


Shielding the Future: Europe's Cyber Threat Landscape



Content

3	Executive summary
4	Introduction
5	Cybersecurity risks are rising
11	Wide-ranging impact of cybersecurity incidents
13	Organizations recognize the cybersecurity risks and are investing
15	A mixed picture of solution deployment
20	Executive unfamiliarity is a barrier to Zero Trust adoption
21	Cybersecurity incident response
22	Data compliance: an increasing challenge
23	Hybrid working continues to challenge cybersecurity infrastructure
24	Summary and recommendations



Executive summary

It's no great surprise that cybersecurity threats are rising. Our survey of more than 4,000 security professionals across multiple industries in Europe validates what most of us have experienced: organizations in many fields continue to be targeted by frequent attacks. Chief Information Security Officers (CISOs) and their teams know that more attacks are coming. But a shockingly small percentage of organizations say they are prepared for what lies ahead.

No one is immune to cyberattacks. In our survey, 72% of respondents reported experiencing at least one incident in the last 24 months. Though technology, transportation, and energy companies were the most frequently targeted, organizations in education, gambling, healthcare, and other fields were not far behind. Medium-sized organizations were only slightly more vulnerable than those of other sizes.

As our survey shows, the frequency of attacks is increasing. Among organizations that were attacked in the past year, 84% reported more incidents compared to past years. In fact, 43% of those organizations had experienced an astounding 10 or more attacks in just 12 months.

While attackers are using a variety of methods, phishing and web attacks top the list. Once attackers have access to enterprise networks, they mostly try to steal money or plant spyware.

The financial impact of these attacks has been substantial. Nearly two-thirds (63%) of organizations that have experienced a cybersecurity incident in the past year have lost at least €940,000. A quarter of those attacked lost €1.88 million or more.

Most respondents anticipate more attacks within the next year. But very few feel ready. Remarkably, only 29% of respondents say they are well prepared for future incidents. Respondents from small organizations are least confident in their readiness, though not many more security professionals from medium-sized and large organizations feel better prepared.

The good news? Many leaders are committed to addressing this preparedness gap. Over half of respondents (54%) anticipate that their organization will dedicate more of their IT budget to cybersecurity in the next year. Securing a hybrid workforce will be the focus for many teams.

Organizations will use their IT budget to deploy a wide range of solutions. At the same time, respondents realize that simply adding numerous point solutions is not the answer. Nearly half (48%) ranked simplifying and consolidating their cybersecurity stack as one of their top three priorities. Moving toward Zero Trust security could help — but 86% of respondents reported that their leadership do not yet fully understand this model.

How should your organization prepare for future attacks? Our survey identifies key threat trends, highlights areas of investment, and pinpoints persistent obstacles. This report combines these insights with specific recommendations for change, helping you optimize your strategy for addressing an increasingly challenging threat landscape.

Introduction

This report is based on the findings of a survey conducted in March 2024 of 4,261 leaders responsible for cybersecurity in their organizations. We spoke to a wide range of relevant people, including those in cybersecurity leadership roles, roles running the day-to-day operations of security teams, technical roles, and executive roles.

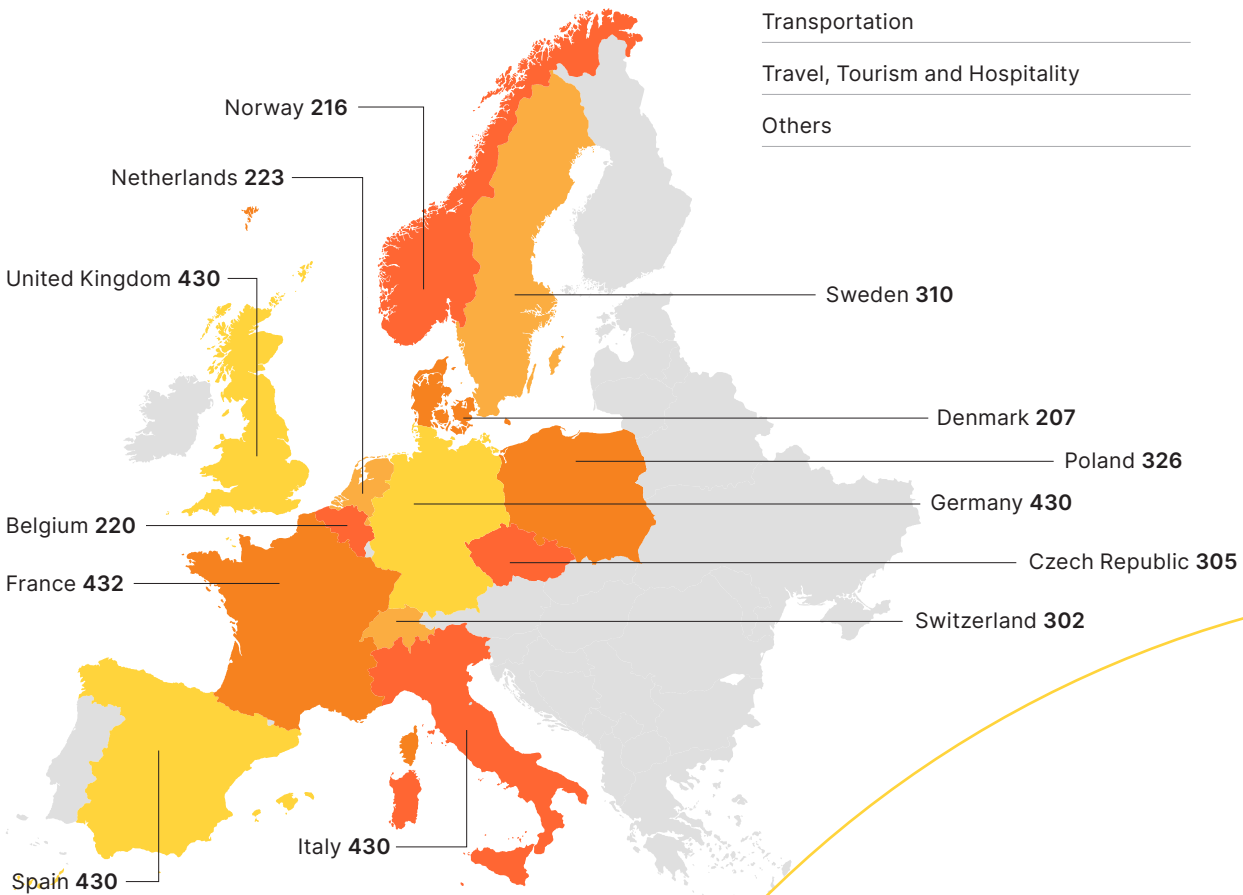
The research was conducted in 13 European countries: Belgium, Czech Republic, Denmark, France, Germany, Italy, Netherlands, Norway, Poland, Spain, Sweden, Switzerland, and the United Kingdom.

Respondents were drawn from organizations of diverse sizes, with 24% from small enterprises (150-999 employees), another 24% from medium-sized enterprises (1,000-2,499 employees), and the remainder (52%) from large organizations (more than 2,500 employees).

The participants span a range of sectors

Industry	Number of respondents
Business and Professional Services	347
Construction and Real Estate	233
Education	182
Energy, Utilities and Natural Resources	122
Financial Services	527
Gaming (gambling, e-sports, game developers etc.)	36
Government	237
Healthcare	274
IT and Technology	942
Manufacturing	449
Media and Telecoms	95
Retail	258
Transportation	230
Travel, Tourism and Hospitality	174
Others	155

Distribution of respondents



Cybersecurity risks are rising

Incidents impact organizations far and wide

Cybersecurity incidents have increased significantly in recent years in terms of frequency, severity, and complexity to manage. Nearly three-quarters (72%) of all respondents said their organization had experienced an incident in the past 24 months, and nearly four in 10 (40%) have suffered an incident in the last year.

Medium-sized organizations are revealed to be the most vulnerable, with 42% having experienced an incident in the past year. Smaller organizations were less likely to have been affected, with just over a third (34%) experiencing an incident in the past year.

Taking a market perspective, respondent organizations in the UK (48%), Spain (47%), and Sweden (47%) have been most affected by incidents, while Belgium

(22%) and Italy (25%) were least affected. In terms of industries, gambling and esports emerged as those least impacted, which is surprising given the high volumes of money at stake in both.

Meanwhile, energy, utilities and natural resources (43%), and financial services (37%) are commonly targeted. The lower frequency of incidents in healthcare is counterintuitive — the industry tends to be a highly targeted sector because it often suffers from a lack of investment¹ and because systems hold vast amounts of sensitive and potentially valuable patient data. IT and technology is the most affected sector.

1. [The elephant in the room: cybersecurity in healthcare](#), Anthony James Cartwright, 2023

% of respondents reporting cybersecurity incidents in the past 12 months

Most affected countries



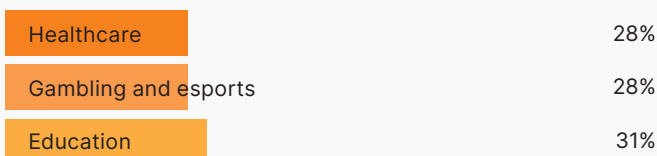
Least affected countries



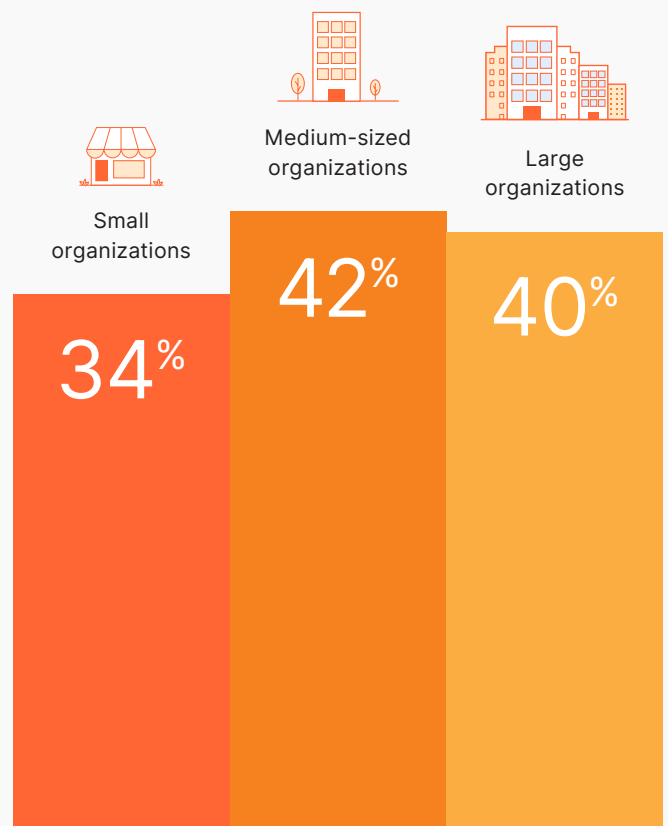
Most affected industries



Least affected industries



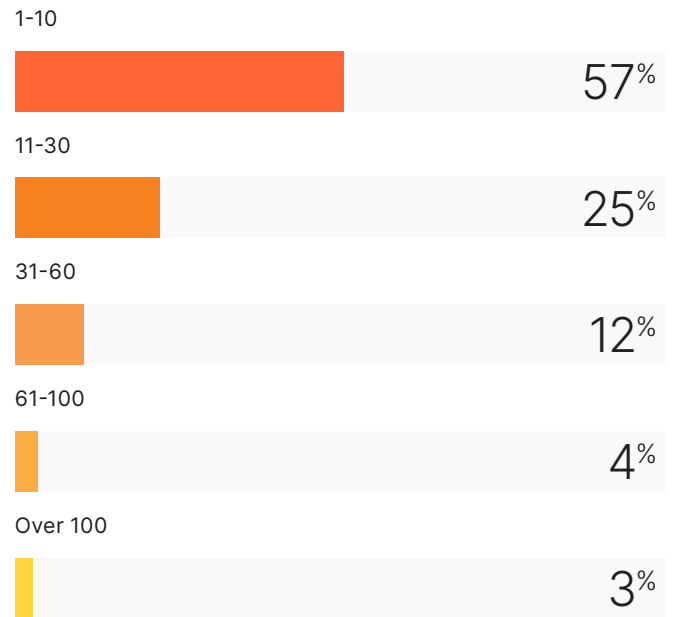
By organization size



Organizations that suffer one incident often find that these are not isolated cases. Among the respondents who reported that their organization had experienced an incident in the last 12 months, 43% experienced 10 or more. In fact, a quarter of this group reported between 11 and 30 incidents, while a further 16% experienced between 31 and 60 — a rate of one incident every six to 11 days.

For many organizations, cybersecurity incidents are a constant threat. Of those that have suffered an incident in the past 12 months, 84% report that the frequency of incidents has increased over the same period. Nearly a third (31%) say the volume has increased significantly.

Number of attacks in the past 12 months among affected respondents



Disparity in cybersecurity preparedness

The ongoing popularity of remote and hybrid working — with its attendant security risks — has created an environment where attacks are highly likely to increase in volume. Concerningly, only 29% of respondents say they are well prepared for cybersecurity incidents in the future.

Looking at cybersecurity preparedness across the continent, respondents from Italy and Switzerland were the least affected by incidents but also among the least prepared. Respondents in Spain seem to have taken the right steps to prepare, but they certainly need more help given this country was the second-most vulnerable to incidents.

Looking at industries, those that experienced fewer incidents — gaming and healthcare — were also among those least prepared, alongside organizations from the education, government, and transport sectors.

The reverse is true for businesses in the IT and technology sector. A high volume of attacks has seemingly put organizations in this field on their guard, helping them become one of the most prepared sectors alongside those in media and telecoms and financial services.

When looking at organizational size, the lack of preparation by smaller businesses is a particular concern. Only a quarter claim to be well prepared. Medium-sized and large organizations do not fare much better, with only 27% and 32%, respectively, claiming high levels of preparedness.

% of respondents claiming high cybersecurity preparedness

Most prepared countries

Denmark	43%
Spain	43%
Poland	36%

Least prepared countries

Italy	21%
Germany	24%
Czechia	24%

Most prepared industries

IT & Technology	35%
Financial Services	32%
Retail	31%

Least prepared industries

Healthcare	18%
Education	19%
Manufacturing	26%

By organization size



Outlook for cybersecurity incidents by region and organization size

	Incident likely within next 12 months	Incidents to increase within next 12 months
Benelux	61%	65%
CEER	60%	63%
DACH	66%	73%
Nordics	68%	73%
Southern Europe	60%	62%
UKI	70%	60%
Small organizations	59%	65%
Medium-sized organizations	67%	68%
Large organizations	64%	65%

Most business and IT leaders believe the threat level will remain high, with nearly two-thirds (64%) believing a cybersecurity incident will likely occur in the next 12 months. Among the industry segments, medium-sized organizations are the most likely to be affected, with 67% believing they will most likely experience an incident in the next 12 months.

Most respondents also expressed pessimism about the frequency of cybersecurity incidents. Two-thirds (66%) believe they will see more incidents within the next year. The outlook seems particularly stark for those in Germany, Switzerland, and the Nordic region, and for medium-sized organizations.

Looking at specific industries, those in the transport and IT and technology sectors expect to face the greatest challenges. Both sectors forecast that incidents in the next 12 months are likely (72% and 66%, respectively) and that there will be an increased volume of incidents over the same period (74% and 68%, respectively).

Outlook for cybersecurity incidents by industry

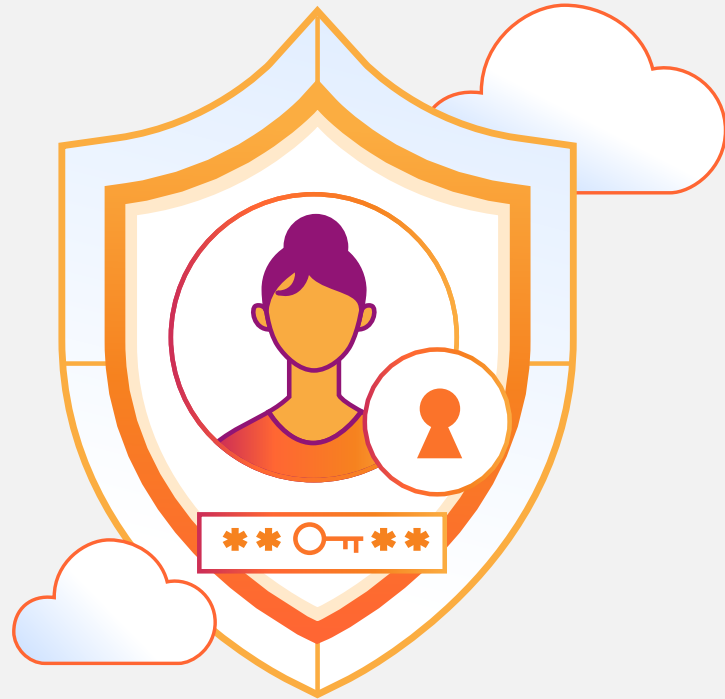
	Incident within next 12 months likely	Incidents to increase within next 12 months
Retail	63%	74%
Construction and Real Estate	62%	73%
Healthcare	56%	68%
IT and Technology	66%	67%
Government	66%	67%
Business and Professional Services	61%	66%
Travel, Tourism and Hospitality	61%	66%
Energy, Utilities and Natural Resources	62%	66%
Manufacturing	67%	65%
Education	62%	65%
Financial Services	64%	63%
Media and Telecoms	59%	62%
Others	57%	62%
Transport	72%	61%
Gaming	53%	56%

A challenging cybersecurity landscape

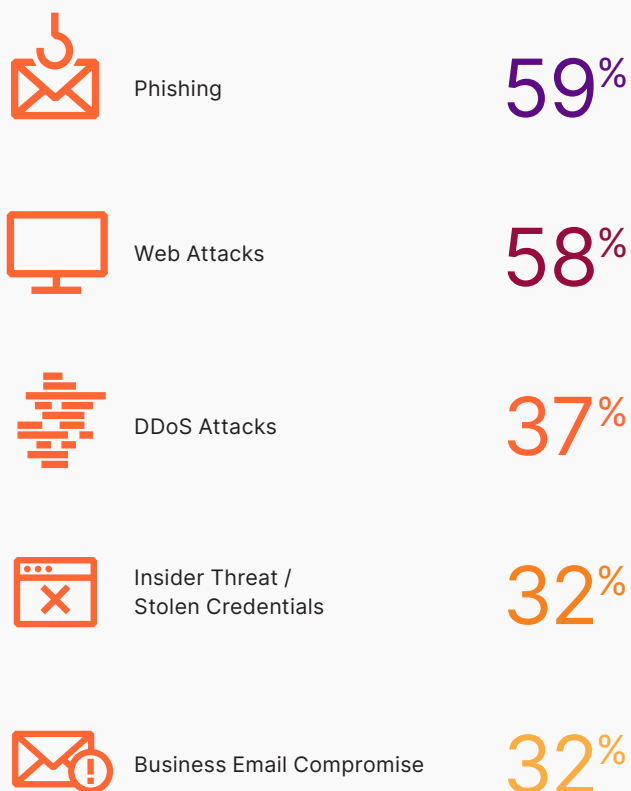
Additionally, our respondents believe the cyberattacks they have experienced have a range of objectives. Most respondents (53%) believe they were used to plant spyware, while financial gain was at the heart of almost half of the attacks (48%). Attacks aimed at planting ransomware were reported by 48% of our respondents.

When we asked about the types of cyberattack experienced, phishing was the most commonly reported, followed by web attacks.

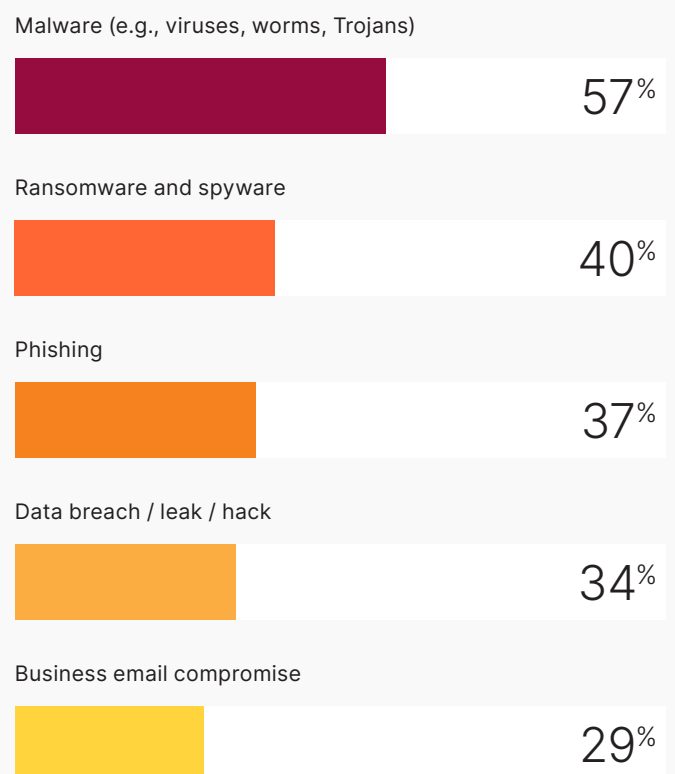
As for threats, malware — which we define as viruses, worms, and Trojans — appears among the top three risks for 57% of our respondents. Other common threats are ransomware and spyware (40%), phishing (37%), data breaches (34%), and business email compromise (29%).



Top five most commonly experienced cyberattack vectors



Named among the top three threats by respondents

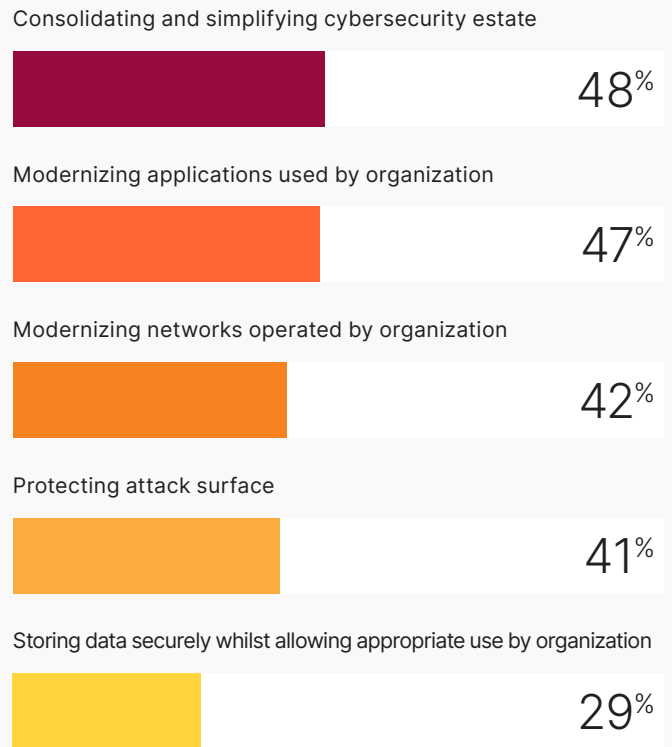


Cybersecurity response is trending up

In more positive news, it appears business and IT leaders are taking action. Nearly half (48%) ranked simplifying and consolidating their cybersecurity solutions stack as a top-three priority. A further 47% rank modernizing applications to counter threats as one of their top-three initiatives, while 42% are seeking to update their networks. Protection of the attack surface, or any area of potential exposure to a cyber threat, is a priority for 41%, while secure data storage is on the agenda for 29%.

Despite their plans, many feel they are still not ready for what lies ahead, and there is a significant 'confidence gap' in key areas for a large number of respondents. Showing the key areas of cybersecurity preparedness, the following chart indicates that our respondents are least prepared in terms of the devices they use.

Ranking among top three most important cybersecurity initiatives by respondents



Wide-ranging impact of cybersecurity incidents

The impact of cybersecurity incidents can be deep and long-lasting. For 39% of our respondents, the immediate financial cost was the most significant effect. However, reputational damage — a much longer-lasting and potentially more costly side-effect — was the second most likely to be ranked as the greatest impact.

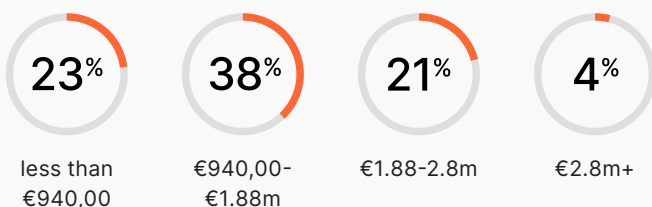
The financial losses arising from incidents can rack up remarkably quickly. Among the 39% of respondents whose organizations experienced a cybersecurity incident in the past year, two-thirds (63%) estimated the financial impacts to be at least €940,000, while a quarter (25%) estimated the loss to be €1.88 million or more.

Financial loss is not the only impact organizations have suffered. More than three out of 10 organizations have had to put growth plans on hold in the aftermath of an incident, while nearly one in five (19%) have had to lay off staff as a result of the financial impact. Other organizations have been subjected to legal action or been forced to pay fines as a result of incidents.

Wide-ranging negative impacts of cybersecurity incidents

Immediate financial cost	39%
Reputational damage	17%
Loss of data / IP	16%
Loss of customers	10%
Loss of employees	6%
Increased insurance costs	6%
Increased regulation	5%

Financial impacts of cybersecurity incidents in the past 12 months



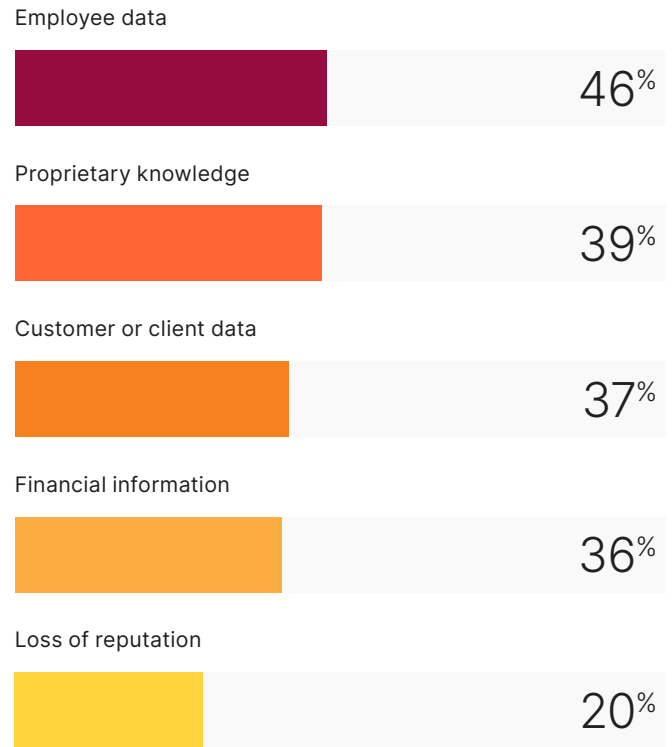
Ramifications of cybersecurity incidents

Put growth plans on hold	31%
Reduced or restricted hybrid work	29%
Temporarily suspended business operations	28%
Disclosed incident(s) to authorities	26%
Experienced legal action	23%
Increased insurance premiums	23%
Paid fines	22%
Lost revenue	22%
Forced to lay off workforce due to financial impact/loss	19%
Lost customers	11%
Lost employees	8%

Our respondents experienced a wide range of data losses as a result of cybersecurity incidents, but the most common is the loss of employee data. This was the case for nearly half (46%) of those who experienced incidents. Other common data sets lost include customer or client data (37%), while nearly two in five (39%) lost proprietary information — which of course could have calamitous long-term effects on competitiveness.

Almost nine out of 10 respondents in regulated markets reported an incident to relevant authorities, including 53% who did so voluntarily. Nearly one in five (18%) did not report the breach, including 2% who were in fact obliged to and thus ran the risk of heavy fines and other penalties.

Most common losses inflicted by cybersecurity incidents



Organizations recognize the cybersecurity risks and are investing

While cybersecurity has not always received the investment needed to adequately protect organizations, this looks to be changing. The pressures brought about by the shift to remote and hybrid working in the wake of the COVID-19 pandemic threw this into sharp relief, and we have seen rapid rises in cybersecurity budgets.

Perhaps due to the lack of preparedness and confidence already mentioned, investment in cybersecurity is again under the microscope, and over half (54%) of respondents expect the proportion of their IT budget dedicated to cybersecurity to rise






over the next year. Just 16% foresee a decrease, and 29% foresee no change. This is a positive sign, as organizations need to prepare for the increased volume of incidents they predict in the year ahead.

25% of business and IT leaders expect cybersecurity to make up at least 20% of their organizations' IT spend over the year ahead. Of those expecting a budgetary increase, two-thirds (66%) anticipate a rise of more than 10%.

For most, protecting their networks remains the number one investment area, with nearly 24% of the budget allocated to this pillar on average. Devices are set to receive the second lowest allocation of budget share despite being the area where respondents see a significant lack of preparedness.



Allocation of cybersecurity budget over the past 12 months by area

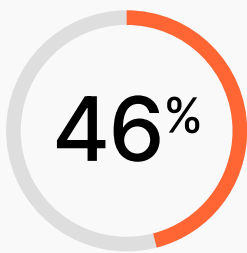
	Networks	24%
	Data	21%
	Applications	19%
	Devices	19%
	Users	18%

The rationale behind budget allocation within cybersecurity is complex, according to our respondents. Of the nine different factors our survey looked at, the top two determinants were the number of incidents experienced and the cost of dealing with them. It thus appears that most organizations are still largely reactive in how they allocate funding.

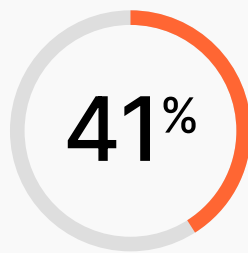
Determinants of cybersecurity budget allocation



Top challenges to cybersecurity preparedness



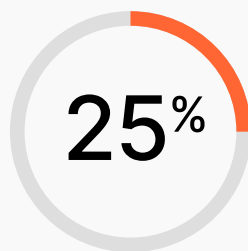
Lack of funding/
investments into
cybersecurity



Lack of talent with the
requisite expertise to
handle modern-day
cybersecurity challenges



Evolving business
requirements and
user needs



Lack of buy-in from
leadership

Lack of funding remains our respondents' single biggest concern. However, it is not the only thing that is keeping leaders up at night. A lack of talent available in the jobs market and/or a lack of the right in-house expertise is another major concern for many.

Interestingly, despite the increasing volume of attacks, many cite a lack of buy-in from leadership as a key challenge. Perhaps this is a case of cybersecurity fatigue, but whatever the cause, senior leaders cannot afford to ignore the challenges facing their organizations.

A mixed picture of solution deployment

Our respondents identify three clear problems with the architectures they currently use: applications and data stored in the public cloud; limited oversight over IT supply chains; and over-reliance on VPNs to protect applications (each factor mentioned by 34% of respondents).

Given these issues, it is no surprise that securing a hybrid workforce is by far the number one priority, representing one of the top three priorities for more than a third (36%) of our respondents.

Deploying effective countermeasures is crucial to protecting an organization. However, across a range of solutions, our respondents told us they are a long way from full deployment, and many have not even begun rolling them out.

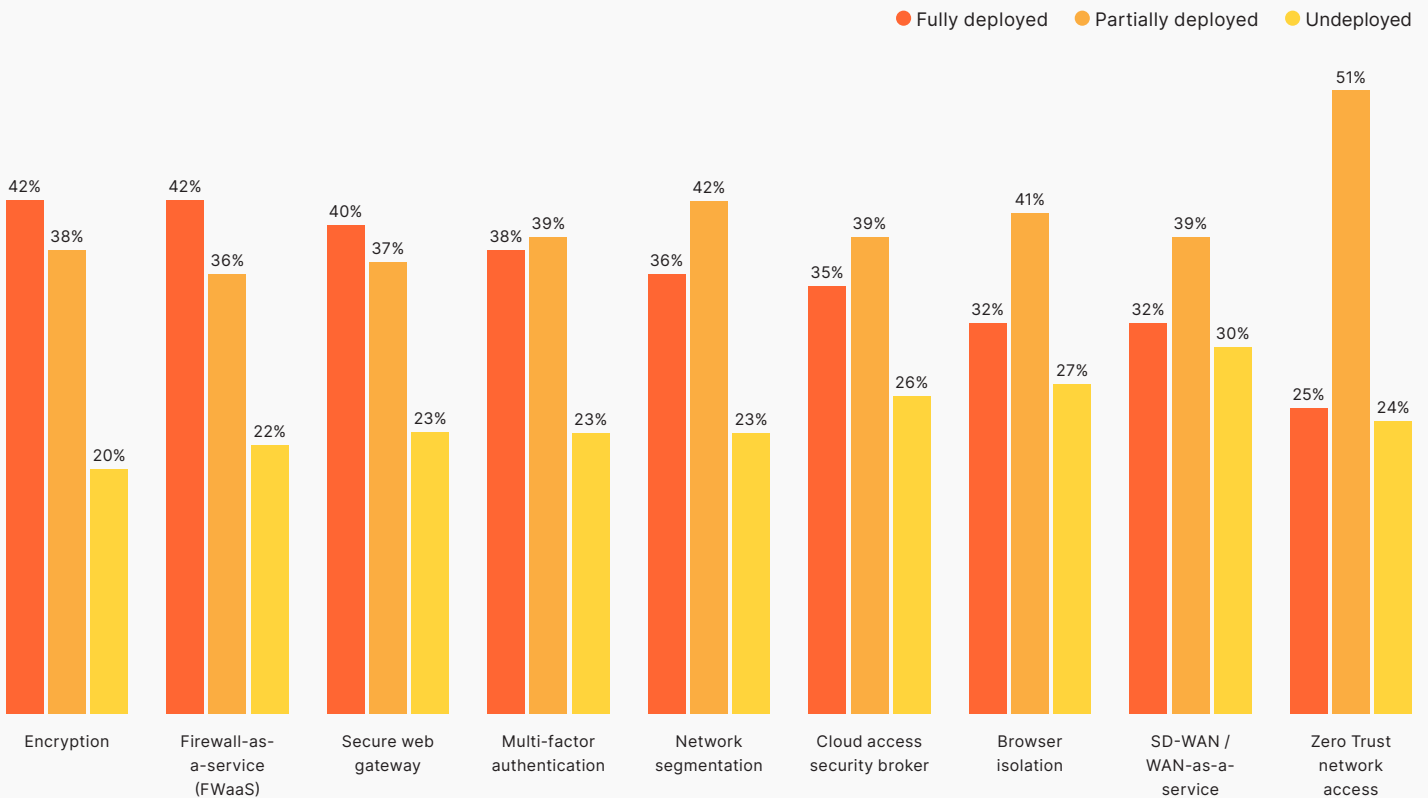
Encryption is currently organizations' most deployed solution, with secure web gateways and firewall-as-a-service (FWaaS) not far behind. Looking specifically at SASE, only 10% have fully implemented this model, 29% have achieved advanced implementation (76-99%), 35% have progressed towards implementation (51-75%), 21% have achieved partial or early-stage implementation, and 5% have made no progress or are unsure of their progress.



Organizations' current, most pressing cybersecurity priorities

Securing a hybrid workforce	36%
Defending against cyberattacks	17%
Deploying Zero Trust across the organization	13%
Moving towards a SASE architecture	7%
Securing customer correspondence/data	7%
Securing organization's networks and data	7%
Workload security	3%
API security	3%
Protect organization's financial information	3%
Protect consumer-facing applications	2%
Allowing safe use of AI in the workplace	2%

Levels of Zero Trust solution deployment



Optimism around how cybersecurity can enable business growth (by region)

	Benelux	DACH	France	Nordics	UK
Move to a Zero Trust architecture enabling a better user experience and more cloud native possibilities	45%	41%	49%	36%	50%
SASE or SSE being a way to reduce old tech and enable your business to use more cloud applications	43%	48%	48%	47%	45%
Better cyber risk understanding by the board leading to funding for essential projects	38%	42%	42%	41%	44%
Modernization in the workplace	33%	38%	32%	35%	44%
Executive buy-in to the needs of robust risk management	26%	33%	28%	30%	35%
Better visibility of threats affecting critical systems	26%	29%	25%	25%	37%
Improved execution around mergers and acquisitions	7%	7%	12%	8%	13%

If we break this down further, four out of the five components of SASE (SD-WAN, cloud access security broker, FWaaS, ZTNA, and secure web gateways) in fact show a reasonable level of deployment. And there is cause for optimism, as seven in 10 respondents are now working with a single SASE vendor, which should reduce complexity and help speed up deployment.

Zero Trust network access is a long way behind, despite widespread recognition of its ability to protect hybrid or remote workers. That said, our respondents are optimistic about how Zero Trust can consolidate technology upgrades.

Optimism around how cybersecurity can enable business growth (by industry)

	Move to Zero Trust architecture meaning better user experience and more cloud native possibilities	SASE or SSE as way to reduce old tech and enable business to use more cloud applications	Better cyber risk understanding amongst board enabling funding of essential projects	Modernization in the workplace	Executive buy-in to the needs of robust risk management	Better visibility into threats affecting critical systems	Improved execution around mergers and acquisitions
Travel, Tourism and Hospitality	47%	30%	53%	30%	30%	30%	10%
Business and Professional Services	41%	50%	59%	38%	26%	32%	12%
Education	35%	37%	65%	40%	22%	19%	7%
Construction and Real Estate	40%	47%	60%	30%	27%	19%	10%
Manufacturing	39%	47%	61%	36%	33%	32%	9%
Financial Services	40%	53%	60%	33%	36%	28%	8%
Government	46%	31%	54%	38%	25%	28%	9%
Healthcare	39%	44%	61%	40%	28%	28%	10%
Retail	36%	48%	64%	37%	31%	27%	6%
IT and Technology	44%	49%	56%	36%	34%	29%	10%
Media and Telecoms	51%	45%	49%	47%	35%	27%	15%
Transport	45%	47%	55%	43%	30%	30%	11%
Energy, Utilities and Natural Resources	42%	53%	58%	45%	25%	25%	12%
Gaming	38%	52%	62%	33%	29%	33%	10%
Others	38%	37%	62%	33%	23%	25%	9%

Looking specifically at cybersecurity tools, data recovery and backup has the highest level of deployment, underlining the critical role it plays in overall cybersecurity strategy. Data encryption is not far behind and, encouragingly, management processes to handle cyberattacks are fully deployed in nearly four out of 10 of our respondent organizations.

Less positively, nearly a quarter of those surveyed had not undertaken leadership or general employee training, despite widespread acknowledgment that this is a simple win for most organizations. This perhaps explains why more than one in five (21%) business and IT leaders rate their organizations' cybersecurity culture as weak or neutral.

Another hindrance for many of our respondents is complexity: nearly half (49%) deal with more than 11 different products and solutions. They navigate a complicated web of products and solutions, and nearly three-quarters of those surveyed (72%) believe that the complexity of their cybersecurity stacks has had a negative impact on their effectiveness.

Unfortunately, this problem not only looks set to continue, but for many it will get worse — two-thirds (67%) expect the number of products and solutions they use to increase over the next 12 months. In fact, nearly one in five (18%) plan to increase the number significantly, and just 6% plan to simplify their solution architecture.

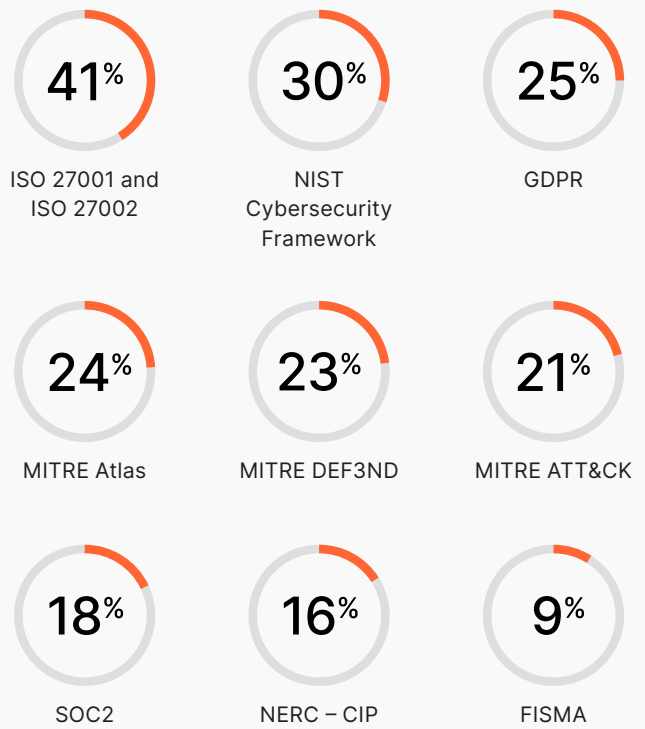
Deployment levels for cybersecurity tools and solutions

	Fully deployed	Partially deployed	Undeployed
Data recovery and backup	45%	35%	20%
Data encryption	43%	36%	21%
Cybersecurity management processes	38%	41%	21%
Next-generation firewall (NGFW)	38%	38%	24%
Security information and event management (SIEM)	38%	40%	22%
Network behavior analytics	37%	41%	22%
Leadership team training	36%	41%	23%
Intrusion prevention system (IPS)	35%	41%	24%
General employee training	35%	42%	23%
Endpoint protection platform (EPP)	34%	41%	25%
Threat intelligence platforms	33%	41%	26%
Extended detection and response (XDR)	25%	46%	29%

The most commonly applied cybersecurity frameworks are ISO27001 and ISO27002, both comfortably ahead of the third most used framework. However, there are others — particularly NIST and MITRE — which also have their advocates.

Among mandatory government-backed frameworks, the most prominently adhered to among our respondents was the European Union's Cybersecurity Act. Respondents from organizations in BENELUX, CEER, DACH, and the Nordic countries report high levels of compliance with the EU framework, but those in southern Europe reported less compliance. Organizations in the UK — perhaps because of Brexit — tend to favor a local framework (Cyber Essentials).

Cybersecurity frameworks in use by organizations



Adherence to government-backed cybersecurity frameworks

	Benelux	CEER	DACH	Nordics	Southern Europe	UK
Cybersecurity Act — EU	64%	60%	64%	72%	57%	42%
NIS Directive — EU	45%	53%	43%	53%	46%	29%
Cyber Essentials — UK	31%	21%	19%	19%	23%	84%
BSI — German	18%	27%	51%	12%	18%	10%
ENS — Spanish	17%	20%	14%	12%	38%	10%



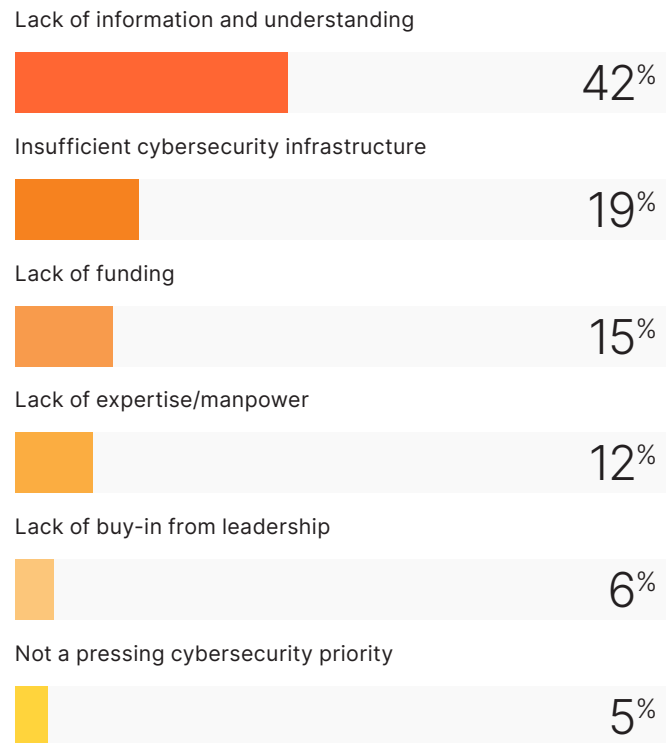
Executive unfamiliarity is a barrier to Zero Trust adoption

We have already seen that the complexity of cybersecurity solutions and insufficient budgets affect the preparedness of business and IT leaders to stave off the increasing volume of incidents.

However, our respondents also indicated a lack of faith in their leadership teams' understanding of Zero Trust. In fact, almost nine in 10 (86%) believe their leadership does not fully understand Zero Trust, while nearly one in five (16%) say their leadership has either partial or no real understanding.

This is a key reason why over half (58%) say that Zero Trust adoption is still in its early stages, as we saw in the previous section. Additionally, 42% believe that a lack of understanding is the single biggest barrier to adoption.

Barriers to Zero Trust adoption



Cybersecurity incident response

Our respondents were in no doubt that attacker dwell time (how long a cyber intruder remains undetected) has increased over the last 12 months. Close to two-thirds (62%) felt this way, while 15% claim it has increased significantly.

For most (57%), the average dwell time is up to 24 hours, but for a sizable minority (37%) it is between one and three days. 7% said their average dwell time was between three days and a week, and 3% of our respondents — representing more than 150 organizations — said that it averages more than a week.

The consequence of these dwell times is often that the system goes down, and four in 10 respondents say their services or solutions have been impacted and/or offline for at least six hours per incident. This

is significant when considering the number of incidents suffered by many and the fact that businesses can lose vast amounts of time as a consequence.

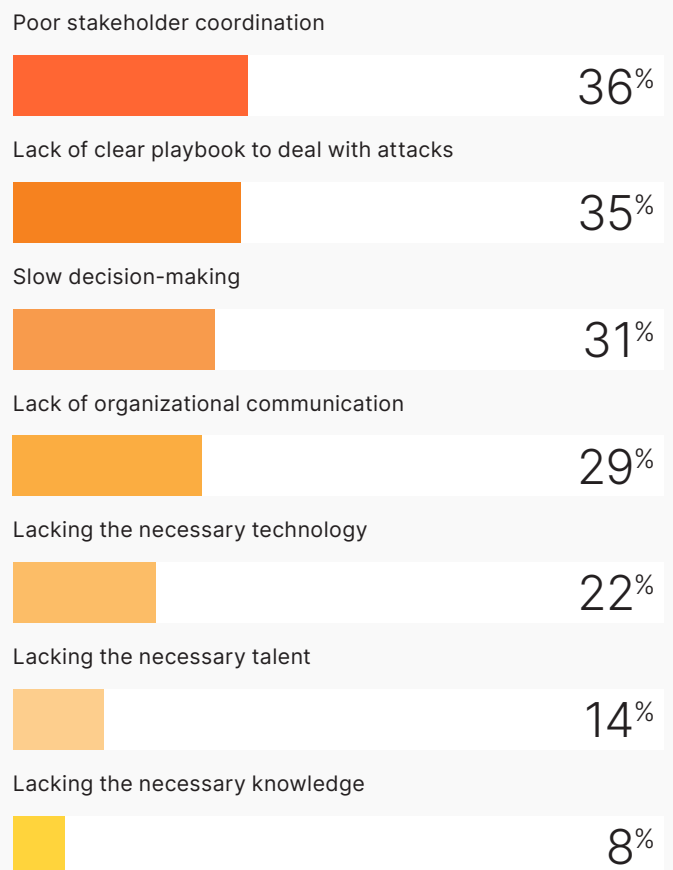
While there is room for improvement in dwell times, resolution times are more encouraging. Most respondents (52%) have been able to resolve an incident within six hours, and more than three-quarters (77%) claim they have become quicker at dealing with incidents over the last 12 months. Among those reporting faster resolution times, most (52%) attribute this to greater investments in technology, but there are also nods to improved security cultures, having a clear playbook, and better talent.

For those unable to shorten their organization's resolution times in the past year, the key barrier was poor stakeholder coordination. This also underpins the second, third, and fourth barriers, which all hinge on coordination.

Factors influencing faster cybersecurity incident response time



Barriers to shortening cybersecurity incident response time



Data compliance: an increasing challenge

Our study finds that data compliance is fast becoming another area of complexity. Half (50%) of respondents say they are challenged by the number of siloed tools and homegrown solutions for data protection, security, sovereignty, localization, residency, and privacy.

Most of the responsibility for controlling and securing data flows lies with CISOs (40%) or CIOs (34%). Chief Privacy Officers (15%) and CTOs (11%) are less likely to be involved in the process. Similarly, in terms of departments, responsibility tends to lie with both the Security and Data Storage or Management functions (38%) or, for just under a third (32%) of organizations, within Security.

For some organizations, the situation is exacerbated by archaic manual processes that are used to consolidate logs and meet audit requirements (47%). Other common challenges for compliance include slow application performance due to data localization constraints (33%) as well as the adoption of AI (30%).

Looking ahead, our respondents are focused on three main priorities to strengthen data governance, with policies and procedures front and center for most (55%).

Data compliance priorities

Strengthening governance policies and procedures for robust data compliance	55%
Implementing technology for threat detection, access controls, and data encryption	50%
Investing in skills development and fostering a culture of data security	48%
Addressing GDPR compliance measures	29%
Addressing industry-specific regulations (e.g., HIPAA, PCI DSS)	12%



Hybrid working continues to challenge cybersecurity infrastructure

Nearly three-quarters of respondents' organizations (74%) in Europe still operate a hybrid or remote working environment, with the most common format reported to be 1-3 days a week in the office (51%).

However, nearly half (46%) of respondents expect hybrid and remote working to decrease in the next 12 months. Most (41%) cite pressure from coworkers to be in the office more often, while 39% believe job prospects are harmed by spending less time in the office.

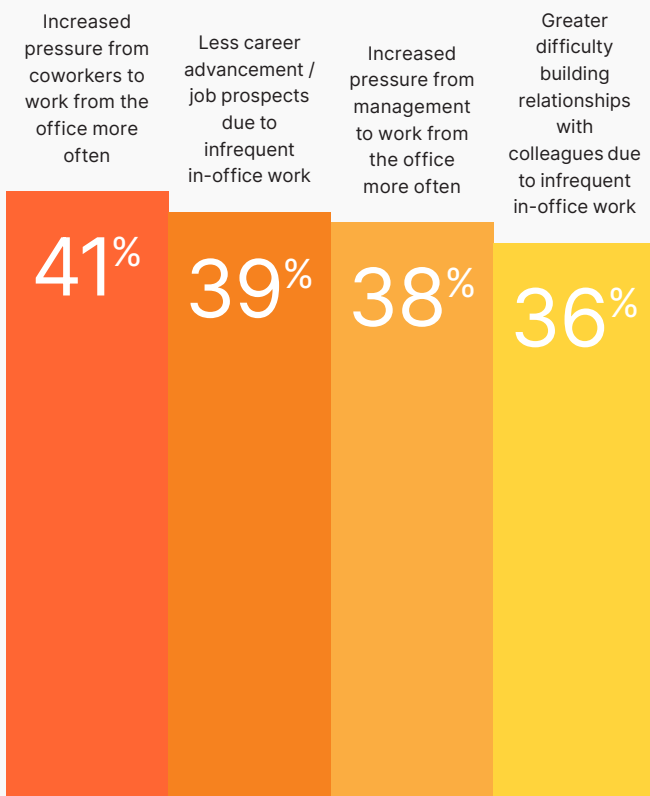
Pressure to change working practices will have a knock-on effect throughout organizations. Half (50%) predict that it will increase the complexity of cybersecurity, but at the same time nearly half (48%) believe it will yield increased productivity and better collaboration between employees across different geographies.

For organizations not expecting a reduction in remote or hybrid working, challenges remain in securing employees and their data. The two most pressing concerns are the use of unknown or poorly secured WiFi networks, an issue for nearly two-thirds (62%) of respondents, while using personal devices to access their organization's network or data was an issue identified by 61%.

Those concerns explain why nearly a third (31%) report significant investments in cybersecurity measures to support remote and hybrid working. The same number are also planning to invest significantly over the next 12 months.

The key investment currently needed to support remote and hybrid working is in cybersecurity talent. The dearth of investment in this area is an issue for more than four in 10 respondents (41%), although underinvestment in the broader cybersecurity infrastructure and a lack of awareness among management are also areas that need to be addressed.

Hybrid work trends foreseen over the next 12 months



Challenges to improving cybersecurity posture to support hybrid and remote work



Summary and recommendations

This report shines a light on the persistent and increasing threat of cyberattacks across Europe. It also underlines the challenges faced by CISOs: budgetary restrictions, talent shortfalls, and an increasingly volatile cybersecurity landscape.

These challenges require organizations to take a new approach to digital security. Here are our five key recommendations for organizations that recognize the need to maintain a robust cybersecurity framework:

1. **Simplify security architectures:** Instead of complex and disparate systems, business and IT leaders should adopt a comprehensive 'Everywhere Security' approach that gives their workforces secure access to both web and multi-cloud environments, while simultaneously protecting against sophisticated cyber threats, securing sensitive data, and simplifying operations.
 2. **Preparation is everything:** Failing to prepare is preparing to fail — nowhere is this more true than in cybersecurity, yet less than 30% of organizations in Europe currently rate themselves as well prepared. Much greater investment is needed in consolidated solutions, which can help organizations respond to an increasingly multifaceted threat environment. Zero Trust is one such approach, but as barely 10% of executives understand the solutions on offer, improvements will involve time and effort.
 3. **Strong security culture:** Building a strong security culture at all levels can help organizations prepare in multiple ways. To begin with, good understanding and awareness create a first line of defense that can help organizations react to and repel attacks more quickly. This also creates a better business case, meaning CISOs do not need to wait for incidents to occur and can instead proactively mitigate the risk of grave financial loss. Organization-wide understanding will also help senior executives understand that cybersecurity is mission-critical, and that they need a holistic approach to ensure their staff, suppliers, and clients all adhere to best practices.
 4. **SASE can improve preparation:** Preparation can be accelerated by reducing the number of solutions deployed. SASE is essential to streamline cybersecurity and improve outcomes, while also enabling organizations to mitigate the impact of an industry-wide talent crunch.
 5. **Streamlining data compliance:** Reliance on legacy security solutions and manual processes has added complexity to an already hard-to-navigate, evolving regulatory landscape. CISOs and CIOs need a streamlined approach to comply with security controls for user access to business-critical and SaaS apps, inspection of HTTP traffic to prevent sensitive data exfiltration, client-side security, and end-user browser protection from supply chain attacks, as well as integrated logging of firewall events, HTTP requests, and moves to preferred SIEM or cloud destinations. Organizations can meet the regulatory needs of today and tomorrow by adopting a modular approach to security while reducing costs, enhancing app performance, and delivering an improved user experience.
- 

Cloudflare can help your organization adapt to the cybersecurity challenges of today, regardless of your current security posture. Our platform is for organizations of any size, at any stage of implementation, and with any level of preparedness. We can help you simplify cybersecurity, compensate for talent constraints, and defend against any type of cyber threat.

To learn more about Cloudflare's platform of solutions and request a demo or POC from a sales representative, please visit:

cloudflare.com

We will evaluate your existing security posture and create an action plan to strengthen cybersecurity for your people, applications, devices, networks, and data.



© 2024 Cloudflare Inc. All rights reserved.
The Cloudflare logo is a trademark of Cloudflare. All other
company and product names may be trademarks of the
respective companies with which they are associated.

1 888 99 FLARE | enterprise@cloudflare.com | [Cloudflare.com](https://cloudflare.com)