July 2022

MARKET REPORT

The state of industrial security in 2022

Insecure remote access, lack of network segmentation, and insufficient automation are leaving organizations open to attacks. »

Barracuda®
Your journey, secured.

Contents

Introduction

Industrial security: Challenges and opportunities

Security for the industrial internet of things (IIoT) and operational technology (OT) is in its infancy in many organizations. Several factors — including security incidents — are driving awareness and improvements. There's certainly plenty of room for both, considering more than 90% of organizations surveyed acknowledged experiencing a security incident in the last 12 months.

From web application attacks to distributed denial-of-service (DDoS) attacks and everything in between, global businesses are dealing with a wide range of potential cybersecurity risks. In addition, respondents are also concerned about the impact that the current threat landscape and geopolitical situation could have on their organizations. While that largely sits outside an organization's control, it impacts them in some shape or form and is a concern.

Security threats are rife, and organizations should be protecting themselves, especially those in the critical sectors, such as oil and gas. Just one successful supply-chain attack can have wide-reaching, catastrophic impacts. Indeed, the high level of incidents underscores the vital need for IIoT/OT security to adequately protect all organizations, in every sector.

This report takes an in-depth look at IIoT/OT security projects, implementation challenges, security incidents, technology investments, and a variety of issues related to cybersecurity risks.

Methodology

Barracuda commissioned independent market researcher Vanson Bourne to conduct a global survey of senior IT managers, senior IT security managers, and project managers responsible for IIoT/OT in their organization. There were 800 survey participants from a broad range of industries, including agriculture, biotechnology, construction, energy, government, healthcare, manufacturing, retail, telecommunications, wholesale, and others. Survey participants were from the U.S., Europe, and Australia. In Europe, respondents were from the United Kingdom, France, Germany, Austria, Switzerland, Belgium, the Netherlands, Luxembourg, Denmark, Finland, Norway, and Sweden. The survey was fielded in April 2022.

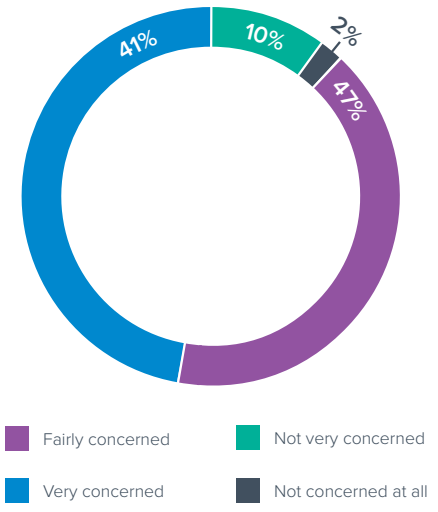
FINDING #1

Most organizations have experienced security incidents

Initially, we asked respondents about their general feelings and concerns about the threat landscape to get an indication of how much awareness this topic gets and to help put the rest of their responses in context.

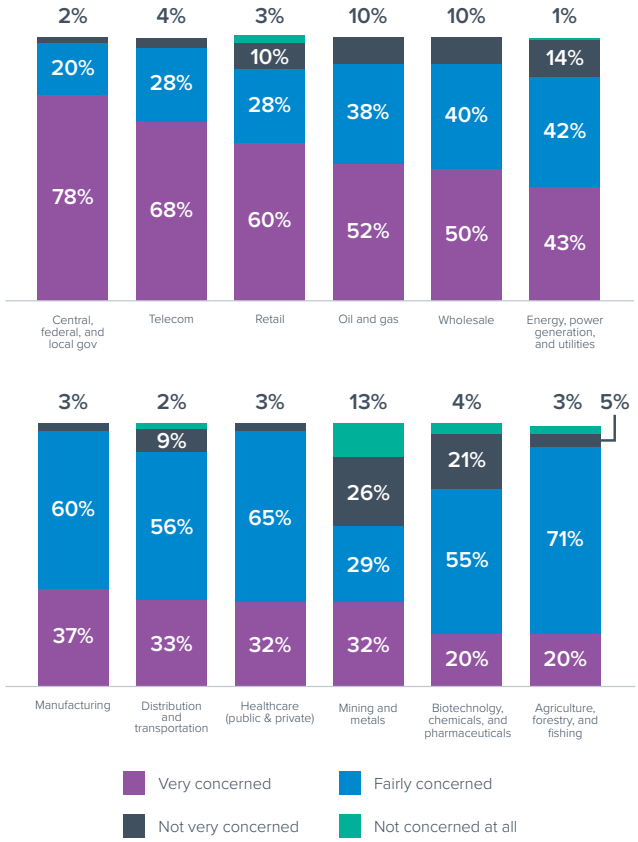
How concerned are you about the current threat landscape and geopolitical situation in terms of the impact it may have on your organization?

(n=800)



Overall, respondents are concerned about the impact that the current threat landscape and geopolitical situation will have on their organizations, with 88% very or fairly concerned. While the current threat landscape and geopolitical situation is something that largely sits outside an organization's control, it impacts them in some shape or form and is a concern for organizations.

Respondents from the U.S. and Australia are most likely to be very concerned, while respondents from France are the least likely to be concerned. The level of concern not only varies by region but also by industry.

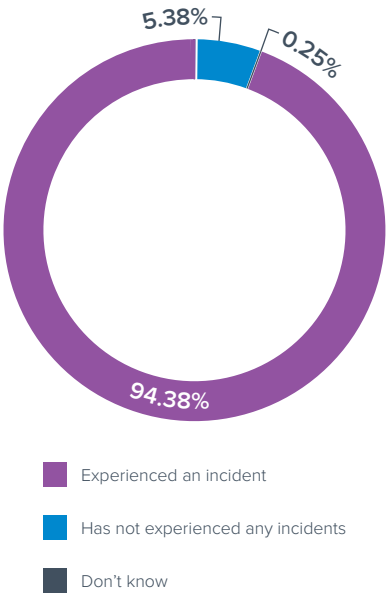


Understandably, concern is more prevalent in sectors likely to feel the effects of the current threat and geopolitical landscape. Government respondents are the most likely to be very concerned. The overall level of concern, when looking at those who are both very and fairly concerned, is also high among other critical sectors, including oil and gas and healthcare. Critical sectors will be on high alert during periods of uncertainty, as any impacts could have wide-reaching implications.

Next, we wanted to better understand the security situation in industrial environments.

Has your organization experienced a security incident in the last 12 months?

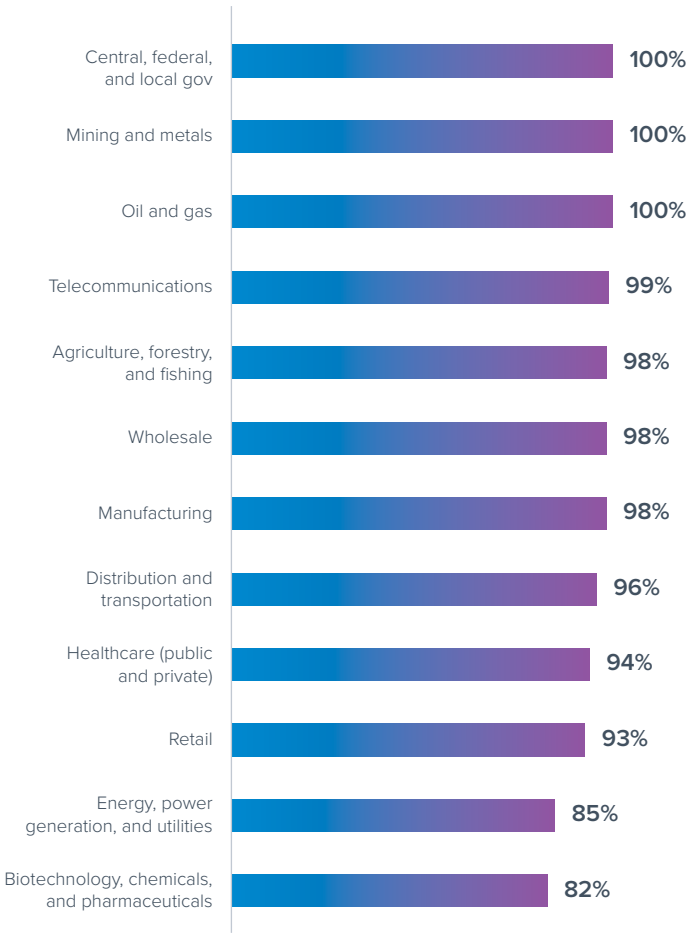
(n=800)



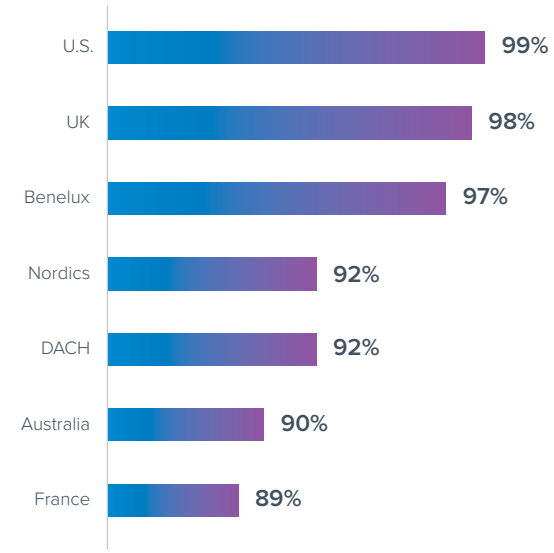
Most organizations (94%) have experienced some sort of security incident in the last 12 months, which is a surprising and alarmingly high number.

Looking at the detailed results by region and industry, this appears to be a general problem.

By industry



By geography

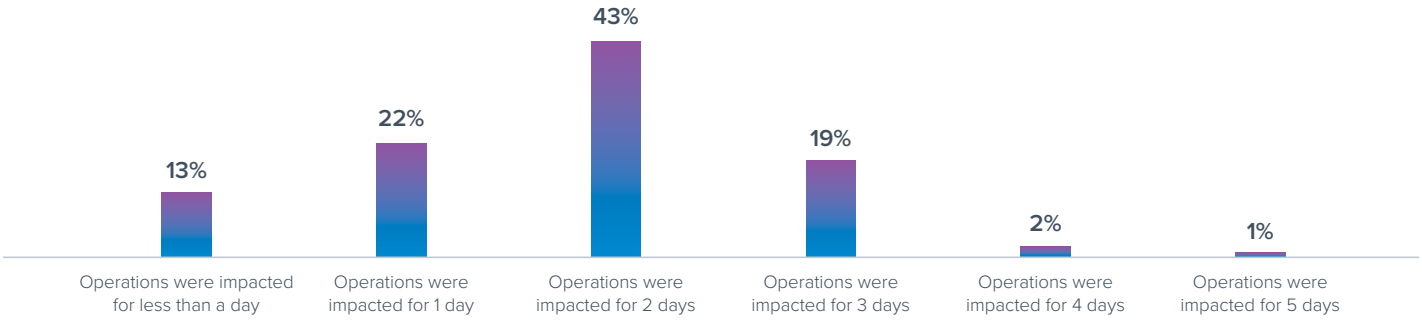


All government, mining and metals, and oil and gas respondents say they've experienced at least one incident. Given the critical nature of some of these sectors, it's essential they bolster security to avoid disastrous impacts.

Because so many organizations have been hit by a security incident, we wanted to know more details, especially about the impact and duration of these incidents.

How long were your organization's operations impacted due to the most significant security incident experienced in the last 12 months?

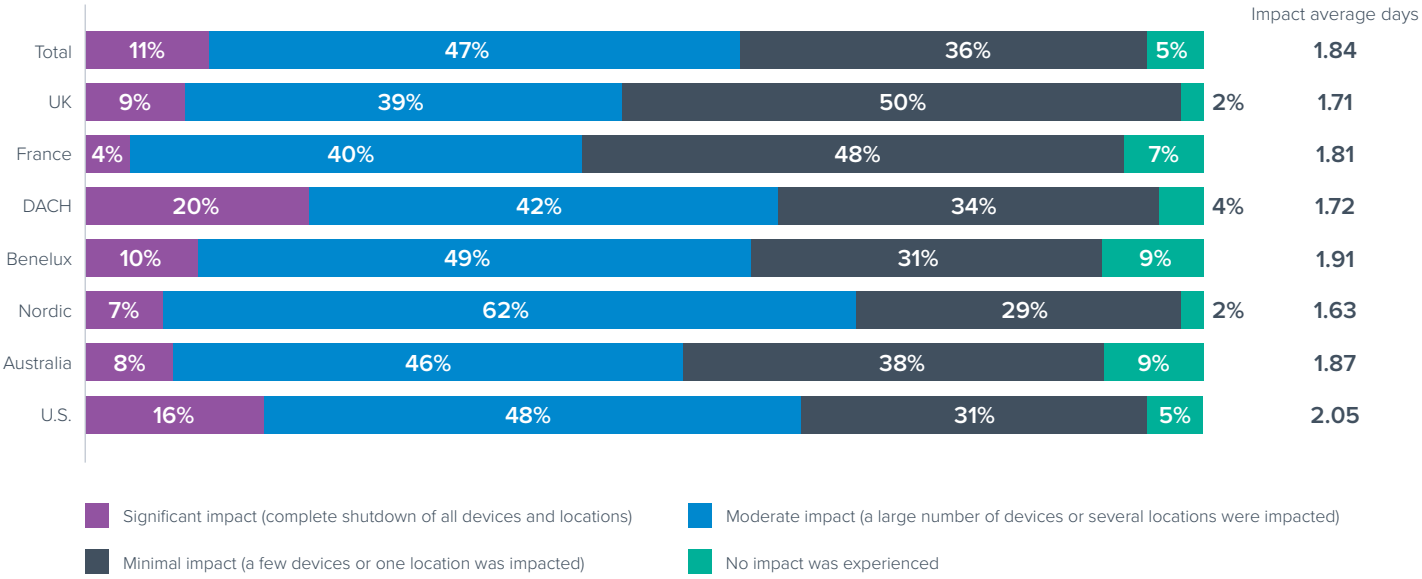
(n=715)



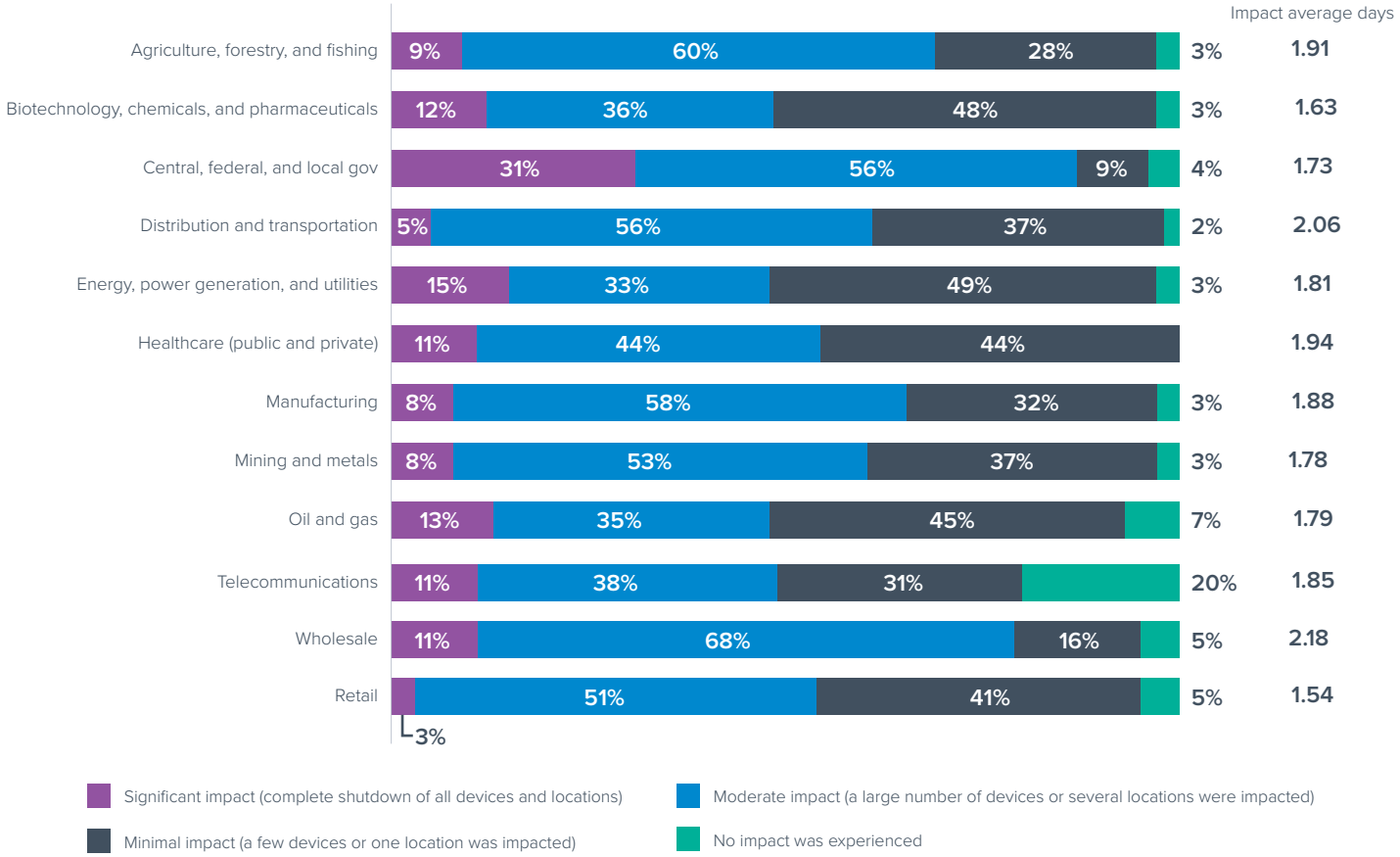
87% of organizations that experienced an incident were impacted between one and five days. On average, it took organizations 1.84 days to resolve the issue. Looking at the provided severity of the impact of those incidents explains why it took so much time to remediate.

Q: What impact did the most significant security incident experienced in the last 12 months have on your organization's operations?

(n=755)



Those in the DACH region (Germany, Austria, and Switzerland) and those in the U.S. were more likely to experience significant impacts from their most significant security incident in the last 12 months. Those in the U.S. were impacted for an average of just over two days. Experiencing a complete shutdown of all devices and locations for this length of time can have catastrophic implications for organizations, and it's a situation that can be avoided by making relatively modest investments in security.



When combining significant and moderate impacts, the scale of these incidents demonstrates how some organizations have been struggling.

While government organizations are still the most likely to have experienced a significant or moderate impact, those in wholesale; and agriculture, forestry, and fishing also have over two-thirds of respondents reporting the same. Given the impacts include a complete shutdown or many devices being impacted, organizations cannot afford to become complacent in this area.

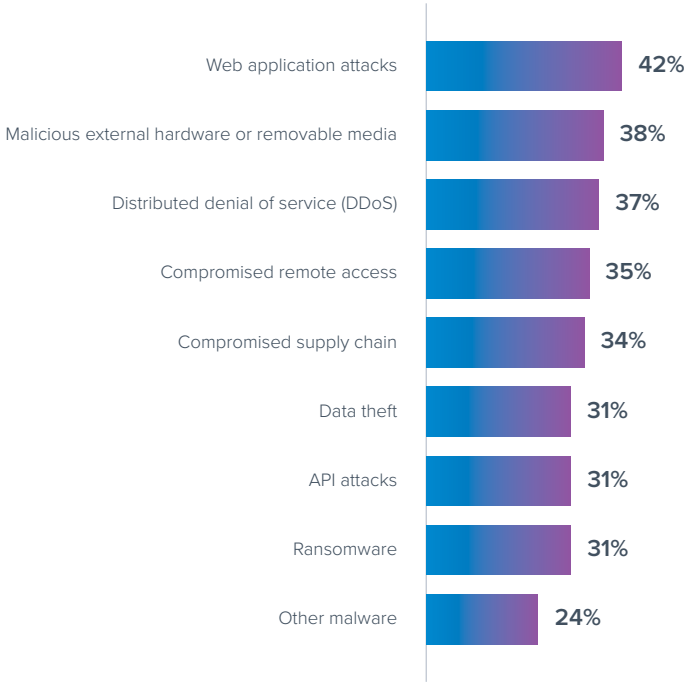
FINDING #2

The most common attack vectors

To get the next level of detail around security incidents that have significantly impacted operations, we asked respondents about the attack types their organization has experienced in the past year.

Which of the following security incidents has your organization experienced in the last 12 months?

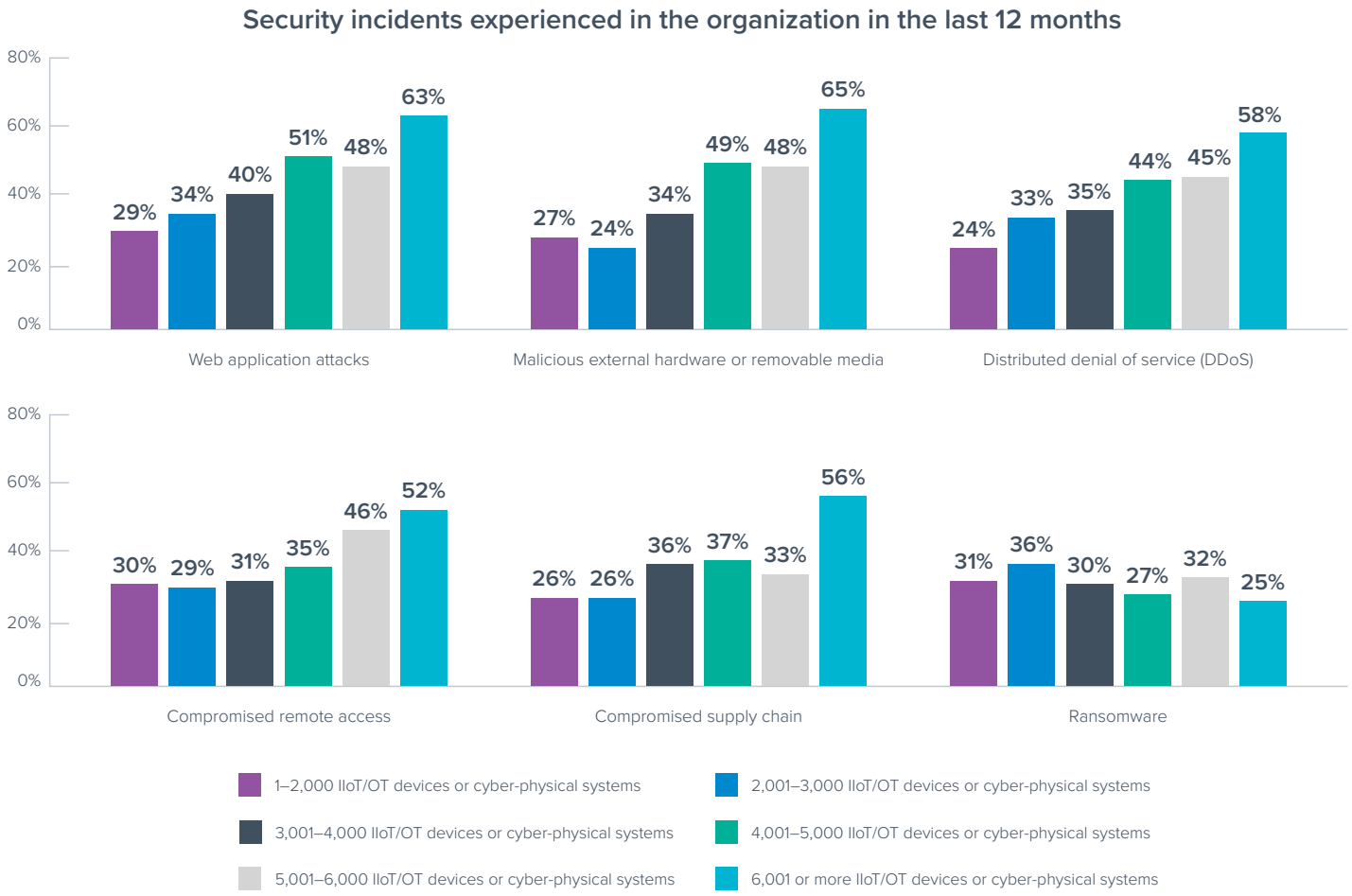
(n=800)



The most common incidents were web application attacks, malicious external hardware or removable media, DDoS, and compromised remote access.

Web applications and APIs are popular attack vectors. In the future, as automation increases, APIs will be a bigger target for attacks. APIs and management interfaces, which are not intended for public access, need robust protection and should never be exposed. The issues with malicious external hardware and removable media, like USB sticks, were ranked surprisingly high. IoT/OT environments require temporary third-party access for maintenance as well as troubleshooting. The high ranking of compromised remote access shows the urgency for getting this fixed.

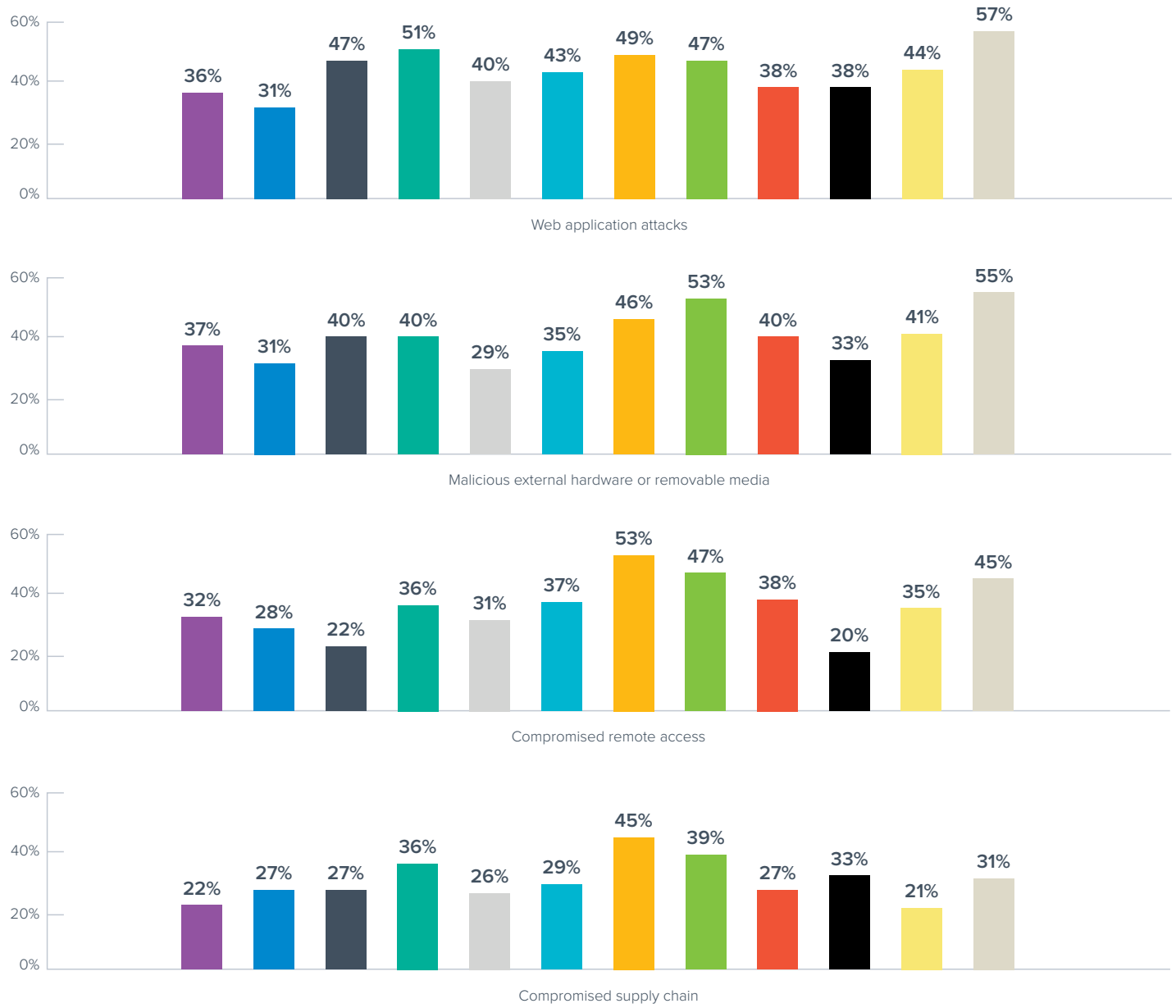
Another finding was that organizations with more devices experience more attacks, especially in the top attack categories. Interestingly, ransomware attacks are more evenly distributed across organizations with differing numbers of devices.



The high level of incidents underscores the vital need for IIoT/OT security to adequately protect all organizations. This is probably why 96% agree their organization needs to invest more in the security of IIoT and OT.

In some critical sectors, organizations experienced fewer incidents. In biotechnology, chemicals, and pharmaceuticals, nearly 20% had no incidents in the last 12 months. In energy, power, and utilities, 15% had no incidents in the last 12 months. Overall, we see significant differences in both probability and attack vector across different industry verticals.

Security incidents experienced in the organization in the last 12 months



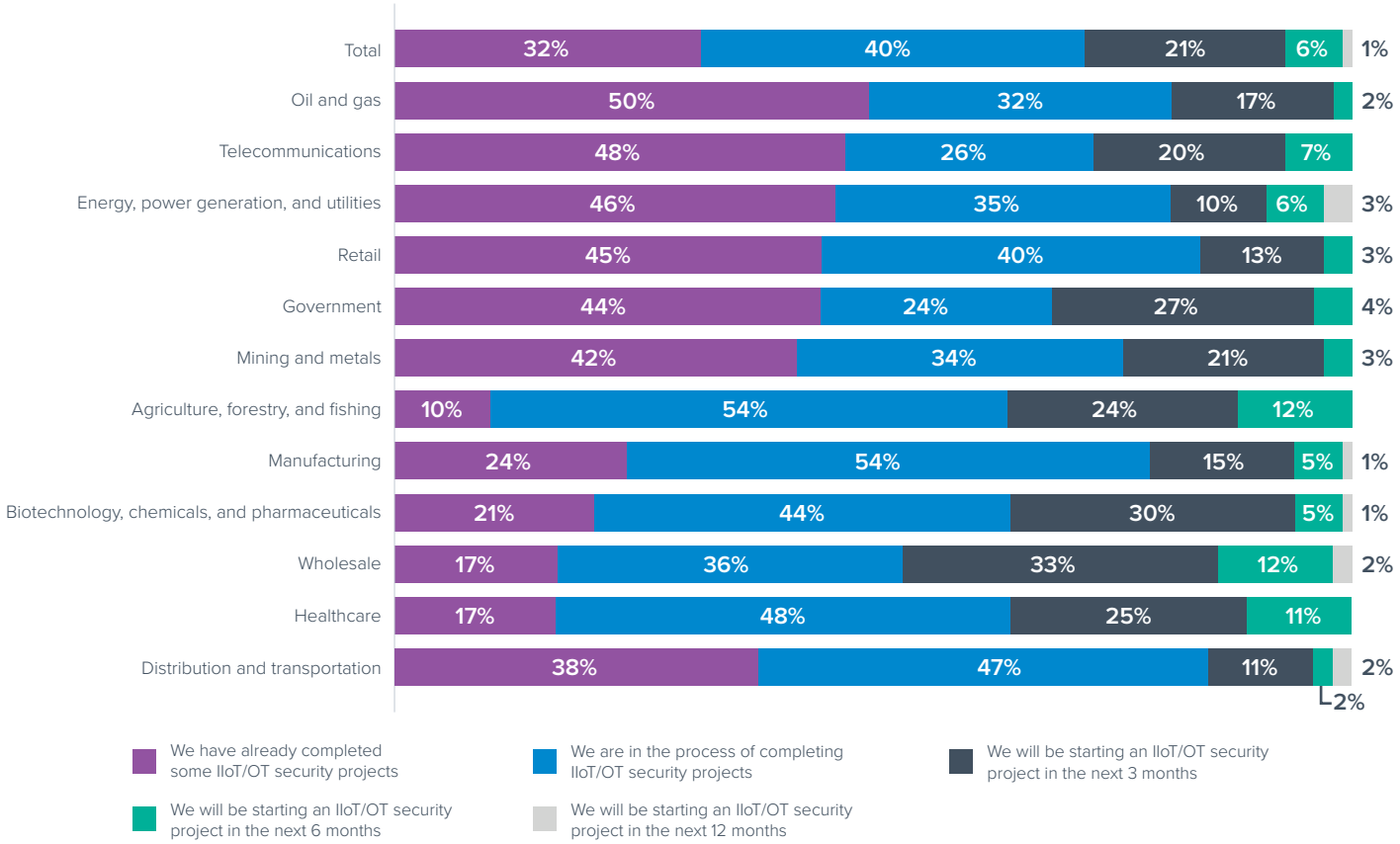
FINDING #3

Organizations are investing in security

To put the rather frightening results of the security incidents and successful attacks into perspective, we asked respondents how far their organization's operational technology and industrial IoT security projects had progressed.

What stage is your organization at when it comes to IIoT/OT security projects?

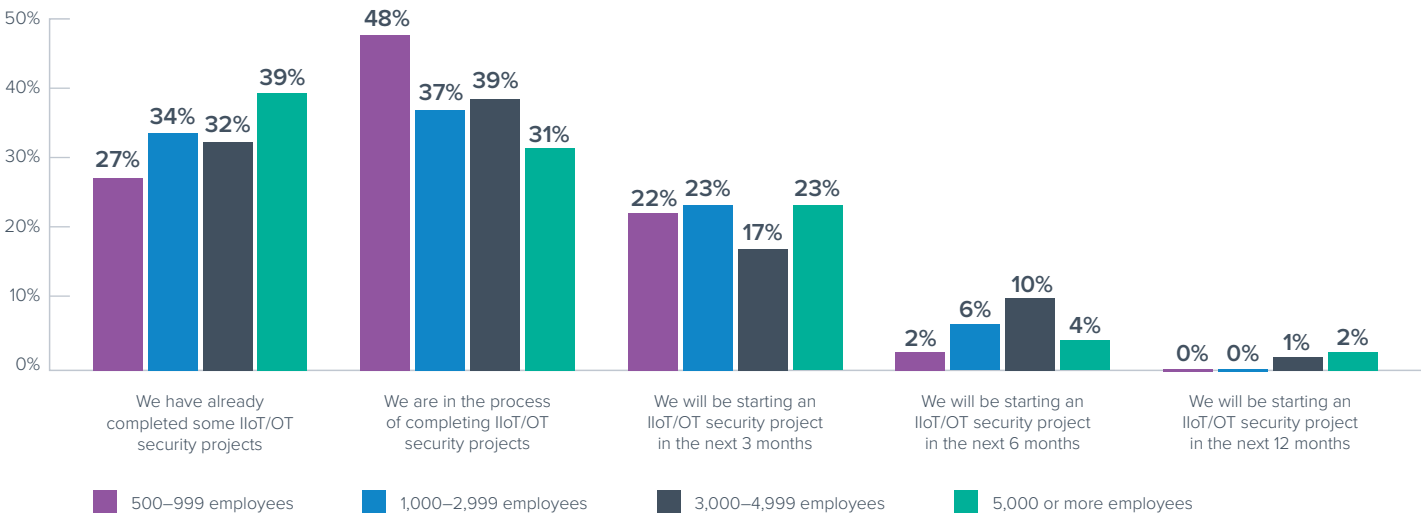
(n=800)



Organizations are facing a multitude of hurdles when it comes to IIoT/OT security projects, leaving their networks and infrastructure open to the risks of security incidents. Many organizations are in their infancy when it comes to IIoT/OT security projects. Overall, while 72% are at least in the process of completing these projects, only just under a third have already done so.

Oil and gas are the furthest ahead when it comes to completing some IIoT/OT security projects. Agriculture, forestry, and fishing are much less likely to have done this. In biotechnology, chemicals, and pharmaceuticals, only a fifth of respondents have completed projects. Manufacturing and healthcare are also among the lowest. Given the impacts if some of their devices are hacked, it should be a larger focus for all sectors.

We thought it would be interesting to analyze the state of IIoT/OT security projects not just by vertical, but also by the size of the organization.

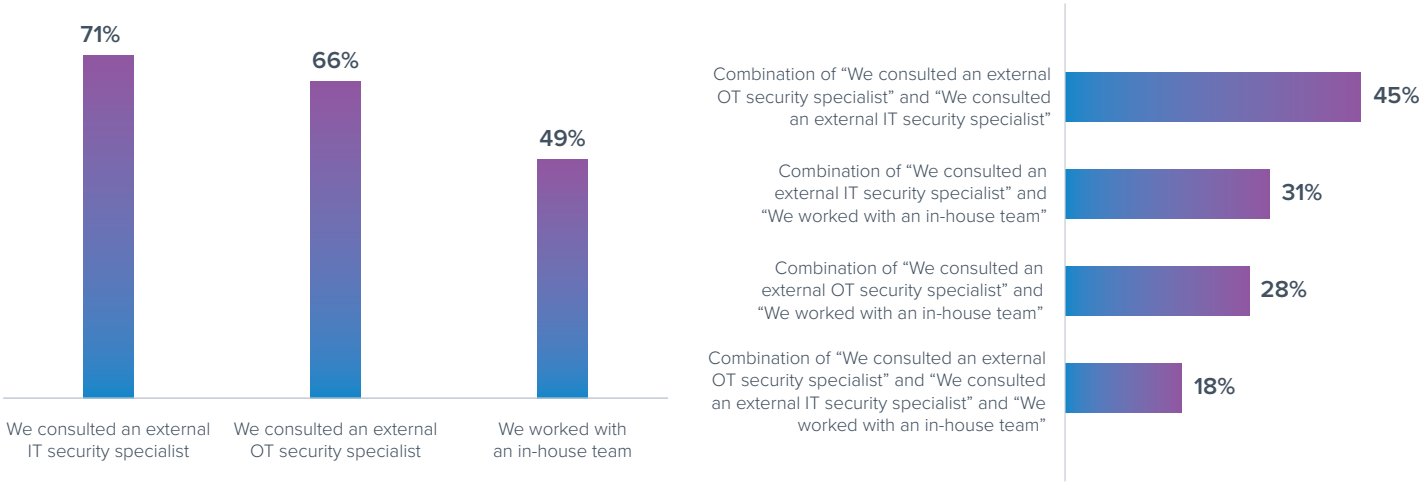


Analyzing the state of IIoT/OT security projects when grouping organizations by the number of employees, apparently enterprises with more than 5,000 employees are more likely to have completed projects already, whereas the majority of small companies are still working on it.

We also wanted to know if organizations implement IIoT/OT security on their own or if they work with external experts on these types of projects.

Did your organization consult an external security specialist when developing its current IIoT/OT strategy?

(n=800)



Organizations are more likely to be looking to both external IT and OT security specialists when developing their current IIoT/OT security strategies, rather than just relying on their in-house teams. The majority sought external help to develop their IIOT/OT security strategies.

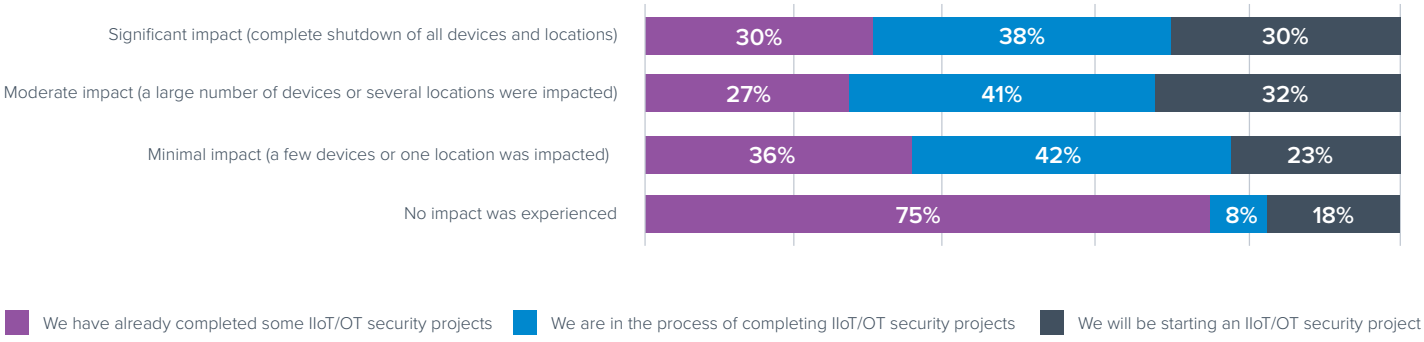
FINDING #4

Security measures do help

Next, we'll be reviewing to what extent industrial security projects mitigate the risks implied by the ever-evolving threat landscape. To highlight the requirement for security, we compared the state of IIoT/OT security projects with the most significant impact experienced after an incident.

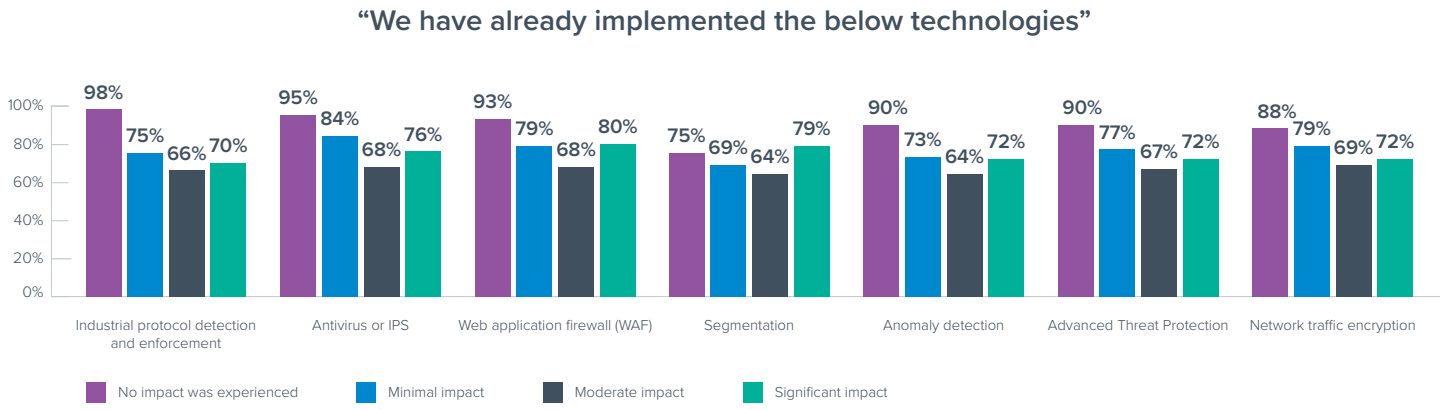
What impact did the most significant security incident experienced in the last 12 months have on your organization's operations?

(n=755)



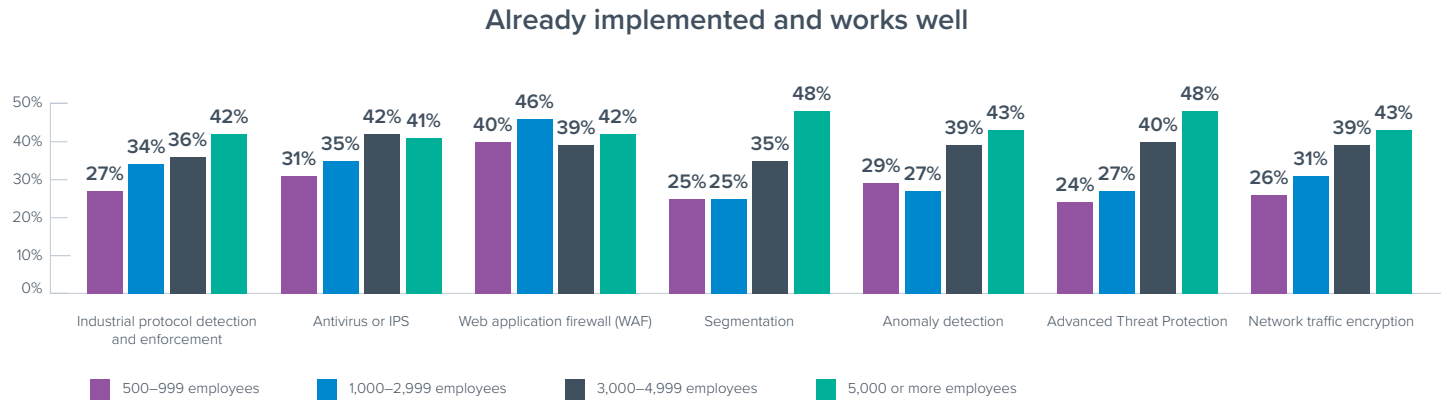
Investments in security are paying off for organizations by reducing the impact of incidents when they happen. Organizations that have already completed some IIoT/OT security projects are more likely to not experience an impact.

There are a variety of different technologies available, though, so we also wanted to know which security measures organizations have implemented and how it improved their IIoT/OT security posture.



All these technologies are valuable in reducing impacts, especially industrial protocol detection and enforcement and anti-virus/IPS.

Overall, out of respondents that already implemented IIoT/OT security and think it works well, enterprise organizations represent the majority, and it seems smaller businesses have made less progress in implementing their security strategy. There is a clearly visible relation between the implementation status of security measures and the size of the organization.

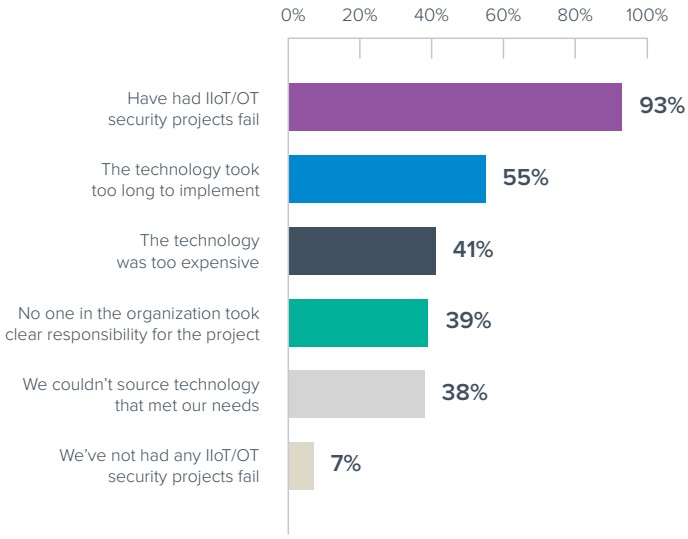


Security and technology adoption is generally higher in enterprise organizations, and the largest organizations are successfully implementing more advanced security technologies.

However, organizations still face a variety of challenges when it comes to implementing IoT security projects, which is perhaps why so many have had projects fail.

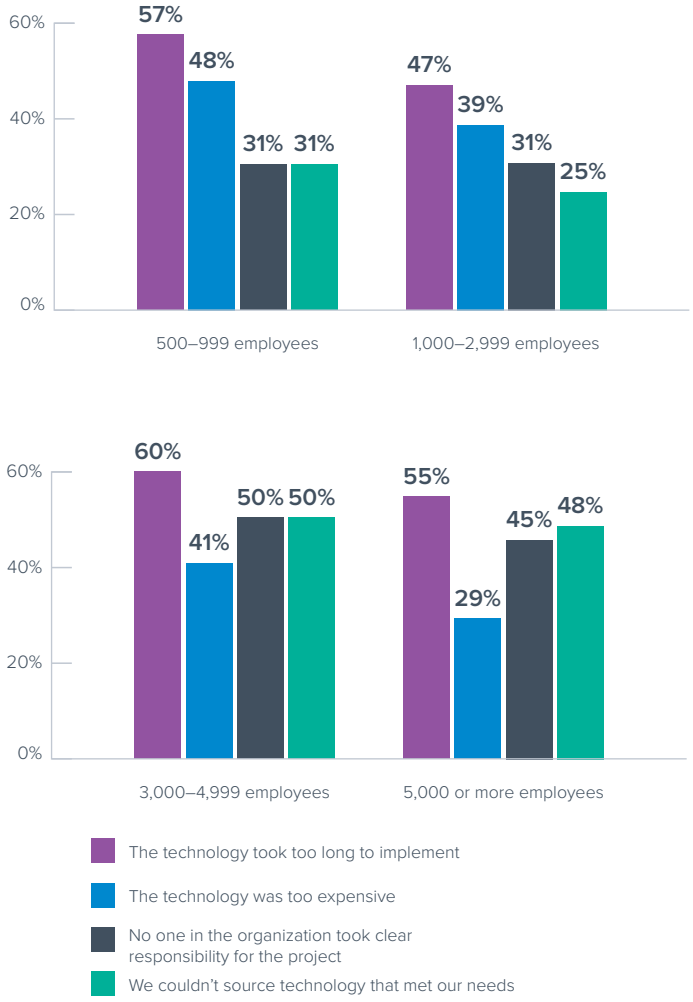
Why, if at all, have any previous IIoT/OT security projects failed within your organization?

(n=755)



93% had a failed project, due to a variety of challenges related to technology and costs. The top challenge, according to more than half of the respondents, was that implementation took too long. Costs have also held back organizations; 41% of those with failed projects said the technology was too expensive. Organizations are in dire need of a streamlined, simple, and cost-effective approach to manage and run their IIoT/OT security projects, to help reduce the risk of impact from security incidents.

Reasons for failed projects vary depending on the size of the organization.

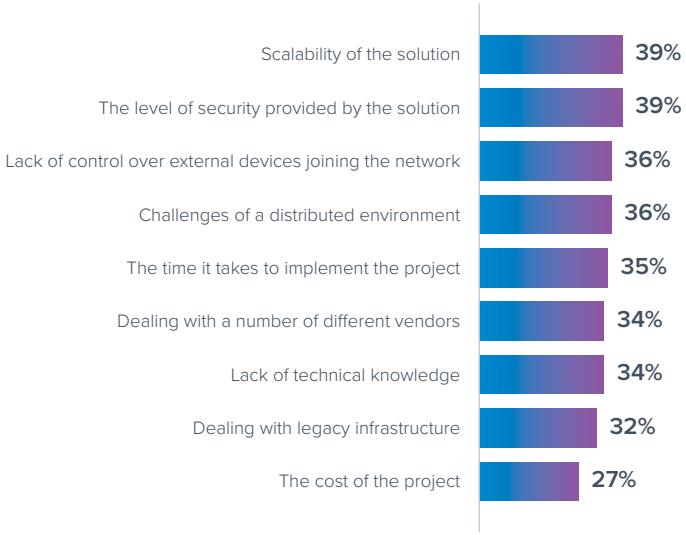


Cost is less of a problem for large organizations. Instead, responsibility and technological requirements are the most common problems for these organizations.

In addition to the challenges they actually faced, organizations have and expect to face a variety of implementation challenges when it comes to IoT security projects.

Which of the following challenges did/do you think your organization would/will face when implementing IIoT/OT security projects?

(n=793)

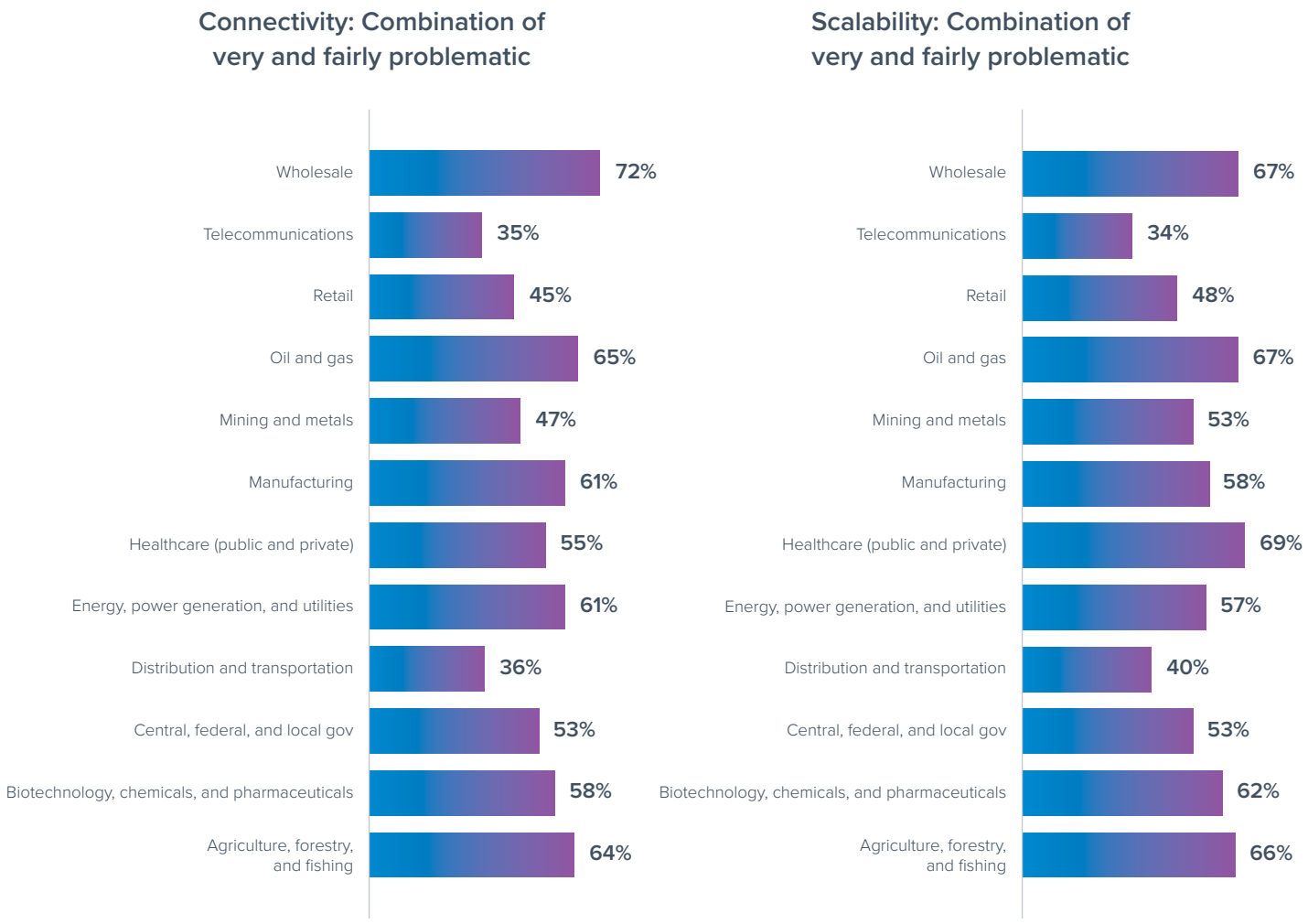


Nearly all respondents say their organization has or expects to face challenges when implementing IIoT/OT security projects, including scalability, security, technical knowledge, and cost.

39% of respondents stated that scalability of the solution is a main concern, so we did a deeper analysis by vertical.

How problematic are the connectivity and scalability of your organization's IIoT/OT networks?

(n=800)



Overall, 58% of respondents say the scalability of their organization's IIoT/OT network is very or fairly problematic. 56% say the same when it comes to connectivity. Some industries, such as healthcare and wholesale, are experiencing more challenges with connectivity and scalability.

FINDING #5

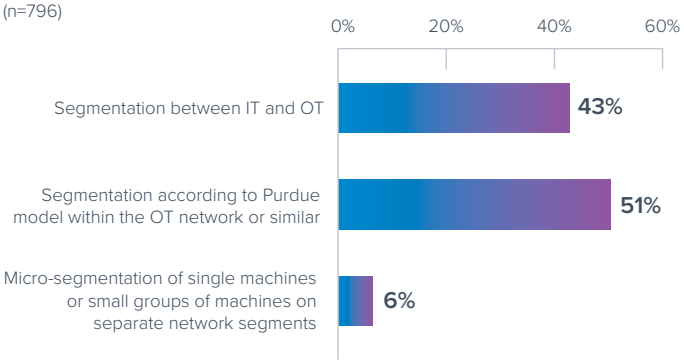
Infrastructure is at risk

When infrastructure is hit by an attack, it is essential to stop lateral movement.

Micro-segmentation is the best practice to mitigate the impact of an incident. That way, potentially vulnerable devices on the network can be isolated from the rest, and only legitimate network traffic is permitted.

How is/will your organization's network be segmented?

(n=796)

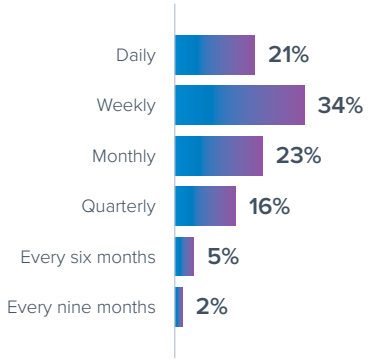


Looking at how organizations segment their networks, only 43% of organizations have implemented segmentation between IT and OT. That basic segmentation is usually the first step, but security should be improved further by introducing additional segmentation on the OT network. That is necessary to combat threats on the local network, such as malicious media devices and compromised remote access. 51% have done that by creating network segments according to the Purdue model — a common reference architecture — or similar means. Only 6% have taken the further step of implementing micro-segmentation, providing the best possible protection by isolating each single device or small groups of devices.

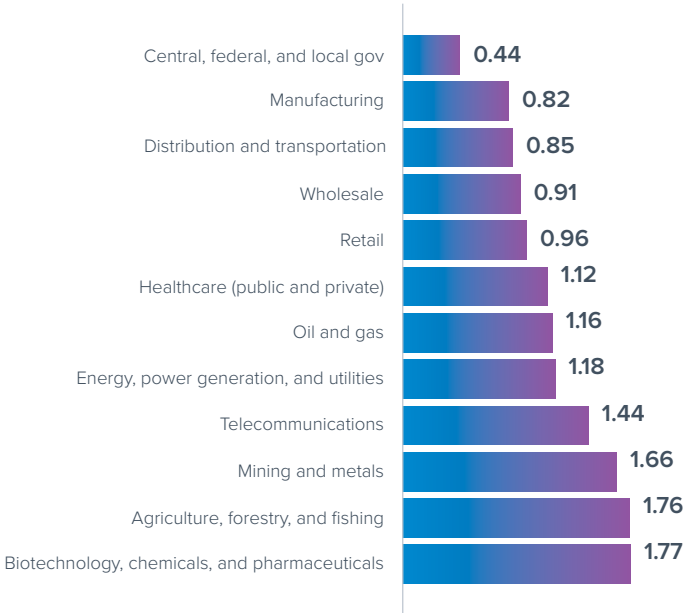
Besides micro-segmentation, one of the most important mechanisms to reduce the attack vector and avoid security incidents in the first place is to keep the infrastructure and devices fully patched and up to date. So, we also inquired about the frequency of updates applied to OT and IIoT devices.

How often are security updates for your organization's IIoT/OT devices applied?

(n=800)



Average number of months security updates are applied



On average, security updates are applied every 1.25 months. Those in government are doing this most often, around twice a month on average. This higher frequency could be explained by the fact that they are one of the most likely sectors to have experienced security incidents in the last 12 months. Nearly one-quarter apply updates monthly. Only 6% apply updates every six to nine months. It appears that in many cases, updates are reactionary after an incident, as opposed to proactively preventing them.

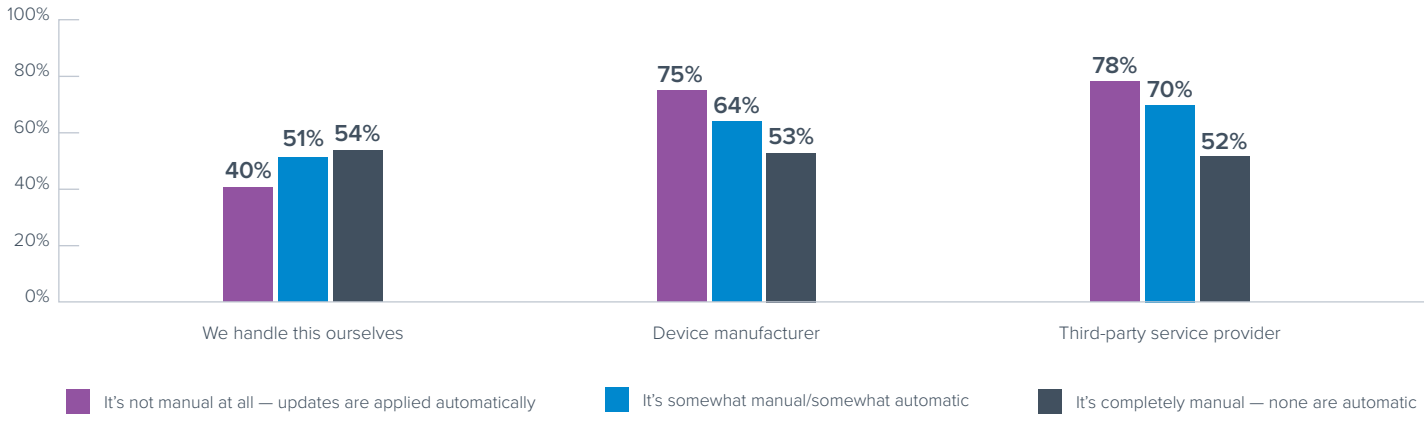
Average number of months organizations apply security updates to IIoT/OT devices

The frequency of these updates varies depending on who applies the update and if the updates are automatic or manual.

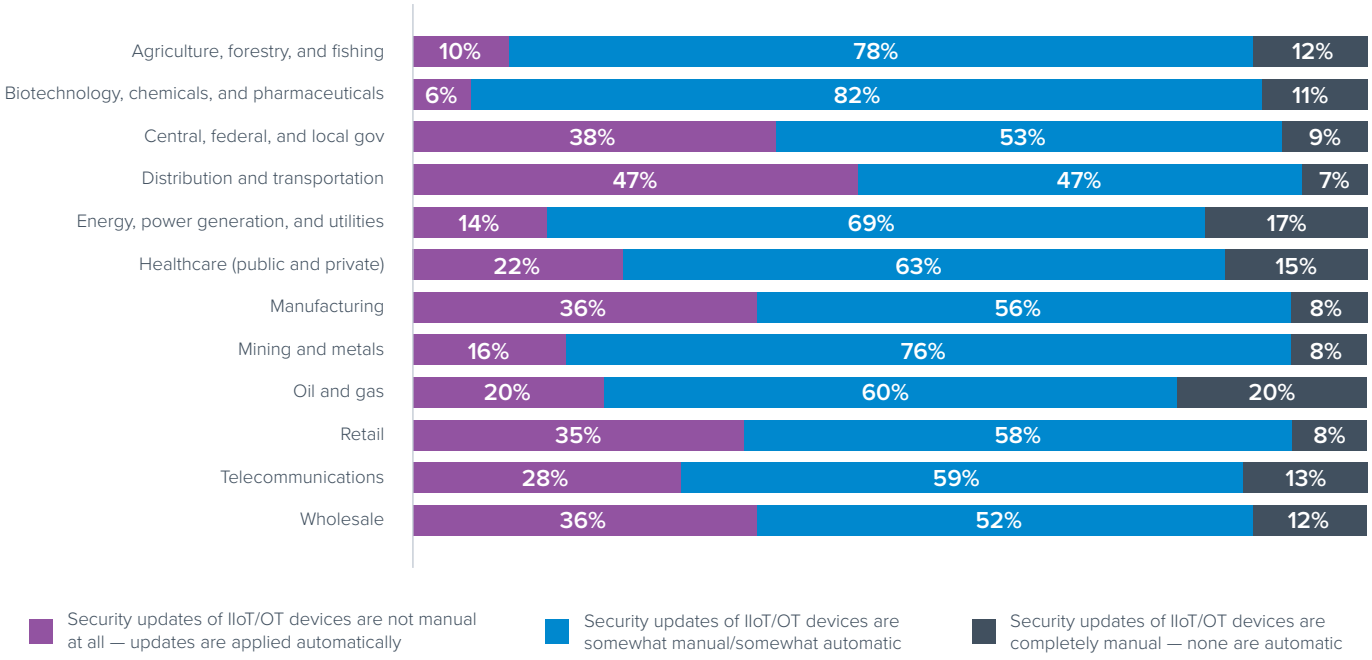
For around two-thirds of respondents, security updates are applied to these devices through a third-party service provider or a device manufacturer. Just less than half of organizations handle updates themselves.

How are the security updates for your organization's IIoT/OT devices applied?

(n=800)



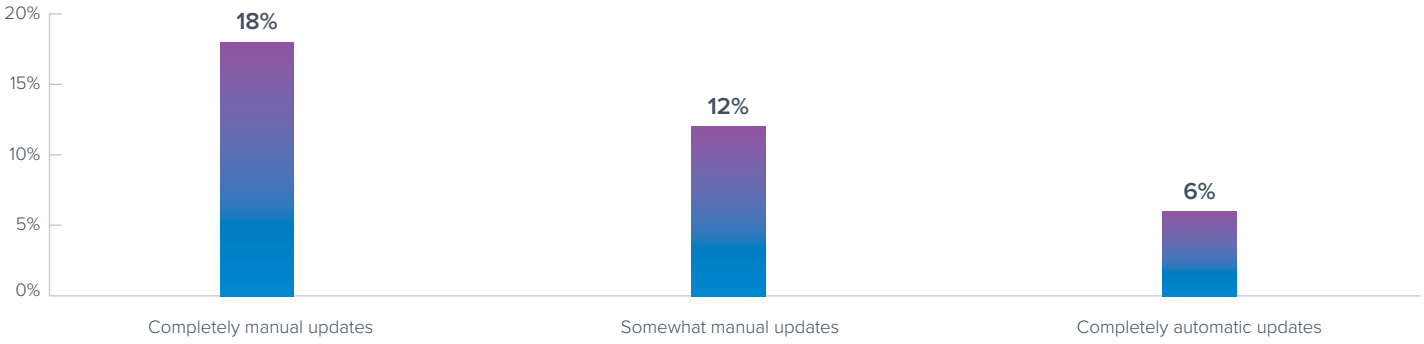
Automation is higher when updates are managed externally, which is one of the primary benefits of doing so. There is demonstrated value in having a third party manage updates, as they tend to be performed automatically. Internally, updates tend to be handled manually.



The level of automation varies across the different verticals. In energy, power, and utilities, 86% of organizations are using a partially manual process, leaving themselves exposed to the risk of breach if not done regularly or correctly.

The degree of update automation clearly has a relation to the severity of incidents, showing that frequent updates help to defend against cyberattacks.

Incidents resulting in complete shutdown



For those applying updates manually, nearly one-fifth said the most significant security incident led to a complete shutdown of all devices and locations. It's clear that the level of automation plays a major part in the impact security incidents have on organizations. Where security updates are applied automatically, just 6% experienced a complete shutdown of all devices and locations following an incident.

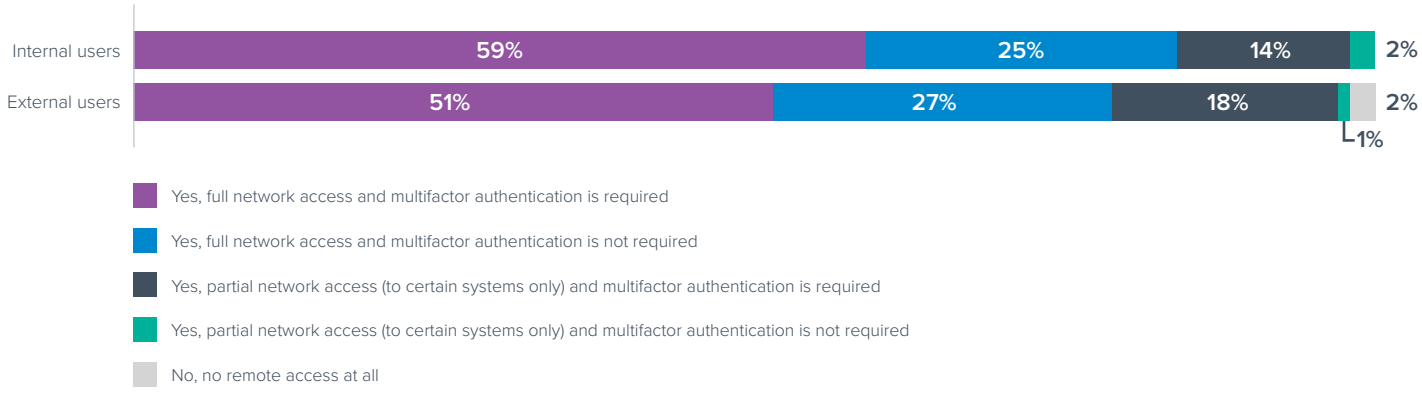
FINDING #6

Remote access security requires immediate attention

Virtually all organizations allow both internal and external users to access OT environments remotely. The frequent usage of remote access mechanisms requires robust security and authentication measures.

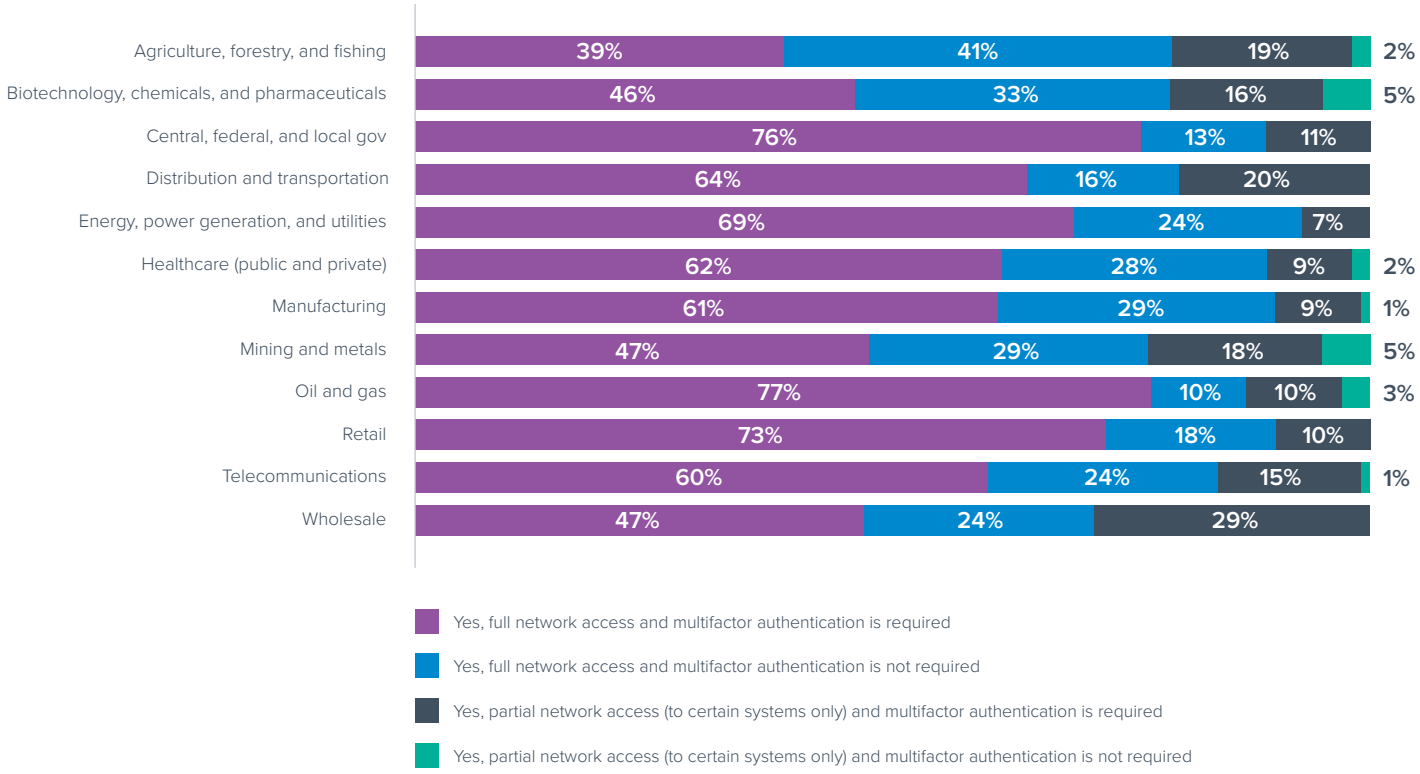
Does your organization allow remote access into OT environments?

(n=800)



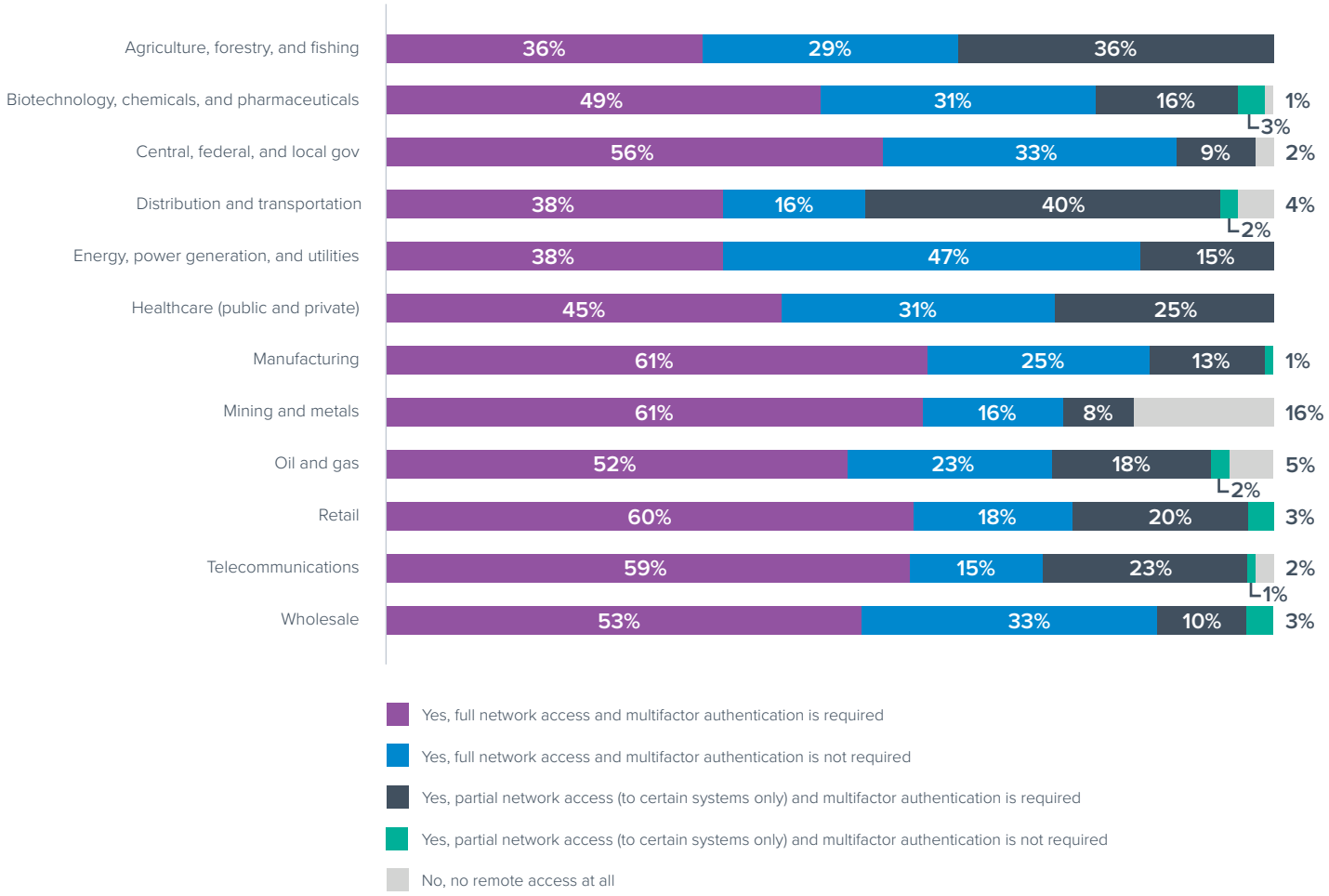
The majority allow full network access, but around a quarter of this group report that multifactor authentication (MFA) is not required. Only 18% of companies restrict network access and enforce MFA when it comes to remote access into OT networks. Given the sensitive nature of these environments, organizations should be taking every precaution necessary to keep them as secure as possible.

Remote access for internal users



Across the different sectors, most internal users have full network access, but MFA is not as widespread. In biotechnology, chemicals, and pharmaceuticals, for example, a third of respondents said internal users can access OT environments remotely without using MFA. This might be because they are further behind on their IIoT/OT projects. This is an area that these organizations need to be aware of, given the implications if their devices are compromised.

Remote access for external users



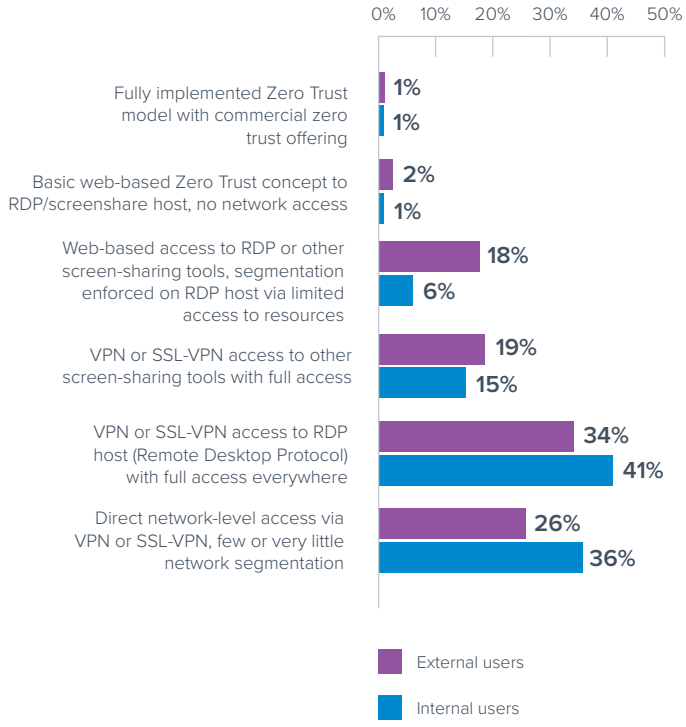
Similarly, the majority allow external users full network access to OT environments. The use of MFA to do this is widespread, but it is severely lacking for some sectors. Energy, power generation, and utilities is the most likely sector to allow full network access without the requirement of MFA.

This situation should never exist in critical sectors and should be addressed immediately. As we saw with the attack on Colonial Pipeline, just one successful remote access attack can have wide-reaching, catastrophic impacts.

The market offers a variety of different remote access mechanisms, from simple traditional VPN to highly secure Zero Trust solutions.

Which of the following tools is your organization using for remote access?

(n=800)



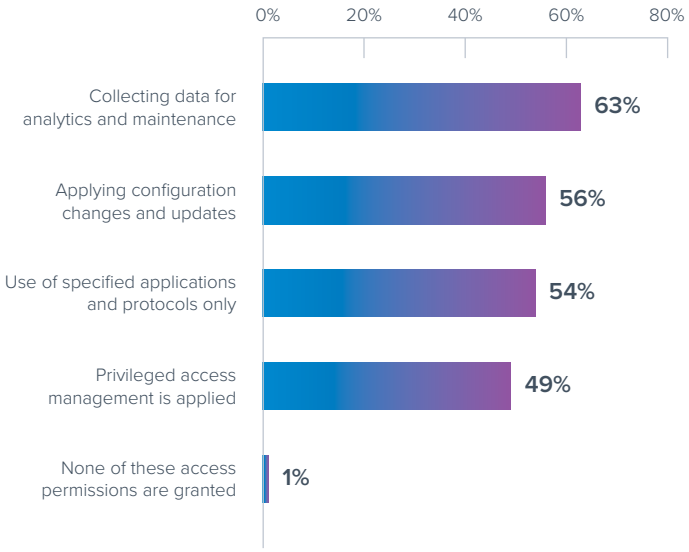
Zero Trust Network Access (ZTNA) is the most secure way to provide remote access, including granular permissions based on user id, device id and type, health state, and geographic location. It's not one-time access; it's continuously applied, and permissions are continually verified. With only 1% of respondents using ZTNA for either internal or external users, it's clearly in its infancy in the OT space. This represents an easy opportunity for the industry to improve their security posture quickly when it comes to remote access.

The majority of organizations provide direct network-level access without further security. All network traffic from remote connections should run through detailed security inspection and be limited to specific target systems only. In particular, the use of screen-sharing tools and remote desktop connections are often inadvertently bypassing existing security measures in many cases. Given that compromised remote access is a common problem, addressing these weaknesses could increase the level of protection significantly.

In addition to who can access the network, organizations also need to consider what users are allowed to do on the network. Access rights and security policies for single users or user groups need to be defined.

In your organization, which of the following access permissions are granted via remote access for internal and external users?

(n=800)



There are a range of access permissions granted via remote access for both internal and external users: collecting data for analytics and maintenance (63%); applying configuration changes and updates (56%); use of specified applications and protocols (54%); privileged access management is applied (49%). Just 1% say none of these access permissions are granted. If access to an organization's OT environment fell into the wrong hands, especially in a critical sector, the impacts could be detrimental.

Worryingly, over half (57%) of respondents report that external users who have full network access are able to apply configuration changes and updates, a very high-risk situation for a breach.

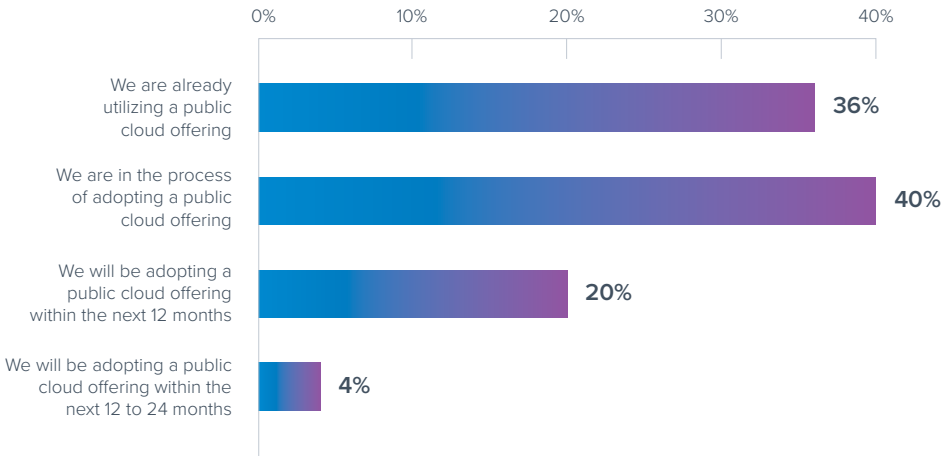
FINDING #7

Digital transformation drives new technology

The adoption of the public cloud, software-as-a-service (SaaS), and secure access service edge (SASE) is changing the way corporations operate and the network architecture they require. We wanted to know where businesses are on this journey to digitalization.

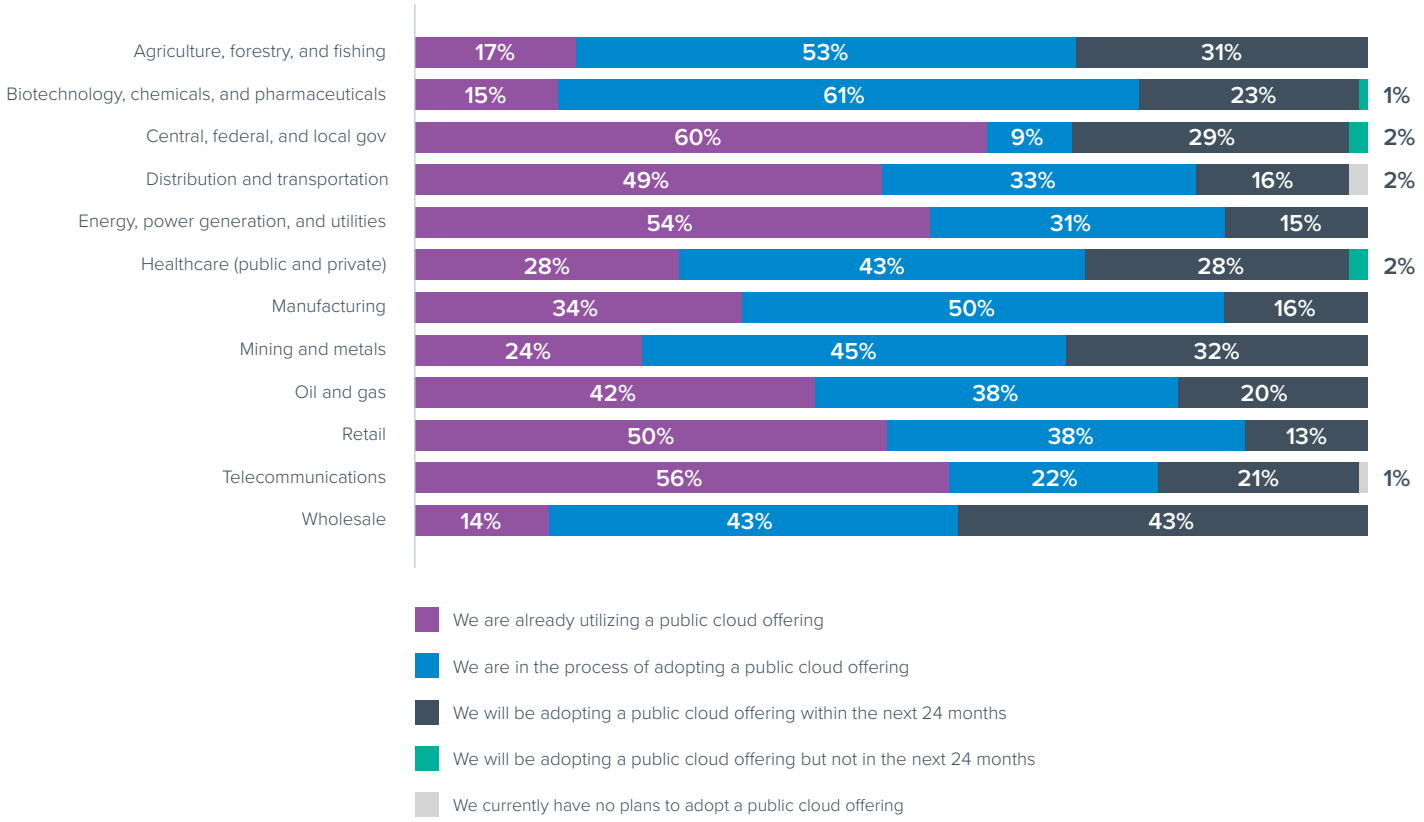
Does your organization plan to utilize a public cloud offering for digital transformation?

(n=800)



Virtually all organizations have committed to the adoption of public cloud. 96% are already using public cloud, are in the process of adopting a public cloud offering, or have plans to do so in the next 12 months. However, the level of adoption shows significant differences between industries.

Public cloud adoption by industry

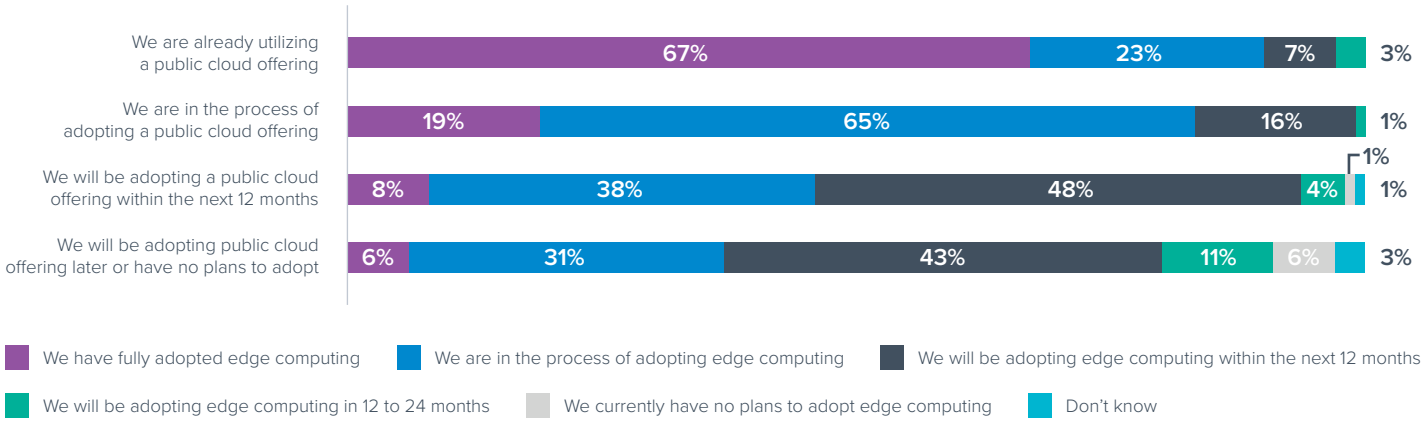


The adoption of public cloud is widespread in some industries but still being worked on in others. Interestingly, in the government sector, where the use of IIoT tends to be for managing critical infrastructure, the use of public cloud is very high at 60%. On the other end of the spectrum are the healthcare; mining and metals; agriculture, forestry, and fishing; biotechnology, chemicals, and pharmaceuticals; and wholesale verticals, all with an adoption rate below 30%.

Public cloud is not a security risk. In general, companies using public cloud seem to be more willing to adopt technology and invest in security. The same group is also seen adopting edge computing more often, and public cloud appears to be a driver for that technology. So, we wanted to know if this is in fact the case.

To what extent has your organization adopted edge computing?

(n=800)



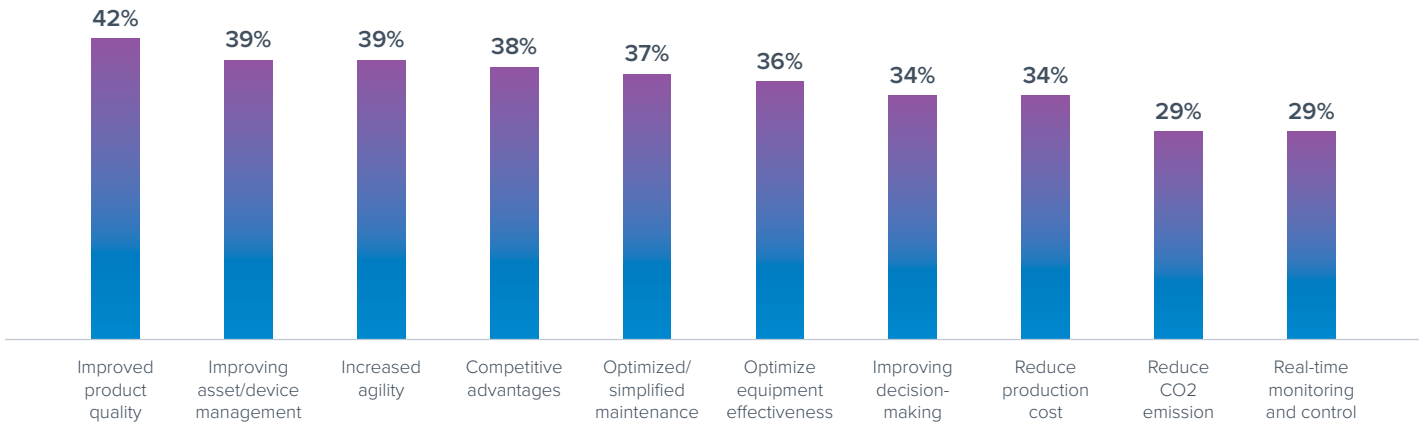
Edge computing is considered an important part of an organization's setup by the vast majority of respondents and will likely continue to gain in popularity in the future.

Over two-fifths of respondents say their organization is in the process of adopting edge computing. About one-third say edge computing has been fully adopted. About one-quarter say their organization will be adopting edge computing within the next 12 to 24 months. Based on the data, it's clear edge computing helps businesses take advantage of public cloud, with adoption among those who are already utilizing a public cloud offering reaching 67%.

Looking at the popular IoT edge platforms, Google IoT Edge, AWS Greengrass, and Azure IoT Edge are the most likely edge computing tools being considered, according to respondents.

Which of the following benefits has/do you think your organization would gain by adopting always connected IIoT?

(n=800)



When asked about the importance of digitalization in general, there is overwhelming agreement from respondents when it comes to three items:

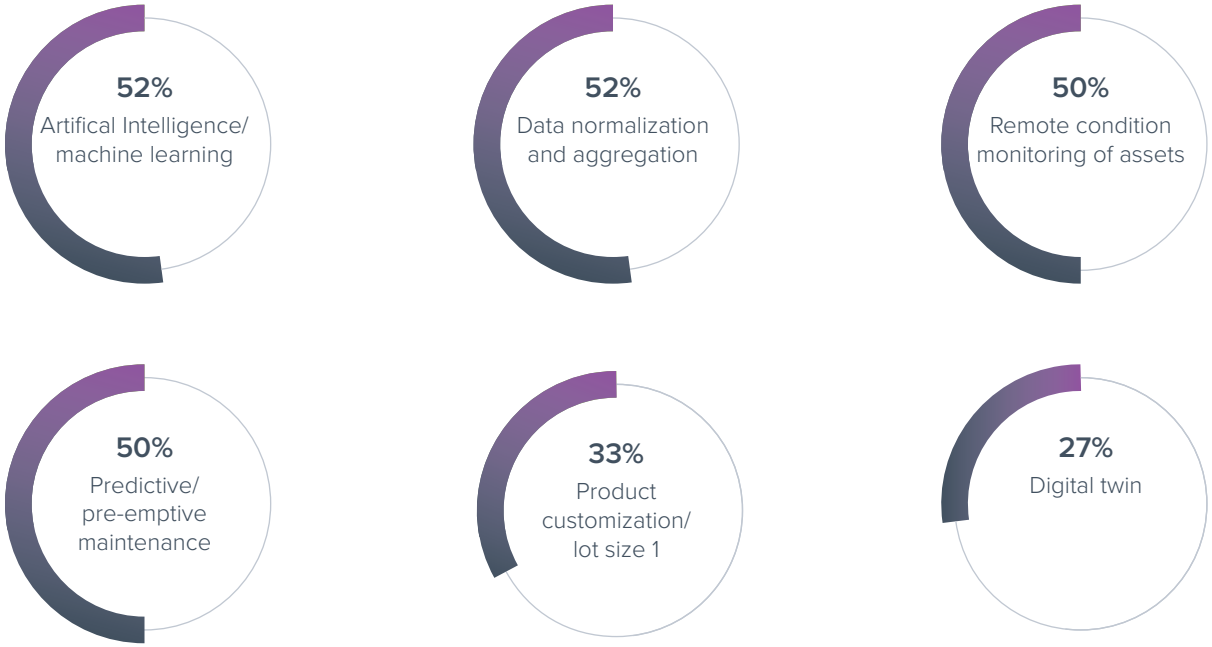
- Always connected IIoT/OT is viewed as competitive assets for organizations
- Edge computing is considered an important part of an organization's setup
- Organizations need to invest more in the security of IIoT and OT

In more detail, improving product quality, asset/device management, and agility were cited as top benefits of always connected IIoT.

Our final question in this survey was about the most important use cases for future digitalization projects.

Which of the following would your organization consider when digitally transforming your organization?

(n=800)



Looking forward to the adoption of additional technologies, organizations are considering a number of solutions and strategies, including the use of AI/ML and better data management.

Conclusion

In today's uncertain geopolitical environment, people and organizations are highly concerned with potential cyberattacks. The most concerning are possible attacks on critical infrastructure and industrial assets. Unfortunately, IIoT/OT security currently requires a lot of improvement.

This report shows nearly all — 94% — of organizations have experienced at least one security incident, which likely impacted their industrial IoT infrastructure. These incidents had significant impact on organizations, with 87% of them reporting their operations were impacted for one day or more. The incidents involved a wide range of attacks, with web application, malicious external hardware/removable media, and distributed denial of service attacks being the most frequent.

The good news is the majority of organizations are already implementing or planning IIoT/OT security projects. Even better news is organizations that didn't experience an impact are more likely to have already completed some IIoT/OT security projects, so these projects seem to be effective. There are many challenges, however, in successfully implementing IIoT/OT security, including long implementation times and high costs. In fact, 93% of organizations had a failed project on their journey to IIoT/OT security.

Some of the areas that require attention are the lack of network segmentation, reactive rather than proactive security updates, and insufficient automation. One area that requires urgent attention is remote access security. While most organizations allow both internal and external users access to their OT environments, roughly a quarter are not requiring multifactor authentication, leaving organizations wide open to attacks.

Fortunately, effective solutions to IIoT security challenges are available, including secure endpoint connectivity devices and ruggedized network firewalls, all centrally deployed and managed via a secure cloud service. These solutions can enable effective network segmentation and advanced threat protection, provide multifactor authentication, and even implement Zero Trust Access. In addition, web application firewall services can be deployed to protect the infrastructure from web application and DDoS attacks.

Nearly all — 94% — of organizations have experienced at least one security incident, which likely impacted their industrial IoT infrastructure. These incidents had significant impact on organizations, with 87% of them reporting their operations were impacted for one day or more.

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-first, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level.

Get more information at barracuda.com.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and Their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit vansonbourne.com.

Barracuda
Your journey, secured.