Architecting the Next Generation for OT Security

Powered by the Ponemon Institute

Publication Date: December 2021

Ponemon INSTITUTE

Applied Risk

Executive Summary

pg. 3-4

1

Architecting the Next Generation for OT Security

pg. 5-7

2

Key Research Findings

pg. 8-22

3

Recommendations

pg. 23-25

4

Methodology

pg. 26-29

5

Conclusion

pg. 30-32

Executive Summary

This is a time of change and challenges. It's an era that is both transformative and disruptive, shaped by digital technologies that are improving billions of lives around the world, even as they make us vulnerable in ways we never anticipated.

This digitalisation has been a fact of life for quite some time, but it is also becoming a factor in the operation of critical infrastructure and other industrial environments at an accelerating speed. At the same time, the Operational Technology (OT) systems that monitor and control industrial equipment, assets, processes and events in critical infrastructure are facing more and more threats from increasingly sophisticated malicious actors, including nation states.

In this dynamic environment, it is important to understand the thoughts and concerns that drive organisations to take action to keep their OT domains safe, secure and resilient. Applied Risk has undertaken the research needed to gain that understanding and to take a forward-looking approach to crucial questions about how to architect the next generation of OT Security solutions.

In this document, we present the results of that research, which is based on data collected from IT and OT security practitioners. We use these data to assess current trends in the OT Security space, paying special attention to people-, process-, and technology-related issues, and offer recommendations on responses to these trends. Additionally, we describe current conditions in the OT Security realm and offer insight into the OT Security trends that are likely to emerge over the next two to four years.

This report was based on data compiled by the Ponemon Institute, which acted on Applied Risk's behalf to survey 1,005 IT and OT security practitioners in the United States (597) and Europe (408).[1] Respondents to the survey were asked to answer questions about how to architect the next generation of OT Security solutions. All respondents have responsibility for securing or overseeing cyber risks in the OT environment and understand how these risks impact the state of cyber security within their organisations. The research was then complemented by input from Applied Risk's own engagements and assessments as well as analysis from our subject matter experts.

1 European countries include the United Kingdom, France, Germany, the Netherlands, the Nordic states and Switzerland.

The results of this survey indicate that there are three major factors at work – People, Processes, and Technology. Here's how they play out in relation to Prevailing Practices, Current Conditions, and Future Directions:

	People	Processes	Technology
Prevailing Practices Have been evolving	• Low OT Security headcount • Plans for hiring additional staff • Ownership of OT Security Leadership not adequately defined • Lack of dedicated OT Security teams	• Widespread adoption of OT-specific, risk-based standards • Legislation helps drive adoption of standards • Lack of incident response plans • Lack of clarity on third-party and supply-chain security practices	• Convergence of IT/OT systems important and beneficial • Adoption of zero trust measures • Air gaps still in use • Use of advanced and enabling technologies still lagging behind • Interest in Security Operations Centres (SOCs) growing
Current Conditions Snapshot	• Rising number of sophisticated nation-state attacks • Lack of industry-wide governance models	• Continuity and compliance are key drivers of investments in OT Security • Gaps remain in risk reduction, incident response, asset identification • Top source of concern: access management	• OT networks lack technology that can maximise security • Systems are isolated and fragmented • Emerging technologies such as cloud computing are gaining attention
Future Directions Next two to four years	• Additional hires: OT Security headcount may double in 2-4 years • Making greater efforts to develop skill pool for OT Security	• Supply chain audits and introduction of vendor security requirements are likely to increase as supply chain attacks are expected to happen more often • IT/OT convergence should be part of the solution	• Adoption of advanced and enabling technologies will be crucial • Continued reliance on existing technologies • Security Operations Centres (SOCs) are likely to make an impact

1 Architecting the Next Generation for OT Security

1. Architecting the Next Generation for OT Security

Maximising safety and minimising unplanned outages are the top operational priorities for the organisations represented in this research. Reducing inefficiencies and minimising operating costs are also high priorities, as is the ability to maintain plant connectivity. Respondents see the convergence of IT and OT systems as one of the primary drivers toward meeting these organisational targets. At the same time, though, they note that attackers are focusing more and more on industrial environments and are quickly developing OT skills – and that this shift that has resulted in more sophisticated and clandestine attacks.

The results of the survey indicate that companies are struggling to develop their OT Security maturity at a pace comparable to speed with which attackers are developing their own skill sets. Meanwhile, the OT landscape is becoming more complex due to IT/OT convergence and to the introduction of Industrial Internet of Things (IIoT) devices, virtualisation, and cloud computing in these environments. The overall sense of the respondents is that they need to do more to ensure that the business benefits of these new technological developments can be realised in a secure manner.

More than half of the respondents believe that their cyber readiness is not at the right level yet and that they are not able to adequately minimise the risk of cyber exploits and breaches in the OT-environment. As such, it is clear that there is still work to be done in general and across the board.

The respondents are aware that they need to upskill their staff and that of their service providers and that they need better procedures. But above all, they understand that they will need enabling technologies to accelerate OT Security maturity. In summary, a combination of people-, process-, and technology-centric controls will remain key.

The current state of cyber readiness in the OT environment

On a scale from 1 = low readiness to 10 = high readiness, 7+ responses presented

Figure 1

> "Overall, increased connectivity and new technologies have been a great improvement for our OT systems, but they've also introduced clear risks. We can't address those risks properly unless we take an architectural approach to designing those systems – not just the OT systems themselves, but the links to IT too. In this highly integrated and complex IT-OT environment vulnerabilities are easily overlooked. Embedding architecture thinking gave us what we need to guard our operations against future threats to our assets and our data."
>
> Site Automation Manager - Medical device manufacturer

Prevailing Practices in OT Security

The research conducted by Ponemon identifies a number of prevailing practices in OT Security. Such trends offer insight into the question of how the next generation of OT Security should be architected. The identified practices fall into three categories: People, Processes and Technology:

People

- OT Security Leadership is a topic that continues to lack clear definition. Ownership of OT Security floats between Operations, Engineering, IT, and Risk and Compliance, and there is no clear industry-wide accepted model for governance. These gaps should be filled to maximise the effectiveness of OT Security.
- Less than half of the respondents say their organisations have enough staff to manage cyber security risks today. On average, organisations expect to double the headcount dedicated to OT Security within the next two to four years.
- Not all organisations have a team dedicated to OT Security programmes.

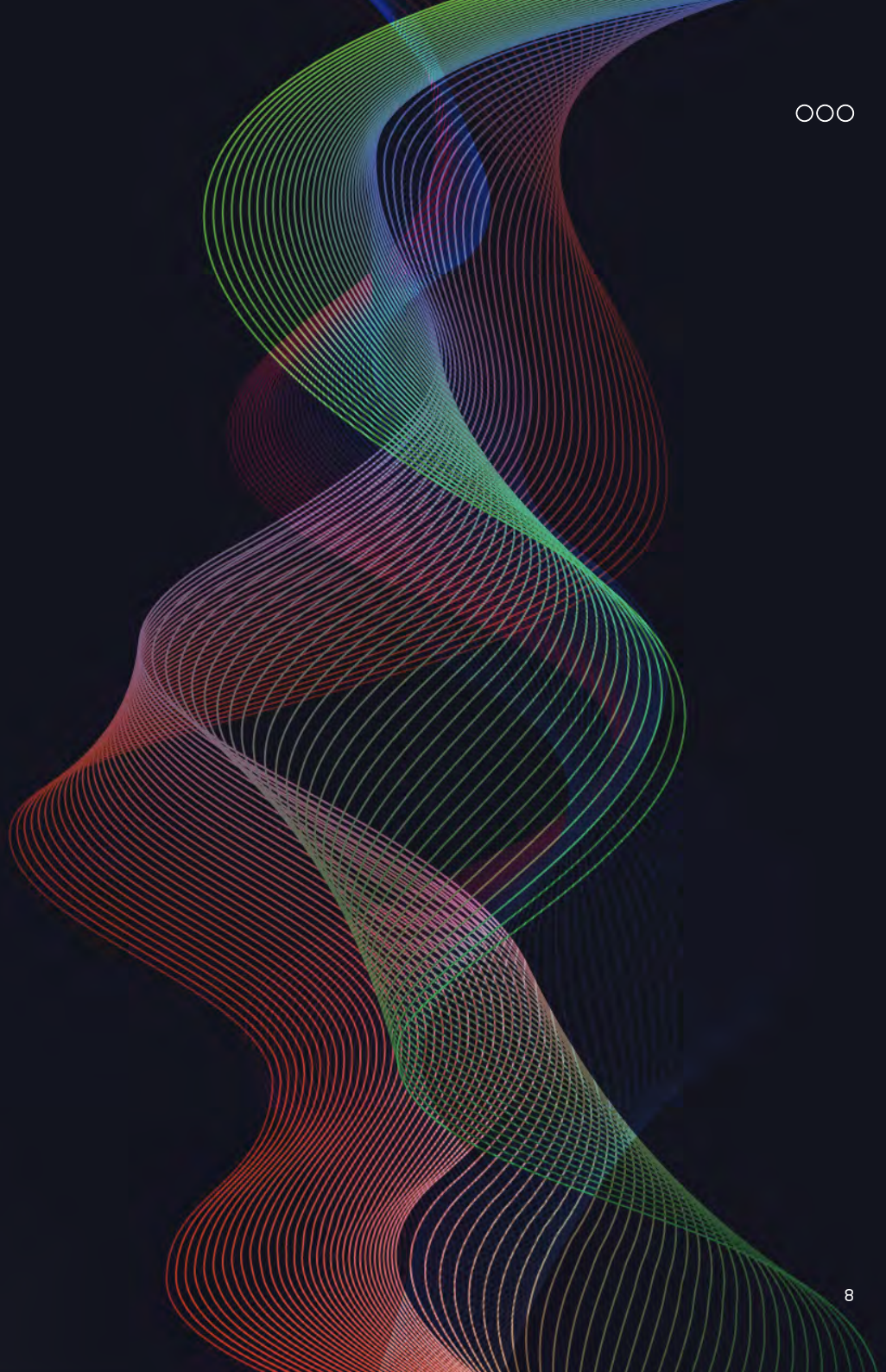
Processes

- Just over 75% of the respondents say their organisations use an OT/ICS-specific cyber security standard to manage their security programme. Within this group, the most commonly adopted standard for minimising OT Security risks is the IEC 62443 series.
- Almost all standards take a risk-based approach, based on the concept that it is neither efficient nor sustainable to try to protect all assets in equal measure.
- Not all organisations have an incident response plan.
- The majority of respondents say their organisations are at risk because of their inability to ascertain the security practices of relevant third parties and to mitigate cyber risks across the OT external supply chain.
- Legislation and regulation are important drivers for starting an OT Security Programme.
- Despite concerns about the security of the supply chain, comprehensive audits are rarely conducted. Only 33% of respondents say their organisations conduct regular audits of their own main suppliers, and only 27% conduct due diligence prior to contracting with new suppliers. Respondents agree that their organisations are at risk because of their inability to ascertain the security practices of their suppliers.

Technology

- The importance of IT and OT systems convergence will continue to increase, since it brings business benefits. The benefits of this convergence can be realised when strong OT security programmes are implemented.
- Basic technical measures such as patch management and secure remote access are still considered most effective in securing the OT domain. However, new security solutions continue to emerge or cross over into the OT domain.
- Zero trust is seen as an important driver in securing OT domains.
- Security Operations Centres (SOC) are expected to transform how OT cyber security risks are managed. Organisations are expected to integrate IT- and OT-related SOC services.
- Organisations have been slow to adopt advanced technologies such as automation, machine learning, orchestration, and artificial intelligence (AI), making rapid detection of security exploits and data breaches difficult.
- Air gaps are not seen as the ultimate remedy to prevent security compromises. However, 32% of the respondent are still using air gaps to prevent compromises, a surprisingly high number in view of the increasingly digitalised business landscape.
- The respondents see that the lack of enabling technologies undermines their organisations' ability to deal with the rising number of attacks perpetrated by increasingly sophisticated attackers, including nation states. Their number-one worry is the prevalence of sophisticated attacks targeting their organisations.

2 Key Research Findings



2.1 The current state of OT cyber security

What keeps OT Leadership awake at night?

OT Leadership is concerned about multiple topics, some of which blur the boundaries between People, Processes, and Technologies. Many of these worries stem from recent events. Notably, survey respondents' most commonly reported concern was the rise in increasingly sophisticated attacks against critical infrastructure, as shown in Figure 2. This seems to be related to the second most common point of concern, which is the supply chain. (This makes sense, in light of recent attacks exploiting SolarWinds and vulnerabilities in Microsoft Exchange.) At the same time, OT Leadership also flagged the ongoing digitalisation of the OT domain (OT/IT convergence, cloud computing, etc.) as a significant OT Security concern, saying they did not believe this was being implemented in a controlled way.

Interestingly, respondents with an OT background scored all these items higher than those with an IT background. This may stem from the fact that these concerns are already quite well known in the IT domain but are relatively new to the OT domain.

> We are moving more and more functionality away from the on-premise model to the cloud. It is a positive step that gives us more flexibility, but it works because we take an architectural approach to the system and place special focus in managing access control effectively. Cloud cyber security is on our horizon because we expect that the introduction of IIoT devices will make this even more relevant in the near future."
>
> Global systems and Networking Architect for Substations and Metering – Large power utility

In the future, what OT trends will keep OT leadership awake at night?

More than one response permitted

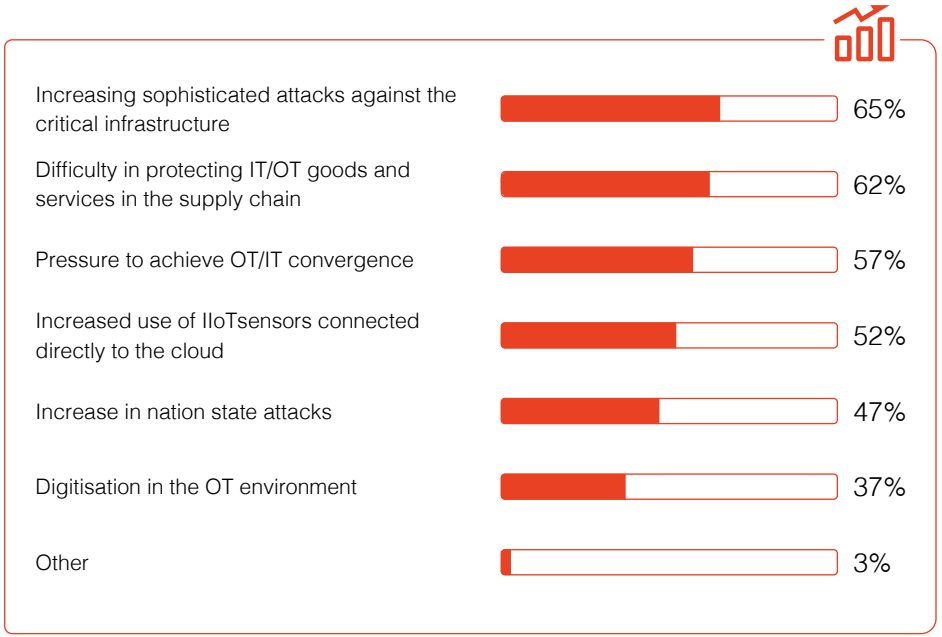


Figure 2

Pain Points in managing OT Security

Respondents were asked to rate the “pain” associated with managing cyber security within the OT environment, ranging from 1 = minimal pain to 10 =severe pain.
The results are completely in line with responses to the question of what keeps OT Leadership awake. The distribution of severe pain responses (that is, responses of 7+ on the 10-point scale) shows that the respondents are worried about three main things:

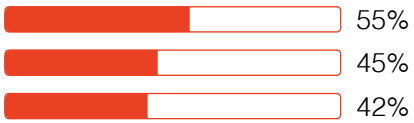
- The rise of sophisticated attacks (66%)
- The growing complexity of their own environments (55%)
- The fact that the defensive capacities lag behind:
  - People (e.g., lack of skilled personnel, 51%)
  - Process (e.g., dependency on manual processes that are prone to errors and unreliability, 51%)
  - Technology (e.g., not having the necessary technologies in OT networks, 59%)

Why is the management of OT security painful?

Seven responses permitted

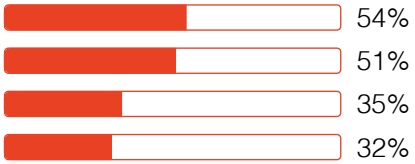
Attack surface

Complexity

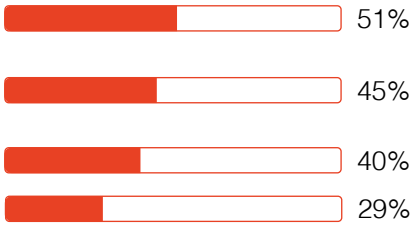


Defences

People



Process



Technology

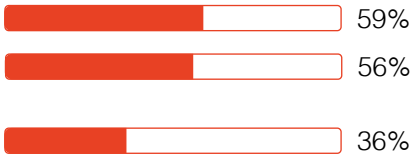


Figure 3

Main business drivers to invest in OT Security

The main driver for investing in OT Security is ensuring that business operations can continue as planned. As shown in Figure 4, the top two reasons for organisations to engage in OT cyber security programmes are avoiding production stoppages and financial losses and remaining competitive with their peers. Compliance is another strong driver for investing in OT Security. Meanwhile, current and emerging laws and regulations are also having a definite effect.

> Getting the C-suite to commit to building up the OT security team was a journey, and a big part of that journey was explaining the ways in which cyber protection is a necessary investment. I had to make a strong case to convince our leadership that the OT security solutions we were asking for were crucial to allow production processes to run smoothly and stay on schedule."
>
> Business Information Security Officer - Major chemical leader

What best describes your organisation's primary motivation for administering an OT cyber security programme? *One choice permitted only*

Figure 4

OT Security governance model

There is no clear industry-wide accepted governance model. OT Security Leadership is still a topic that is not clearly defined. Ownership of OT Security is still floating between the Operations, Engineering, IT, and Risk and Compliance divisions.

According to Figure 5, 39% of respondents say that their IT divisions are responsible for OT Security Leadership, while 20% say IT security leader and 19% say CIO/CTO. In 42% of cases, the person in the OT Leadership position is someone from the Engineering division (OT Security leader, head of product engineering, head of industrial control systems, head of process engineering, head of safety, head of quality engineering). The second most common answer is that OT Security Leadership is currently a function of the Risk and Compliance division.

This lack of industry-wide governance models increases risk. To achieve convergence and mitigate cyber security risks, organisations should consider creating cross-functional IT and OT security teams to avoid conflicts created by turf wars and silo issues that could be a barrier to successful convergence.

Who is the primary person for ensuring cyber security objectives in the OT environment?

Only one choice permitted

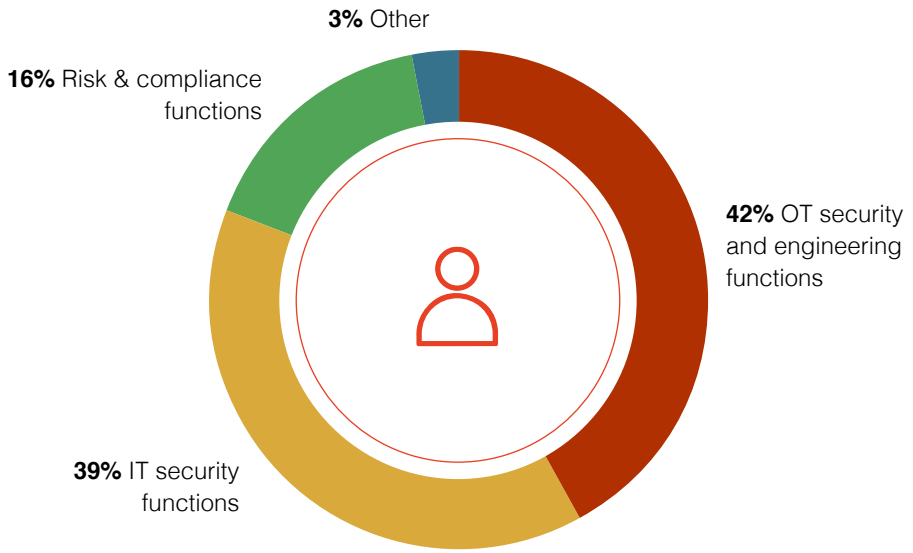


Figure 5

2.2 Understanding the risk and impact of cyber security incidents

Improvement in OT Security risk management needed

When asked how effective their organisation is with respect to identifying and reducing cyber risk in the OT environment, just over half of respondents say they execute risk reduction tasks very effectively. However, when the tasks in question become more technical and hands-on, such as digital asset inventorisation, we notice a decline in reported efficiency, with less than half of respondents claiming to have a very effective response. This indicates that the deployment of technical security controls within the OT environment is still a hurdle for many organisations.

Only 51% of respondents claim they can identify their high-value assets very effectively. This is significant, as identifying high-value assets ("crown jewels") is not only an important task but should also be one of the first steps taken to launch a successful security programme. Classification frameworks designed to help identify high-value assets do exist, but there is no one-size-fits-all solution. As such, proper identification of high-value assets will require cross-functional collaboration within each organisation.

Effectiveness in reducing cyber risk in the OT environment

On a scale from 1 = low to 10 = high, 7+ responses presented

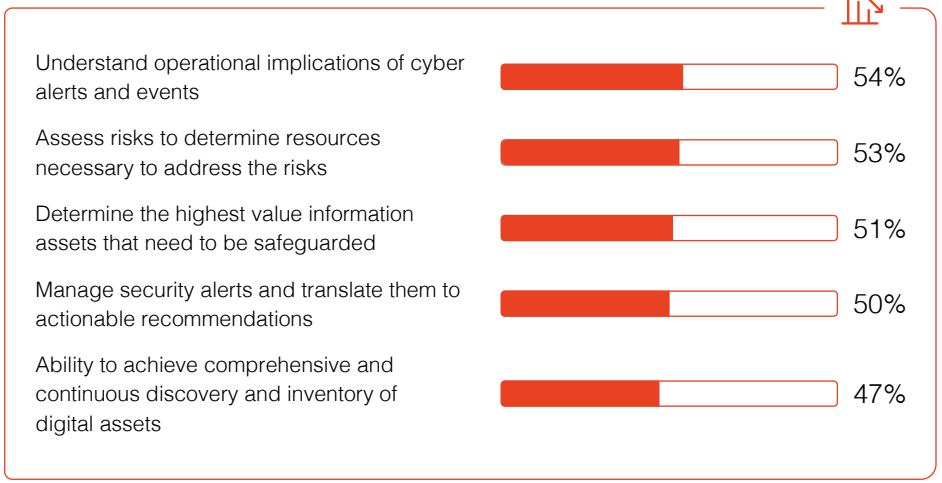


Figure 6

> Performing an asset inventory turned out to be a more complicated task than we initially anticipated. When we took a close look at our systems last year, we realised that they had been become significantly more complex due to the addition, in several phases, of extra sensors, monitors, and so on. We had to think carefully about the importance of each part of the systems."
>
> OT Security Lead – Major power distribution company

Top OT Security threats

Unauthorised remote access is the top cyber security threat to critical operations. Respondents identify unauthorised remote access as the top cyber security threat affecting critical operations in the OT environment. Meanwhile, their list of top threats includes a mix of external threats (such as attackers) and internal threats (such as unintentional breaches). This indicates that It is important for organisations not to focus only on external threats, since they are only part of the equation. Instead, measures should be taken to mitigate both types of cyber security threats.

What are the top six cyber security threats that may affect critical operations in the OT environment?

Top six responses presented

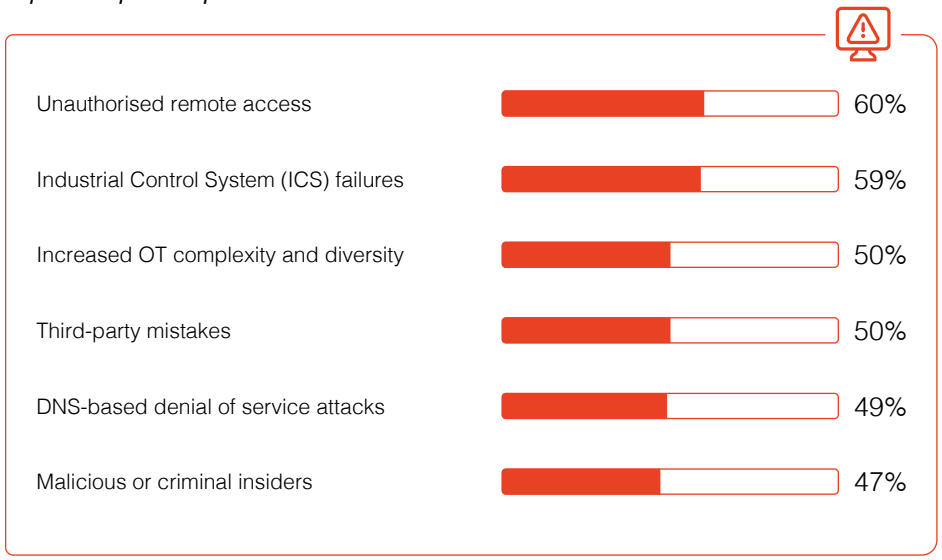


Figure 7

Inadequate incident response capabilities

Not all organisations have an incident response plan and team dedicated to their OT cyber security programmes. Just over half of respondents (52%) say their organisations have incident response teams dedicated to their OT Security programmes. According to Figure 9, of the respondents, 64% say they have a tested backup and restore plan in place, while 60% say they assign engineers to the team to investigate OT-related cyber security incidents and 58% say annual incident response simulations are conducted.

These numbers are concerning, as organisations require a comprehensive response plan that is regularly tested to develop strong incident response capability. A response plan greatly reduces the cost of cyber incidents, as it is the key to swift action and sure-footed remediation. With 58% of respondents stating that they do not have a yearly simulation test and another 23% stating they do not have a plan at all, we can conclude that a substantial portion of the organisations that depend on OT Systems does not have adequate response capabilities in place yet. Given the rising number of attacks on OT, we expect to see these organisations experiencing more cyber breaches that lead to long outages and that have extensive impact on already fragile supply chains.

Figure 8

What does an incident response plan for the OT cyber security programme include? *More than one response permitted*

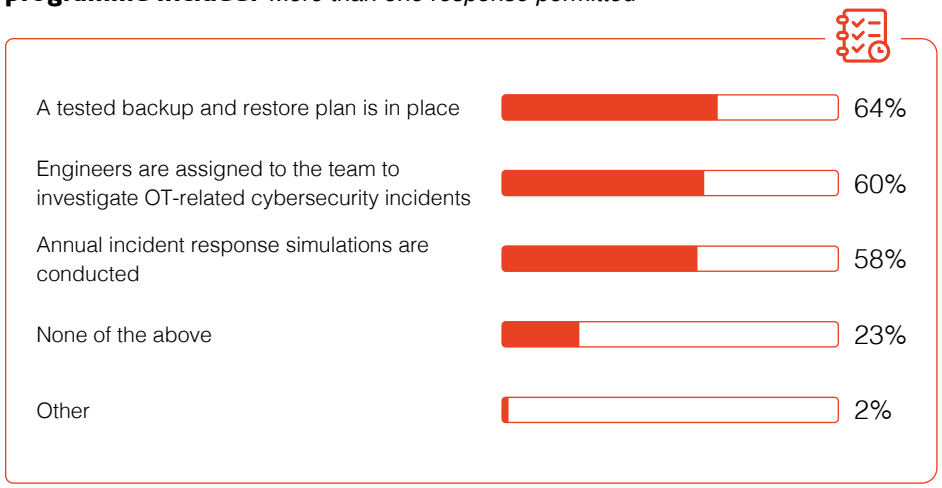


Figure 9

> Digitalisation is a factor in maritime operations, just as it is in so many other industries these days. That means we're as vulnerable to cyber attacks as any onshore business, and our assets are no easier to guard. I think they're harder, in fact. Imagine being the security chief who has to try and keep malicious actors away from a fleet of oil tankers! New connected systems added to the legacy equipment increases the attack surface, which requires constant vigilance. It becomes even more challenging due to the fact that we are now also required to bring all of our systems in line with IMO cyber security standards."
>
> Chief Information Security Officer - International gas shipping company

2.3 Future Directions in OT Security: More about People, Processes, and Technology

People: Headcount for OT Security will increase

Staffing levels are not adequate to meet cyber security objectives or mission in the OT environment. Only 42% of respondents say their organisations have enough staff to manage OT Security risks today. They also expect, though, that conditions will change – and that the headcount dedicated to OT Security will double within the next two to four years.

Figure 10

Processes: Supply chain risks in the OT environment

Supplier assurance remains a pain point. According to Figure 11, some 61% of respondents say their organisations are at risk because of the inability to ascertain the security practices of third parties, and 59% of respondents say their organisations have difficulty mitigating cyber risks across the external OT supply chain. Supplier assurance processes would help develop the maturity of OT Security capabilities within organisational supply chains.

Perceptions about risks in the supply chain
Strongly Agree and Agree response combined

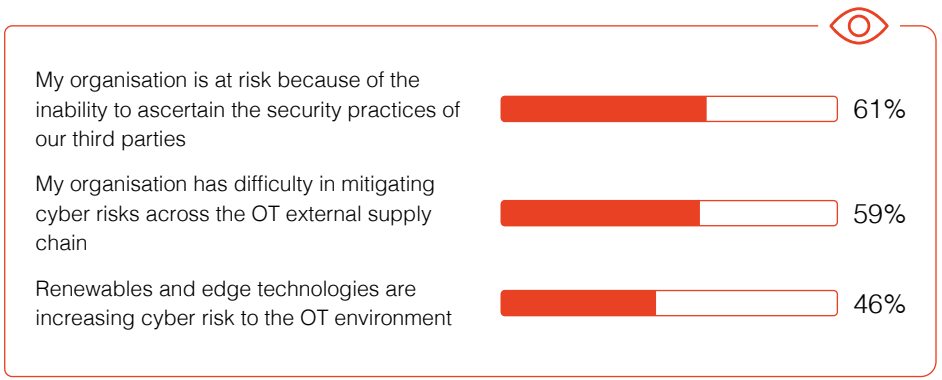


Figure 11

Despite concerns about the security of the supply chain, comprehensive audits are conducted rarely or seldom. As shown in Figure 12, some 39% of respondents say audits are conducted every two years or even less frequently. Another 22% say they have never conducted audits of their supply chain.

How often does your organisation conduct comprehensive audits of its supply chain?

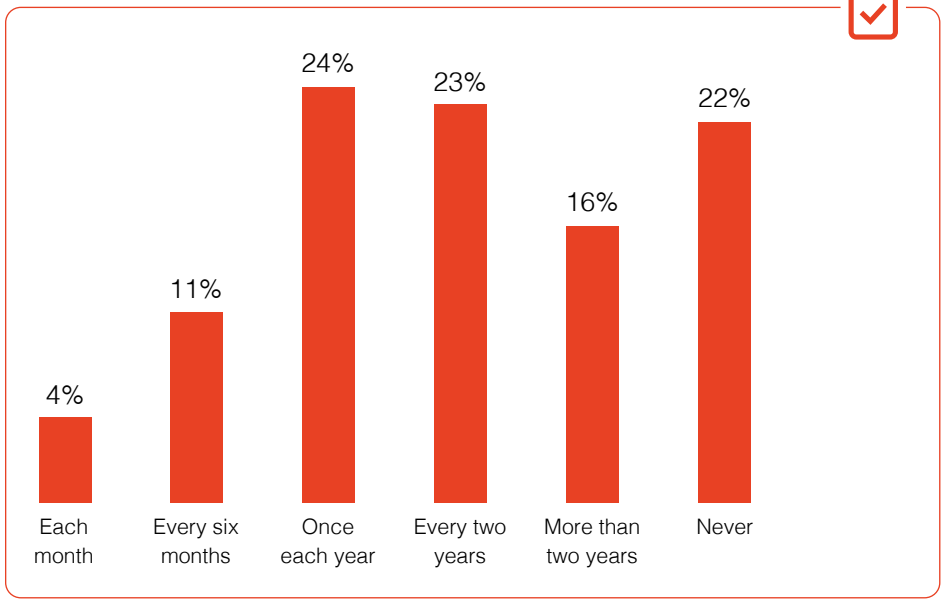


Figure 12

Adding requirements around cyber security in contracts with suppliers is still uncommon practice. As shown in Figure 13, some 49% of respondents say their contracts include cyber security requirements for their organisations' suppliers. Only 27% of respondents say their organisations conduct due diligence prior to contracting with new suppliers.

Does your organisation take the following steps to secure the supply chain?

More than one response permitted

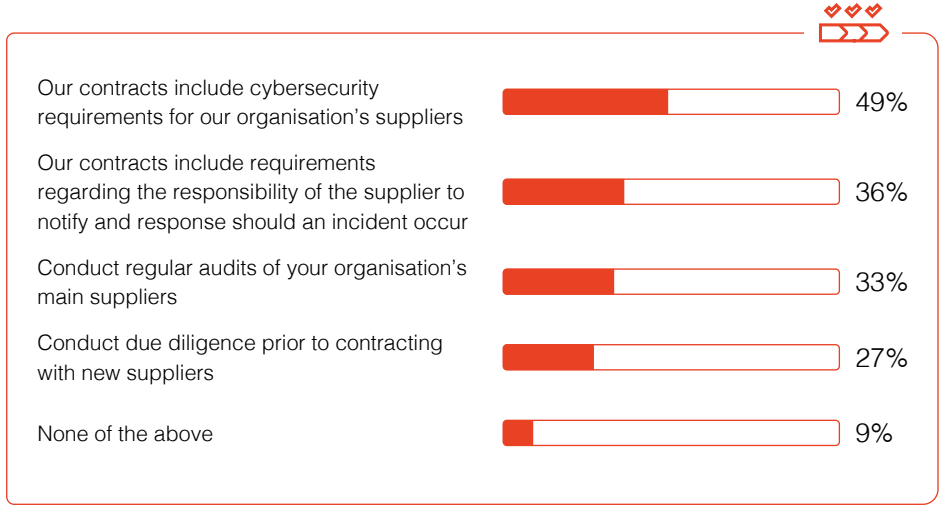


Figure 13

> We decided in late 2019 that the time had come to require that our vendors meet stricter cyber security standards, but we were slow to put the new requirements in place. In light of recent events, I wish that we had taken action more quickly. Our experience has been that questions about vendor security can compound the impact of supply chain disruptions."

Global Engineering and Automation Manager – Major pharmaceutical leader

Technology: Timelines for adopting enabling technologies

Organisations have been slow to adopt enabling technologies such as automation, machine learning, orchestration and AI, thereby making rapid detection of security exploits and data breaches difficult. The lack of enabling technologies is undermining organisations' ability to deal with increasingly sophisticated attacks, which have already been identified as one of decision makers' top worries.

As shown in Figure 14, only half of the respondents say their organisations have used automation to monitor and secure their OT assets, and the number of those adopting other advanced technologies is even smaller. Meanwhile, almost one third (31%) of respondents say their organisations are not using any of these technologies to monitor and secure their OT assets.

What technologies does your organisation use to monitor and secure OT assets?

More than one response permitted

Figure 14

Technology: Still relying on the “known things”

For the next two to four years, OT Leadership is likely to remain focused primarily on known technologies. When asked to rate the effectiveness of cyber security technologies or managed services that foster security and compliance with standards in the next two to four years (on a scale of 1 = not effective to 5 = very effective), the main focus of the respondents is on existing technologies. The top four, as shown in Figure 15, are patch management for OT, Secure Remote Access, Industrial firewalls and OT inventory, and asset management systems.

This seems to be in line with the fact that respondents think that other enabling technologies are not mature enough yet to make the impact needed.

> Based on my observations, the creation of the Security Operations Centre (SOC) has made a considerable difference in our management of security risks. The SOC gives us a way to monitor cyber threats, both for OT and for IT, on a constant basis. It allows us to make practical use of the visibility we’ve built into systems, and it helps us mount an incident response more quickly. We are due to build another assembly plant next year, and I will recommend that the new facility be fully integrated with our SOC from day one.”
>
> Global Cyber Threat Defence Manager - Food and beverage manufacturer

Effectiveness of cyber security technologies or managed services that seek to foster security and compliance with standards in the next two to four years

On a scale of 1 = not effective, 2 = minimal effectiveness, 3 = somewhat effective, 4 = effective, 5 = very effective

Figure 15

Technology: Means of Enabling OT Security

The integration of IT and OT Security Operations Centres (SOC) will transform how cyber security risks are managed. When asked which emerging technologies are most likely to change how their organisations manage cyber security risks, the respondents identified operational activities such as SOC, cloud computing and central firewall and vulnerability management as the most impactful for the next two to four years. As Figure 16 shows, some 63% percent of respondents say the integration of IT and OT SOC services will have the biggest impact on the management of cyber security risks, followed by cloud computing (61% of respondents) and central firewall and vulnerability management (56% of respondents). The top six technologies all require IT-OT convergence.

Further on the horizon seem to be emerging technologies that offer a new generation of software to upgrade already existing operational tasks (such as EDR). These are deemed less likely to transform how risks are managed over the next two to four years. Likewise, innovative concepts such as Digital Twins are also seen as having a bigger impact over the long term.

Emerging technologies and operations that will change how the organisation manages cyber security risks in the next two to four years

More than one response permitted

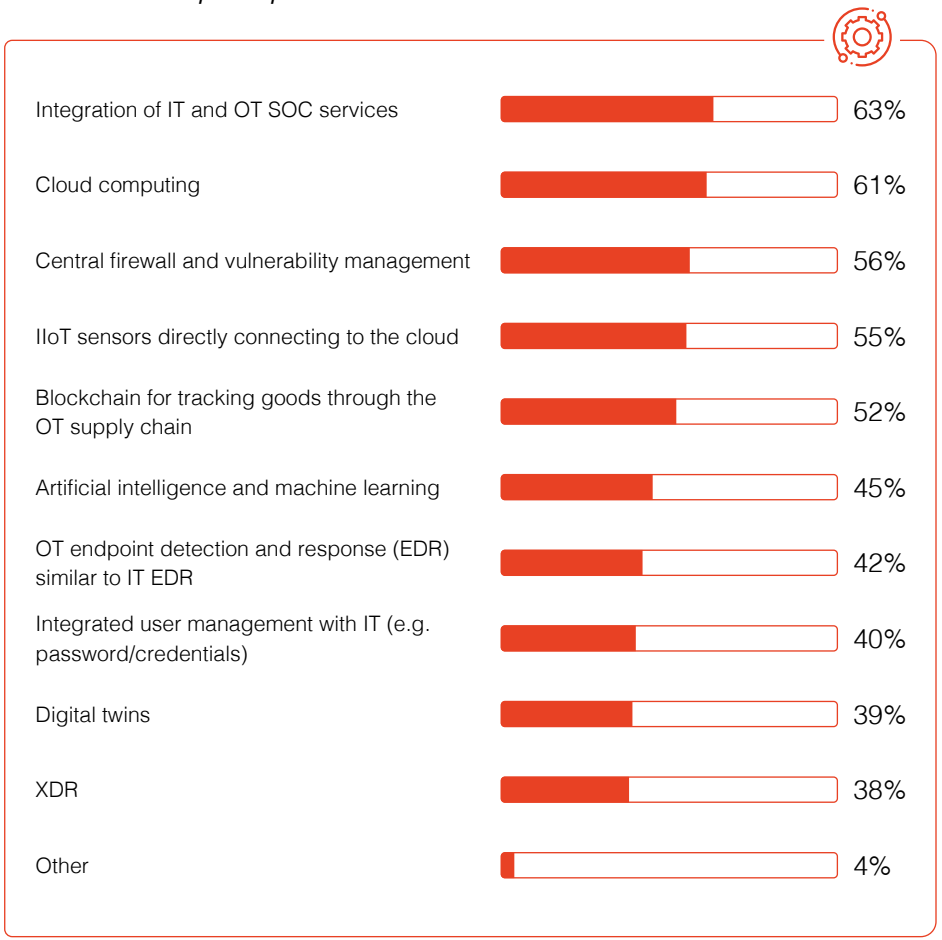


Figure 16

Technology: Top obstacles to minimising OT-related risks

The respondents see outdated control systems and vulnerable software in facilities as the two main obstacles to minimising OT-related risks, with each of these drawing 62%. This indicated that obsolescence and vulnerability management should have a prominent place in OT Security programmes. Meanwhile, another high-ranking worry is remote work arrangements for operations and maintenance. These arrangements have seen exponential growth within the last two years, especially in response to the coronavirus (COVID-19) pandemic, but the right solutions and associated controls may not have been implemented. At the same time, it should be noted that 82% of the respondents say plant connectivity is necessary. As such, security solutions for connectivity are extremely important from a business perspective.

What are the top obstacles to minimising OT-related risk in your organisation?

Five responses permitted

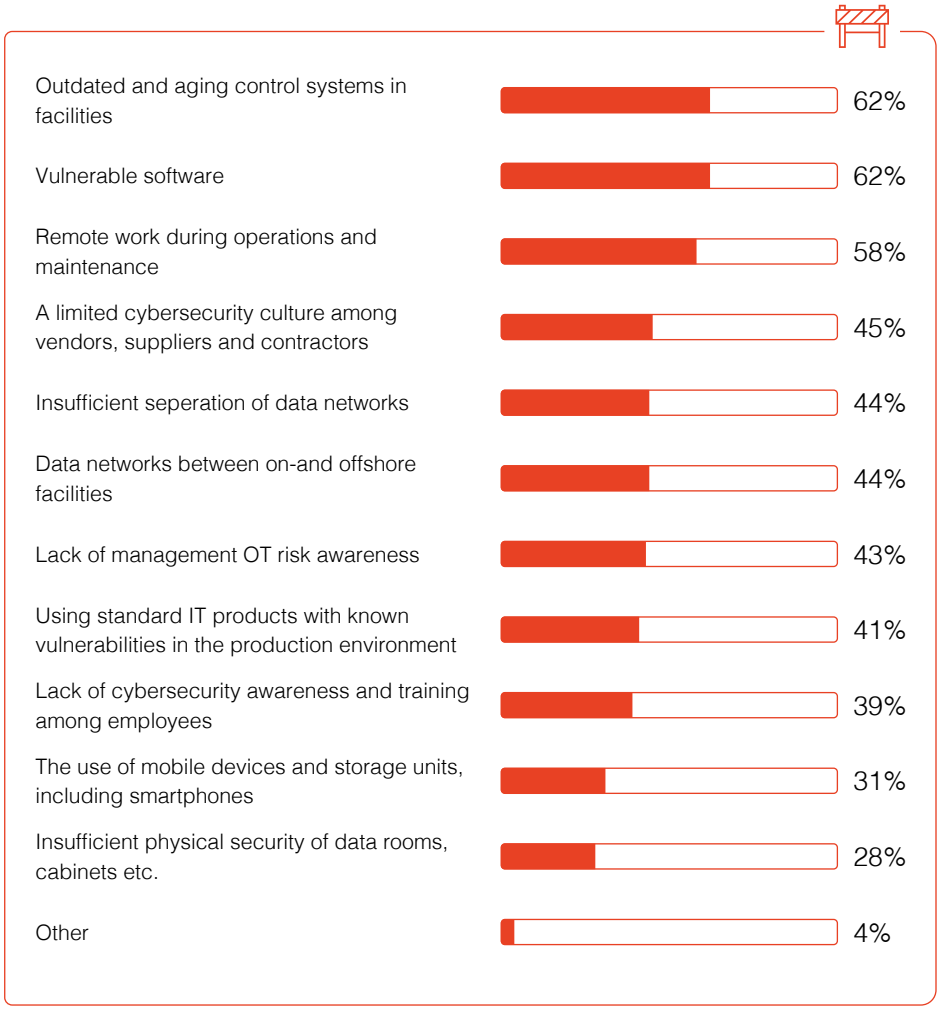


Figure 17

Technology: Zero trust adoption

Zero trust is a security concept that hinges on the belief that organisations should not automatically trust anything inside or outside their perimeters and instead must verify anything and everything trying to connect to its systems before granting access. Additionally, the concept is based on continuous monitoring practices that enable immediate action if something anomalous or suspicious is detected. This aligns with the previously mentioned capability of SOC to minimise the impact of incidents.

Some 53% percent of respondents say their organisations use zero trust significantly or moderately, with 20% selecting “significantly” and 33% selecting “moderately.” Of these 53%, some 60% of respondents say they do so to improve operational efficiency, while 53% do so to support the IT security team.

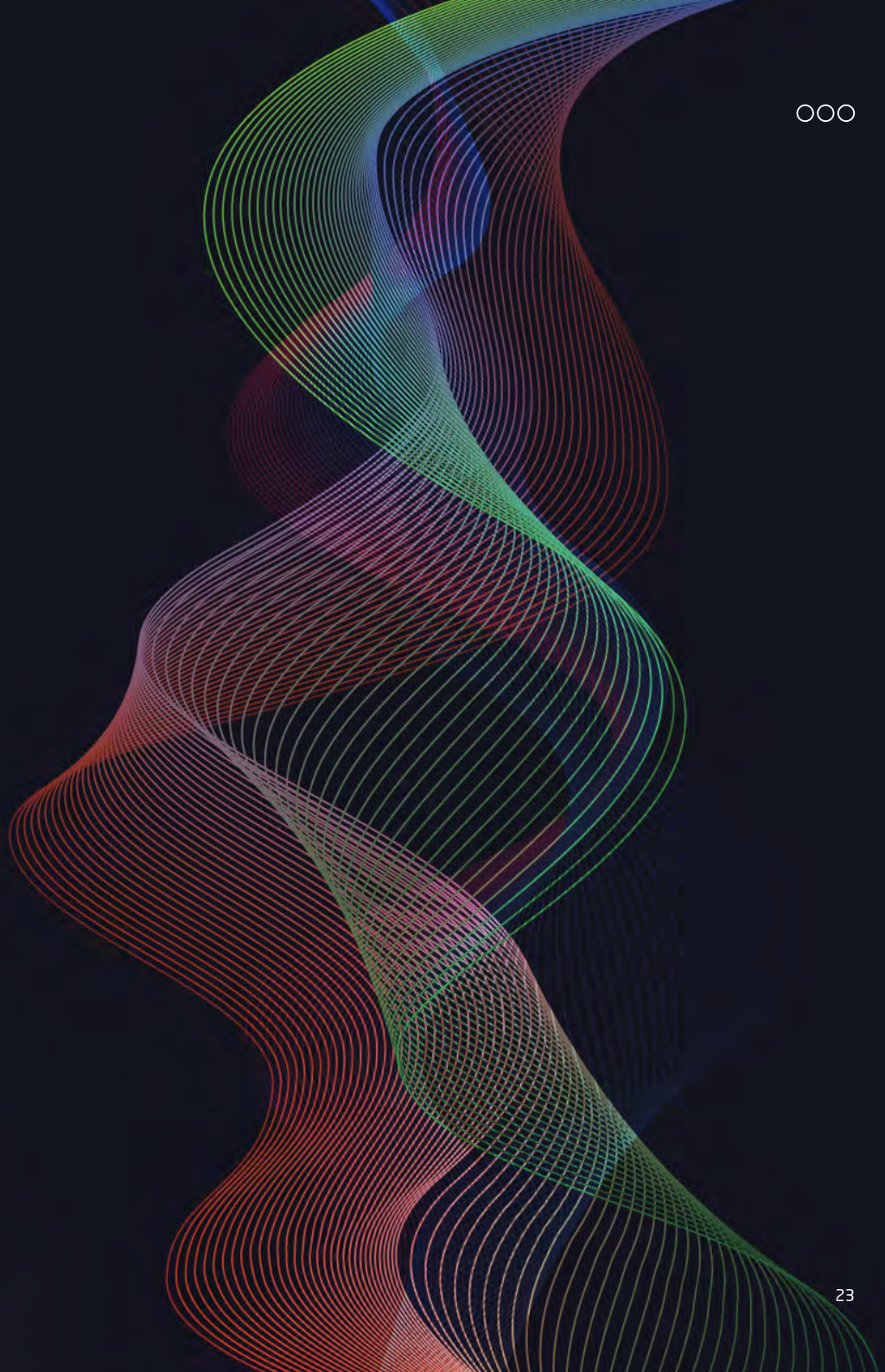
It should be noted that respondents’ replies are based on the zero trust concept and mindset being well adopted. Even though the implementation of the zero trust concept is still in an early stage, the responses given demonstrate the importance of the concept and the need to implement zero trust solutions.

Why does your organisation make significant or moderate use of zero trust?

More than one response permitted

Figure 18

3 Recommendations



3. Recommendations

New challenges will require a radical shift in reviewing security strategies and proposing sustainable long term solutions. Moreover, technological developments such as IT-OT convergence and cloud computing have increased the need for enabling OT Security technologies that can help organisations become more secure. As such, Applied Risk recommends that the following actions be taken to help architect the next generation of OT Security.

- IT/OT convergence keeps OT Security decision makers awake at night, but it could also become **part of the solution** to safeguard the OT domain in the changing environment. Converged IT/OT networks can be secured and monitored by collecting data across systems used to identify potential cyber security threats. For example, IIoT sensors are seen as an extra burden on the security team, as they are yet another thing to patch. However, data from IIoT devices could be leveraged to detect intruders into OT systems, turning this non-security-driven investment into a security win.

- To achieve IT/OT convergence and at the same time mitigate cyber security risks, organisations should consider creating cross-functional IT and OT security teams to avoid conflicts created by turf wars or silo issues that could be an obstacle to successful convergence. **Establishing a good governance model is key**.

- **Zero trust is an important concept within the future of OT Security.** This concept hinges on the belief that organisations should not automatically trust anything inside or outside their perimeters and instead must verify anything and everything trying to connect to its systems before granting access. It also assumes that the OT domain must be monitored continuously for anomalies and suspicious behaviors.

- **This makes concepts like Identity and Access Management (IAM) and Privileged Access Management (PAM) even more important.** Access management is most often used to prevent security compromises and is seen as a priority. Fully 65% of respondents say they use two-factor authentication for all privileged services, while 57% say their organisations are developing secure password policies and enforcing them across both IT and OT domains.

- **The majority** of respondents say the lack of **enabling technologies** makes it painful to reduce cyber security risks in the OT environment and to keep up with attackers. Although it remains important to meet basics requirements (patching, anti-virus scans, management of changes, etc.), enabling technologies such as automation, machine learning, orchestration, and AI will be needed for rapid detection and response to security exploits and data breaches.

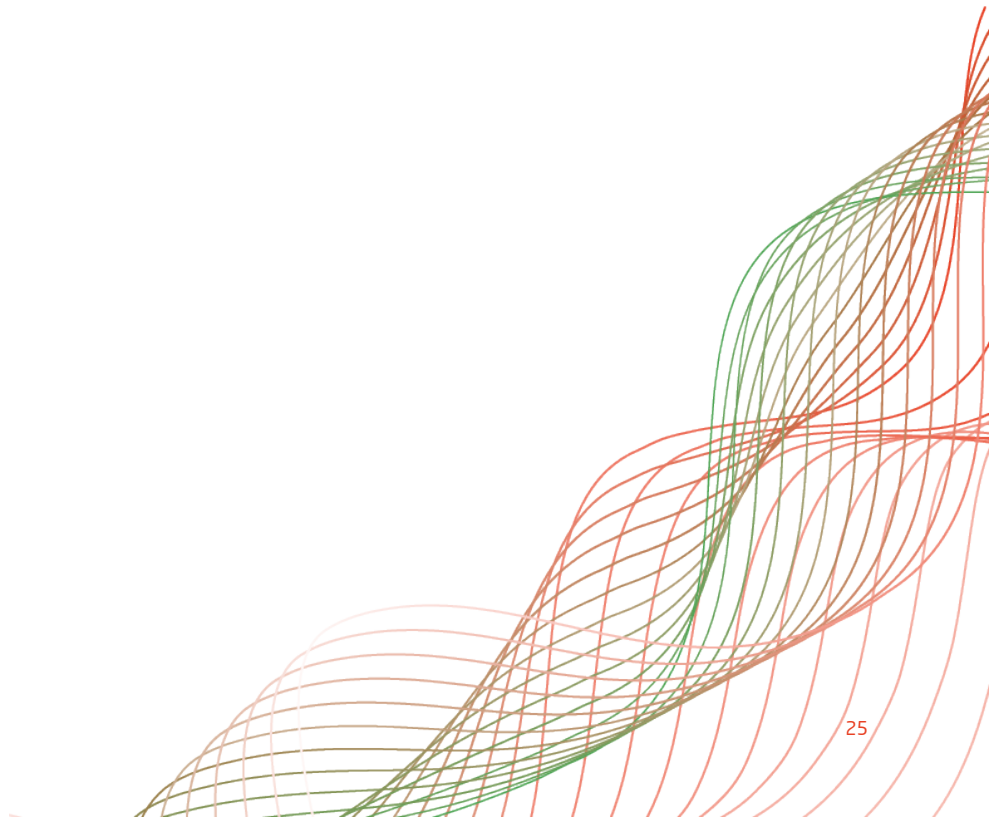
> “These control systems play a central role in our operations, and we can’t afford to leave them open to attack. We have had to make OT Security part of our daily practice, and now security procedures are built into our regular routines. Everyone who deals with these connected controls has to learn and practice. They have learned what they have to do when they are using the controls, and they have learned to speak up if they see that a co-worker has made a mistake such as forgetting to log out..”
>
> Cyber Security Technical Lead – Mining company

- **More effort will be needed to develop the OT Security skill pool.** There is a growing demand for professionals with OT Security skills. These do not all need to be OT Security specialists, but OT Security needs to be embedded in the profiles of managers, engineers, operators, procurement specialists, and others. Workforce development will be one of the most important means of achieving this goal.

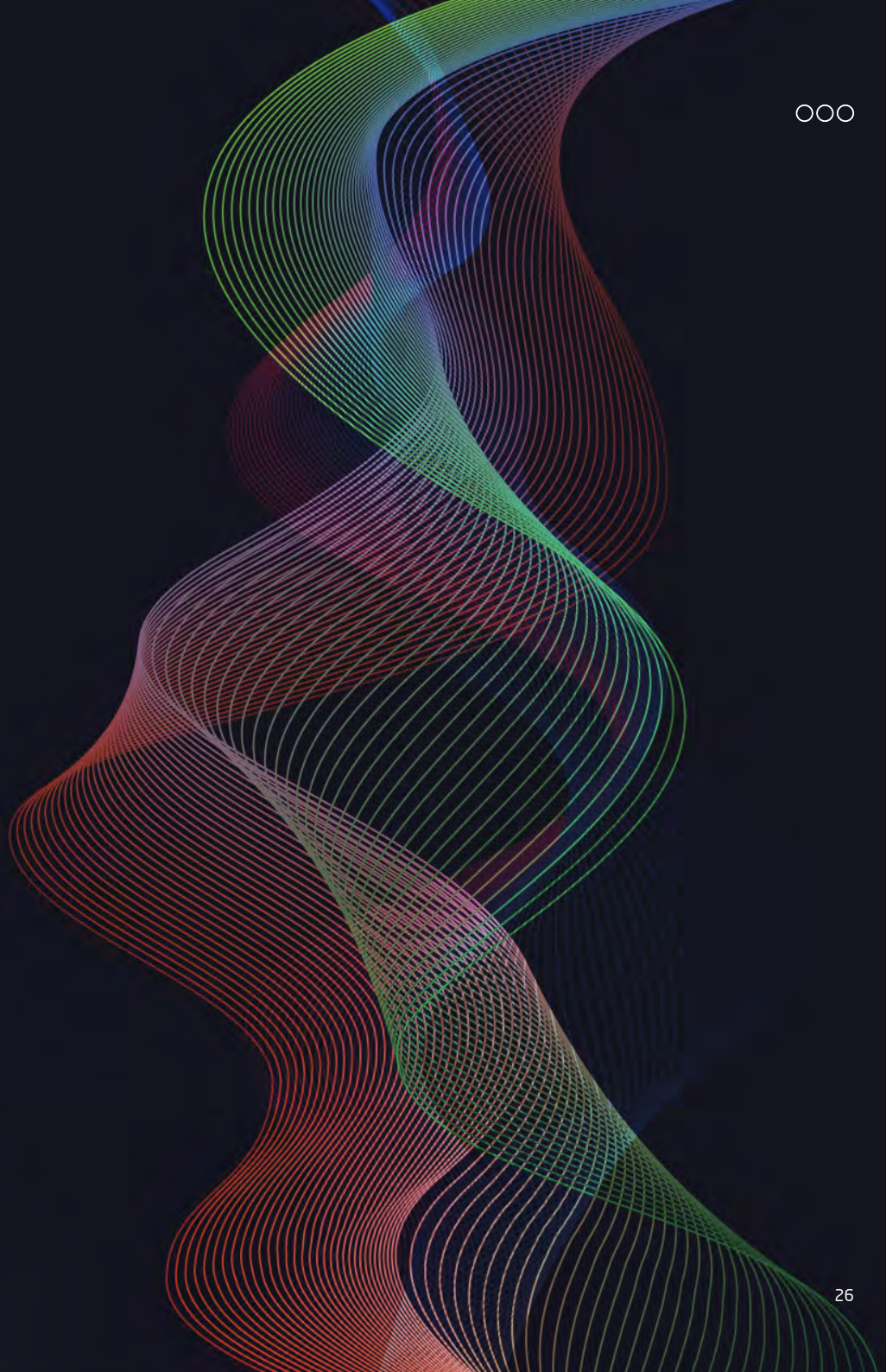
- In order to respond quickly and effectively to security compromises and data breaches in the OT environment, **organisations should have incident response plans that are dedicated to OT cyber security.** A strong incident response capability requires a comprehensive response plan that is regularly tested. A response plan greatly reduces the cost of cyber incidents, as it is the key to swift response and sure-footed remediation.

- **Supplier assurance is key.** Many companies rely on third parties to manage large numbers of (or even all of) the applications, systems and networks in the OT domain. Regular reviews of third parties in the supply chain should be conducted.

- **Risk assessments are critical.** Organisations should conduct risk assessments on a regular basis to understand the vulnerabilities and risk in their OT environments. They should then analyse and act on the results of these assessments to improve their cyber readiness and to identify the resources necessary to address these risks, as part of continuous improvement processes.



4 Methodology



4. Methodology

In this report, our findings are based on several sets of observations:

- Applied Risk carries out many security assessments every year on behalf of clients around the world. Our findings are based partly on input and intelligence from assessments carried out in 2020-2021, as well as information that is publicly available.
- Applied Risks's subject matter experts (SMEs) provided additional input and analysis,
- Applied Risk received data collected by the Ponemon Institute in a survey that addressed questions about current conditions and emerging trends in the OT Security realm. (More information about Ponemon's methodology is included below.)

These observations and data were reviewed, analysed, and integrated to yield maximum insight on the OT Security landscape and trends.

4.1. Ponemon's methods

A sampling frame of 27,865 experienced IT and IT security leaders located in the United States and Europe were selected as participants to this survey. To ensure knowledgeable responses, we ascertained that all respondents have responsibility for securing or overseeing cyber risks in the operational technology (OT) environment and understand how cyber security impacts the state of cyber security within their organisations. Figure 19 shows 1,106 total returns. Screening and reliability checks required the removal of 101 surveys. Our final sample consisted of 1,005 surveys (3.6% response rate).

Figure 19. Sample response

	US	Europe	
Total sampling frame	15,850	12,015	**27,865**
Total returns	650	456	**1,106**
Rejected surveys	53	48	**101**
Final sample	597	408	**1,005**
Response rate	3,8%	3,4%	**3,6%**

Figure 20 reports the respondent's organisational level within participating organisations. By design, more than half (60%) of respondents are at or above the supervisory levels. The largest category, at 29% of respondents, is technician.

What organisational level best describes your current position?

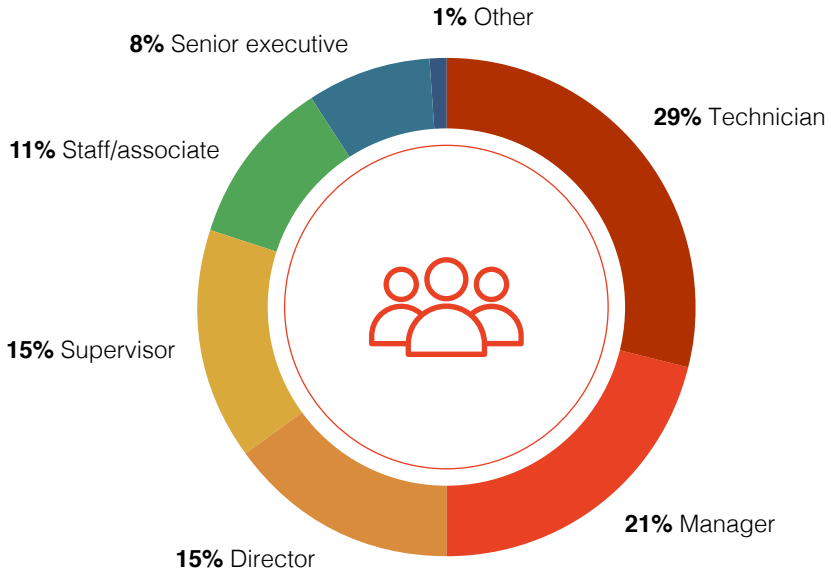


Figure 20

Figure 21 reports the primary person to whom the respondent reports within the organisation. Some 21% of respondents report to the IT security leader, while 19% of respondents report to the CIO/CTO, and 18% of respondents report to the head of industrial control systems.

Primary person respondent reports to within the organisation

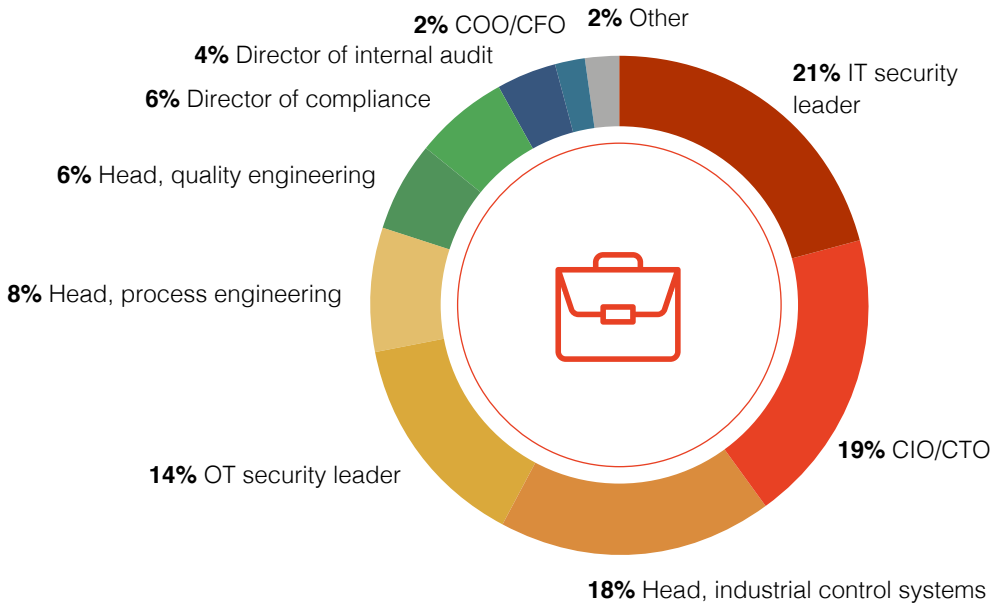


Figure 21

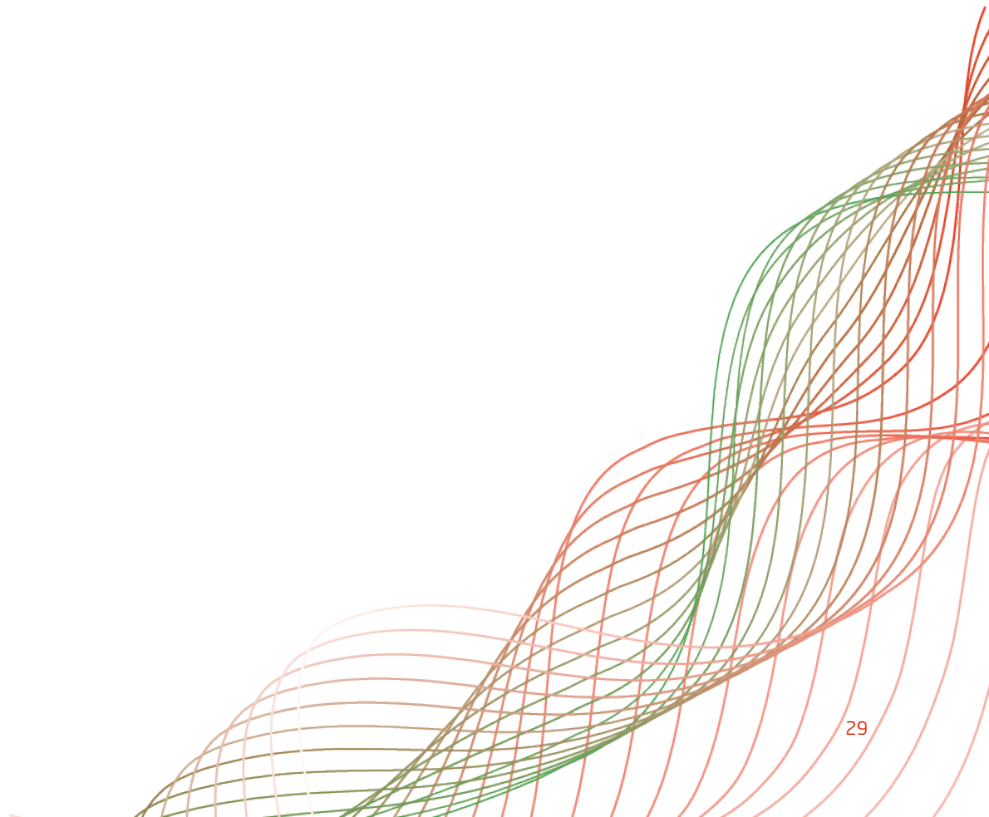
4.2. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

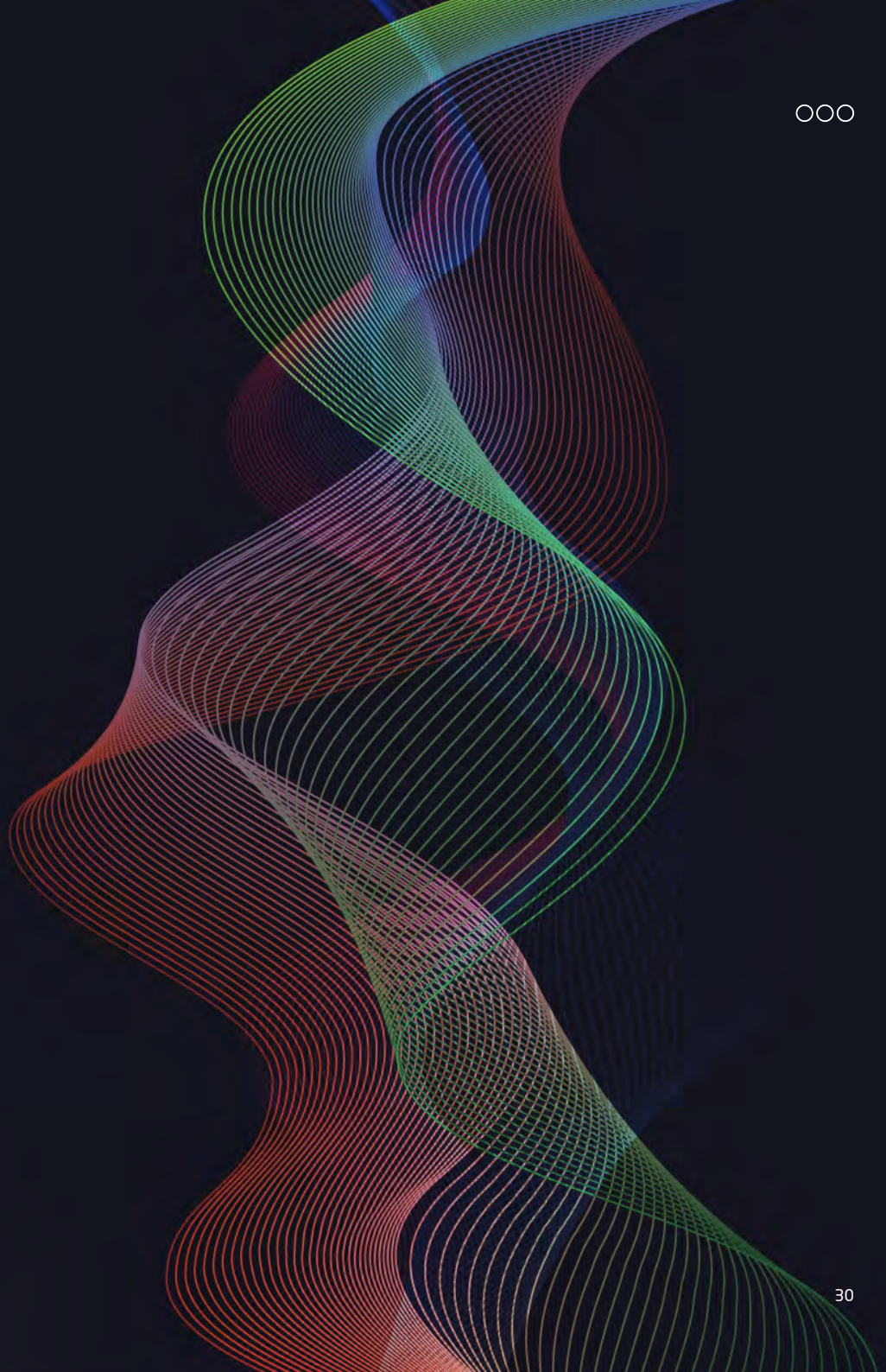
- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT and IT security practitioners located in the United States and Europe. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.



5 Conclusion



5. Conclusion

This report has comprehensively covered the challenges still facing the OT Security realm – namely shortages of appropriately skilled personnel, gaps in the implementation of procedures that help reduce risk and the slow pace of adopting advanced technologies. These challenges are real, and there's still much to be achieved against a backdrop featuring a rising tide of cyber attacks perpetrated by nation states and other sophisticated opponents.

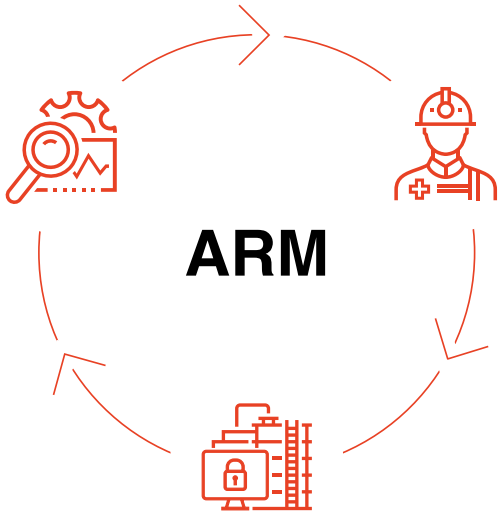
Nevertheless, we at Applied Risk see plenty of reasons for optimism – especially now that we've been able to delve more deeply into the trends and pain points that are uppermost in the minds of those responsible for OT Security. We view increased awareness as part of the movement toward practical, actionable solutions. Understanding practitioners' concerns about low headcounts can encourage creative approaches toward expanding the skill pool for cyber security, and unburdening their worries about supply chain security can serve as a stepping stone toward introducing and enforcing tighter security requirements for vendors. Likewise, data about increased use of new technologies such as cloud computing offer insight into the kinds of problems that security solutions are likely to confront in the not too distant future.

These insights have helped identify themes, that in turn assisted us to look further forward and towards what we believe the next-generation of OT Security will look like:

- Progressive reference architectures that are more tolerant of change and support advanced security services, whilst still maintaining mission critical availability requirements.
- Identity and Access Management (IAM) solutions integration as a Security Operations Centre (SOC) data feed. This will greatly enhance OT Security situational awareness enabling businesses to understand, profile and baseline who and what is accessing OT resources and whether it's at the right time and for the right reasons.
- Improvements within incident response processes gained through better situation awareness from SOC integration.
- Continuous risk assessment performed automatically by AI and machine learning security services. Solutions will use cloud-based infrastructure for crowd-sourced real-time analytics.
- More upskilled security personnel positioned in cross functional roles (IT / OT). This will require accelerated training curriculums aided by interactive experiences and simulation. This will most likely result in the prevalence of more accessible OT cyber range offerings.
- More regulatory scrutiny of OT Security, including Third Party Security (Supply Chain) risk.

In short, what we've learned will bolster the Applied Risk Methodology (ARM) we've developed to provide guidance for improving our clients' security postures through a continuous, interactive and collaborative process of **A**ssessment, **R**emediation, and **M**anagement. It will put us in a better position to develop OT Security solutions that integrate People and Processes rather than just relying on Technology.

Assess
Situational Awareness and a quick scan with focus on weak network entry points, know and unknown risks and potential vulnerabilities



Remediate
Prioritised approach with risk based actional remediation steps aligned with industry standards

Manage
Empower OT System Custodian to manage and sustain a safe and reliable operation in a cost-effective manner

Figure 22

Until just a few years ago, we didn't pay much attention to OT Security. We just told the IT team to take care of it and figured that would be sufficient. But the more we started hearing about other utilities getting targeted in cyber attacks, the more we started realising it wasn't enough. So we took a deep breath and hired dedicated OT security professionals. Now we have a whole OT Security team working, and they're well worth the trouble and the expense because they keep us above water, if you'll pardon the expression. They're people on a mission. They understand just how critical the water supply is and why we have to guard it so carefully."

Chief Operations Officer - Water-processing plant

About Applied Risk

As a trusted partner for industrial cyber security, Applied Risk is committed to safeguarding the critical infrastructure upon which our society depends. Using its combination of cyber security knowledge and experience in operational technology, Applied Risk provides tailored solutions that assists asset owners, system integrators, and suppliers to develop, deploy, and maintain cyber-resilient operations. Based in The Netherlands, Applied Risk operates on a global scale, helping protect industries such as oil and gas, electric power, water management, pharmaceuticals, healthcare, manufacturing, maritime, and transport. To learn more, visit www.applied-risk.com

About the Ponemon Institute

The Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organisations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant, or improper questions.

Applied Risk

Ponemon INSTITUTE