RESEARCH

Tripwire State of Industrial Cybersecurity Report

October 2019

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

As news of cyberthreats targeting industrial environments like energy utilities and manufacturing plants continues to surface, Tripwire surveyed security professionals who work in these industries to understand how industrial organizations are protecting themselves.

The survey findings revealed insights on the security professionals' levels of concern, investment in cybersecurity, and how they are organizing their teams around cyber issues.

The report found that:

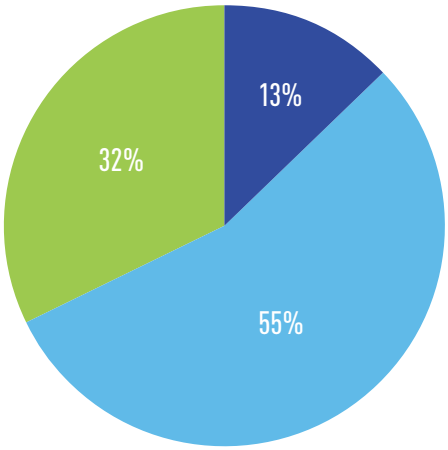
- Most organizations are worried about cyberattacks having physical operational consequences and impact to business
- Moderate investments are being made, but not enough
- Visibility into the OT environment remains an issue
- Training and building up teams is a top need

The survey was conducted by Dimensional Research in September, 2019. Read on for detailed findings.

Participants

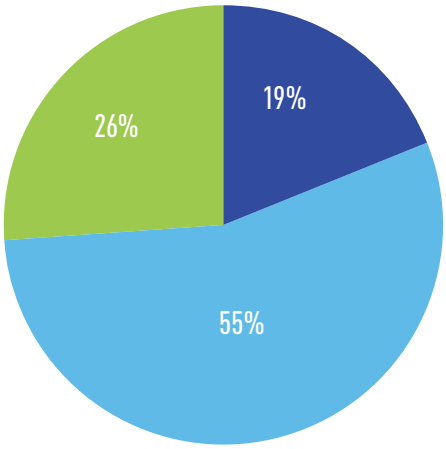
A total of 263 qualified individuals completed the survey. All participants had direct responsibility for the security of ICS systems at an energy, manufacturing, chemical, dam, nuclear, water, food, automotive or transportation company with more than 100 employees.

Responsibility



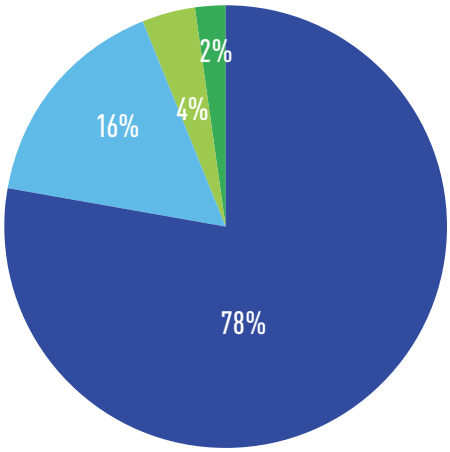
- OT security
- IT security
- Both OT and IT security

Job Level



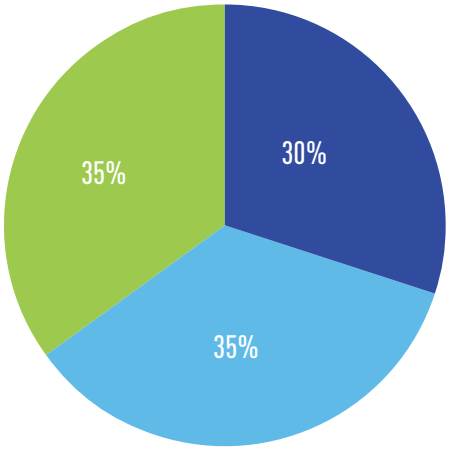
- Executive
- Team manager
- Individual contributor

Region



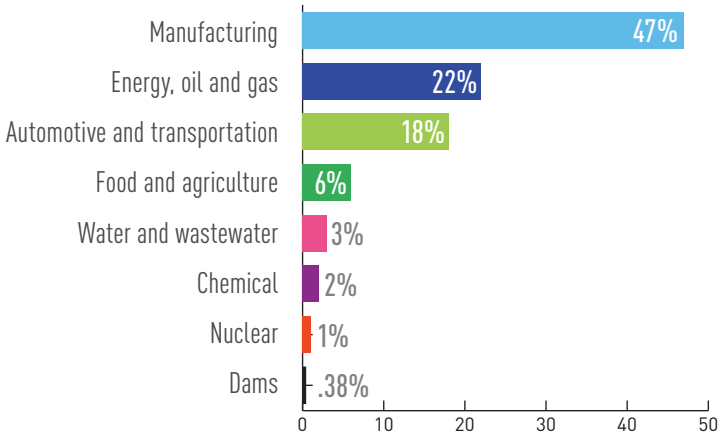
- United States or Canada
- EMEA
- APAC
- LATAM

Company Size



- 100–1,000 employees
- 1,000–5,000 employees
- More than 5,000 employees

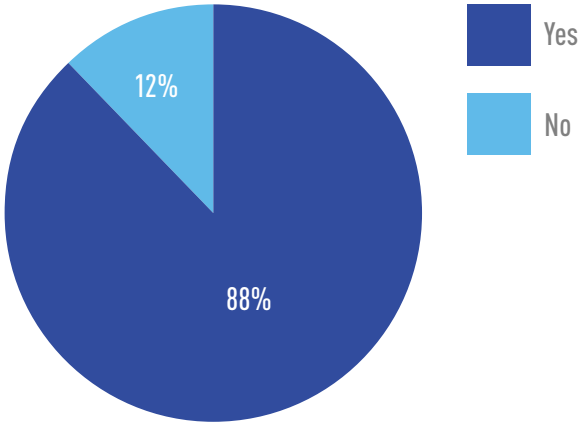
Industry



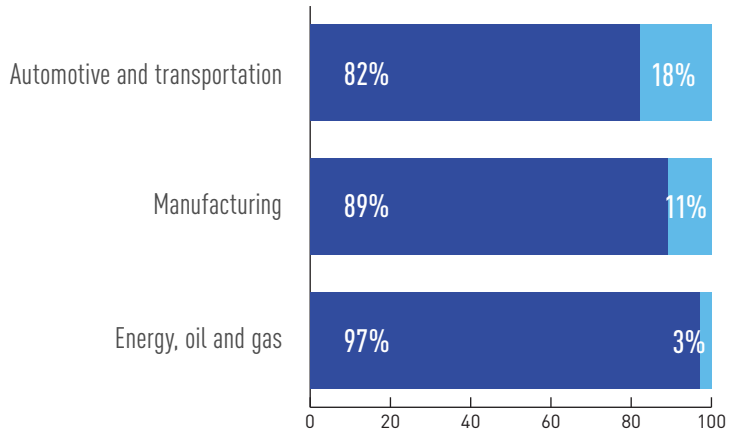
Cyberattacks: A Real Concern for Industrial Organizations

Eighty-eight percent are worried about the threat of ICS cybersecurity attacks, with the highest rate of concern in the energy and oil & gas industry.

Is your company worried about the risk of cybersecurity attacks on your ICS?

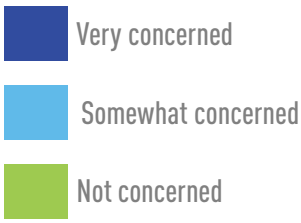


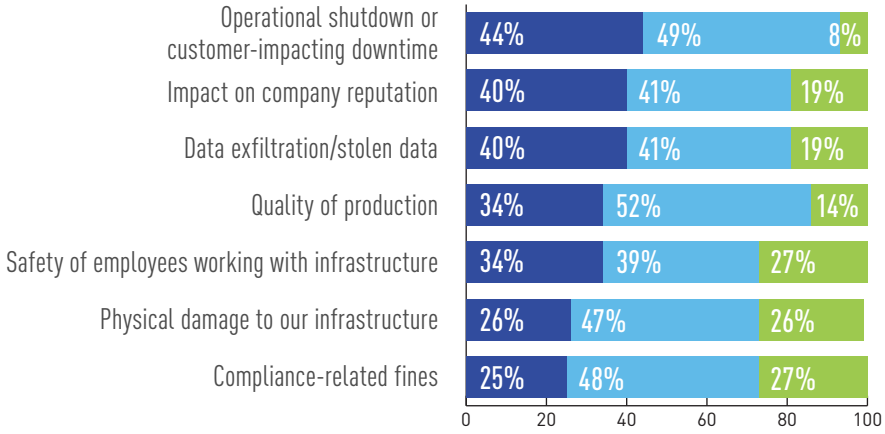
By industry



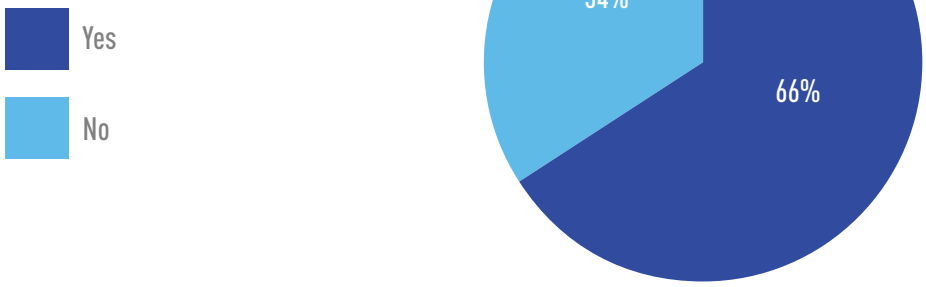
Industrial organizations have emphasized concern on the physical consequences of a cyberattack. Operational shutdowns and downtime are the biggest concern. Two-thirds (66 percent) believe an ICS attack could be catastrophic.

In the case of a cybersecurity attack on your ICS systems, how concerned is your organization about these specific impacts?



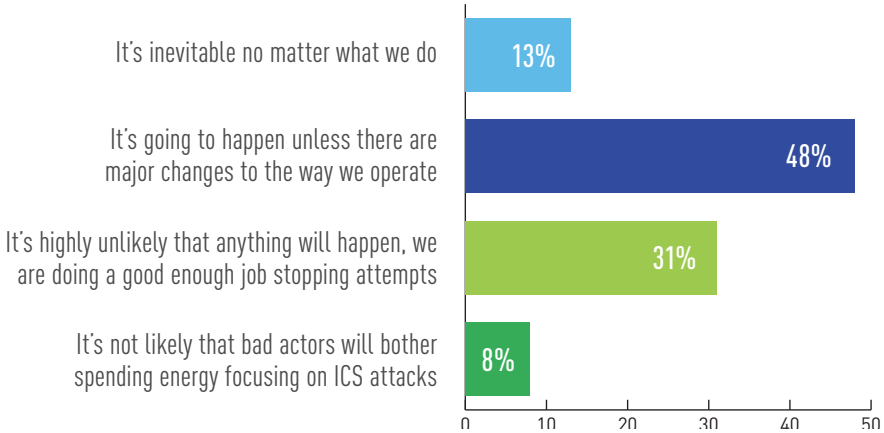


Given your knowledge of your ICS systems, are you concerned an ICS cybersecurity attack could result in a catastrophic event (i.e. explosion)?



Almost two-thirds (61 percent) think they could be hit by a successful ICS attack in the next 10 years.

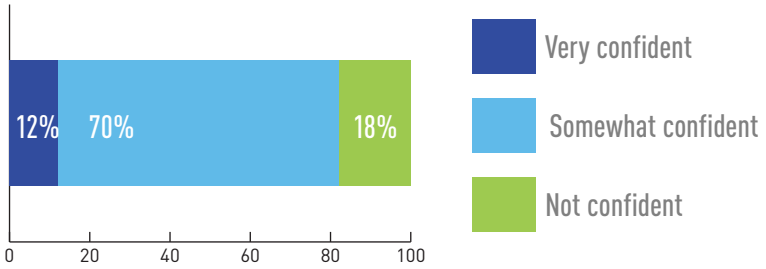
In your opinion, how likely is it that there will be a successful cybersecurity attack on your ICS in the next ten years?



Investing in Cybersecurity

Only 12 percent have a high level of confidence in their ability to avoid business impact from a cyber event.

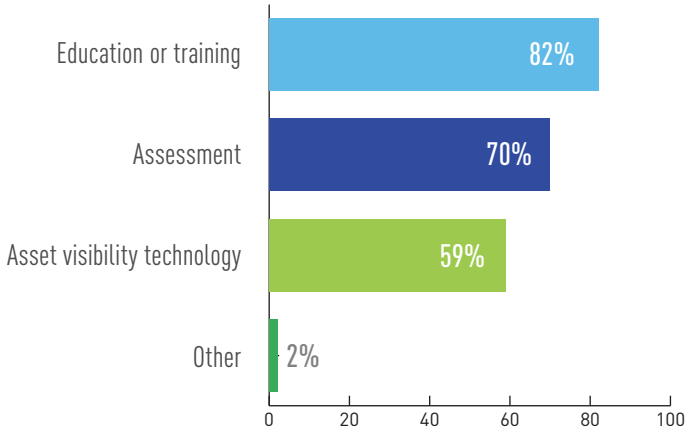
How confident are you in your organization's ability to identify and respond to a cyber event *before* it can impact the safety, productivity and quality of your operations?



Over the past two years, 77 percent said they have made cybersecurity investments in their industrial environment.

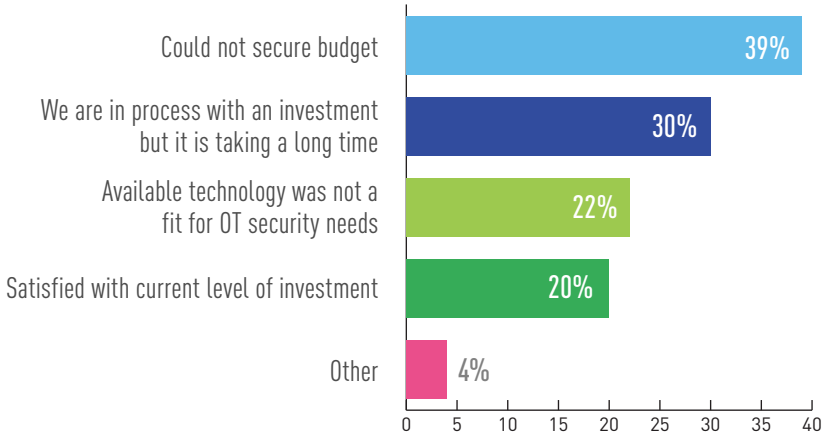
Of those, the top investments were in education, security assessments and technology for gaining asset visibility.

What types of investments have you made in your industrial environment in the past two years?



Of those who have NOT invested in cybersecurity over the past couple years, lack of budget was the top reason.

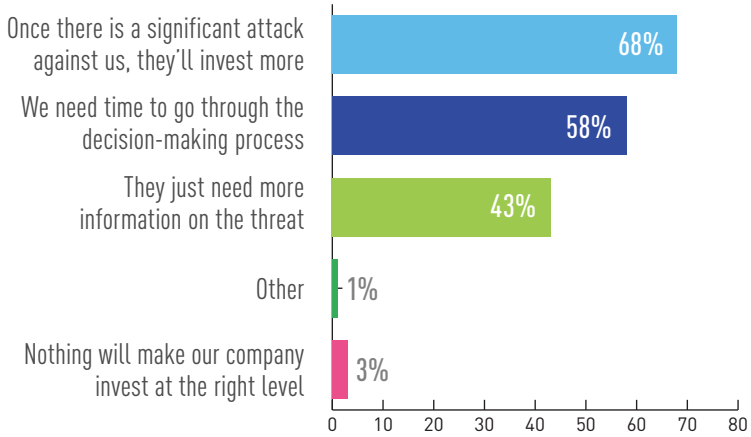
Why haven't you made investments in your industrial environment in the past two years?



Fifty percent do not believe their company is investing sufficiently in ICS cybersecurity.

Of those, 68 percent think they'd need to experience a significant attack in order to invest more.

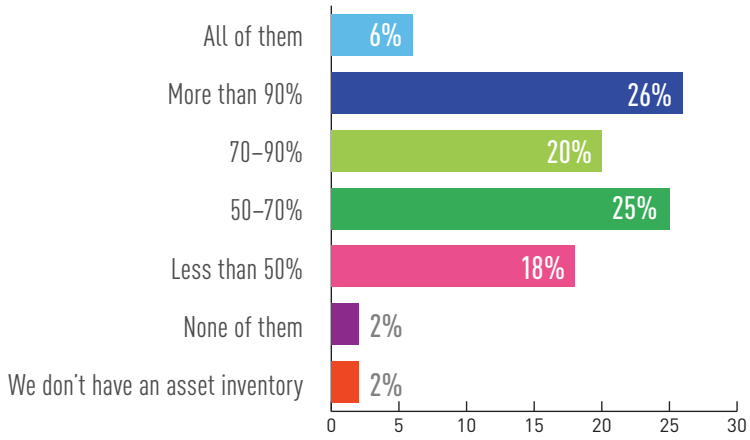
What do you think will be necessary for your company to invest sufficiently in ICS cybersecurity?



Strategies for Stronger Security

Only half (52 percent) have more than 70 percent of their assets tracked in an asset inventory.

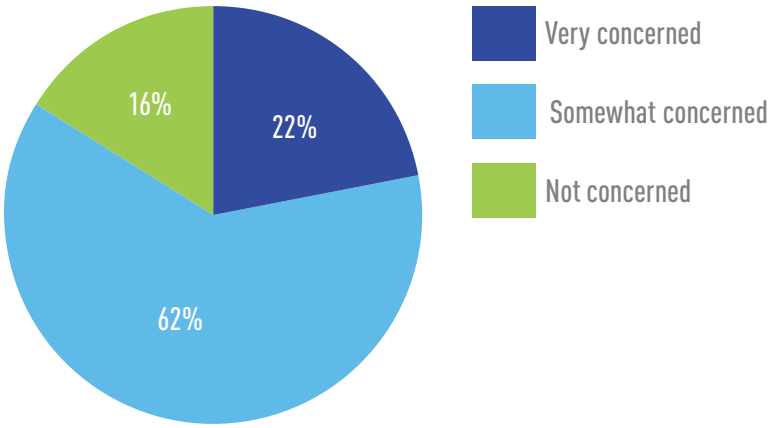
To the best of your knowledge, approximately how many of your company's OT assets does your company have tracked in an asset inventory?



Having visibility into all of the assets on the OT network is essential to understanding where cyber risks lie in the industrial environment. Organizations should understand which devices are connected, if they are configured correctly, if they vulnerable, and if they are operating properly.

Lack of visibility could partly be due to the fact that 84 percent were concerned about applying new cybersecurity tools in their OT environment.

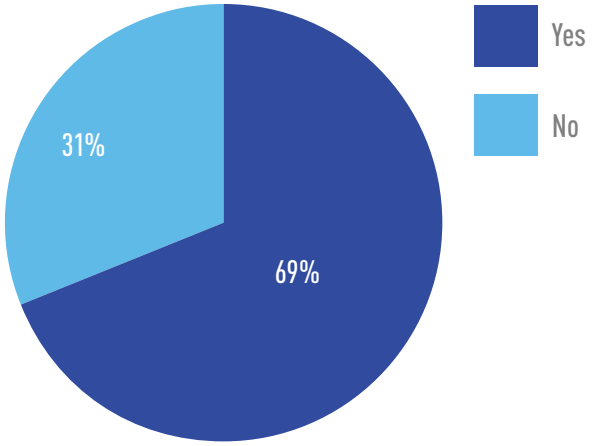
How concerned are you that applying new cybersecurity tools in your OT environment could interrupt your processes or operations?



Some of the cybersecurity practices that are common in IT cannot simply be repeated in OT environments. Solutions that are built specifically for OT cybersecurity will provide visibility using methods that will not interrupt industrial processes, such as passive monitoring and using the right industrial protocols.

About a third of organizations don't have a baseline of normal behavior for their OT devices, nor a centralized log management solution.

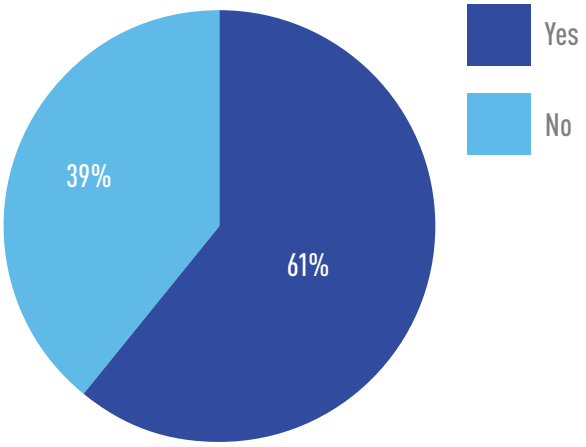
Does your company have a baseline of normal communications behavior of your OT devices and OT network?



By baselining normal user behavior and normal network traffic, organizations can be alerted to anomalies. By reading network traffic, OT cybersecurity solutions can map assets and the flow of traffic between them. Machine learning and visualization can make it easy to spot bad actors or unusual activity.

Almost two-thirds (61%) have a centralized OT log management solution.

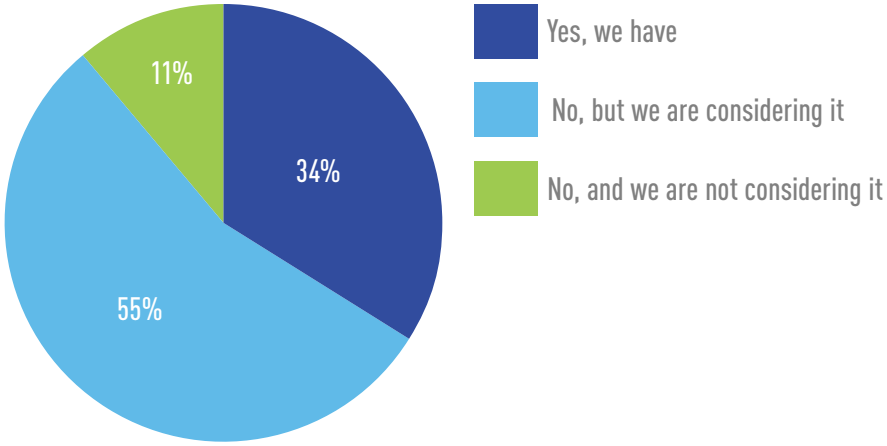
Do you have a centralized log management solution in place for your OT devices?



In the same way that a data historian captures and replays process events and sensor measurements, there is an equivalent function in cybersecurity with log management. Logs can tell you when a cyber event occurs that can interfere with your ability to view, monitor or control your process. A log management solution is also helpful in investigating outages and correlating events of interest.

Only a third (34 percent) have had an industrial security assessment, but more than half (55 percent) are thinking about having one.

Has your organization ever had an industrial cybersecurity assessment performed?



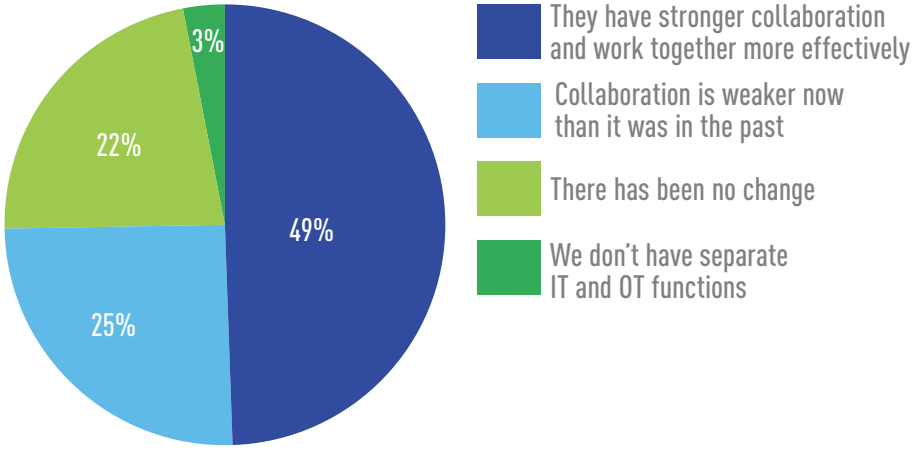
Assessment services are a good launching point for building up a cybersecurity program. Assessment provides organizations a tangible understanding of their security weaknesses and risks up front, providing a roadmap for building a cybersecurity strategy.

Building Industrial Cybersecurity Teams

With cybersecurity a relatively new issue for industrial environments, organizations are still driving to bridge the IT and OT gap and build up their industrial cybersecurity teams.

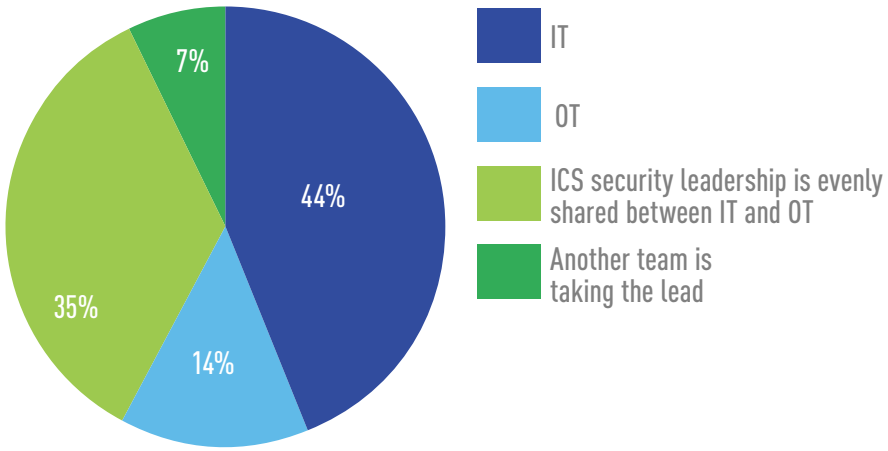
Nearly half (49 percent) report that collaboration between IT and OT is improving.

How are your IT and OT teams or functions working together now compared to two years ago?



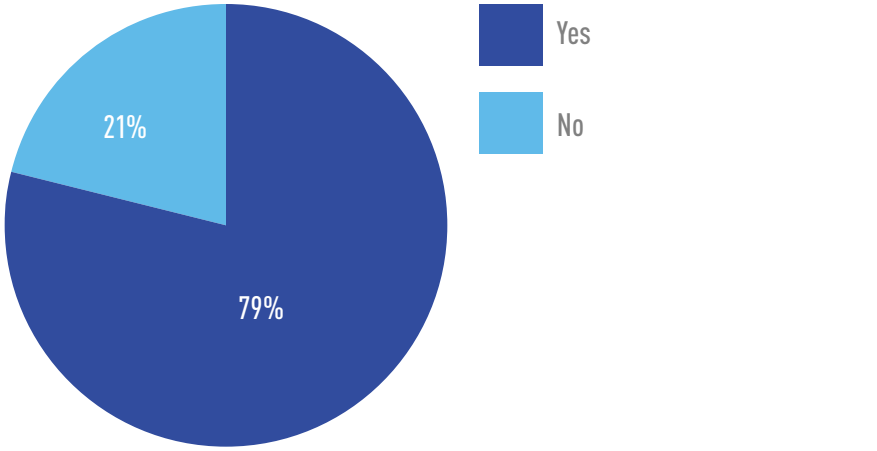
Of the organizations that have both IT and OT teams, IT seems to be taking the lead on ICS security responsibility.

What organization is taking the lead on ICS security needs?



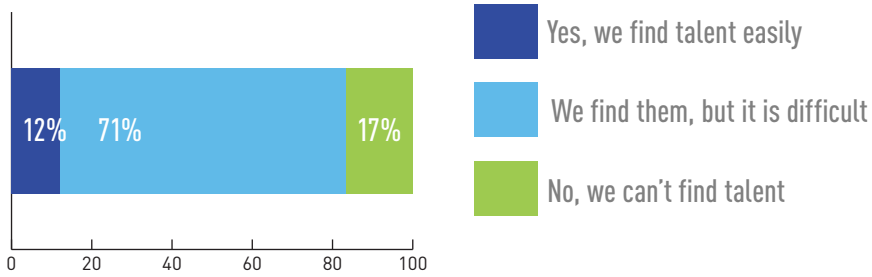
Most (79 percent) reported the need to better train their teams on OT security.

Does your company feel you have a gap in terms of training OT and IT staff around the unique needs and requirements for securing your OT environment?



Today 88 percent still have a hard time finding ICS security talent.

Is your company able to find needed talent for your industrial cybersecurity needs?



To learn about how Tripwire helps with industrial cybersecurity, please visit: https://www.tripwire.com/solutions/industrial-control-systems/

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

BRDRICS1a 1910