SCADAfence

THE 2022 STATE OF OPERATIONAL TECHNOLOGY

Findings of an international survey of 3500 cyber security professionals across the globe

Executive Summary

2021 was the most challenging year for industrial cyber security in history. The industrial sectors experienced ransomware attacks against Colonial Pipeline and JBS Foods, and an industry-changing intrusion at the water treatment facility in Oldsmar, Florida. These successful security events raised the importance of industrial Cyber security for OT networks to organizations' boardrooms.

The U.S. government also took notice as they have highlighted the criticality of securing ICS/OT systems and networks for the first time in executive orders, security memorandums, and sector-specific reports. The U.S. government is trying to increase the awareness among industrial operators and emphasize the threat level to national security and public safety that OT attacks can result in.

SCADAfence surveyed over 3,500 security experts, ranging from OT security professionals, consultants, customers, prospects and direct competitors.

To get a better understanding of how industrial organizations view OT security, SCADAfence surveyed over 3,500 security experts, ranging from OT security professionals, consultants, customers, prospects and direct competitors. The respondents were questioned about the different security implications of operational technology, the ongoing shortage of OT security experts, and how industrial organizations are converging IT & OT networks. The purpose of this report is to provide tangible, actionable insights into the OT security industry.

The results in this report are striking.

Most are very or extremely concerned about the shortage of OT workers in general. The majority believe that the increasing shortage of OT security staff is decreasing the effectiveness of their organization's OT security which is resulting in security gaps.

The lack of OT staff isn't the only concerning insight from this report.

79%

of respondents believe that internal human errors are the key to attackers compromising their OT systems. Almost half of the OT security experts surveyed see a lack of complete visibility as their biggest challenge for managing OT risks.

Besides security risks or shortage of OT resources, one of the bigger concerns with OT professionals is the lack of communication when converging IT-OT networks.

50%

of respondents believe that the communication between IT and OT teams is the most important factor in ensuring a successful IT-OT convergence process.

One of the less surprising insights from this report is that

84%

of the surveyed OT experts said that the responsibility of a successful attack on the organization's OT environment falls on the shoulders of the CISO.

This OT security report is an important resource for anyone who is working in the industrial sector. The data delivered presents a picture of the current status of industrial Cyber security and where and how organizations can improve their OT security against incoming security threats.

Content

Key Findings of the Survey

69%

of OT security professionals say the lack of OT security staff is diminishing the effectiveness of their organization's OT security.

79%

of OT experts believe that human error is the greatest risk for compromise to OT systems.

84%

of OT professionals think the CISO takes responsibility for a cyberattack on OT systems.

83%

of OT leaders believe there is a significant shortage of OT workers overall.

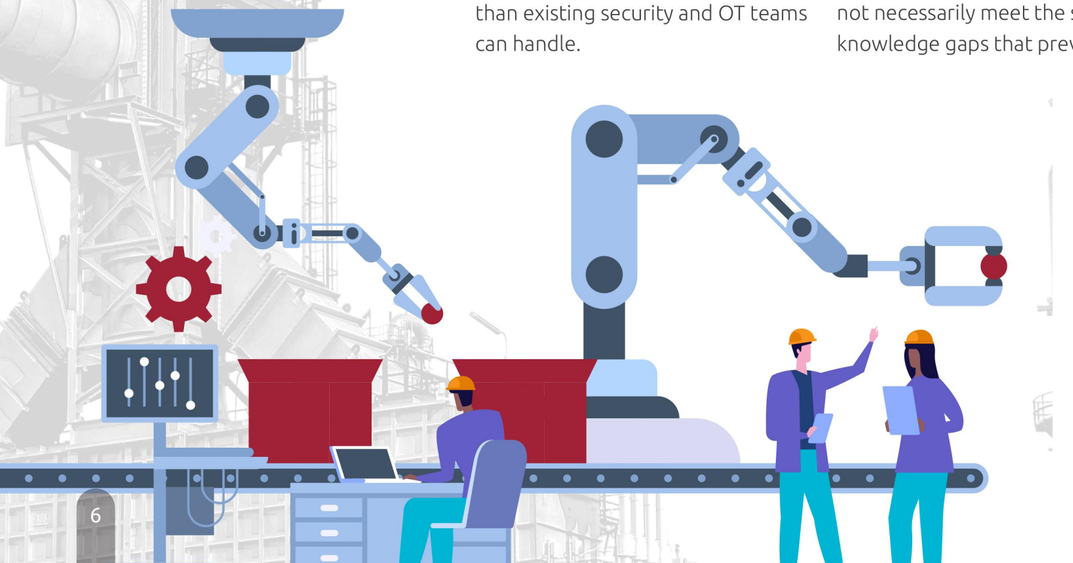
50%

believe the communication between IT and OT teams is the most important factor in ensuring a successful IT-OT convergence process.

Explaining the Problem and Purpose of the Report.

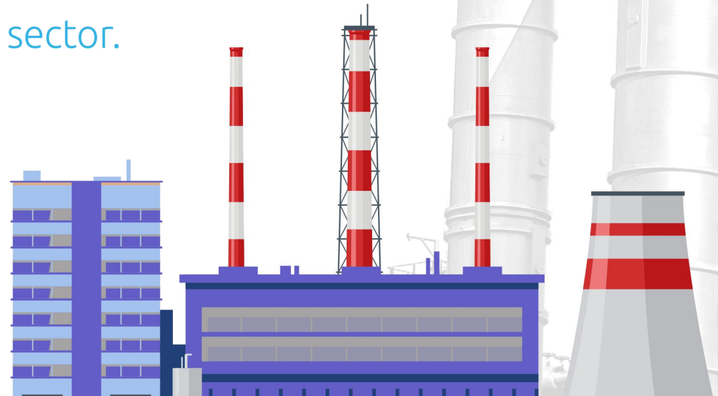
2021 presented all industrial sectors with a set of challenges no one could have expected. The rise of ransomware attacks on critical infrastructure raised a lot of uncertainty in the OT industry, specifically the lack or shortage of security experts. The industrial sector is facing a chronic shortage of operational technology (OT) security talent as new technologies and evolving threats increase the level of cyber risk at a faster pace than existing security and OT teams can handle.

Talent shortage tends to be even greater in the OT security sector, where the responsibility of security professionals is not only to ensure the industry's securities best practices but also to handle the different security challenges of the once legacy industrial processes and control systems. Higher wage rates could help bridge the gap over time as people shift from other careers into Cyber security, but counting on higher wages alone will not necessarily meet the skill and knowledge gaps that prevail.



Recent industrial cyber security attacks, such as the SolarWinds supply chain, Colonial Pipeline ransomware attack, and other Cyber security incidents, are a clear reminder for organizations' stakeholders that the lack and shortage of OT security skills are very alive and exist in the industrial sector.

Concerns about the OT security skills shortage, plus a deep desire to address the problem, have driven SCADAfence's research team to commission a study and start understanding the issues better.



Audience

JOB SENIORITY

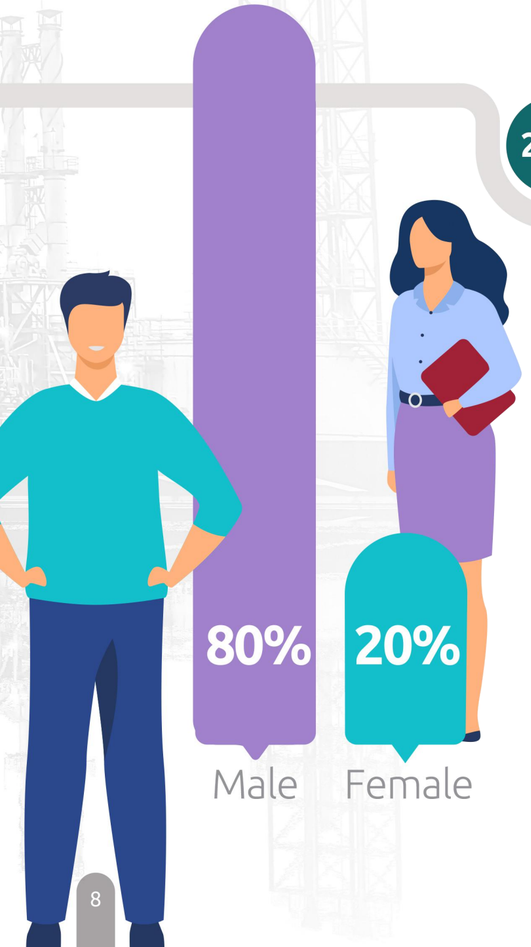
C-Level 22%

Manager 22%

Other 10%

Director 36%

Team Lead 10%

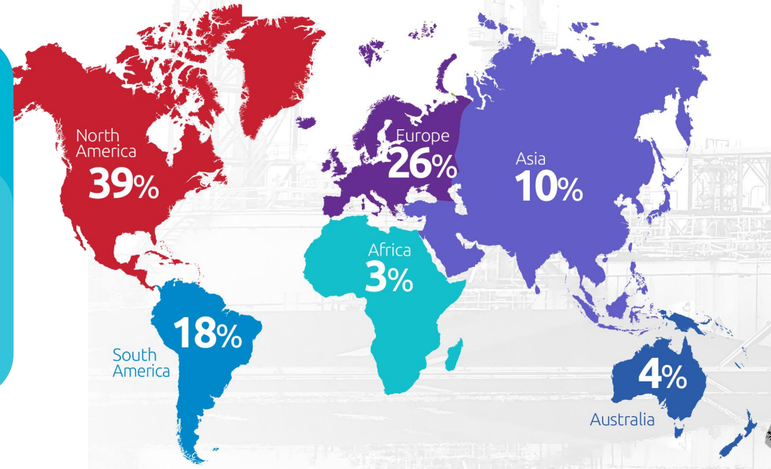


80% Male

20% Female

0%	15%	47%	28%	10%
20-29 years old	30-39 years old	40-49 years old	50-59 years old	60+ years old

SURVEY RESPONDENTS GLOBAL REPRESENTATION



32% Manufacturing	14% Water	13% Oil & Gas	10% Pharmaceuticals
4% Food & Beverage	9% Automotive	19% Other	

OT Security Risks

Human Error and Lack of Visibility Biggest OT Security Concerns

The technology of industrial systems and networks is advancing and becoming more connected to the Internet, it has increased the exposure to security vulnerabilities. This forced industrial organizations to adapt from closed, or air-gapped systems, to open and interconnected systems which provide many technological advances, but also exposes the OT equipment to new security challenges and risks that need to be resolved.

Q1

What is your organization's perception as to the level of OT security risks to your company's overall risk profile?

As industrial operations become more digital, the need to secure their systems and networks against cyber security threats becomes increasingly critical.
A comprehensive security strategy requires a thorough assessment of the current state of the organization's OT environment, including policies, procedures, technologies, and best practices.

55% of OT experts believed that their OT security risks level was high for the company's overall risk profile.

55%
High

21%
Severe

20%
Moderate

4%
Unknown

While the results are a snapshot of the industrial sectors, it highlights the need to present OT security to one's board and C-suite executives to discuss how important it is for the overall cyber risk profile.

Q2

What elements do you consider to be at the greatest risk for compromise to your OT/control systems?

79%
Human Error

11%
Technology

10%
Processes

For years, “human error” has consistently been identified as a major contributing factor to cyber security breaches. Employees and external personnel such as maintenance or construction workers, working in an ICS environment, often pose challenges for security teams.

Systems can be compromised by unauthorized or incorrectly configured software and hardware. Employees can (unwillingly) install malware or provide access to attackers being unaware of the risks that are being posed by such actions.

The majority of OT attacks tend to target the weakest parts of OT networks. Many of these attacks take advantage of the complexities caused by a lack of protocol standardization, and a sort of implicit trust strategy that seems to permeate many OT environments. This trend is not limited to specific locales or sectors. Exploits are increasing in volume and prevalence for almost every SCADA vendor.

79% of respondents believed that human error is the greatest risk for compromise to OT systems, followed by 12% technology and 10% processes.

Q3

What is the biggest challenge for managing OT risks?

42%
Lack of Visibility

36%
Disconnect between OT & IT teams

22%
Lack of skills

The operational technology sectors have recently opened up their networks and systems in ways we haven't seen before. The majority of industrial organizations networks are cloud-based and fragmented, making complete visibility into them quite difficult.

Effective OT/ICS security begins with visibility. When OT security professionals are continuously monitoring every device on their network, they can detect and respond to cyber incidents faster and more efficiently.

This is followed by 36% saying disconnect between OT & IT teams and 22% saying lack of OT skills.

Protecting the expanding OT attack surface without disrupting sensitive systems presents challenges. Any security countermeasure needs to begin with deep and broad visibility across the entire OT network, whether it is confined to a single production facility or spans a complex system.

42% of OT security professionals believe that lack of visibility is the biggest challenge for managing OT risks.

Shortage of OT Security Experts

According to the SANS Institute 2021 survey, over 52% of organizations believe that their IT staff do not understand OT operation requirements.

The shortage of people with the skills and knowledge of OT cyber security is a huge challenge for the cyber security industry. In many cases, it is not budget that holds organizations back, but the ability to find skilled people to fill the slots they need to achieve the objectives they've set.

In OT, this talent gap is even more pronounced as many of the foundational elements of systems management are not followed today. Conducting these activities on sensitive OT systems is potentially operationally risky.

Q1

Do you feel there is a shortage of OT security workers overall?

Talent shortage tends to be even greater in the OT security sector, where the onus on Cyber security professionals is not only to safeguard and understand cyber security but also to deal with the security challenges of the complex and legacy process and control systems.

Recent ransomware attacks and other cyber security incidents on critical infrastructure have highlighted the ongoing gap of OT security skills in the industrial sectors.

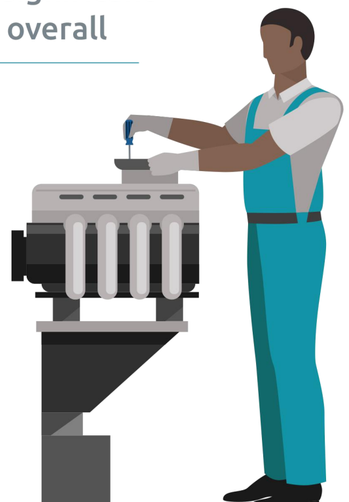
While there is an increasing demand for OT/ICS security skills, most organizations are not filling the gaps with more specialized OT staff that have the right skills and expertise to manage incoming OT security challenges.

83% Significant Shortage

17% Slight Shortage

When asking respondents about the OT security staff shortage, 83% believed there is a significant shortage of OT workers overall

While the remaining 17% felt a slight shortage. This sample size provides clear insights that OT is far from closing the OT staff shortage and until organizations invest the right level of resources it won't change.



The Problem with OT security staffing

by Paul Smith, Field CTO, SCADAfence and author of *Pentesting Industrial Control Systems.*

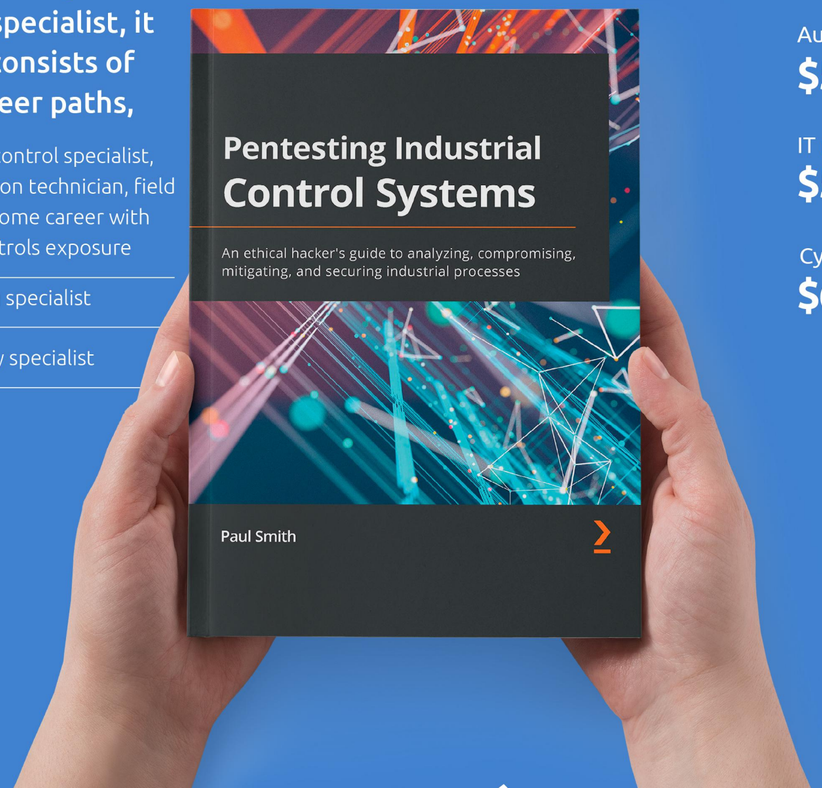
Addressing the industry's need for industrial cyber security specialists is crucial and an ever-growing concern. Industry staff members are going into retirement and legacy equipment is still proliferated out in critical infrastructure. This creates a two-fold problem as knowledge is getting lost at a rapid rate, and spare parts are near impossible to come by. Making sure that legacy technology operations and maintenance is documented and passed on by senior staff members to juniors is critical. Creating a budget and building an internal training program will be beneficial to aid in addressing the talent shortage we have in our industry. This topic helps segway into another discussion and this is more of a political oversight.

When we break down the persona of an industrial cyber security specialist, it actually consists of three career paths,

Automation/control specialist, instrumentation technician, field engineer, or some career with industrial controls exposure

IT networking specialist

Cyber security specialist



Paul Smith

Now if we were to attach salary ranges to each one of these roles, it would look something like the following:

Automation/control specialist

$55,000 - $113,000

IT network specialist

$58,000 - $95,000

Cyber security specialist

$69,000 - $133,000

Companies tend to pick one of these three ranges of salaries to offer an industrial Cyber security specialist, without realizing that this role is actually a variable mixture of all three of these occupations. Meaning that the job consists of more complex responsibilities and consequences for equal or little elevated remuneration. Organizations need to step up and carve out a new pay category for this occupation since doing this will help entice team members to take on the extra responsibilities (and headaches) that this job presents.

Additionally, transitioning members into this position can present some intricacies as each skill set needs to be enriched for automation/control specialists moving to this role. Automation/control specialists tend to have a head start in this area as they have intimate knowledge of the process, technology, and impact of actions in the operational technology space. For them, it is an educational roadmap of more advanced networking and cyber security training that is required.

As for the IT network specialist, it becomes a little bit more of a paradigm shift as every technical action could cause production downtime and losses of revenue. They require a co-op term of working side by side with automation/control specialists to gain the knowledge and experience required for this role.

Cyber security specialists are also lumped into the IT network specialist training schedule as they would face similar challenges when approaching the position.

63%
Lacking OT skills

25%
High Burnout Among Staff

12%
Lack of Resources

Q2

Why are organizations not succeeding to bring on more OT security employees?

According to Gartner, hiring and keeping professionals remains a top challenge in 2022 and beyond.

The global demand for cyber security skills, especially OT skills far exceeds the current supply of traditionally qualified individuals.

A global study of Cyber security professionals by the Information Systems Security Association (ISSA) and industry analyst firm Enterprise Strategy Group (ESG) showed that the Cyber security skills crisis continues on a downward, multi-year trend of bad to worse and has impacted the majority half of organizations.

When asked why it is a struggle to hire more OT security staff, 63% of OT professionals said that it was due to security professionals lacking the right amount of OT skills,

followed by 25% saying high burnout rate and 12% saying their organizations lacked the significant resources.

Q3

Which of these factors do you feel are diminishing the effectiveness of your organization's OT security?

It's hard enough keeping up with today's threats on a good day. But when your OT organization is spread thin, especially in terms of security staff, the challenges mount. An enterprise with insufficient OT security staff is an advantage for attackers, who will quickly take advantage of any possible means of exploitation.

According to a survey by ISACA, nearly three out of five industrial enterprises are struggling to fill Cyber security staff positions and it's hurting the overall OT security posture for these organizations. When a security role isn't filled, the security gap within the organizations continues to be untouched which creates even more security risks.

69% of security professionals surveyed believed the lack of OT security staff is diminishing the effectiveness of their organization's OT security,

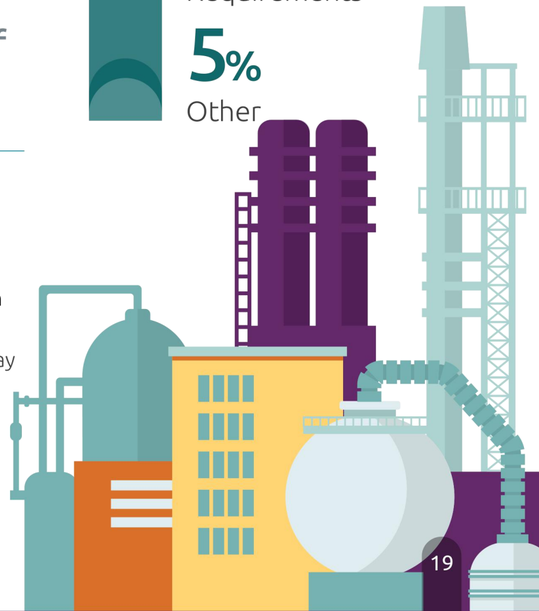
followed by 18% saying the evolving threat landscape and new cyber threats. 8% of the respondents stated that industry compliance regulation requirements also affect the effectiveness of their day-to-day operations.

69%
Lack of OT security staff

18%
New Cyber Threats

8%
Compliance Requirements

5%
Other



Responsibility and IT-OT

For decades, information technology (IT) and operational technology (OT) systems have co-existed in process industry enterprises, often with very little crossover or cooperation between them. The rise of the Industrial Internet of Things (IIoT) and related technologies have greatly impacted IT and OT. The boundaries between these two worlds are steadily evaporating. Smart sensors, new protocols and gateways, and cloud computing are enabling OT to access and share data across the broader enterprise-wide network.

This has forced many industrial organizations to converge IT and OT matters, which is gradually but surely changing the nature of manufacturing

and creating opportunities for innovative improvements to manufacturing processes for those willing to act. The changes come with different security risks for OT systems that were not originally designed to operate on business networks which can introduce new vulnerabilities, threat vectors, and a variety of cyber threats targeting OT systems.

Q1

What is the level of IT-OT Convergence in your organization?

The advantages of merging the realms of information technology (IT) and operational technology (OT) are obvious: cost reduction, improved capabilities, and greater efficiency.

These advantages, however, come with a cost because they have affected the way that industrial control systems operate and have increased the exposure of industrial control systems to cyber risks.

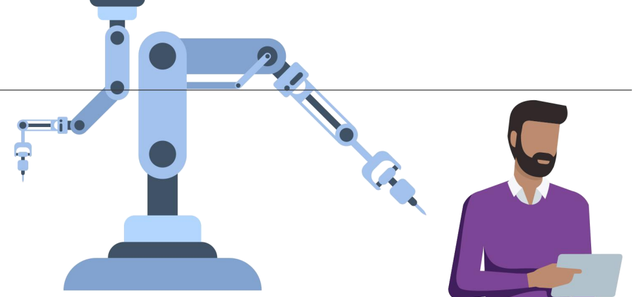
In our survey when asking about the level of IT-OT convergence, 51% of OT experts stated that their organizations had completed the convergence process. Then, followed by 31% of respondents saying that IT-OT convergence is being discussed and 17% saying IT-OT convergence is not happening in their organization.

51% Full IT-OT Convergence

31% IT-OT Convergence is being Discussed

18% No IT-OT Convergence

The increasing adoption of IT-OT convergence is allowing organizations to improve their industrial cyber security. However as seen through our survey, there is still a lot of room for growth converging between both networks.



Q2

What are the most important factors to ensuring a successful IT-OT convergence process?

Industrial systems are increasingly sophisticated and automation plays a critical role in ensuring efficiency, which has led to IT, OT, and IIoT systems becoming increasingly integrated. However, there are several challenges and concerns that need to be addressed to achieve convergence.

According to a recent study by the Ponemon Institute, the inability to control security, safety, and privacy initiatives is seen as a barrier to IT-OT convergence. The study found that a lack of skilled experts and insufficient risk assessments are also complicating the convergence process.

50% of the respondents of our survey stated that communication between IT and OT teams is the biggest factor for successful convergence.

This followed by 21% saying leadership involvement is critical to a successful convergence and 21% defining team roles and 8% being provided the right tools.

To successfully operate in a converged IT-OT ecosystem, organizations must be able to ensure the successful consolidation and integration of cyber security, functional safety, and data privacy functions within IT and OT control systems.

50% Communication Between Teams

21% Defining Roles

21% Leadership Involvement

8% Providing the Right Tools

Q3

Who would take responsibility for a cyberattack on OT systems?

OT security is not only a technical problem. One of the larger challenges is understanding who is responsible for an attack on OT systems. With so many stakeholders involved across the business, with different motivations drivers, culture and competing objectives, it's important to identify everyone's role responsibilities and then determine who should take accountability and who should take responsibility for securing the critical processes.

In the case of understanding who within an organization should take responsibility if a security event occurs within the OT environment, the results were very one-sided as expected.

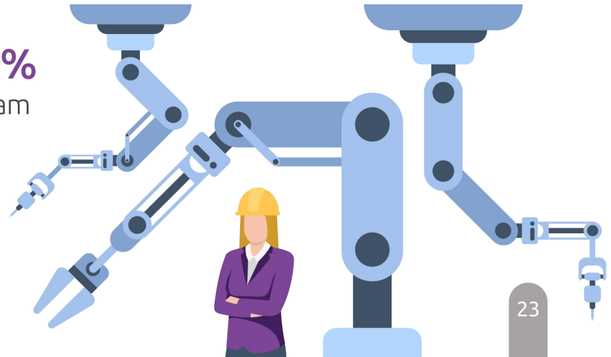
84% of respondents believed that the CISO takes responsibility for a cyberattack on OT systems and only 16% believe it falls on the OT Team.

84% CISO

16% OT Team

Despite the increased adoption of IT-OT convergence, not one person responded that the responsibility should fall on IT security.

As OT becomes more connected, it is more important that the security of OT systems is a part of the larger cyber security infrastructure. If Industrial organizations that evolve and put the responsibility of OT security with their CISOs and other security executives, will allow the organizations to strategize for a more secure environment against incoming attacks.



How Organizations Lacking OT Security Staff Can Take Action Today

We've taken the time to survey thousands of industry experts and collect the data in this report, because we're aware of this lingering issue.

In order to help organizations who struggle with the lack of OT security staff, we offer Managed Services for OT security that requires minimal effort.

We employ and are partnered with hundreds of OT security experts who can deliver the expertise and technology that is needed to effectively control any OT networks with visibility, risk management and vulnerability detection.

For all of the coverage details and benefits, please fill out the form on this page: l.scadafence.com/services or scan the QR code.

It is our mission to protect the world's critical infrastructure & manufacturing, ultimately protecting the lives of innocent civilians.

We are seasoned veterans in the realm of OT security and protect the lives of millions of people around the globe, every single day.

Let SCADAfence Manage Your OT Security

CONCLUSION

One way to compensate for the shortage of qualified workers to handle your OT security is to outsource it. Turning over responsibility for protecting your OT network to a company you trust allows you to stay secure with minimal effort and fewer resources required.

Many of the key takeaways from this report should come as no surprise. The is a lack lack of OT security staff and the appropriate resources are not being allocated to fix the OT staff shortage.

The global OT security workforce gap is substantial, and there is a need to be creative in filling the gap. To find the right talent, industrial organizations need to have two core concepts when filling the workforce gap. Set reasonable expectations and be open-minded about who qualifies for OT security positions. In many cases, organizations base their parameters with strict and restrictive guidelines when building their OT teams. Until the gap is filled, the industrial sectors will continue to experience cyberattacks and it will only get worse.

While industrial organizations are improving their management of OT security, many are still behind the trends. This is clearly shown in our report as most organizations are lacking visibility into their OT environments.

While industrial organizations are improving their management of OT security, many are still behind the trends. This is clearly shown in our report as most organizations are lacking visibility into their OT environments. While each organization has different environments and processes, the challenge of OT security management is occurring at every industrial organization.

Regarding the operation technology world, we at SCADAfence clearly see that if an organization fails to plan, then in fact, they are planning to fail. To help improve managing OT security better, we highly recommend adopting OT security best practices which include getting visibility into the entire network, as it's hard to protect what you cannot see. Additional security practices include network segmentation or even micro-segmentation if possible, and getting continuous network monitoring is even more crucial in preventing attacks on critical infrastructures going forward.

With a more proactive and holistic approach to OT security management by network monitoring, anomaly detection, remote access visibility, and compliance, many industrial organizations can reduce their OT risk level drastically in just minutes. We suggest looking into OT security solutions that are all agentless, not intrusive, and can perform superhuman tasks at a fraction of the cost of one human worker.

Implementing a comprehensive OT security platform that is designed for the industrial sectors and adopting the right OT security best practices, will allow organizations to be more prepared for any incoming attack on their OT environment.

SCADAfence
www.scadafence.com

About Us

SCADAfence is the global technology leader in OT & IoT cyber security. SCADAfence offers a full suite of industrial Cyber security products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access, and IoT device security. A Gartner "Cool Vendor" in 2020, SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing, and building management industries to operate securely, reliably, and efficiently.

To learn more, visit our website, check out our blog, or follow us on LinkedIn.

New York
462 W Broadway
New York, NY 10012
USA
+1-646-475-2173

Munich
Schellingstr. 109a
80798 Munich
Germany
+49-89-2206-1175

Tokyo
5th Floor Nishida Bldg.
2-14-6 Shibuya
Shibuya-ku Tokyo 150-0002
Japan
+81-3-4588-5432

Ramat Gan
2 Shoham St.
Ramat Gan, 5251003
Israel
+972-3-763-0785