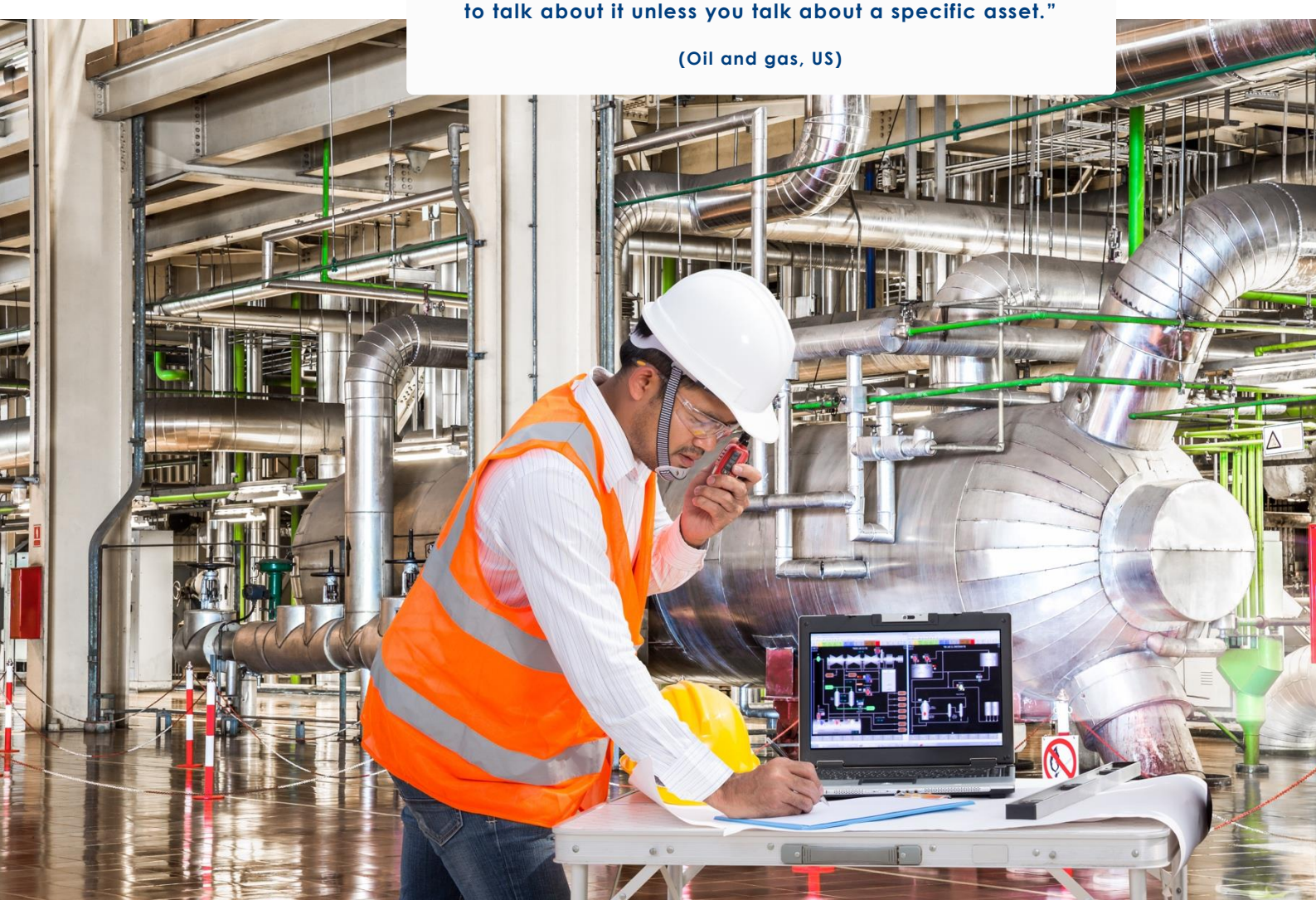
Does your organization comply with any industry or government guidance/regulations around cybersecurity of OT/ICSs? (multiple selection) Is your organization required to report industrial security breaches and incidents to any regulatory bodies?



n = 320

**"There are different compliance requirements depending on the location of the plant.
Every country has different regulations and compliance with respect to processing and management. It is difficult for me to talk about it unless you talk about a specific asset."**

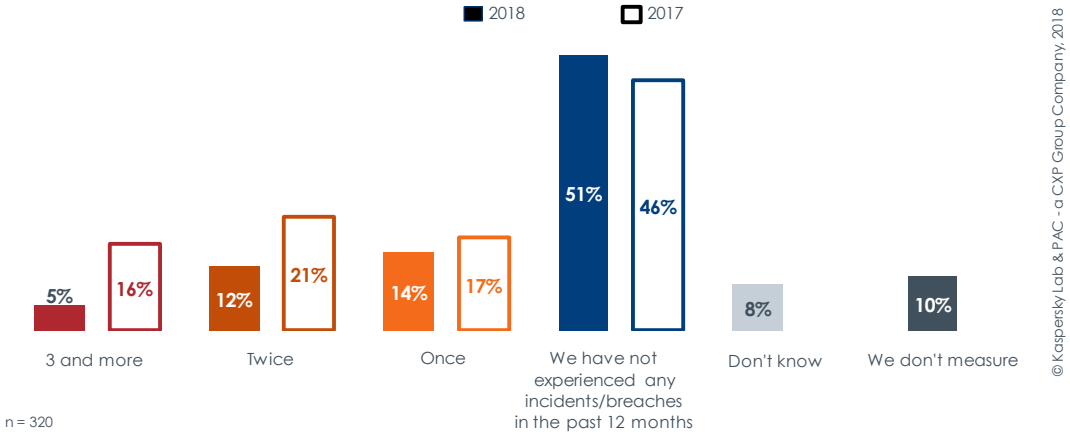
(Oil and gas, US)



ATTACKS AND INCIDENTS

When analyzing the number of attacks or incidents companies experience, it is astonishing to find that 10% of respondents still do not measure the number of incidents and breaches.

How many times did your organization experience any cybersecurity incidents with OT/ICS and/or control system networks in the past 12 months?



n = 320

51% of the companies surveyed did not experience any incidence or breach in the last 12 months. Compared with the 2017 results, the number of these companies has slightly risen.

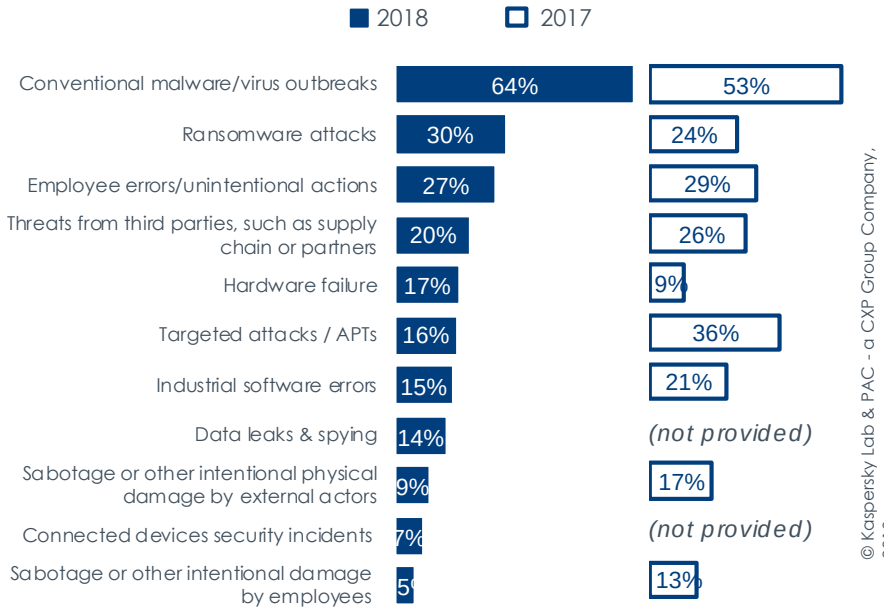
As a result, one can assume that the OT/ICS cybersecurity measures which were implemented over the last year are showing significant results.

When looking more closely at the type of incidents that occurred, there are some interesting insights.

51%

of the companies surveyed state that they did not experience any incident or breach in the past 12 months.

What caused those OT/ICT cybersecurity incidents that occurred in the past 12 months?



Breakdown of responses from companies which have suffered at least one OT/ICS cybersecurity incident over the past 12 months, expressed in % (n = 99)

With increasing connectivity of OT/ICS environments to IT systems and the outside world, conventional malware and virus outbreaks are becoming more and more problematic in the OT/ICS area, too. 64% of companies experienced this in the last 12 month, slightly more than a year ago. The same is true for ransomware (30% in 2018).

Targeted attacks and APTs are a decreasing challenge in the OT/ICS space, maybe due to a better understanding of what a real targeted cyber-attack on the ICS domain is.

It is very interesting to compare this question to the one on page 9 about the most feared attacks, as we see important differences in perception and between what is happening and what is being feared: APT and data leaks/spying are top fears – they rarely happen, but their potentially dire impact makes them very threatening.

If there are security incidents or breaches, usually there are immediate consequences. 54% of those who experienced an incident in the last 12 months noticed damage to their products or services, a significant increase from last year's 29%. 40% detected a loss of customer confidence, while 28% experienced environmental damage.

22% of the companies surveyed experienced a loss of contracts or business opportunities, while 15% suffered damage to equipment. Both could have an immediate impact on the bottom line and revenues.

A violation of regulatory requirements was recognized by 15% of the companies surveyed, which is a pretty stable result compared with last year's results.

Compared to the previous question on the biggest concern on pages 8 and 10, the big difference is the strong rise for the concerns that have the biggest possible impacts, like casualties, criminal liabilities, or national security issues.

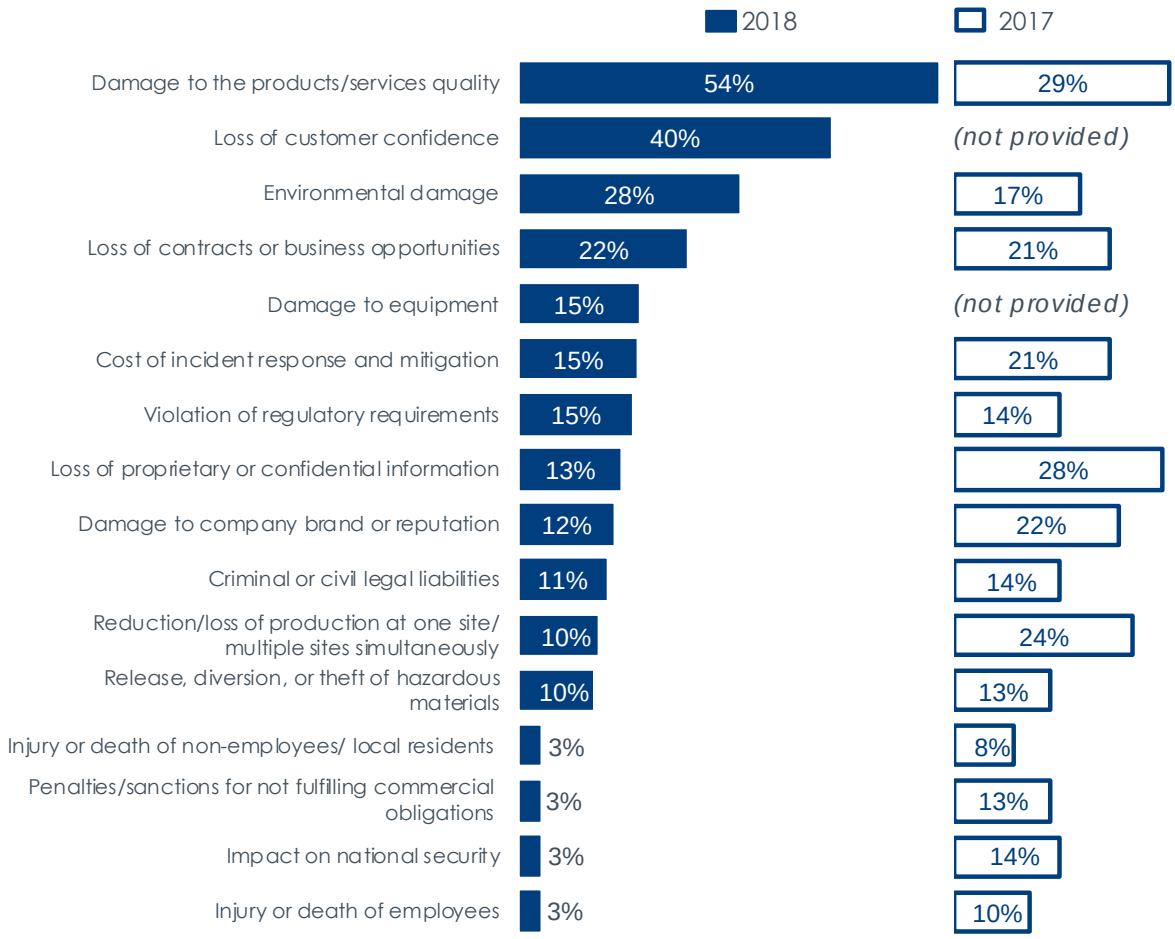
"I don't believe that any external attack would do great harm to our ICS, as we have a strong perimeter defense. On the other hand, internal "attacks" are always an issue and a much bigger problem than any external threat. In fact, our users are a great danger to our ICS since they're not as careful as they should be."

(Metal processing, Russia)

54%

of the companies surveyed with breaches or incidents experienced damage to the quality of their products or services.

And which of the following were the consequences of those breaches/incidents?



Breakdown of responses from companies which have suffered at least one OT/ICS cybersecurity incident over the past 12 months, expressed in % (n = 99)

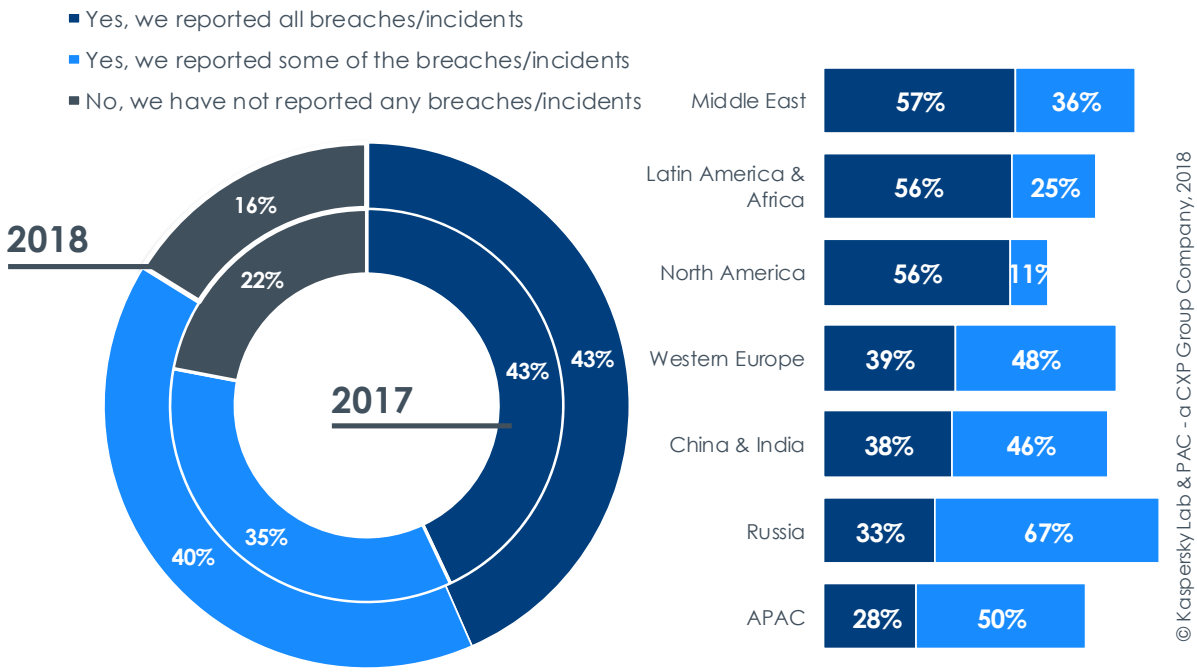
43% of the companies surveyed report all breaches and incidents to a regulatory body, while 40% report at least some incidents and breaches. These findings are pretty stable compared to 2017.

The results by region deliver even more interesting findings. The reporting of all breaches and incidents is much more common in the Middle East, Latin America, and North America. New and even stricter regulations are to be expected all over the world and this will certainly change these differences in the future.

12%

of the companies surveyed with breaches or incidents noticed damage to the company brand or reputation.

Have you reported all, some, or none of those OT/ICS cybersecurity incident(s) to any regulatory bodies?



Breakdown of responses from companies which have suffered at least one OT/ICS cybersecurity incident over the past 12 months, expressed in % (n = 99)

FINANCIAL DAMAGE

Financial damage is always a tricky topic as it is difficult to measure.

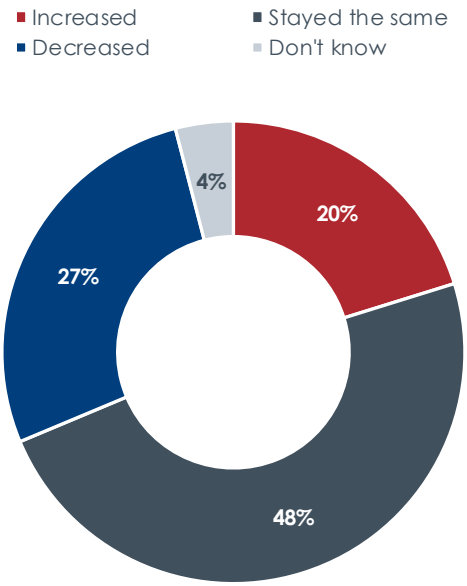
In total, 20% of the companies surveyed experienced an increase in financial costs and damage related to incidents. Compared to the years before, 48% recognized the same financial costs and damage while 27% stated decreasing costs. In view of the constant growth of cyber-attacks, even in the OT/ICS space, the cybersecurity actions being taken are showing positive results at least in some companies.

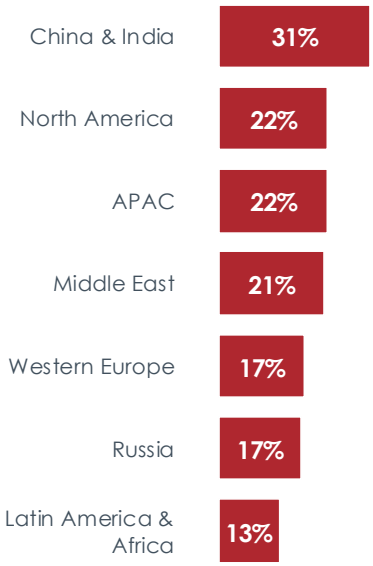
"Cost is one of the most important challenges that organizations face when it comes to ICS cybersecurity implementation. I think making a case for investing money into ICS is tough because there are no direct profits to be gained from doing so."

(Energy and utility, US)

When looking at the regions more closely, it is clear to see that there is quite a difference in the proportion of companies stating an increase in financial costs and damage. While 31% of the companies surveyed in China and India report higher costs and damage, in Latin America this figure is only 13%. This is an indication that giving cybersecurity in the OT/ICS space a major priority helps to prevent incidents and limit the costs and damage associated with it.

Could you please tell me if the overall financial costs/damage of the incident(s) you experienced have increased, stayed the same, or decreased compared to the years before?





Breakdown of responses from companies which has suffered at least one OT/ICS cybersecurity incident over the past 12 months, expressed in % (n = 67)

"ICS systems are very important for us. We're already trying to move on to, for example, the Internet of Things or Industry 4.0. Quite generally, automation in that area is one of the main parts of our future development. Our automation level continues to grow, of course, so we are about to achieve our digital objectives."

(Metal processing, Russia)

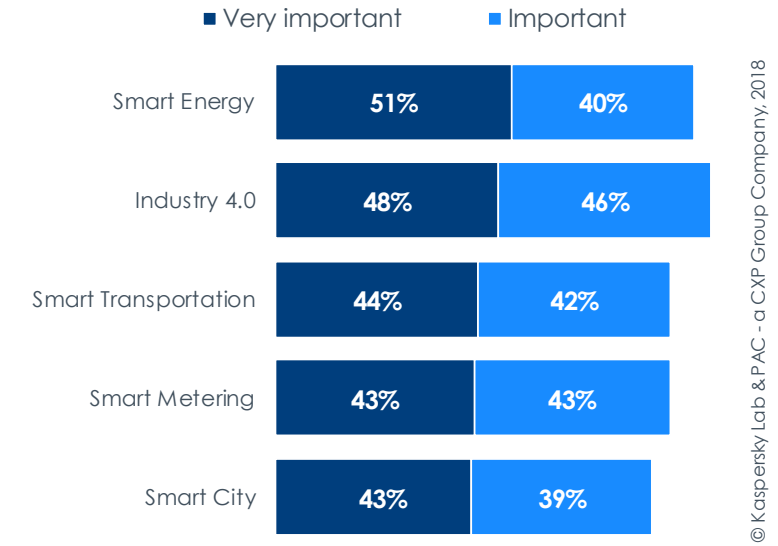
IT TRENDS – THE INTERNET OF THINGS AND CLOUD COMPUTING

Some IT trends and innovations associated with the current digital transformation are not only valid in the IT space, but also affect the OT/ICS area. Most lead to a higher degree of connectivity to the outside world and by that increase operational security risks.

Industrial IoT

Industrial IoT has many different sub-segments, but they are all critical for the future of OT/ICS systems. The most relevant ones for OT/ICS are smart energy and Industry 4.0, smart transportation, smart metering, and smart cities. These segments are all interconnected to various degrees.

Which of the following IoT topics will be very important, important, less important, or not important at all for your organization over the next 12 months?



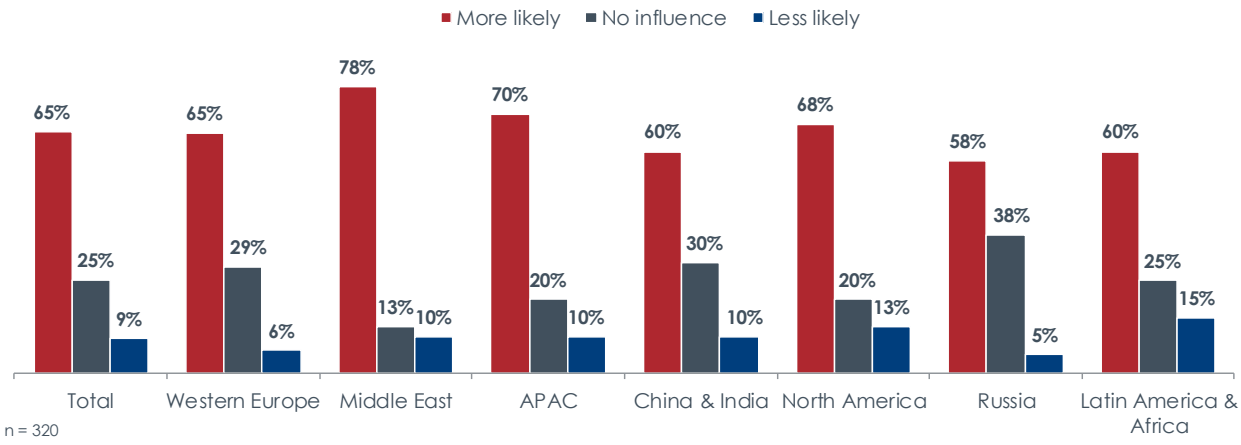
n = 320

("Less important" and "not important at all" not shown)

"Since the business network is always exposed to the Internet, most of the attacks happen through the public network. So, if there were a connection between the process control network and the IT network and the IT network got compromised, the process control network might be affected too."

(Oil and gas industry, UAE)

Do you think OT/ICS cybersecurity risks are more likely or less likely with the IoT or will this not have any influence?



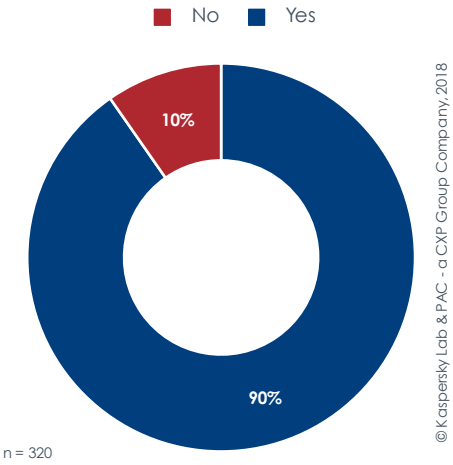
n = 320

The companies surveyed have a pretty clear view on the OT/ICS cybersecurity risks associated with IoT. On a global level, 65% of the companies surveyed expect a higher likelihood of cybersecurity risks due to IoT. 25% expect no influence and 9% anticipate a positive effect. Even if analyzing the different regions, the differences are not huge.

(Wireless) networks and cloud computing in OT/ICS

The IT trends of wireless networks and cloud computing have now reached the OT/ICS space as well. However, one should not forget the additional risks linked to that, e.g. breaches from the outside, intercepts and manipulations of data and control instructions.

Do you use wireless networks for your industrial network?

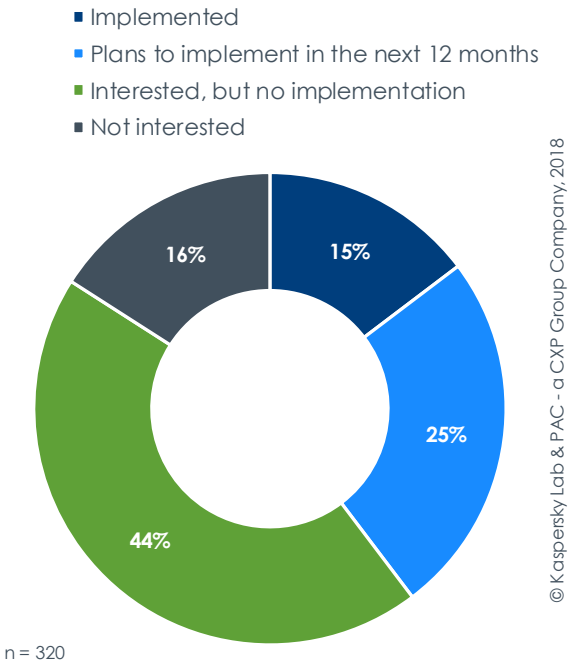


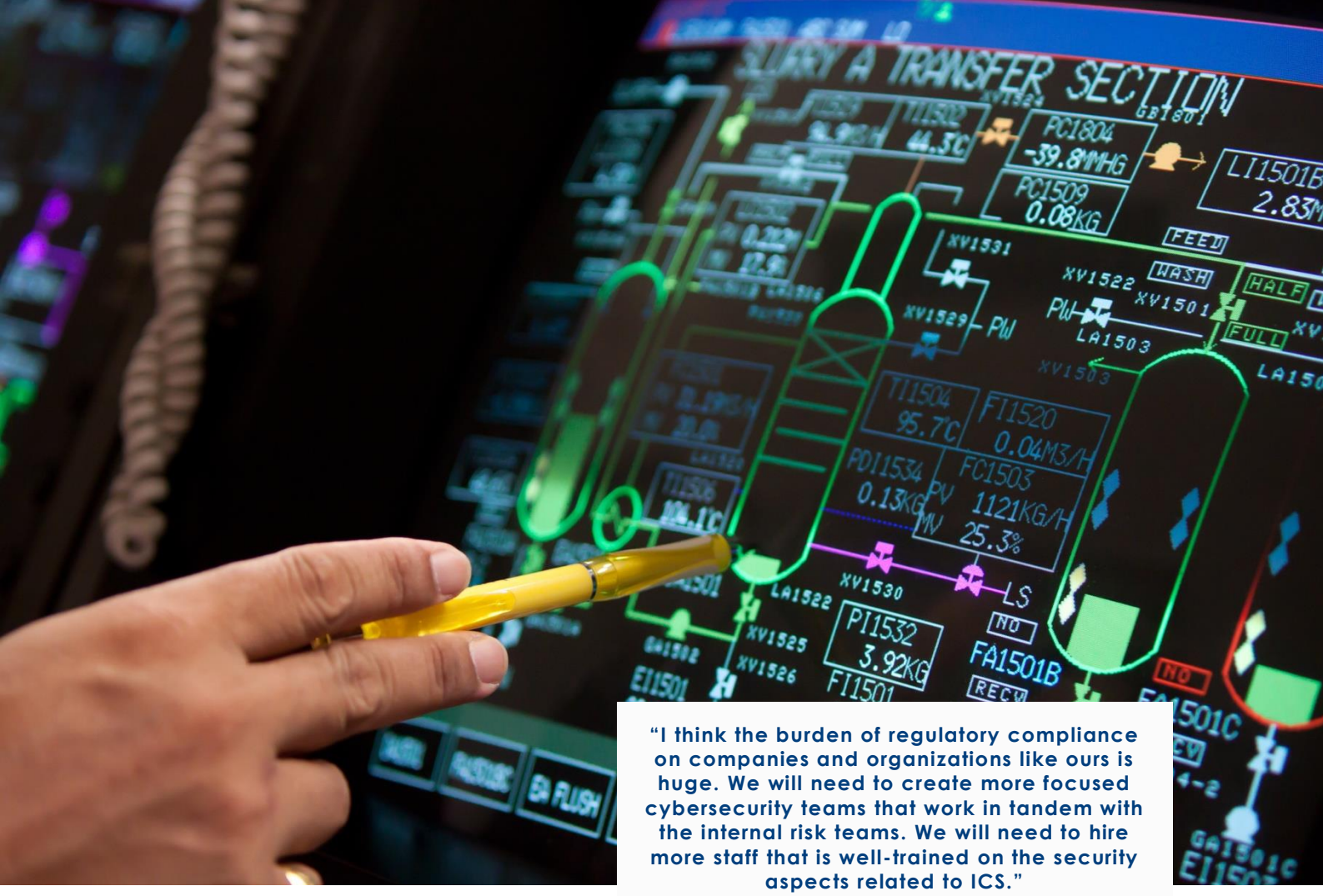
Cloud computing, especially SCADA as a Service, is much less accepted. Only 15% of the companies surveyed have already implemented SCADA as a Service, 25% plan to implement it in the next 12 months, and 44% are interested but have no concrete plans for implementation.

"We have adopted SCADA for monitoring. We are using SCADA for maintaining voltages, currents, trip alarms, the process, the flow rates, and for a lot of sensitive data and information like temperature, flow rates and frequencies etc."

(Energy and utility, US)

Have you already implemented, or do you have plans within the next 12 months to adopt cloud solutions for industrial networks like SCADA as a Service? Or is this not planned, but your company is interested in it?





"I think the burden of regulatory compliance on companies and organizations like ours is huge. We will need to create more focused cybersecurity teams that work in tandem with the internal risk teams. We will need to hire more staff that is well-trained on the security aspects related to ICS."

(Oil and gas industry, UAE)

WHAT'S NEXT: STRATEGIES AND MEASURES

In order to master the OT/ICS cybersecurity challenges, companies need to have a strategy, an organization, and measures in place. Obviously, this organization and these measures need to have sufficient funding to work smoothly.

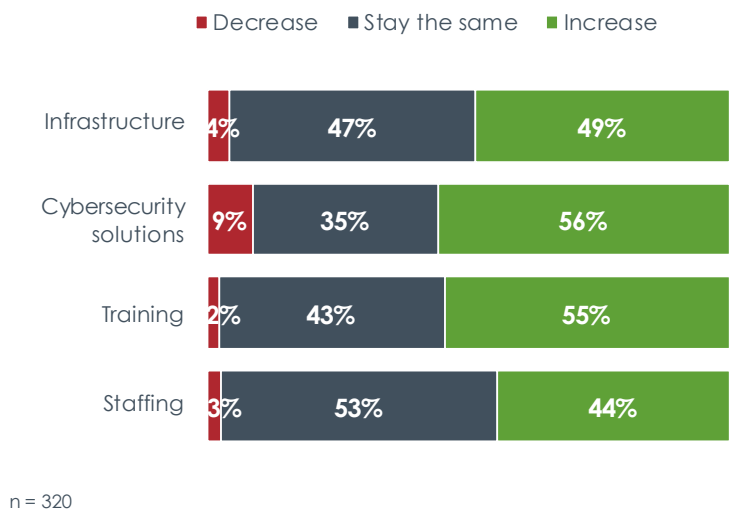
INVESTMENTS

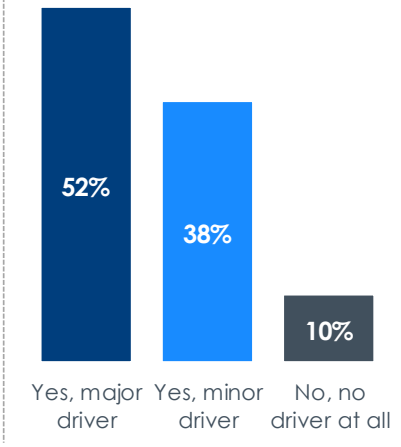
With a growing number of cyber-attacks and increasing risks, a huge majority of companies are increasing their OT/ICS cybersecurity investments or at least keeping the investments steady.

The influence that incidents or breaches have had on investment decisions is also showing a direct connection. 52% of the companies surveyed see incidents and breaches in the past as a major driver of future investments, while only 10% state that they are unimpressed by such events.

In the cybersecurity solution segment, we see a slightly different picture. While 35% of the companies surveyed expect investments to stay the same as in the previous year, 56% expect them to increase.

Do you expect your budgets for the following OT/ICS areas to decrease, to stay the same, or to increase within the next 2 years? Are potential incidents/risks or the breaches you may have experienced before a major, minor, or no driver for these investments?





(ORGANIZATIONAL) APPROACHES AND STRATEGIES

Stakeholders

From an organizational point of view, there are different possible approaches to organizing OT/ICS cybersecurity. The major vectors are:

- the focus on OT/ICS
- production intensity
- outsourcing culture.

"As a middleman, I need to report to the IT, ICS, and specifically the cybersecurity department, which is included in our internal IT."

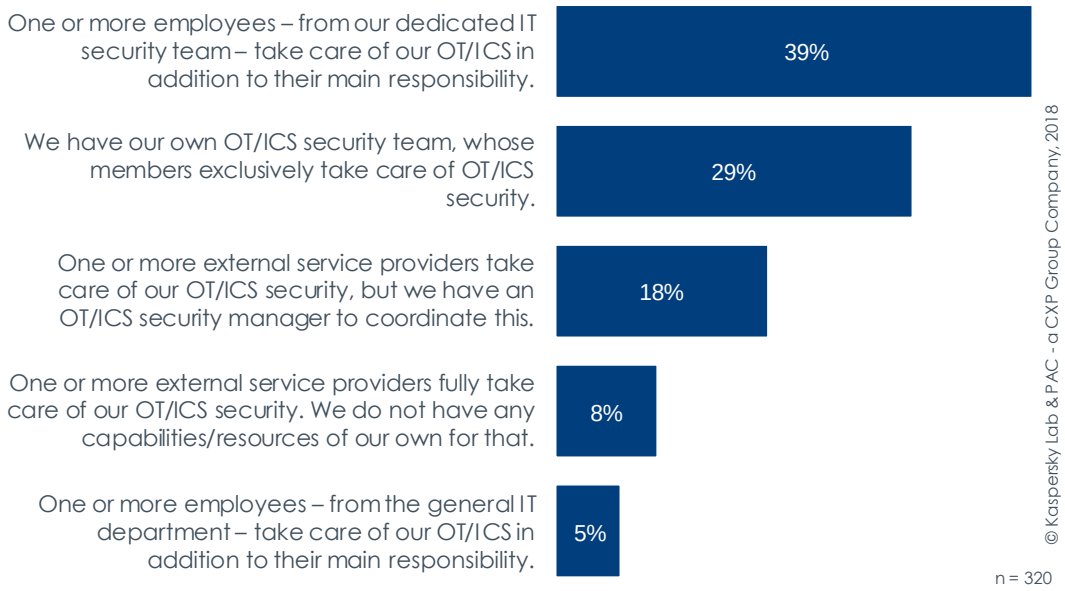
(Metal processing, Russia)

The survey clearly highlights a trend that ICS organizations tend to keep management of their OT/ICS cybersecurity internally, with only 8% of the companies fully outsourcing this function currently. Companies loathe to outsource the cybersecurity of those core parts of their value chain, and furthermore, there are still too few outsourcing providers that are capable of assuming this type of workload.

"There are a lot of threats in the industry today; every few months we hear about instances of hacking, data theft, or a cyber-attack on some plant. This topic should be prioritized at management level and all other levels informed accordingly."

(Oil and gas industry, UAE)

How is the responsibility for OT/ICS security organized in your company?

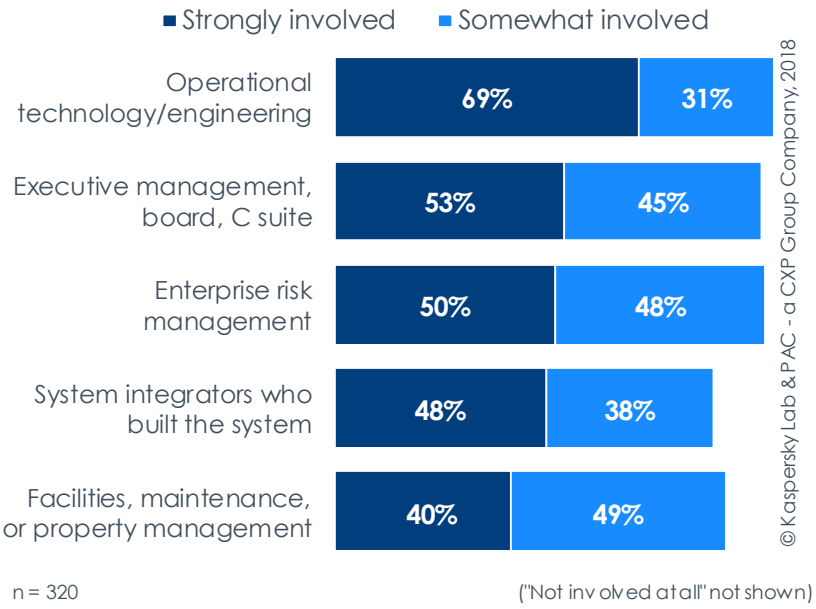


Ideally, OT/ICS cybersecurity is not seen as vicarious agent and is supported by different enterprise functions. Therefore, at 69% of the companies surveyed, operational technology/engineering is strongly involved in OT/ICS cybersecurity, while at 53% of companies, OT/ICS cybersecurity is represented and supported by board or C-suite level members. Also, the system integrators who built the systems (48%) as well as the teams who are in charge of facility, maintenance, and property management (40%) are strongly involved. All these stakeholders are crucial in order to have all information and planning on the table so that OT/ICS cybersecurity is performed correctly. Collaboration is a key catalyst of cybersecurity, and even more so for ICS/OT cybersecurity.

"We have installed a special department for cybersecurity as it is a growing concern for us. We have incorporated some measures regarding cybersecurity specifically for our ICS and we also try to improve the security in our network."

(Metal processing, Russia)

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



n = 320

("Not involved at all" not shown)

"Recently, there has been good progress and we see that top-level executives are getting more involved in discussions about the risk associated with cyber-attacks within our organization. The risk and compliance teams have also played an important role in driving awareness and educating top-level and low-level teams about the impact of these attacks. Overall, I think more effort is required to get the executives to shift from mere awareness to action. I believe there is a need for commitment to ongoing assessments, remedy, and assurance of cyber risk."

(Energy and utility, US)

Strategic approach

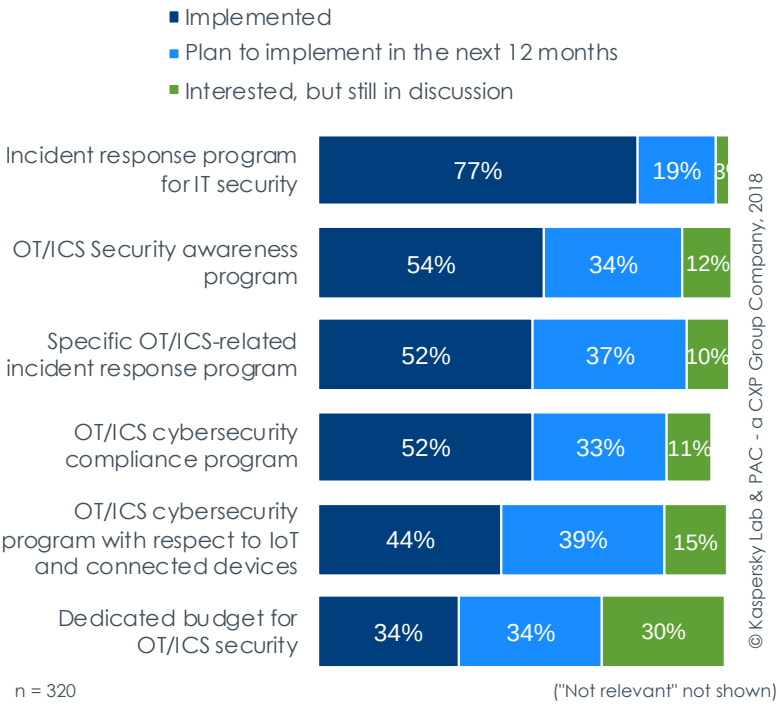
Besides a general IT and OT/ICS cybersecurity strategy, which is essential in our times, a range of dedicated programs are key for a successful OT/ICS cybersecurity approach.

Currently, 77% of the companies surveyed have implemented an incident response program for IT security and 19% are planning to implement such a program in the next 12 months. A specific OT/ICS incident response program has been implemented in only 52% of the companies surveyed; 37% are planning such a program in the next 12 months, while 11% are still in discussion. OT/ICS security awareness programs have been implemented at 54% of the companies surveyed; 34% are planning to implement one in the next 12 months. OT/ICS cybersecurity compliance programs have been implemented at 52% of companies; 33% will implement such a program within 12 months. All this is an indication that OT/ICS cybersecurity is being taken seriously, at least at a first glance.

"The top three challenges in combating cyber threats are understanding the risk, getting a control system engineer on board, and having a clear instructional approach."

(Energy and utility, US)

Which of the following initiatives does your company have already in place, is planned for the next 12 months, of interest but still in discussion, or not relevant?



"We have awareness programs. These are processes we already understand; work practices, policy, and standard operating procedures for each and every service. These programs are already embedded within the training."

(Oil and gas industry, UAE)

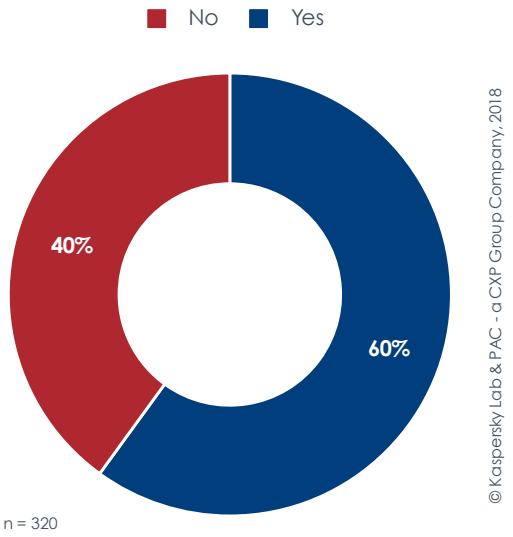
Which of the following initiatives does your company have already in place, is planned for the next 12 months, of interest but still in discussion, or not relevant?

Only 34% of the companies surveyed have a dedicated OT/ICS security budget in place, another 34% will define a budget within the next 12 months, and 30% are still in discussion. However, for a dedicated OT/ICS cybersecurity group or a dedicated manager supervising service providers, a dedicated budget is needed.

Besides individual programs, which are definitely important, a general OT/ICS policy/program should be in place. This general policy or program should be approved by senior management and documented for later reference.

By ICS security policy we mean a program or plan of activities and measures to be taken to protect the security of an organization's industrial control systems, including activities to react and respond to a cyber-attack or threat.

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



60%

of the companies surveyed have an approved and documented OT/ICS cybersecurity policy or program.

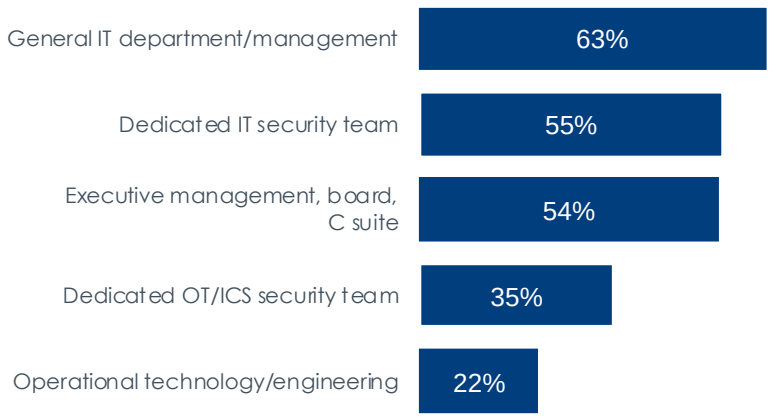
"You also have national standards and similarly you develop a security policy including all requirements and which acts as a base document."

(Oil and gas industry, UAE)

On a worldwide level, 60% of the companies surveyed have such an approved and documented OT/ICS cybersecurity policy and program in place, 40% do not. In terms of geographies, North America is clearly most advanced in this area.

It is interesting to see who is responsible for approving an OT/ICS security policy. It is clear that there is not only one department in charge of this – we see a collaborative approach of the general IT department (at 63% of the companies surveyed), dedicated IT security teams (55%), senior management (54%), and dedicated OT/ICS security teams (35%). Only at a minority (22%) of companies is operational technology or engineering part of the approval center, which could be problematic. Again, the collaborative nature of cybersecurity as well as its enterprise-wide reach and impacts are not fully understood by the companies surveyed.

Which of the following job functions or departments are responsible for the approval of the OT/ICS security policy?



Breakdown of responses from companies which have an approved documented OT/ICS cybersecurity policy, expressed in % (n = 192)

54%

of the companies surveyed state that senior management is responsible for the approval of OT/ICS security policies.

OT/ICS CYBERSECURITY MEASURES

Last but not least, it is important to take a closer look at the different OT/ICS cybersecurity measures that are implemented, planned for the next 12 months, or still in discussion.

"We mainly focus on perimeter security. No vulnerability management involved. We will continue to focus on network protection in most cases."

(Metal processing, Russia)

"It is important to implement an air gap security measure as it ensures that the data is going from one side and restricts the other parties in use of the data."

(Oil and gas industry, UAE)

Technology-oriented measures

For most of the technology-oriented measures, it can be said that what was planned in 2017 has not been realized accordingly.

Anti-malware and antivirus are standard solutions (implemented by 97% of the companies surveyed), as well as application protection (91%).

Other technology-oriented measures are still not implemented at all companies. Even though these technologies are a given in traditional IT cybersecurity, in OT/ICS cybersecurity they are less often in use.

For example, network monitoring and log analysis – a given in traditional IT security – is implemented for OT/ICS purposes at only 56% of the companies surveyed. The same is true for network segmentation (47% of companies) or intrusion detection (45%). These points are the foundation of any viable OT/ICS protection. Air gapping is a must-have. The basic idea is that there is no connection between OT/ICS networks and the traditional IT networks or the Internet. 34% of the companies surveyed state that they have implemented air gapping; 39% are planning implementation within the next 12 months. The low level of maturity is worrying.

In addition, the majority of companies are implementing IoT and Industry 4.0. However, a connection to the OT/ICS systems is needed for these technologies to be effective.

Vulnerability scanning

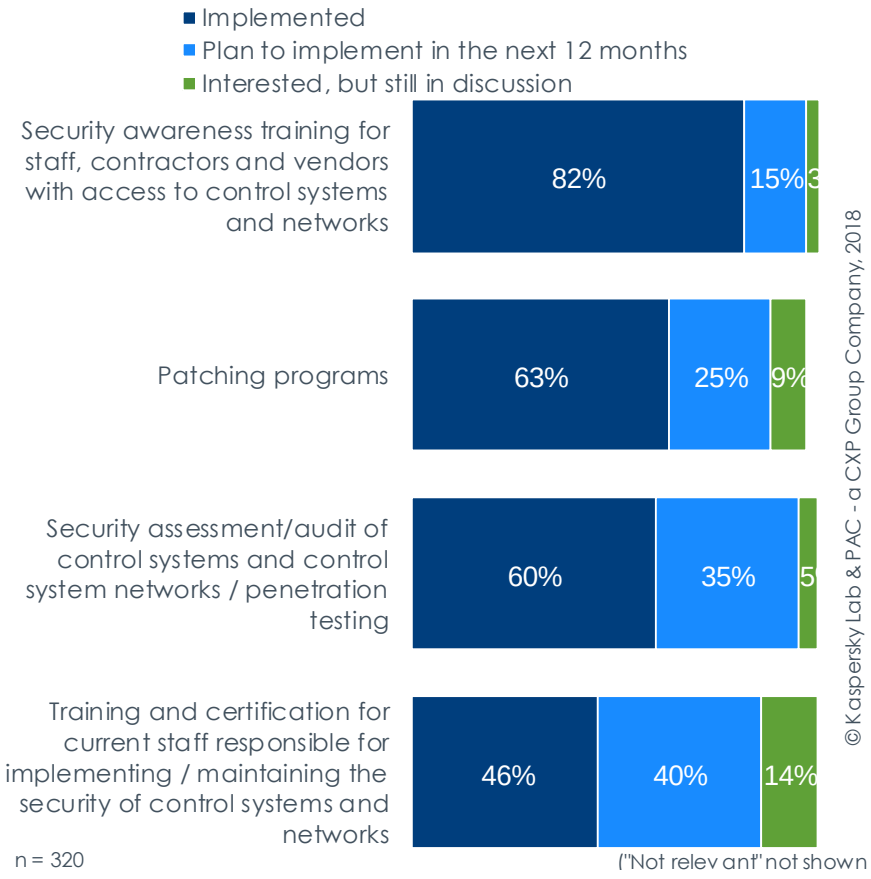
Vulnerability scanning is a fundamental task to make sure systems and applications are up to date and known problems are fixed. Obviously, vulnerability scans should be continuously performed or at least be done with every vulnerability database update. Another example of the lack of maturity in OT/ICS cybersecurity is that most of such scans are targeted only at traditional IT components (like OS for SCADA), not for specific ICS components.

Most of the respondents using vulnerability scanning use it regularly, i.e. every week (46%) or every 2 weeks (26%). The remaining 28% did not understand the concept.

Process-oriented measures

Security awareness training for staff, contractors, and vendors with access to control systems and networks are widely implemented (82% of the companies surveyed). Security assessments and audits of control systems and their networks, including penetration tests, are also important but less often implemented. Only 60% of companies have such assessments and audits implemented, but at least 35% of the companies surveyed are planning to implement such measures in the next 12 months. As in most IT segments, training and certifications for current staff responsible for implementing or maintaining the security of control systems and networks are implemented at only 46% of the companies surveyed; 40% of companies plan to do so in the next 12 months.

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



82%

of the companies surveyed state that they have implemented security awareness training, but only

46%

have training and certification programs implemented for current staff implementing and maintaining the security of control systems and networks!

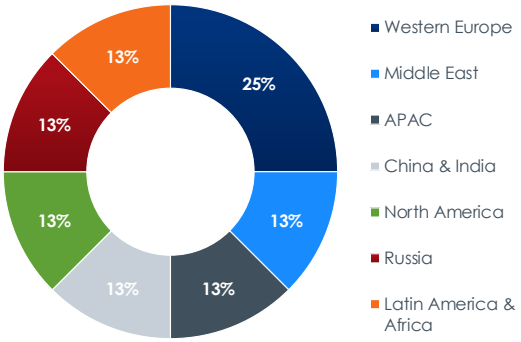
Patching programs are an easy way of securing systems but are limited by the production issues of OT/ICS systems. Patching can alter the way OT/ICS systems work, explaining the low level of implementation of this fairly effective cybersecurity process. While 63% of the companies surveyed have such programs in place and an additional 25% are planning to implement such programs in the next 12 months, at least some parts of the IT industry are talking about evergreen in order to ensure that systems are always up to date and secure. In addition, nearly half of the companies regard Industry 4.0 as very important. Such solutions are usually implemented in an agile manner, which not ideal for a fixed-frequency patching or update program.

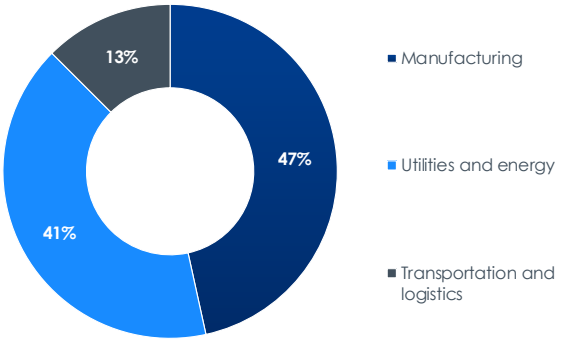
APPENDIX

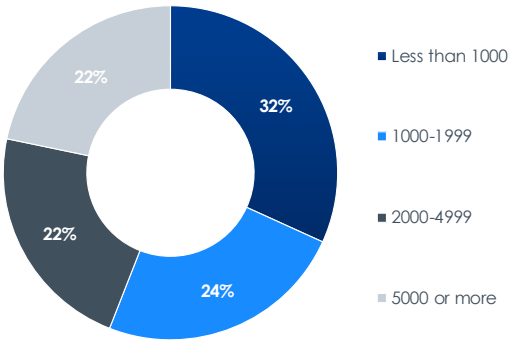
METHODOLOGY

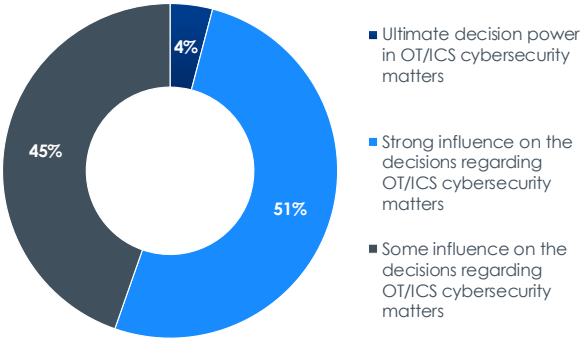
In 2016, Kaspersky Lab launched a new solution, Kaspersky Industrial Cybersecurity. To obtain deeper insights into the current state of ICS cybersecurity, Kaspersky Lab conducted its first ICS Cybersecurity Risk Study in 2017. Within this online study, 359 ICS cybersecurity professionals were surveyed – covering Europe, North America, Latin America, the Middle East, and APAC.

This study report is the outcome of the follow-up project in 2018, which is based on a CATI survey (computer-assisted telephone interviewing). PAC interviewed 320 global professionals with decision-making power on OT/ICS cybersecurity. The computer-aided telephony interviews were conducted with companies from the manufacturing, utilities, and transport sectors.









In addition to the quantitative study, 12 qualitative expert interviews were conducted. The quotations given within this report are an (anonymized) excerpt and are intended to substantiate the study results.

DISCLAIMER, USAGE RIGHTS, INDEPENDENCE, AND DATA PROTECTION

The creation and distribution of this study was supported by Kaspersky Lab.

For more information, please visit www.pac-online.com.

Disclaimer

The contents of this study were compiled with the greatest possible care. However, no liability for their accuracy can be assumed. Analyses and evaluations reflect the state of our knowledge in June 2018 and may change at any time. This applies in particular, but not exclusively, to statements made about the future. Names and designations that appear in this study may be registered trademarks.

Usage rights

Independence and data protection

This study was produced by Pierre Audoin Consultants (PAC – a CXP Group Company). Kaspersky Lab had no influence on the analysis of the data and the production of the study.

The participants in the study were assured that the information they provided would be treated confidentially. No statement enables conclusions to be drawn about individual companies and no individual survey data was passed to Kaspersky Lab or any other third party. All participants in the study were selected at random. There is no connection between the production of the study and any commercial relationship between the respondents and Kaspersky Lab.

ABOUT KASPERSKY LAB

Kaspersky Lab is a global cybersecurity company which has been operating in the market for over 20 years. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into next generation 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 Lab technologies and we help 270,000 corporate clients protect what matters most to them.

Kaspersky Lab maintains a high level of expertise in industrial cybersecurity, supported by Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT). It is a global project launched by Kaspersky Lab 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 Lab 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 technologies and services designed to protect operational technology layers and elements of industrial enterprises – including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers – 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: ics.kaspersky.com.

Contact: cip@kaspersky.com

Follow us: https://twitter.com/KasperskyICS

Kaspersky Lab AO
39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation
Tel.: +7-495-797-8700
info@kaspersky.com
www.kaspersky.com

ABOUT PAC

Founded in 1976, Pierre Audoin Consultants (PAC) is part of CXP Group, the leading independent European research and consulting firm for the software, IT services, and digital transformation industry.

CXP Group offers its customers comprehensive support services for the evaluation, selection, and optimization of their software solutions and for the evaluation and selection of IT services providers, and accompanies them in optimizing their sourcing and investment strategies. As such, CXP Group supports ICT decision-makers in their digital transformation journey.

Further, CXP Group assists software and IT services providers in optimizing their strategies and go-to-market approaches with quantitative and qualitative analyses as well as consulting services. Public organizations and institutions equally base the development of their IT policies on our reports.

Capitalizing on 40 years of experience, based in 8 countries (with 17 offices worldwide) and with 140 employees, CXP Group provides its expertise every year to more than 1,500 ICT decision-makers and the operational divisions of large enterprises as well as mid-market companies and their providers. CXP Group consists of three branches: Le CXP, BARC (Business Application Research Center), and Pierre Audoin Consultants (PAC).

For more information please visit: www.pac-online.com

PAC's latest news: www.pac-online.com/blog

Follow us on Twitter: @CXPgroup

A CXP GROUP COMPANY

PAC – a CXP Group Company
Holzstr. 26
80469 Munich, Germany
Tel.: +49 (0)89 23 23 68 0
info-germany@pac-online.com
www.pac-online.com

CXP Group

BARC · Ie CXP · PAC