FORTINET

REPORT

Independent Study Finds That Security Risks Are Slowing IT-OT Convergence

Table of Contents

Executive Summary

Fortinet has worked with Forrester Consulting for a third time to check in on security trends affecting those who manage and maintain critical infrastructure—including the industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems that manage everything from factories to refineries to telecommunications infrastructure. Based on a global survey, the report identifies four trends:

- Organizations are moving more deliberately than expected in the convergence of IT and operational technology (OT) systems. The primary reason for this seems to be to ensure the security of critical infrastructure.
- Critical infrastructure professionals have many security concerns, including emerging risks from Internet-of-Things (IoT) devices and ongoing and growing priorities centered on compliance.
- The typical organization has not deployed a strategic, integrated approach to OT security, instead deploying multiple technical point solutions on different timelines, and in some cases, relying on one or more third parties to cover specific aspects of security.
- Organizations tend to find themselves stuck in a reactive stance toward security, and as a result, the vast majority have suffered breaches in their ICS and SCADA systems—many as recently as the past 12 months.

The good news is that respondents seem to recognize the need for a more strategic approach, and a few companies have adopted best practices that have enabled them to avoid OT system breaches over the past two or more years. This provides a glimmer of hope for the future as organizations scramble to address emerging threats.

Infographic: Key Findings

15%

of organizations have **fully converged IT/OT systems**, down from 17% in 2018.

Device failure replaced malware as a top-5 ICS/SCADA security concern between 2018 and 2020

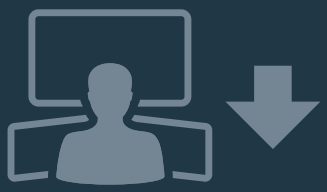
78%

of organizations plan to increase budgets for **ICS/SCADA security** this year

78%

of organizations expect **regulatory pressures** to increase over the next 2 years

Most important regulations for ICS/SCADA:
GDPR, ISA, FISMA



34%

of organizations outsource aspects of **ICS/SCADA security**

58%

of organizations have had at least **one OT security breach** in 12 months

Only 10% report never having had an OT security breach

Top-tier organizations are:

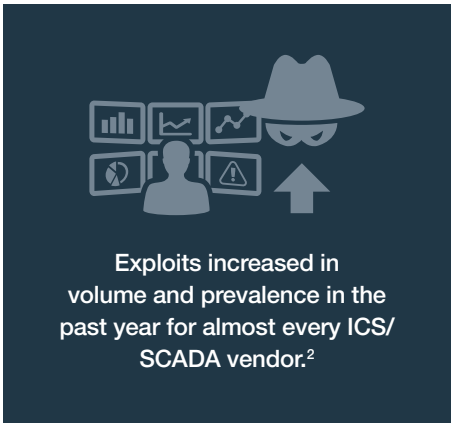
129% more likely to grant **little or no access** to business partners

52% more likely to grant **no more than moderate access** to IT providers

45% more likely *not* to have **outsourced advanced malware detection**

Introduction

Owners and operators of critical infrastructure face ever-expanding risk from a growing body of cyber threats. The story is one of convergence: The ICS and SCADA systems that manage this infrastructure are increasingly connected to IT systems or directly to the internet, exposing them to levels of cybersecurity risk that were unheard of when they were air gapped.



Exploits increased in volume and prevalence in the past year for almost every ICS/ SCADA vendor.[2]

Since many previously disconnected OT systems are now connected to the internet, they are increasingly barraged with both recycled IT-based attacks and purpose-built OT exploits.[1] At the same time, threat actors involved in terrorism, cyber warfare, and industrial espionage—as well as common criminals simply aiming to make a profit—are becoming more sophisticated with their attacks, making them more likely to succeed at organizations without bolstered defenses. These attacks on critical infrastructure can result in financial loss, a risk to brand reputation, and sometimes even loss of life or threats to national security.

Yet integrating IT and OT systems makes good business sense. Benefits include more effective and efficient monitoring of processes, the ability to leverage data from IoT devices to inform decision-making, and significant cost savings in power consumption, reduced raw materials waste, and employee efficiency. As a result, convergence is the clear trend, but the process brings with it a number of security challenges. These include an expanded attack surface, legacy systems whose security features were designed for a disconnected infrastructure, poor visibility into systems, and poor network segmentation.

Methodology for This Study

This report checks in on these trends using a biennial survey. Fortinet commissioned Forrester Consulting to conduct thought-leading research to explore the current perspectives of OT and cybersecurity leaders, their challenges and priorities, and their strategy for securing critical ICS and SCADA infrastructure. Forrester conducted earlier studies on this topic in 2016 and 2018, and this report will make note of shifts that have occurred since our last study.

Forrester conducted a quantitative survey of more than 400 professionals from around the world. Respondents work in job grades ranging from manager to C-level executive. Their responsibilities include the protection of critical infrastructure, internet protocol (IP)-level security, or security for SCADA systems or IoT devices. They work for companies with more than 500 employees—and more than 1,000 employees for U.S. respondents. They come from a wide variety of industries, with a focus on companies that have distributed critical infrastructure sites—notably, those involved in manufacturing, telecommunications, and energy production and distribution.

This report is focused on trends affecting this cohort and the companies they work for—especially with regard to the security of OT systems and the integration of IT and OT. We analyzed the responses from several angles and identified four market trends for 2020. We then did analysis on the security best practices more likely to be employed by companies that have experienced fewer breaches, compared with those who suffered more breaches.

Critical Infrastructure Cybersecurity Trends

Trend: The Convergence of IT and OT Is Complex, and Organizations Are Moving Deliberately

According to one recent study, nearly two-thirds of OT systems are connected—32% directly to the internet, and another 32% through a gateway into the enterprise.[3] While the trend is unquestionably toward convergence, many enterprises have found the process more complicated—and risky—than expected.[4]

In fact, only 4% of respondents to Forrester's survey claim that they do not foresee any specific challenges as they move toward convergence (Figure 1)—meaning that 96% do expect problems. Much of the concern relates to fears that their in-house teams or third-party service providers may not have adequate expertise with either converged technology in general or IoT device security in particular. The result of that lack of expertise could be data leakage—also a concern for more than 40% of respondents. By several percentage points, respondents cited these three concerns more frequently in 2020 than in 2018.

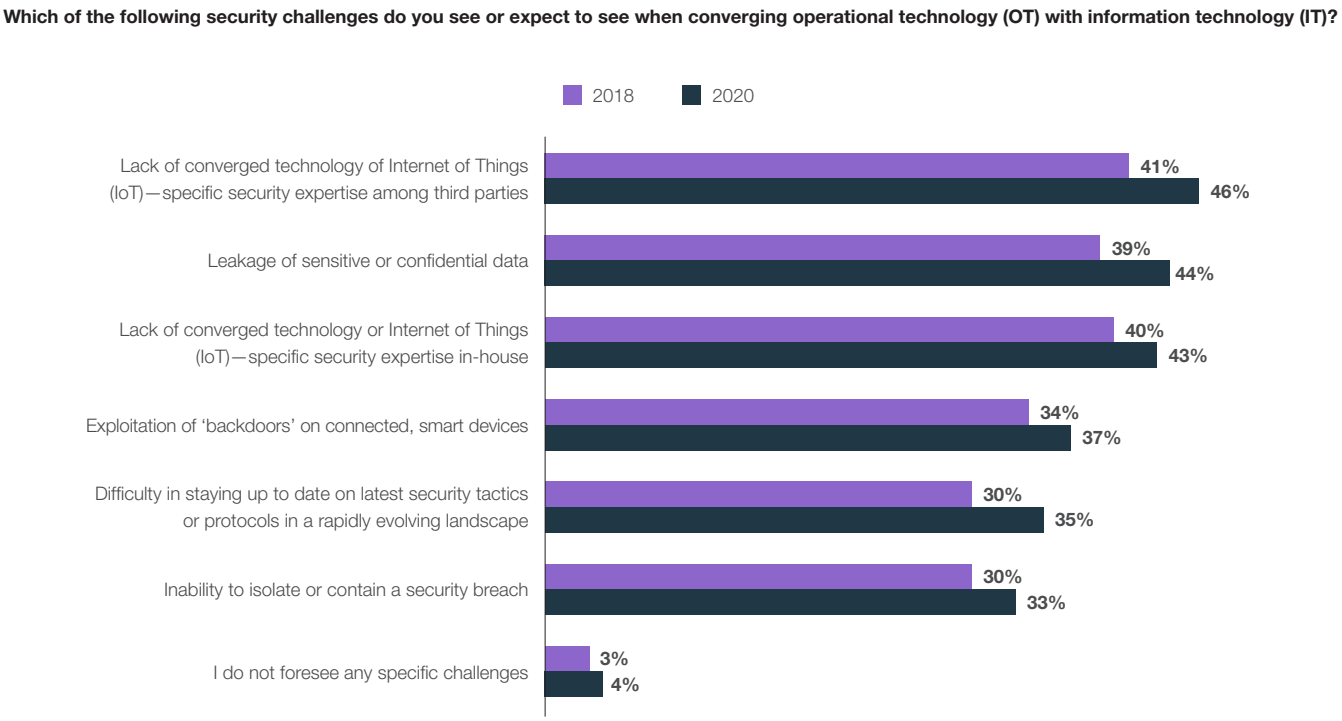


Figure 1: Challenges with IT/OT convergence.

Another data point confirms this anxiety—especially when comparing the 2020 responses with those from 2018. Over that two-year period, the percentage of respondents reporting deeply converged IT and OT systems actually declined by two percentage points—while the percentage of respondents saying that their OT systems are fully air gapped remained flat (Figure 2). While these specific results likely reflect slight differences in the two samples rather than a trend toward isolation of OT systems, they do seem to suggest something other than the rapid move toward convergence that many predicted.

When OT systems *are* connected, it is not always reflective of a deliberate, strategic decision. In some instances, an OT system's gateway to the internet is as innocuous as a single PC that is separately connected both to the OT system and the internet. Another increasingly common path to convergence involves larger-scale deployment of and dependence on IoT devices, which often pull data from the internet or report data out to corporate IT systems. While companies employ a wide variety of IoT devices in their OT environments, real-time location tracking and GPS tracking devices saw the biggest increases over the past two years (Figure 3).

Which of the following best describes how your organization converges operational technology (OT) and information technology (IT)?

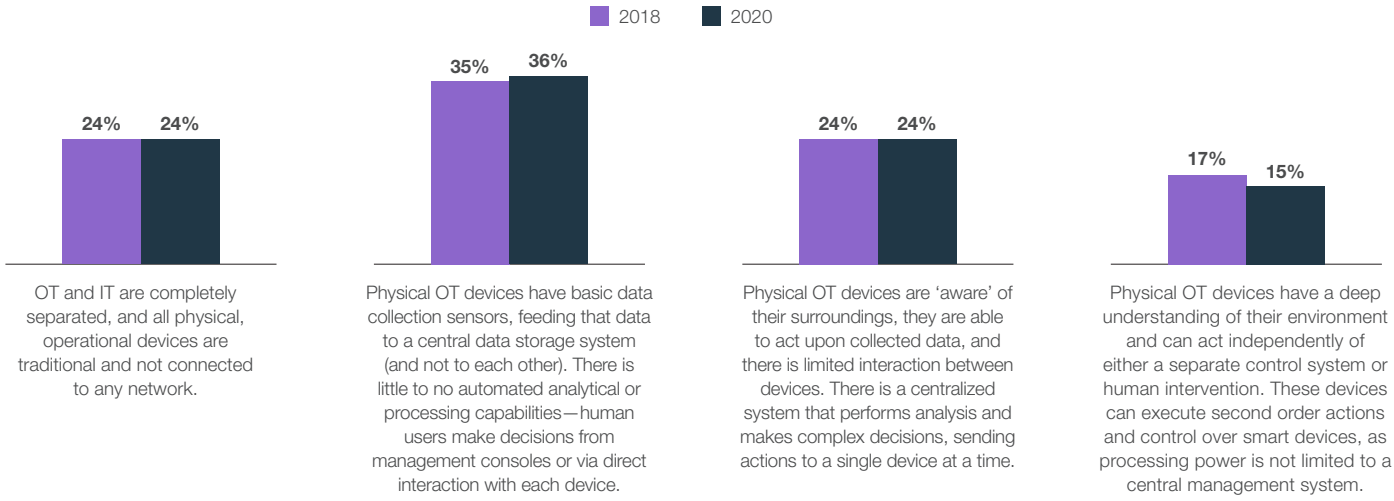


Figure 2: IT/OT convergence at organizations.

Which of the following Internet of Things (IoT) technologies are currently connected to your organization's network? (Select all that apply.)

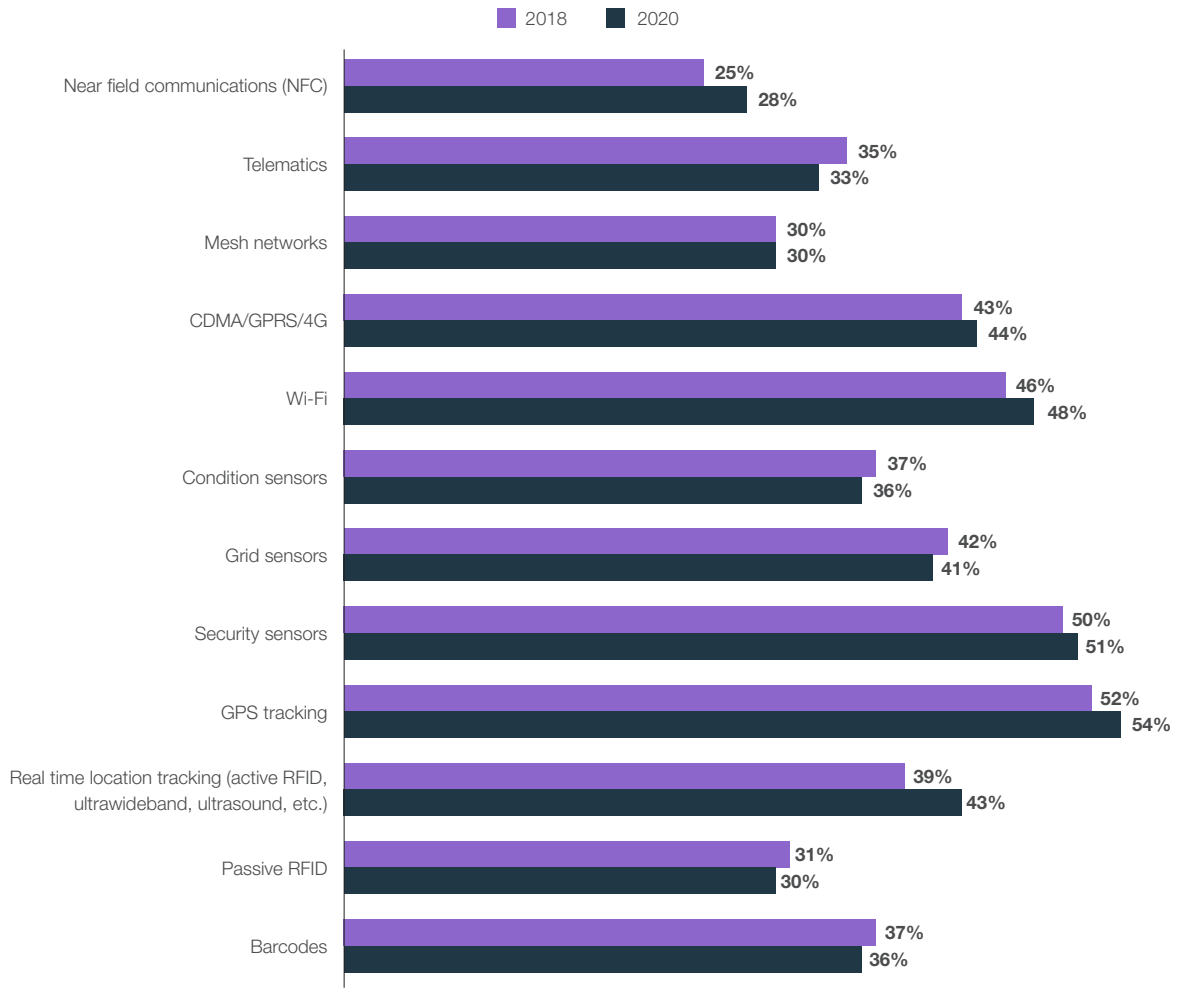


Figure 3: Connected IoT technologies.

Trend: Those Protecting Critical Infrastructure Have Many Security Concerns

When it comes to securing their ICS and SCADA systems specifically, the top concerns of our respondents evolved somewhat over the past two years. While malware was the top concern for critical infrastructure professionals in 2018, this worry fell out of the top five in 2020 (Figure 4), with the percentage citing it dropping by 13 percentage points over those two years. Conversely, device or software failure grew as a concern over the same period, cited by nearly three-quarters of respondents in 2020.

While the reasons behind this evolution are unclear, it may be that companies have bolstered—and increased their confidence in—their anti-malware solutions compared with two years ago. Conversely, as critical infrastructure systems become increasingly dependent on connected IoT devices, the prospect of downtime for those devices might be more worrying.

"Cyber-physical attacks have been touted as a serious threat for several years. But in recent years, these attacks have crept from theory to reality."[5]

Please rate your level of concern with the following as they relate to the security of your SCADA/ICS network.

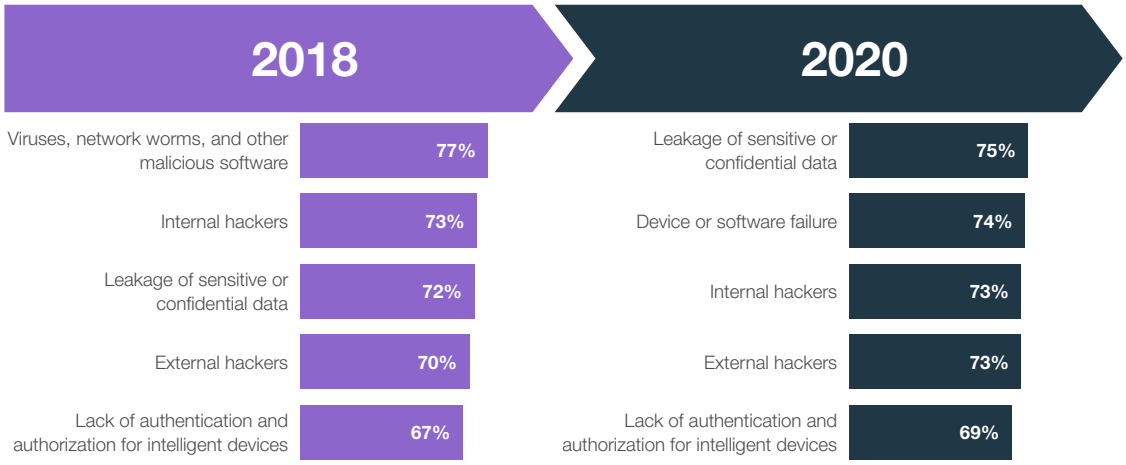


Figure 4: ICS/SCADA security concerns.

Compliance is another huge security concern for companies with critical infrastructure. Seven in 10 respondents say that regulatory pressures on their companies increased over the past year (Figure 5). An even higher percentage—78%—say that these pressures will increase in the coming two years. The staggering number of different requirements that companies face illustrates this: Of 20 distinct standards listed, a majority of respondents said their organizations were "largely regulated" or "fully regulated" by 19 of them (Figure 6).

The top compliance priorities for companies overall, and for their ICS and SCADA systems in particular, are not surprising (Figures 7-8). For both questions, the top three responses were the EU's General Data Protection Regulation (GDPR), International Society of Automation (ISA) standards, and U.S. Federal Information Security Management Act (FISMA) requirements.

With these complex security concerns, organizations are planning significant investments in OT security (Figure 9). Overall, nearly eight in 10 respondents (78%) plan increases in OT security spending in the coming year—and more than half (51%) plan increases of more than 5%. Only 10% of respondents report that the OT security budget will remain the same—less than half the number who report no budget increase for OT infrastructure itself. Overall, more respondents reported a budget increase for OT security than any other spending area listed.

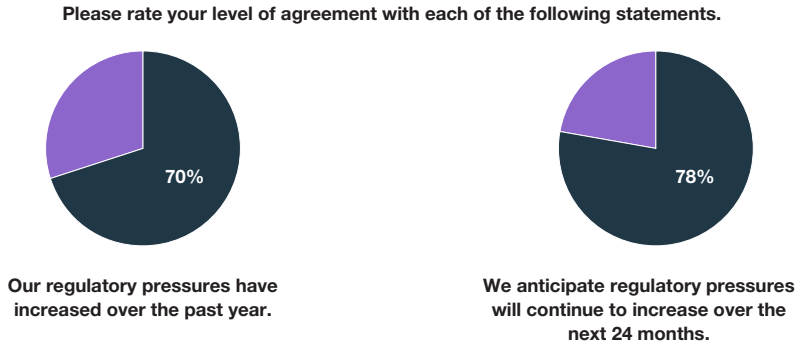


Figure 5: Regulatory pressures on companies.

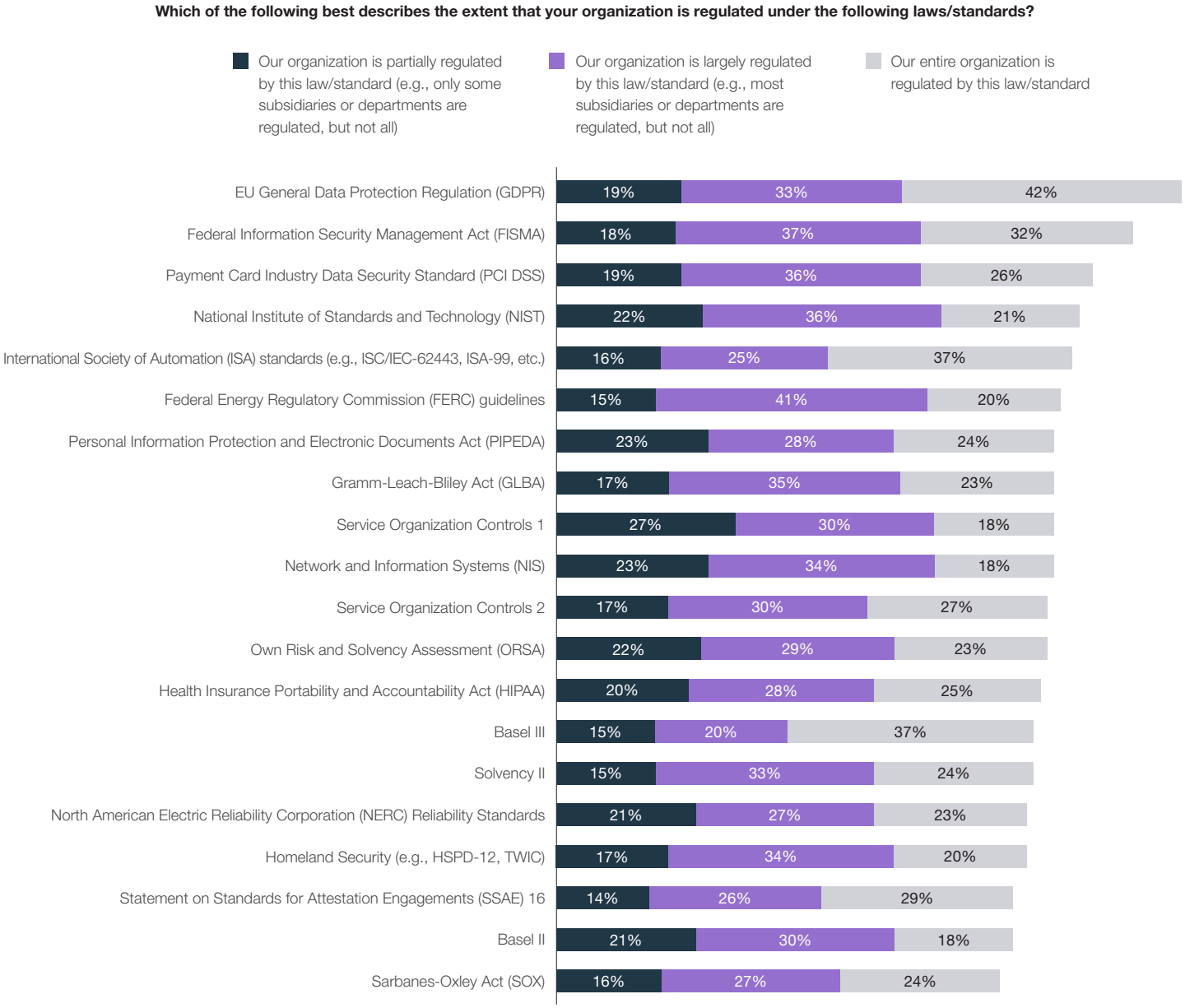


Figure 6: Regulations and standards affecting organizations as a whole.

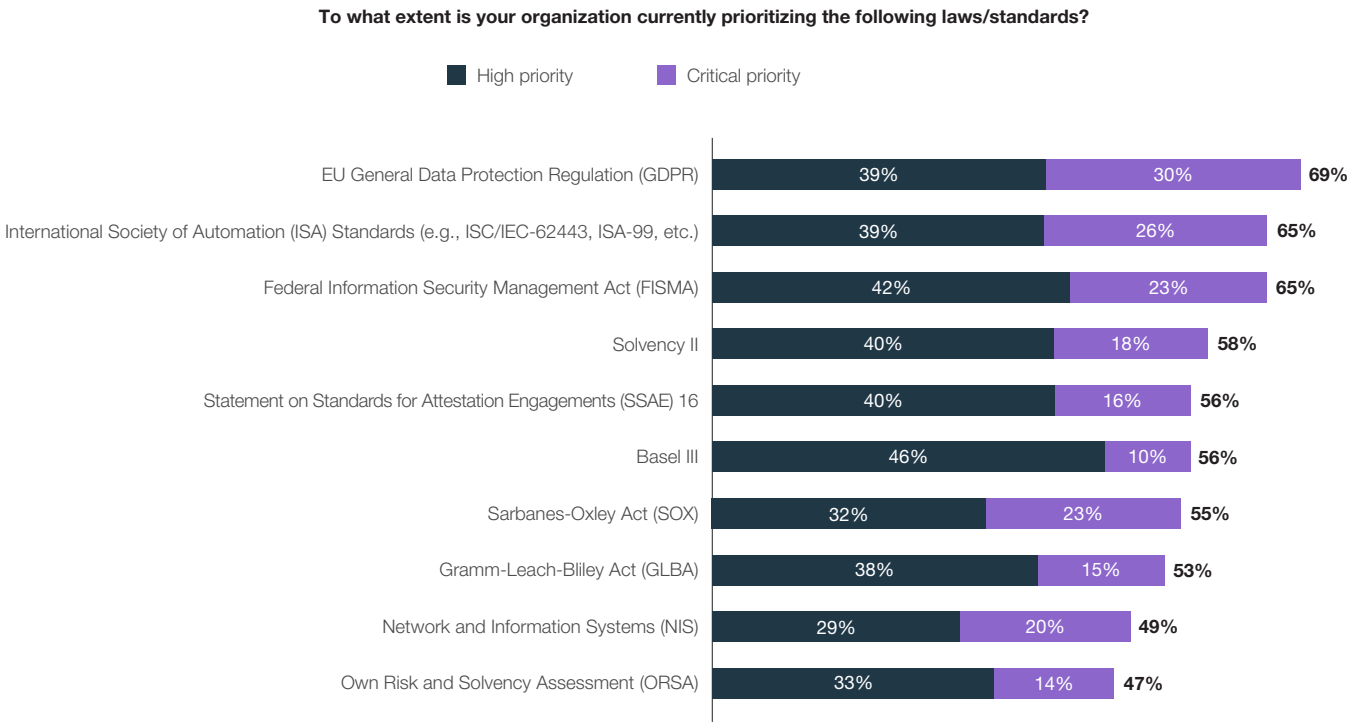


Figure 7: Prioritization of regulations and standards.

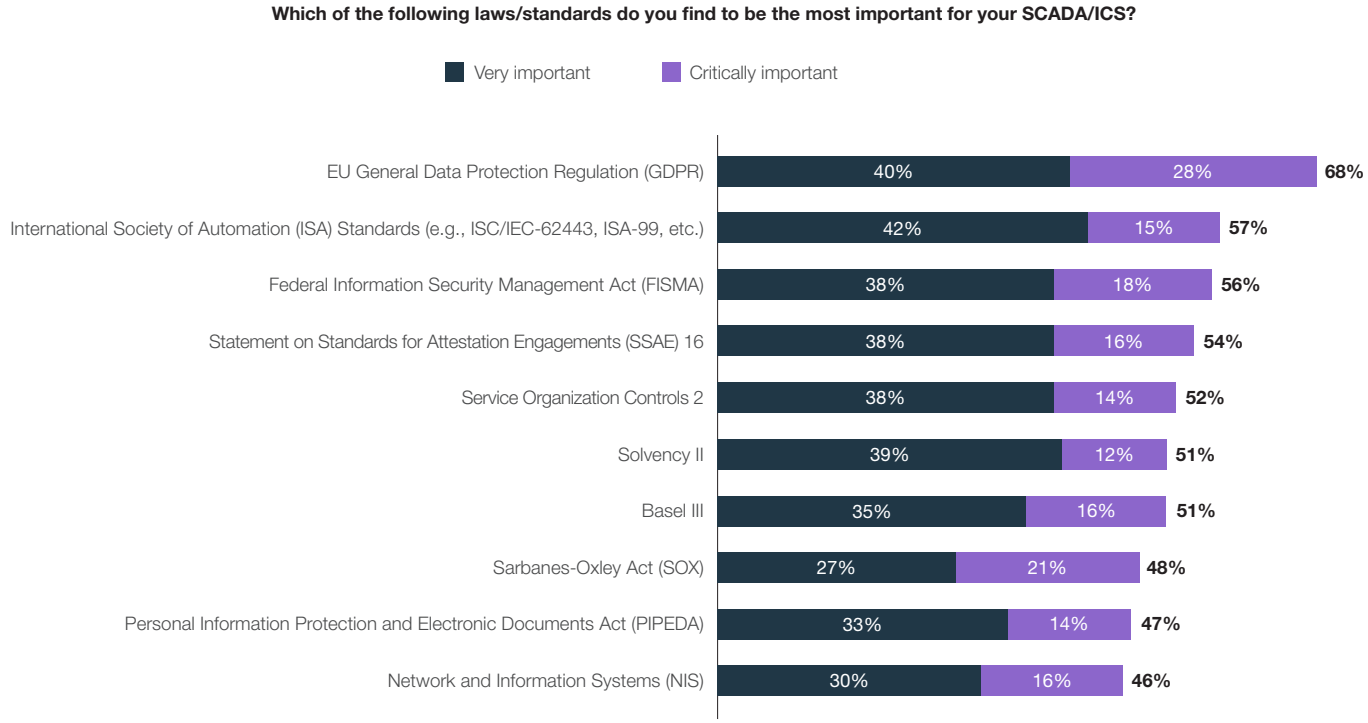


Figure 8: Most important regulations and standards for ICS and SCADA systems.

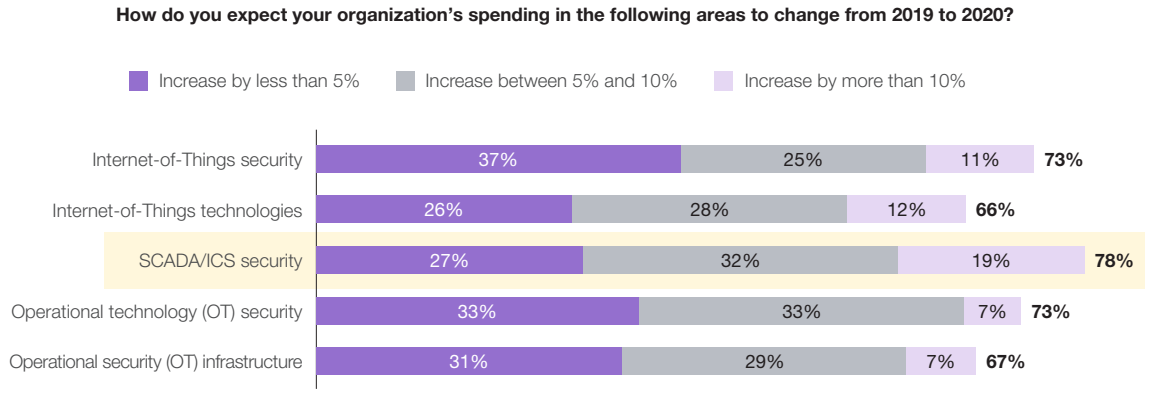


Figure 9: Organizations' security spending priorities for the next 12 months.

Trend: Securing ICS/SCADA Systems Is Complex and Haphazard Approaches Are Not Uncommon

When respondents were asked about different aspects of OT security, it was clear that many are taking a fragmented approach (Figure 10). Security measures currently in use at organizations ranged from 52% for SSH or TLS encryption to 74% for robust security analytics. With encryption currently employed at barely half of organizations, it is not surprising that 30% of organizations plan to deploy it over the next year—the second most common new project behind Privileged Identity Management (PIM) technology (31%; Figure 10).

Present initiatives to bolster security are in response to a threat landscape for OT systems that is increasingly advanced and ominous (Figure 11). When asked what factors contributed to their current ICS/SCADA security strategy, there is more concern this year than in 2018 regarding both typical cyber criminals (75% versus 62%) and nation-state actors (66% versus 62%). More respondents fear an attack that impacts customer-facing systems (75% versus 67%), perhaps reflecting the increasing importance of these systems in a rapidly evolving marketplace. Conversely, respondents are somewhat less concerned with employee use of personal and cloud technology on work devices (58% versus 65%)—perhaps because some organizations have taken steps to deal with issues like Shadow IT and bring-your-own-device (BYOD).

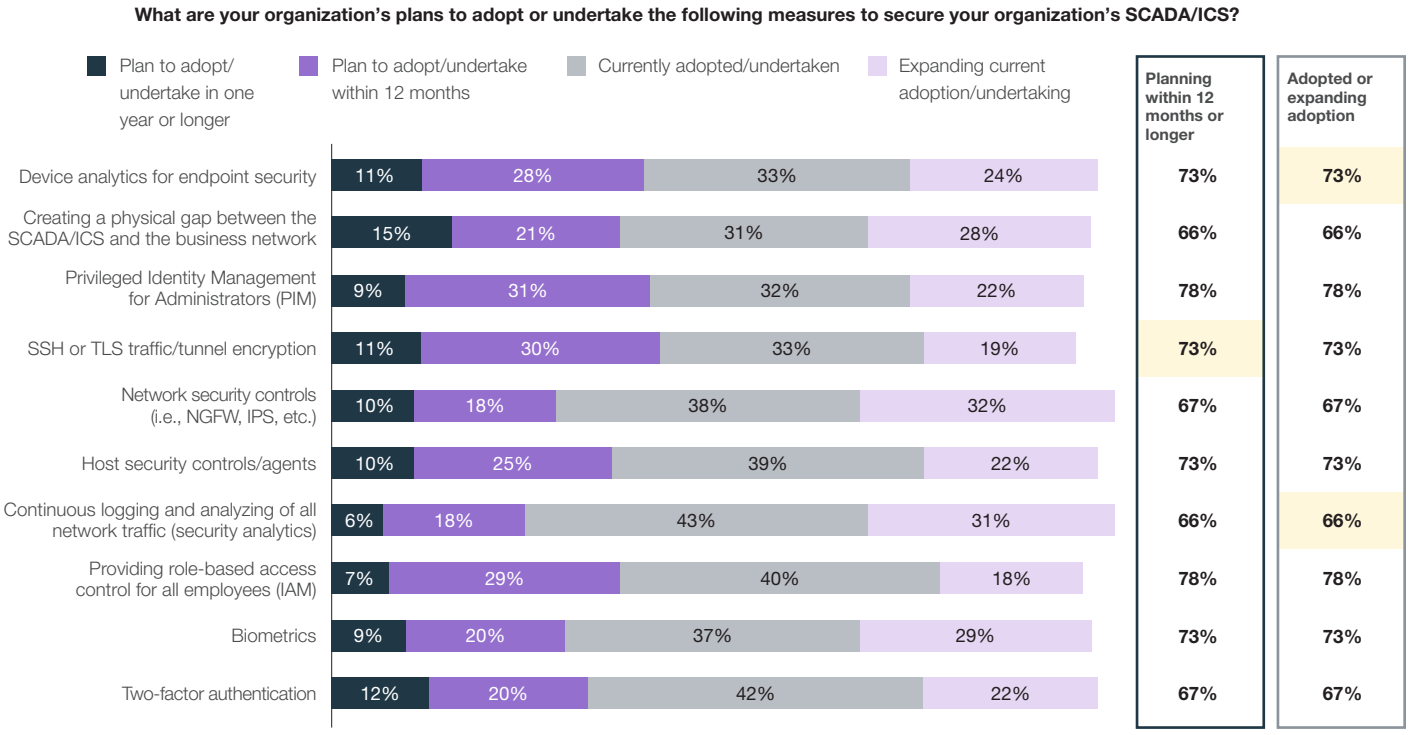


Figure 10: Status of various OT security measures.

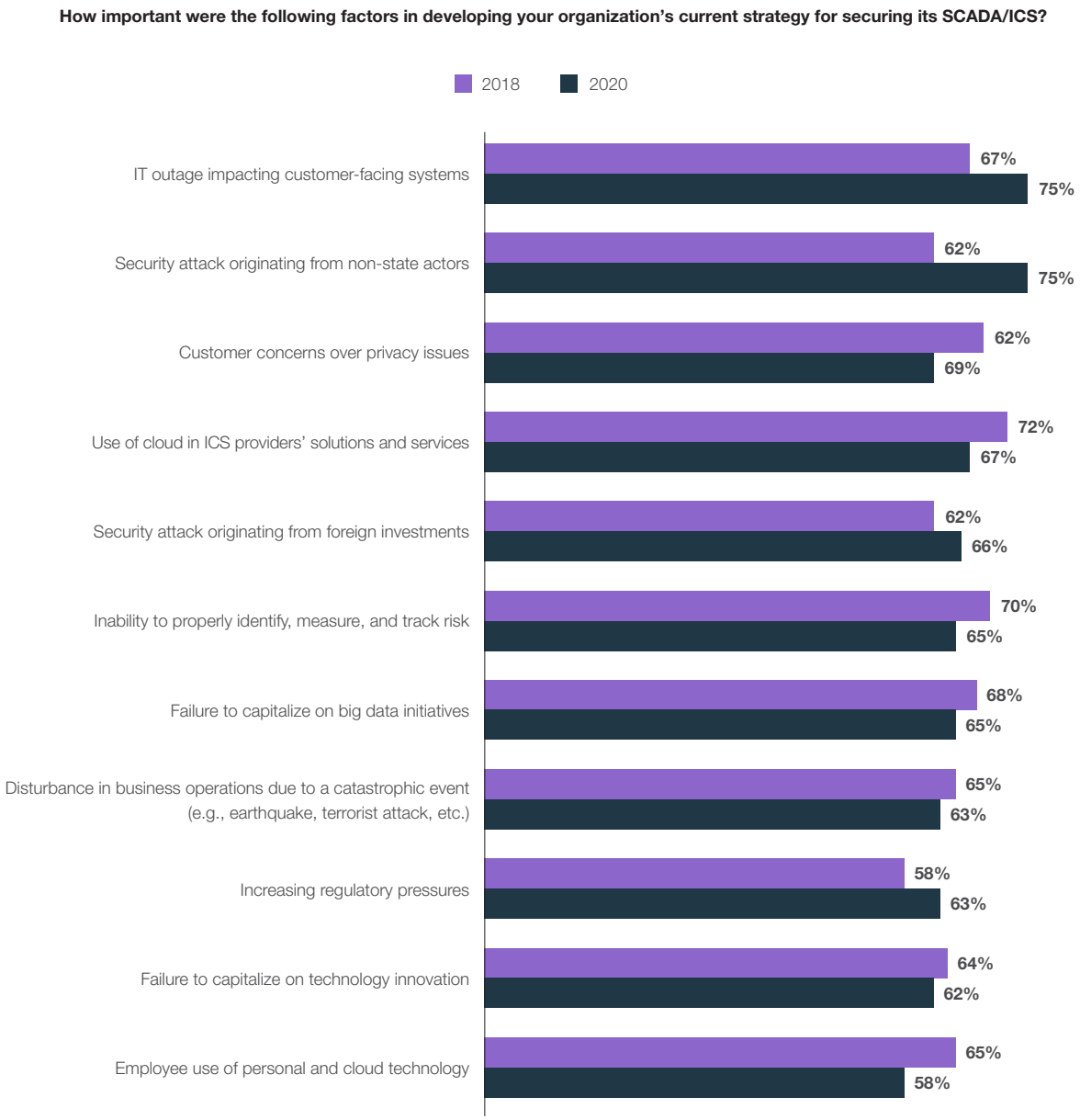


Figure 11: Critically important and very important considerations for ICS/SCADA security strategy.

The piecemeal approach extends to decisions to outsource different aspects of OT security. One-third (33%) of organizations outsource their OT infrastructure, compared with 27% in 2018 (Figure 12). But the percentage of organizations that outsource aspects of their OT security remained steady, declining from 35% to 34%. These differences are small and may just reflect different samples, but it is interesting that companies seem more willing to consider new outsourcing arrangements for infrastructure than for security.

Among those who do outsource some security functions, intrusion prevention system (IPS), wireless security, and IoT security are the most common—all outsourced by 41% of that subset (Figure 13). As an emerging security need, IoT security outsourcing increased by 5% within that group since 2018. Overall, 55% of those who outsource depend on more than one security services vendor (Figure 14). U.S. firms in particular have increased the use of multivendor outsourcing—up from 53% to 67% over two years. Such dependence on multivendor point solutions can exacerbate the fragmentation of OT system protection, increase complexity, and reduce operational efficiency.

Another indication of a tactical rather than strategic approach to security is visible when respondents report the level of access they provide to third parties. Nearly two-thirds (65%) of organizations give complete or very high access to IT providers, while solid majorities give similar access to business partners (59%) and government agencies (53%). Given the fragmented, multivendor approach that so many organizations employ, it is likely in many cases that IT providers and other third parties have more access than required to do their jobs. It is possible that current systems do not allow for the intelligent segmentation that would help them clearly control access according to role.

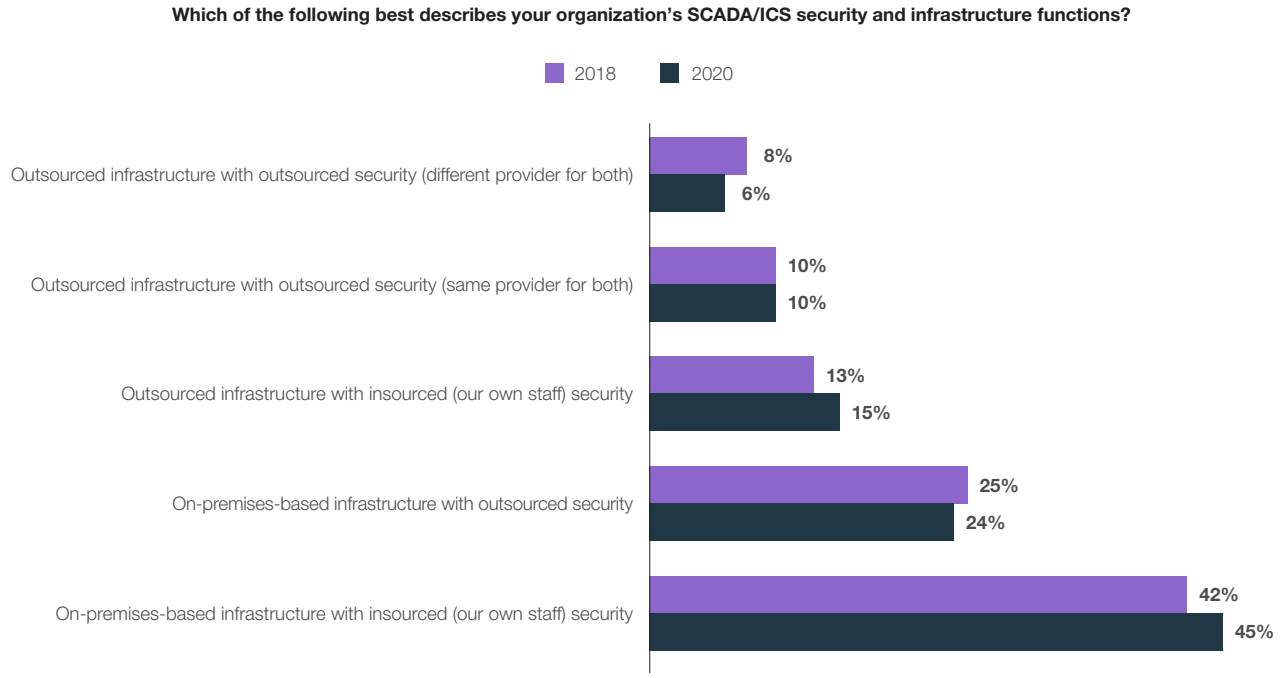


Figure 12: Status of outsourcing for ICS/SCADA security.

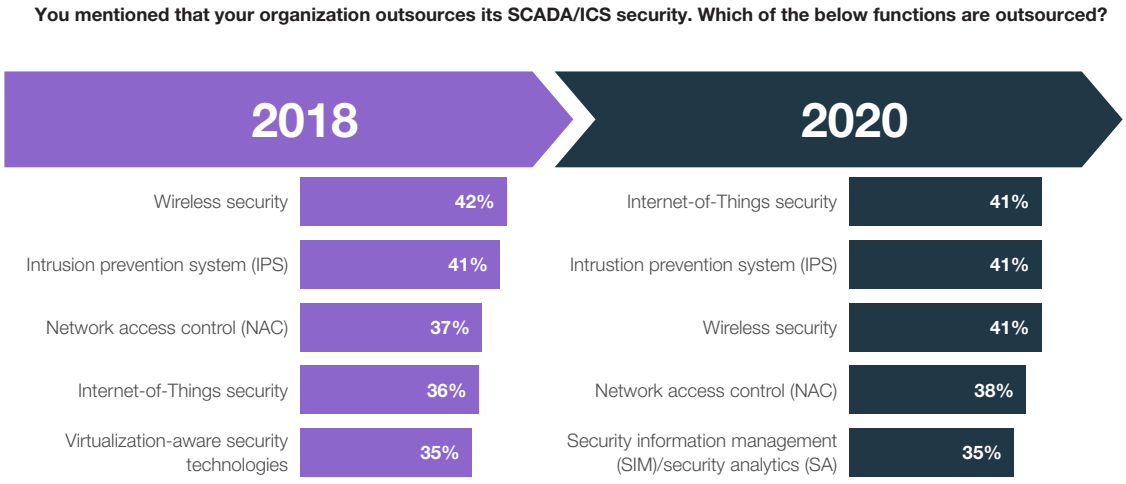


Figure 13: ICS/SCADA security functions outsourced.

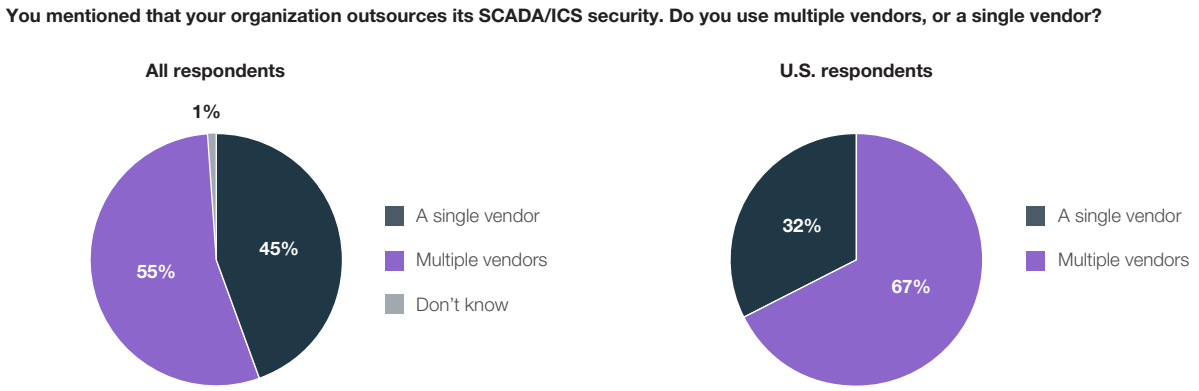


Figure 14: Single vendor/multivendor outsourcing for ICS/SCADA security.

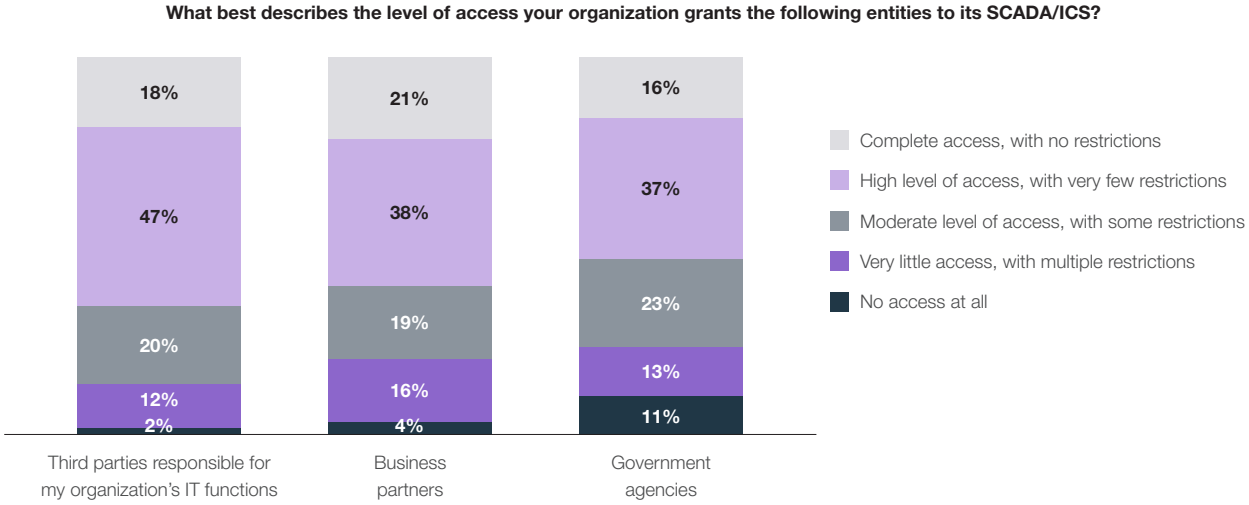


Figure 15: Level of access given to third parties.

Trend: OT Security Tends to Be Reactive, and Most OT Systems Have Suffered Breaches

In addition to this continuing fragmentation, organizations still tend to be stuck in a reactive stance toward OT security. One indication of this is how they expend their resources. On average, respondents estimate that nearly half (49%) of their budget and staff time was spent on responding to attacks, while only 21% is used for the proactive pursuit of threat prevention (Figure 16).

Businesses recognize the need for a more strategic approach. When asked to rank the top three actions they believe will help them overcome challenges they see with IT/OT convergence, the most cited by far was to perform a full business and operational risk assessment (Figure 17). Seeking out third-party assistance is a significant laggard among the options presented in the survey, and perhaps is another indication that organizations realize that the outsourcing of security functions—especially in a fragmented manner—is by no means a silver bullet.

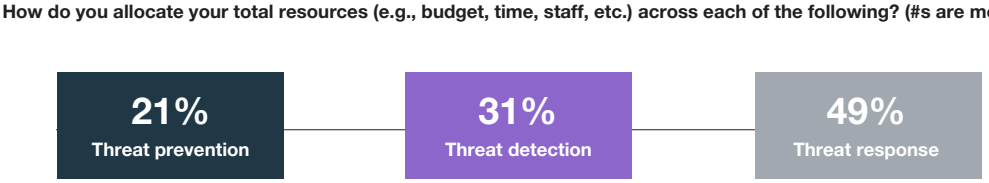


Figure 16: Expenditure of all resources on different aspects of security.

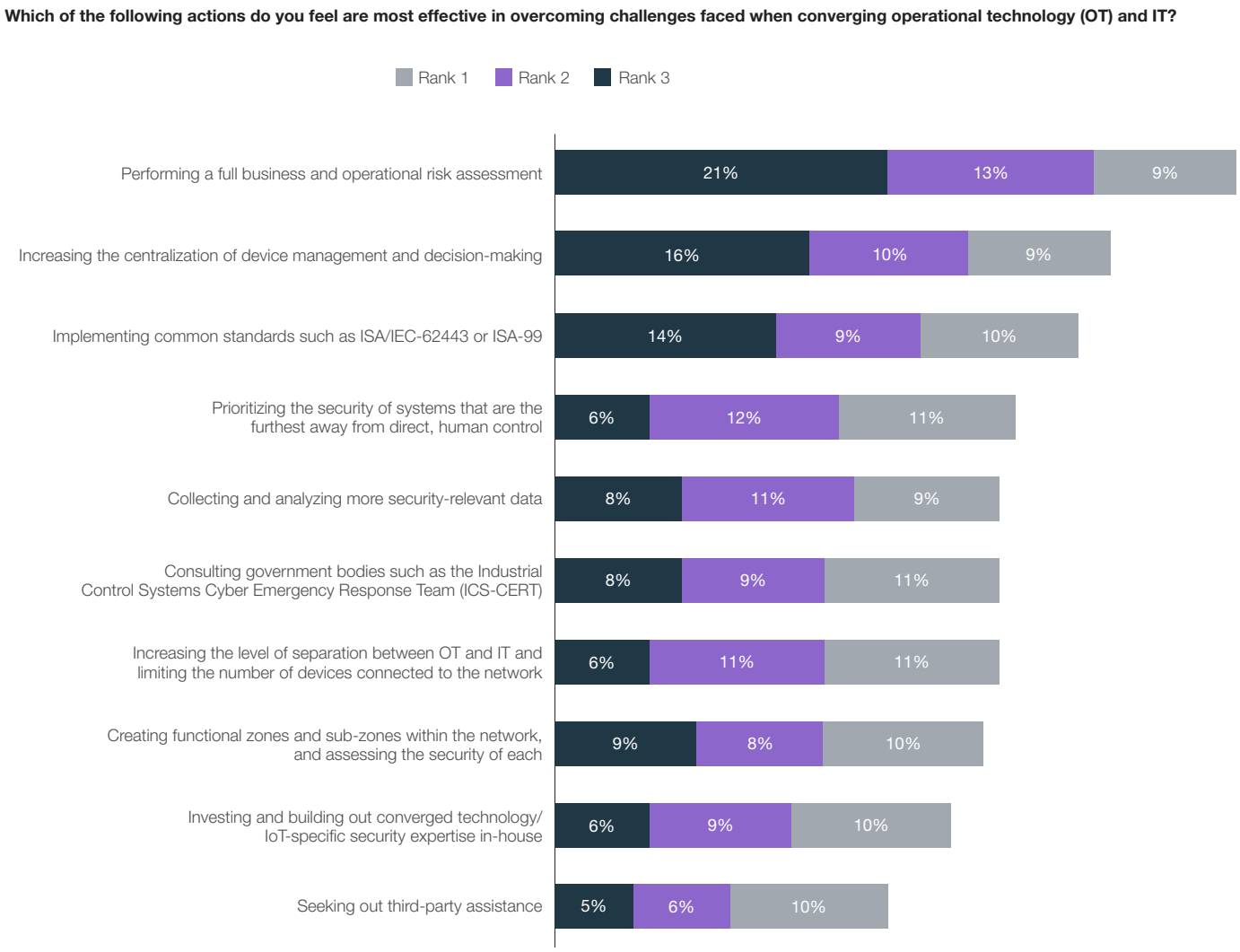


Figure 17: Top actions to address IT/OT convergence challenges.

Given the haphazard, reactive stance toward OT security that many organizations employ, it is perhaps not surprising that these organizations suffer frequent security events. Overall, 58% of organizations have experienced at least one security breach in their OT systems in the past 12 months (Figure 18), and only 10% report never having suffered such an intrusion. Looking at the overall IT and OT infrastructure, nearly two-thirds (66%) of organizations have had four or more security breaches over the past 12 months (Figure 19).

The impact of these breaches is not trivial. More than six in 10 respondents reported that they had suffered compliance, financial, operational, and even physical safety impacts due to attacks on their ICS and SCADA systems (Figure 20).

"Despite seasonal fluctuations and a wide variety of targets, the data is clear on one thing: IT-based attacks on OT systems are increasing."[6]

To the best of your knowledge, has the SCADA/ICS at your organization experienced a security breach?

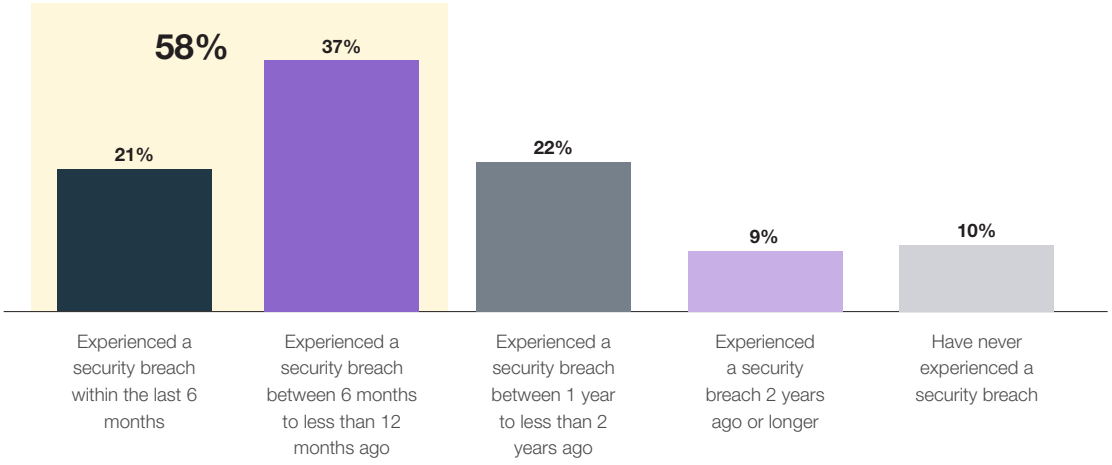


Figure 18: Security breaches for ICS/SCADA systems.

In the past year, how many security breaches has your organization experienced?

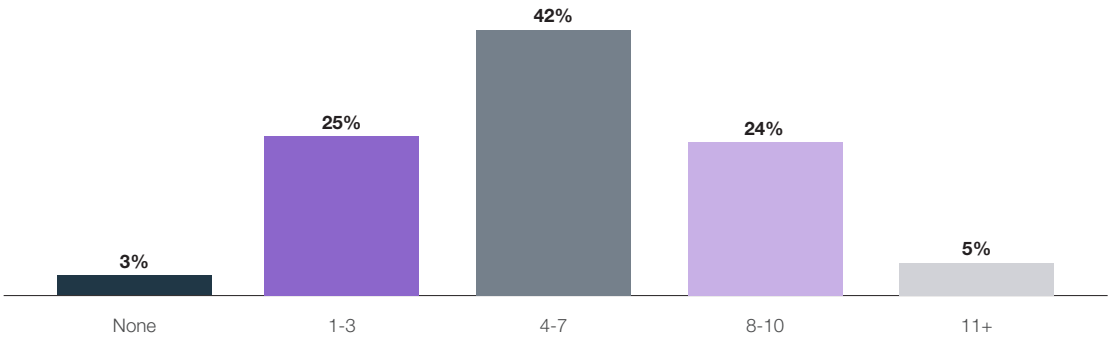


Figure 19: Security breaches of IT and OT systems over 12 months.

To the best of your knowledge, how much were the following impacted due to the security breach to your organization's SCADA/ICS?

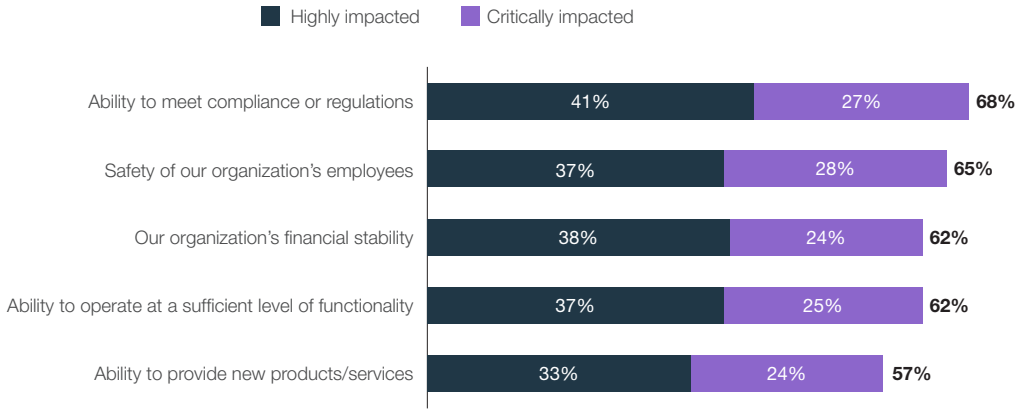


Figure 20: Impacts of ICS/SCADA security breaches.

Best Practices of Top-tier Organizations

As noted, some of the respondents to Forrester Consulting's questionnaire have been more successful than others in preventing intrusions and minimizing risk for their organizations. In fact, 58% of organizations represented in the survey had experienced at least one breach of OT systems in the past 12 months, while only 19% had gone two or more years without such an intrusion.

To analyze the data more deeply, we compared the security practices of these two subsets—the "top-tier" and "bottom-tier" organizations in our sample. We identified the following best practices that were more likely to be followed by those that have *not* experienced a recent breach:

1. Top-tier organizations are 129% more likely to grant very little or no network access to business partners.

While partners often need near real-time access to certain resources, the safest companies are more than twice as likely to be very restrictive with that access—and presumably have intelligently segmented the network in such a way as to make this possible.

2. Top-tier organizations are 75% more likely to severely restrict access to government agencies.

Of course, requirements vary according to location and industry, but organizations that strategically restrict access to data on a need-to-know basis tend to suffer fewer breaches.

3. Top-tier organizations are 52% more likely to grant no more than moderate network access to IT service providers.

These third parties often need significant access to do their jobs, but organizations that enforce strict access policies—rather than granting blanket access—tend to have better results.

4. Top-tier organizations are 45% more likely *not to have outsourced* advanced malware detection.

Certain functions may be executed more effectively in-house for some organizations, and companies that have successfully avoided breaches tend to depend on internal systems for threat detection.

5. Top-tier organizations are 36% more likely *to have outsourced* network analysis and visibility.

For companies that do not have a fully built-out security operations center (SOC), it often makes sense to entrust this big-picture function to a well-resourced partner.

Conclusion

Our research shows a mixed picture for critical infrastructure professionals. On the one hand, both operations and security for OT systems are in a state of uncomfortable flux, with IT/OT convergence slowing or even stalling and security still conducted in a piecemeal, reactive manner. The result is that breaches occur way too frequently, and the impact of these incidents is significant for a company's bottom line.

On the other hand, there is a clear recognition that a more strategic approach is needed that ties the security of ICS and SCADA systems to the needs of the business, and for cybersecurity risk to be integrated into a company's overall risk portfolio. Some organizations have made significant moves in that direction—especially in the area of third-party access—and tend to have fewer breaches as a result.

This positive trend will hopefully spread, leading to a more holistic approach to cybersecurity across a critical mass of converged enterprises, from IT to OT. As this potential transformation begins in earnest, it will be interesting to see how strategies and tactics evolve for critical infrastructure professionals over the coming two years.

References

[1] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, May 8, 2019.

[2] Ibid.

[3] Barbara Filkins, "The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns," SANS Analyst Program, July 2018.

[4] John Maddison, "Is Converging Your IT and OT Networks Putting Your Organization at Risk?" Fortinet, May 9, 2018.

[5] Elizabeth Montalbano, "Six Cyber-Physical Attacks the World Could Live Without," The Security Ledger, January 18, 2017.

[6] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, May 8, 2019.

FORTINET

www.fortinet.com

May 6, 2020 10:36 PM

D:\Fortinet\Work\2020\May\050620\report-forrester

592105-0-0-EN