Brought to you by CSO from IDG

CSO

Global Intelligence Report:

State of Cybersecurity 2021

Sponsored by:

PC Matic | OneNeck IT SOLUTIONS a TDS® Company | deepinstinct™

Global Intelligence Report:

State of Cybersecurity 2021

Brought to you by CSO from IDG

CSO

Platinum Partner

PC Matic

Gold Partner

OneNeck®
IT SOLUTIONS
a TDS® Company

Silver Partner

deepinstinct™

Table of Contents

From the Editor

And the hits just keep on coming 4

Executive Summary

It's getting hot in here 5

Key Finding #1

Financially motivated attacks are taking a toll 8

Key Finding #2

Budgets and policies evolve — with a few notable gaps 16

Key Finding #3

Despite risks, cloud is a net positive for security 23

Key Finding #4

AI + zero trust is the new baseline 28

Looking Forward 32

Survey Methodology 33

Partner Profiles 35

From the Editor

And the hits just keep on coming

Rob O'Regan
Global Content Director
IDG Communications, Inc.

Did anyone have "global pandemic" on their cybersecurity bingo card? In the world of the chief security officer, where careers are defined by staying a step ahead of bad actors, security leaders can be forgiven for not anticipating COVID-19's sudden disruption to the workforce, customers, and supply chains, and the new vulnerabilities remote work and other operational shifts introduced.

And yet here we are. A year and a half later, organizations are still dealing with the fallout of new operating models to support a virtual workforce and more digitally inclined customer and supplier bases. As threats increase, CSOs and their teams are quickly evolving their strategies and tactics to keep pace.

To understand the impact of the pandemic on security practices, and to gauge how security teams are preparing for what's next, we surveyed more than 2,700 technology and security decision makers across the globe. This report, written by Derek Slater, former editor in chief of CSO, is chock-full of insights from respondents about the constantly evolving threat landscape and the tactics security professionals are deploying in response. We hope these findings will help you compare your security posture to your peers and identify next steps to evolve your security strategy — for whatever completely unexpected event comes next.

We'd like to thank our sponsors for their support of this Global Intelligence Report: platinum sponsor PC Matic, gold sponsor OneNeck IT Solutions, and silver sponsor Deep Instinct. ■

Executive Summary

It’s getting hot in here

New and emerging threats, underscored by a growing reliance on digital infrastructure, have everyone’s attention

Read On

For cybersecurity professionals, like everyone else, the past 15 months have been…interesting.

If 2020's COVID-related lockdowns and the sudden, massive shift to remote work weren't enough, more recent events such as ransomware attacks on Colonial Pipeline Company and meat processor JBS made splashy headlines, putting more heat on cybersecurity teams to protect their organization.

But threats have been expanding for years, and high-profile hacks have appeared in the news for decades. As workforces around the globe begin to return to some form of normalcy in the coming months, will digital security truly be different for the remainder of 2021 and beyond?

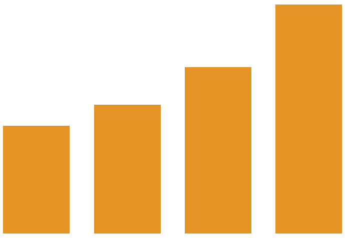
Exclusive research from IDG finds that in crucial ways, it will.

IDG's Global Intelligence Report on Cybersecurity surveyed 2,741 security, IT, and business professionals around the world, examining key topics ranging from the threat landscape to the evolving use of the cloud, artificial intelligence (AI), and zero-trust models to strengthen defenses. The top line: Security has reached a tipping point, commanding full attention and support from the highest levels of the corporate world.

"The board is paying a lot more attention to the business impact of security," says Bob Bragdon, senior vice president and managing director of IDG's CSO. This degree of stewardship has been slow to take hold: Bragdon notes that both the National Association of Corporate Directors and the World Economic Forum issued guidance years ago that security needs to be on the agenda of every board meeting. ▶

79%

of respondents described the potential impact from financially motivated cybercrime, including ransomware, as critical or catastrophic.



71%

of organizations expect their security budget to increase this year.

Our survey underscores why boards need to pay closer attention. Financially motivated cybercrime, including ransomware, is a prevalent concern, with 79% of the respondents describing the potential impact as critical or catastrophic. Damage suffered from previous cyberattacks runs the gamut, from work interruptions and downtime (47% of the respondents have experienced this) to a complete business shutdown (15%). One-third say their organization suffered reputational damage, and nearly one in five organizations (18%) have suffered financial penalties due to liability issues.

In response, most organizations (71%) say their security budget has increased this year. The challenge now is to prioritize that spending across a complex spectrum of risks, seeking to pair maximum protection with increased — instead of reduced — business agility.

Other key findings include:

- Organizations are updating security policies and controls to address remote and hybrid work models — but key gaps remain in some of the supporting tactics they're deploying.
- As organizations shift more digital resources to the cloud, they're adapting policies to take advantage of the cloud's security benefits while addressing lingering concerns about an expanded attack surface.
- Emerging technologies such as AI and the solutions that enable zero-trust security models are experiencing rapid uptake. However, although the technology is evolving, some organizations still lag in core people-and process-focused areas, such as awareness training.

The data in this report can help organizations understand how peers are targeting their spending and the operational changes they are making to better protect the business, striving for both less risk and lower incident impact.

"Companies are starting to see the impact and think, 'Imagine if we had put half of that money into preventing it instead,'" Bragdon says. ■

Key Finding #1

Financially motivated attacks are taking a toll

Incidents are rising, with widespread impact

Read On

Cybersecurity incidents are rising. In other news, water is wet and refined sugar isn't good for you.

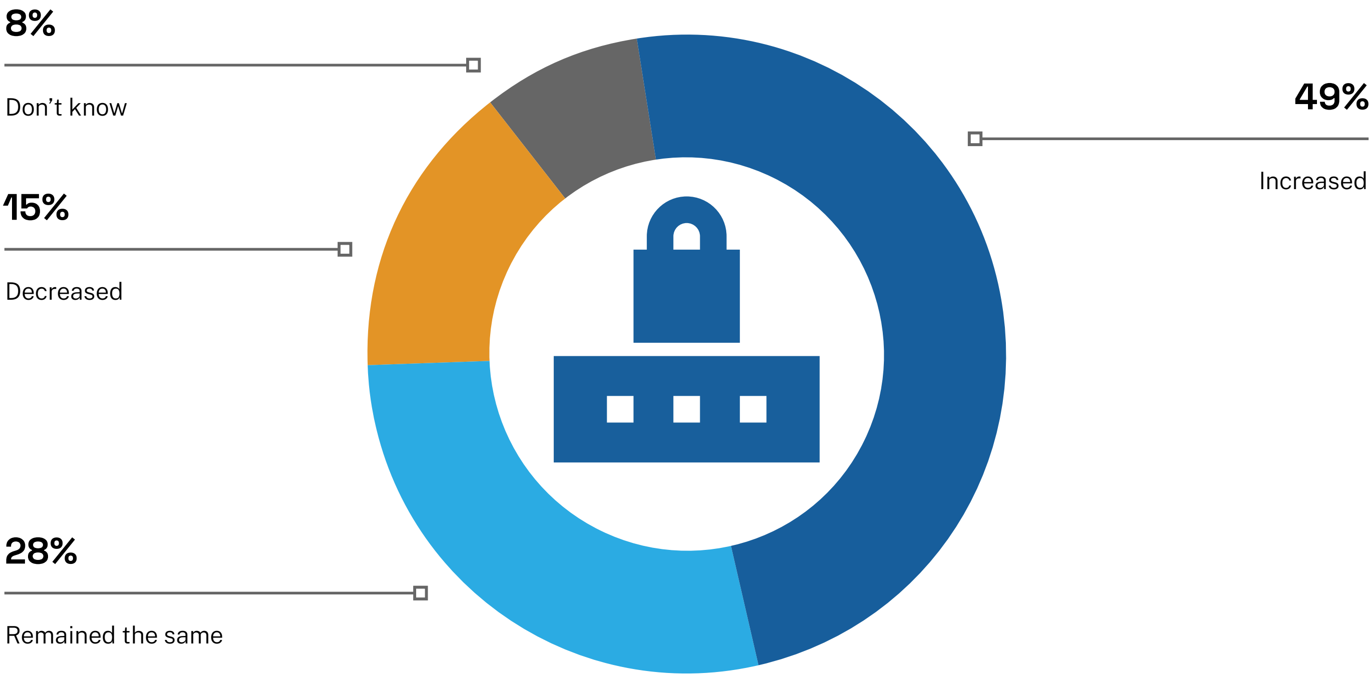
Security and IT pros are well accustomed to the ongoing game of one-upmanship between attack and defense. But the survey uncovered some important insights into where and how new attacks are occurring.

Ransomware is a particular concern, with steady waves of new attacks in both the public and private sectors. Looking forward, 62% of respondents anticipate a ransomware attack on their organization in the next 12 months.

77%

Cybersecurity incidents rose or held steady at 77% of organizations over the past year, increasing by an average of 5% across all respondents.

Change in frequency of cybersecurity incidents 2019–2020



Cyberattacks cause tangible damage. Loss of productivity (47%) and loss of personally identifiable information (PII) (46%) are the most common results. Nearly half of the respondents (46%) report economic damage, with 12% of those organizations having suffered “massive” economic impact.

The results suggest that theft of intellectual property may be more prevalent than generally reported. C-level respondents were more likely than others to report IP theft, at 31%, compared to 25% of the respondents at a mid-management level, a potential indicator that lower-level employees have less visibility into that type of crime.

Consistent with the financial goals of cybercrime, regions with more developed economies are seeing a larger proportion of increased incidents. The U.S. and Canada are the most likely areas to report an increase in incidents (53%), followed by the Asia-Pacific region (50%), Europe / Middle East (48%), Latin America, and Africa (each at 42%).

Enterprises and midsize companies are more likely (at 50%) to report an increase in incidents, versus organizations with fewer than 500 employees (40%). Although larger organizations are likely to devote more resources to security, they also offer more potential points of attack — and potentially more attractive assets for criminals to target. ▶

33%

of organizations experienced reputational damage from a cybersecurity incident.

62% of organizations believe that a financially driven attack such as ransomware is likely over the next 12 months.

Almost half of the respondents report financial damage because of a cyberattack.

These attacks are causing tangible harm. Nearly half of the respondents (46%) report economic damage, with 12% of those organizations suffering “massive” economic impact from a cyberattack.

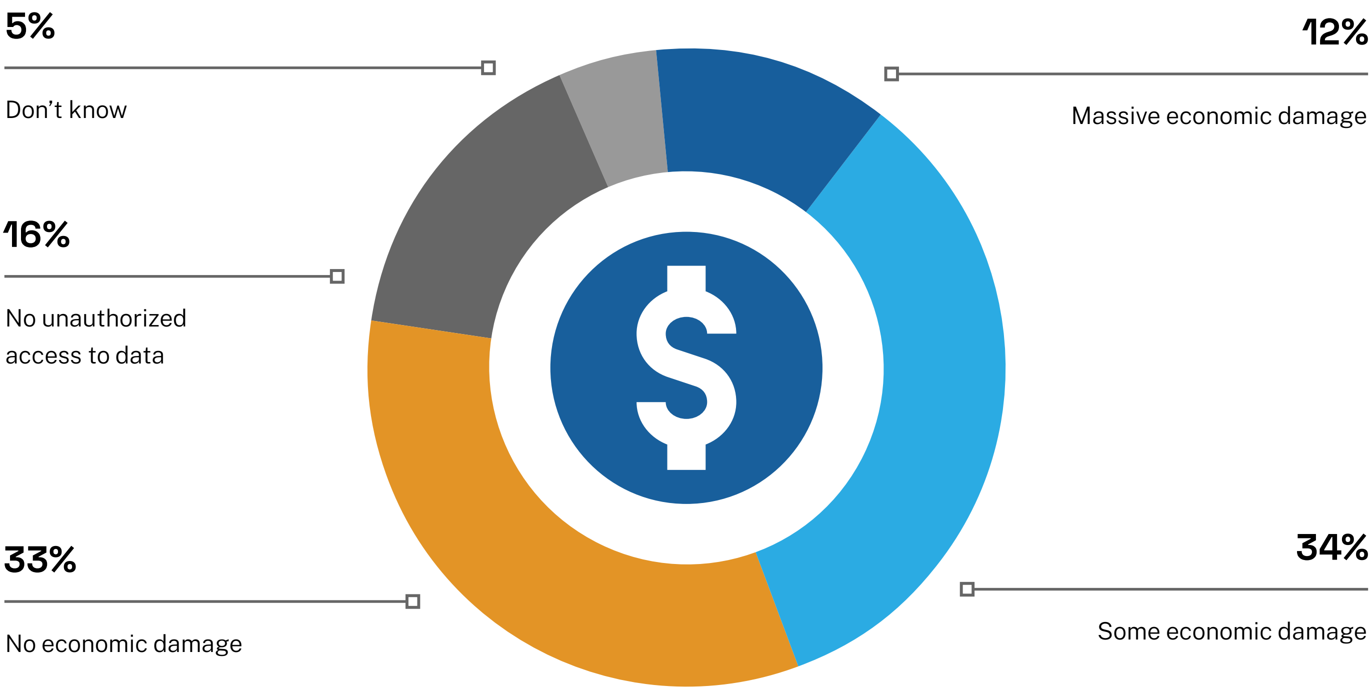
Hacks cost their victims both money and time. Loss of productivity (47%) and loss of customers’ PII (46%) are the most common results from a cyberattack.

And some of the damage extends over the long term: 33% experienced reputational damage, 22% suffered sustained productivity impairment, and 15% experienced a full shutdown of their business. That’s roughly one out of every seven organizations that have suffered an incident on the scale of the Colonial Pipeline attack — a high number for such a drastic impact.

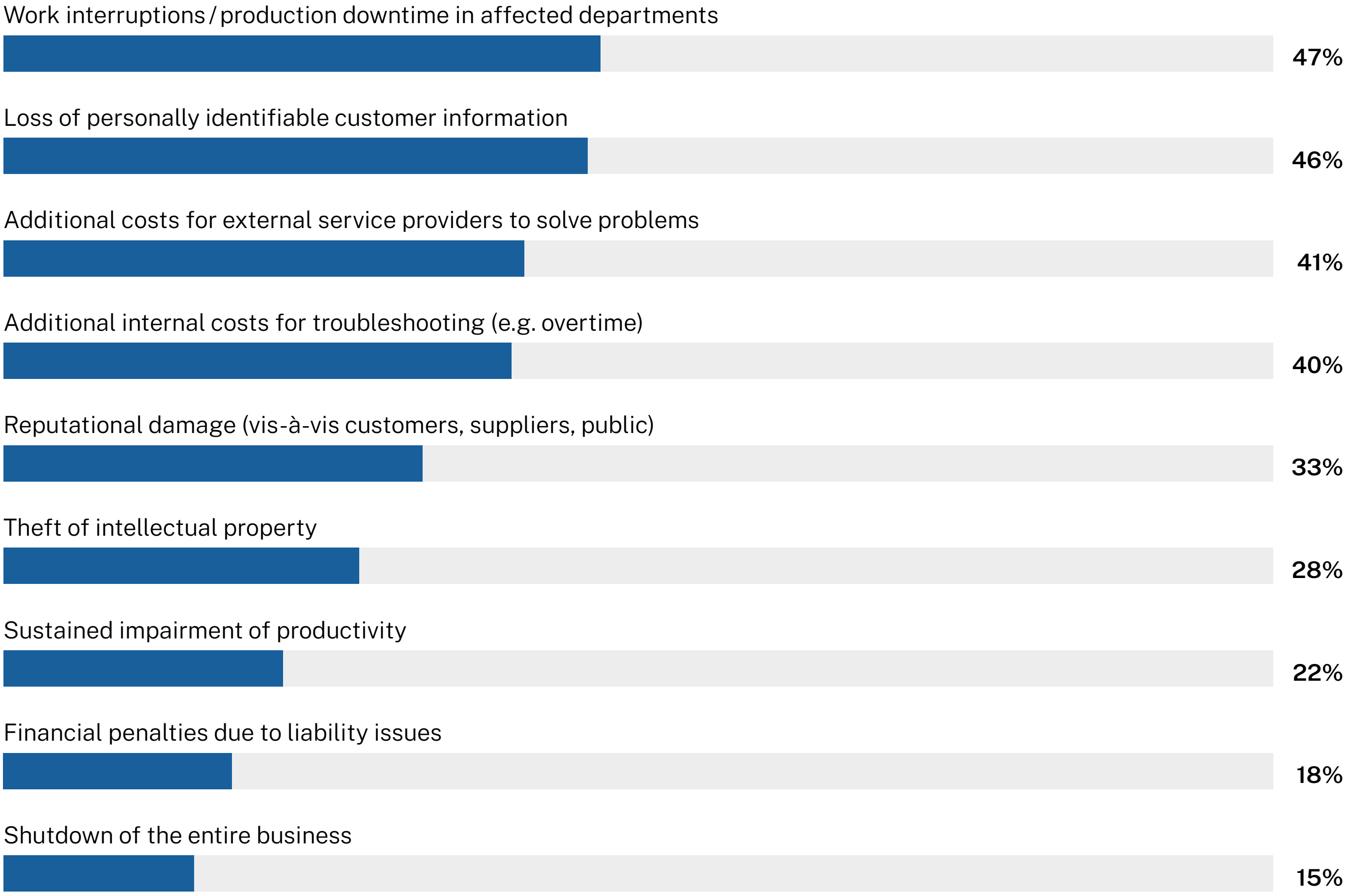
60%

of organizations in the utilities sector report economic damage from a cyberattack, the highest of any industry segment.

Economic damage from a previous cyberattack



Impact of cybersecurity attacks



15%

of organizations had to shut down their business because of a cyberattack.

There were some notable differences in the impact of security incidents across industries:

- Respondents in the transportation and logistics industry were more likely than others to report having to pay additional costs for external service providers to solve problems (54%). These organizations also had a higher rate of sustained productivity impairment (34%).
- Wholesale / retail companies were most likely to report loss of PII, at 58%.
- Utilities / energy companies reporting intellectual property theft topped the list, at 43%.
- Government organizations led the way in terms of incurring additional internal costs for troubleshooting (such as overtime), at 60%. ▶

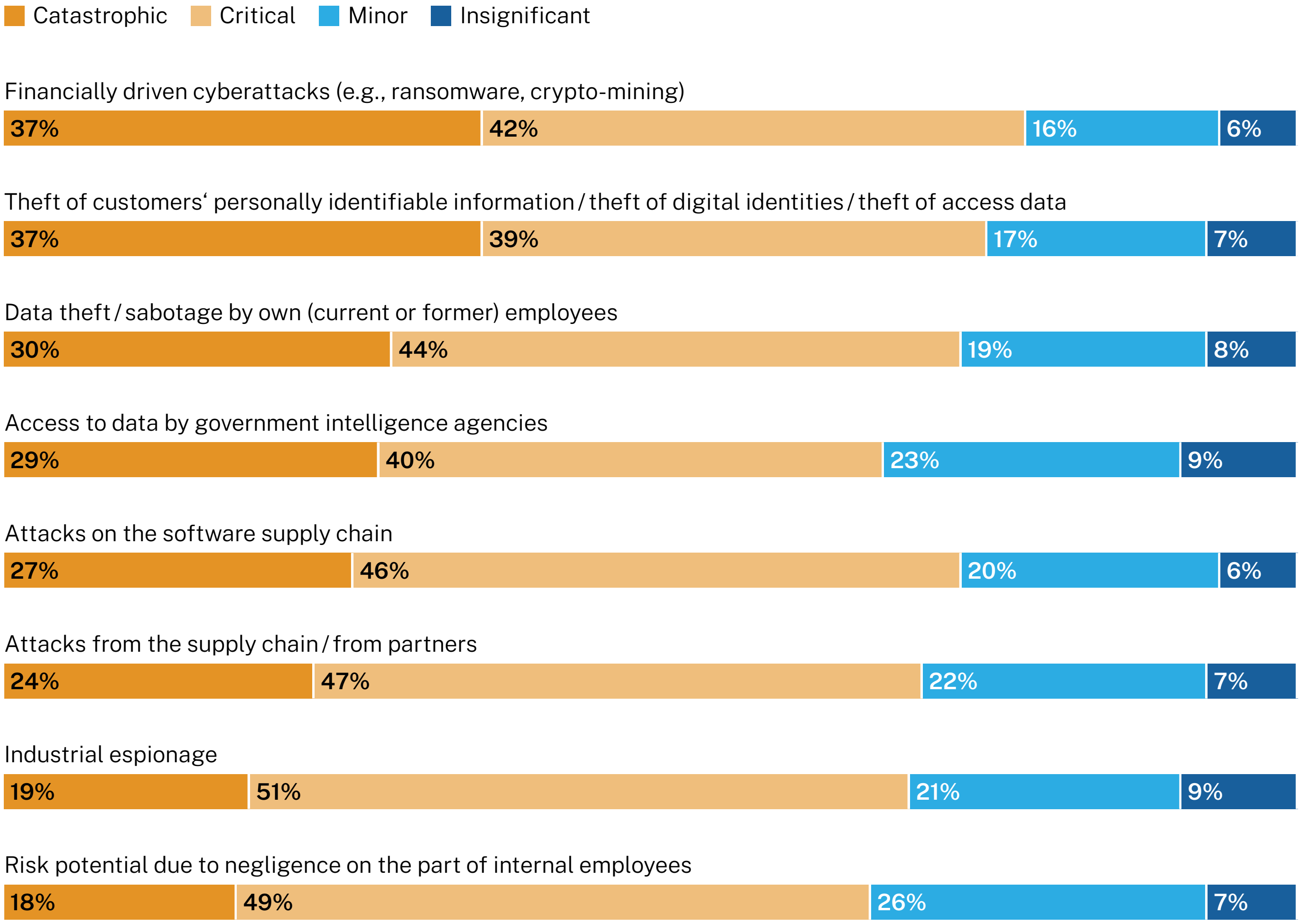
Financially driven attacks are most damaging.

Financially driven cyberattacks (such as ransomware) and identity theft are the most significant threats, considering both likelihood and potential impact.

For example, 62% perceive a financially driven attack as imminent whereas 60% deem identity theft likely in the next 12 months. More than one-third (37%) classify the impact of either of those threats as potentially catastrophic.

Interestingly, companies that rely more on the cloud perceive less risk of catastrophe. Among those with most of their IT services in the cloud, 71% classify theft of customer data or digital identities as potentially critical or catastrophic. For organizations with less than 30% of their data in the cloud, that number rose to 83%. Cloud users are likely more confident in their ability to recover data.

Threat scenarios and potential worst-case impact



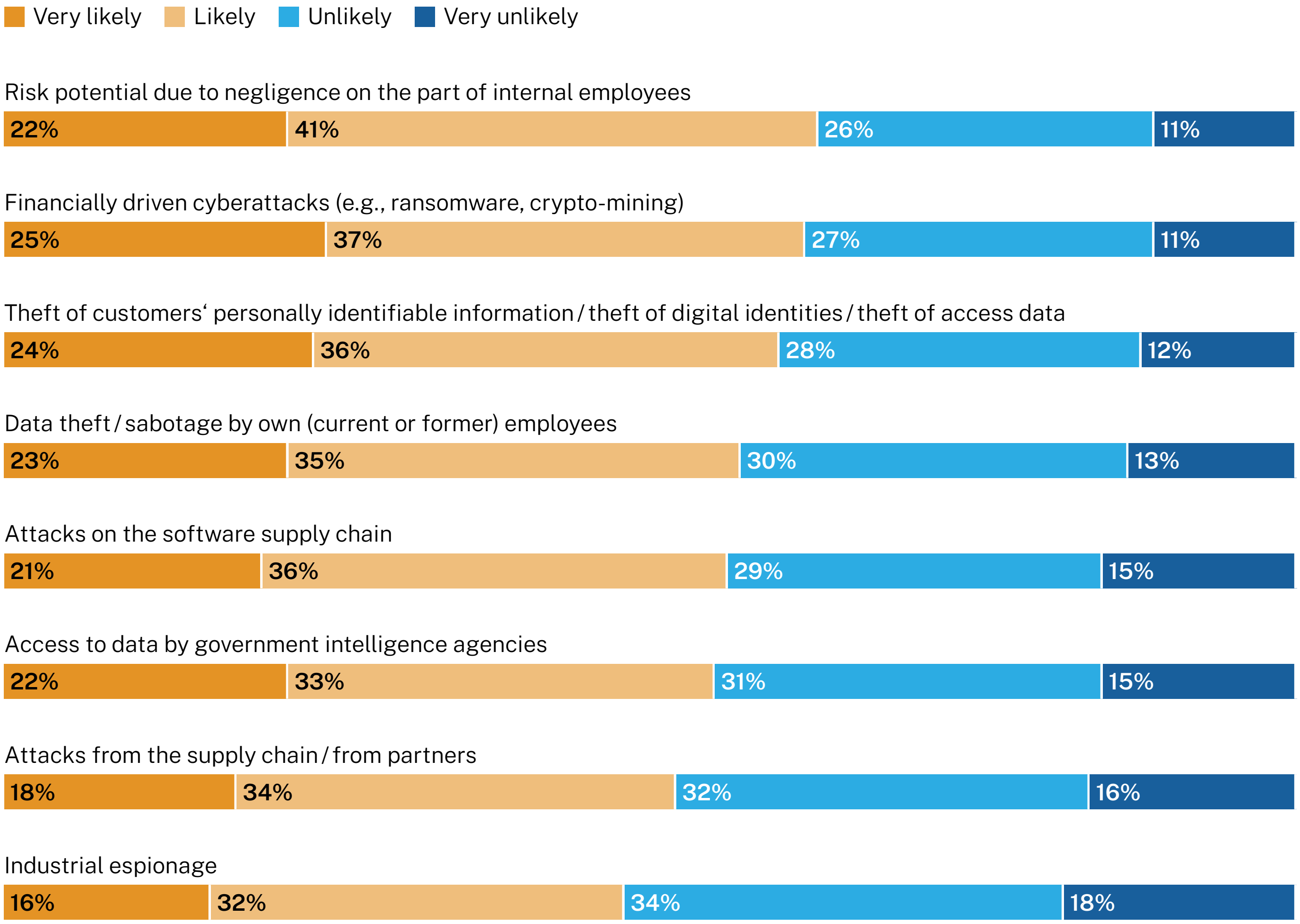
Totals may not equal 100% due to rounding.

Insider incidents are most expected, although potentially less damaging.

The old debate “Who’s more dangerous, insiders or outsiders?” is far from settled. Insiders are seen as the most likely cause of future incidents, with 63% of the respondents (71% in APAC) expecting that negligence by employees will increase risk over the next year. More than half (58%) also anticipate data theft or sabotage by current or former employees in the next 12 months. ▶

The rise in ransomware cases is likely driving an increase in cybersecurity insurance. The goal is to transfer some risk that existing security controls don’t or can’t adequately address. Among the survey respondents, 61% have invested in cybersecurity insurance.

Likelihood of cybersecurity incidents in the next 12 months



Totals may not equal 100% due to rounding.

However, the damage from insider incidents is typically less: Risk posed by insiders is more often perceived as critical (49%) rather than catastrophic (18%). By comparison, 37% see financially driven attacks or theft of PII as causing potentially catastrophic damage.

58%

Believe data theft or sabotage by current / former employees is likely in the next year.

These expectations of ongoing insider negligence or malice strongly suggest that training should play a stronger role in organizations' defensive posture — an issue examined in greater depth later in this report.

Organizations with more than 80% of their IT services in the cloud are twice as likely to have seen massive economic damage from a past event than other respondents (31% versus 14%). What we don't know is whether those organizations moved more IT services to the cloud *before* or *after* the damaging attack. One indication that a previous incident may have motivated IT teams to move to the cloud more aggressively: The organizations expecting the best outcomes going forward are those that are moving aggressively into the cloud.

Next Steps

Implement practices to decrease both the likelihood and impact of financially driven attacks such as ransomware. Bragdon recommends:

1. Deploying multifactor authentication (MFA) to reduce the risk of stolen credentials
2. Increasing the frequency of data backups to reduce the risk of compromised files or servers
3. Segment networks to reduce lateral movement when a breach does occur.

Key Finding #2

Budgets and policies evolve—with a few notable gaps

Spending is rising, but is it going to the right places?

Read On

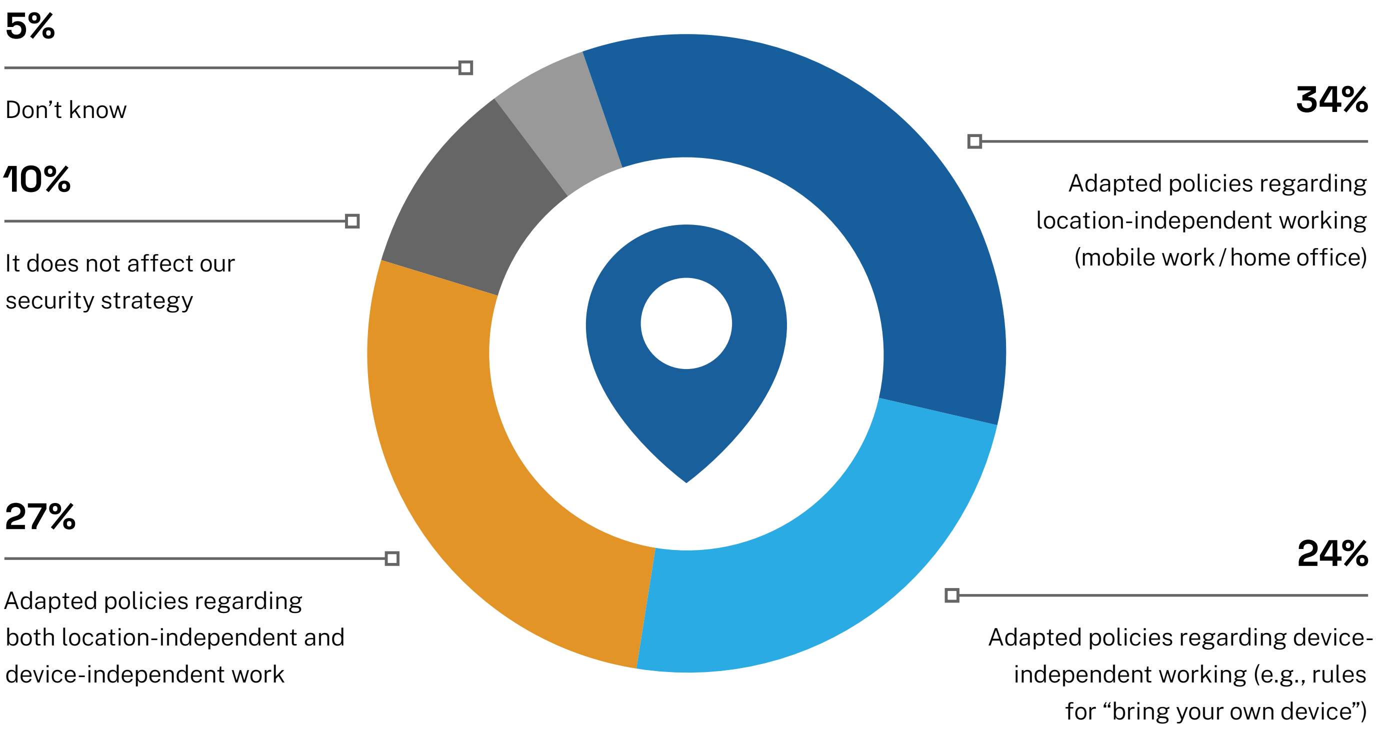
Given the breadth and complexity of the threat landscape, it's common practice for security investments and improvements to run the gamut across people, processes, and technology.

That mix had to be adjusted last year, with 85% of the survey respondents making security policy changes to accommodate new work-from-home models, which for many presented a newly increased attack surface.

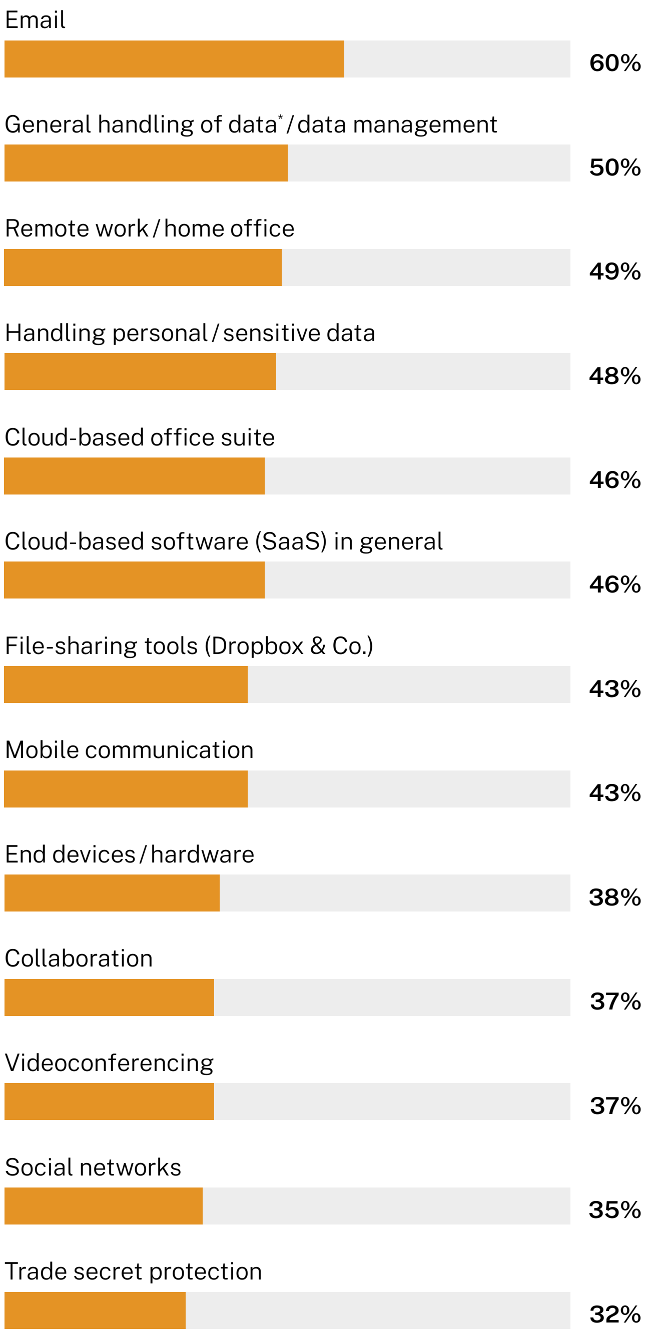
Respondents in the education (36%), financial services (31%), and business services (31%) sectors are the most likely to report that their organization has adopted policies regarding both location-and device-independent work. ▶

Improved endpoint protection is imperative in the world of the hybrid home / remote / office workforce. The proliferation of endpoint devices touching corporate networks, systems, and data is demanding a bigger proportion of the security team's attention. The top five areas of focus for respondents' endpoint protection are data loss prevention (DLP), threat hunting, endpoint detection / response, web filtering, and application whitelisting. Use of AI technology and behavioral analytics is also emerging in this space.

Impact of location-or device-dependent work on security strategy



Areas covered by IT security policy



*e.g., in office documents

Despite this increased emphasis on securely connecting the remote workforce, gaps remain. Although two-thirds of the surveyed organizations say email is covered by their IT security policy, fewer than half have defined policies specific to remote work and related activities that many organizations adopted en masse during the pandemic, including file sharing, use of endpoint devices, collaboration, and videoconferencing.

These are glaring omissions. Consider that Zoom, whose conferencing software became synonymous with team meetings, had to scramble early last year to fix several security gaps.

Bragdon isn't surprised that security teams are still playing catchup. Large organizations with complex IT architectures may have difficulty tracking everything that's deployed outside of the office — which makes it impossible to create consistent security policies that account for all use cases.

"I've asked really big businesses about what kind of visibility they have into what's happening at the endpoint, and they sort of just shrug," he says.

Emerging hybrid work arrangements may create even more complexity. Clearly, many details of securing remote work models still need to be worked out, from both the policy and technical perspectives. ▶

Most organizations will spend more on security in 2021.

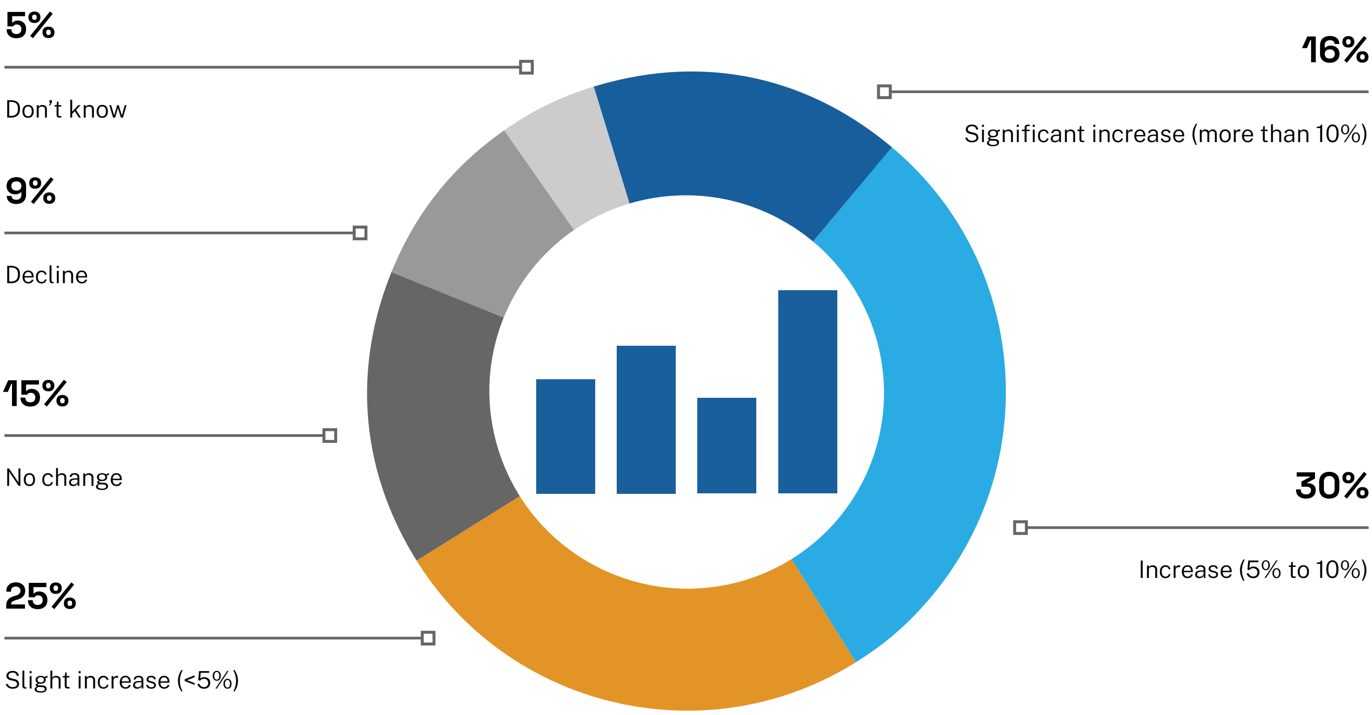
Seven in 10 companies expect their security budget to increase this year, with an average increase of 4% across all respondents. So who's spending? For starters, big companies with more resources.

Enterprise and midsize companies, at 74%, are more likely to report an increase in IT security budget than those with fewer than 500 employees (66%).

Companies in financial services (21%), transportation (21%), and technology (19%) are most likely to report an increase of more than 10% in their IT security budget in 2021.

Respondents in APAC (43%), Latin America (52%), and Africa (59%) are more likely than those in Europe / Middle East (28%) and U.S. / Canada (25%) to plan investments in data privacy over the next year, likely because legislation such as GDPR has already pushed European companies ahead in that area.

Expected YoY change in 2021 IT security budget



These are positive findings for security teams, with most companies committing to invest to improve their security posture. With so many organizations anticipating future attacks, this data suggests they are working to get out in front of the problem, taking action rather than just hoping for the best.

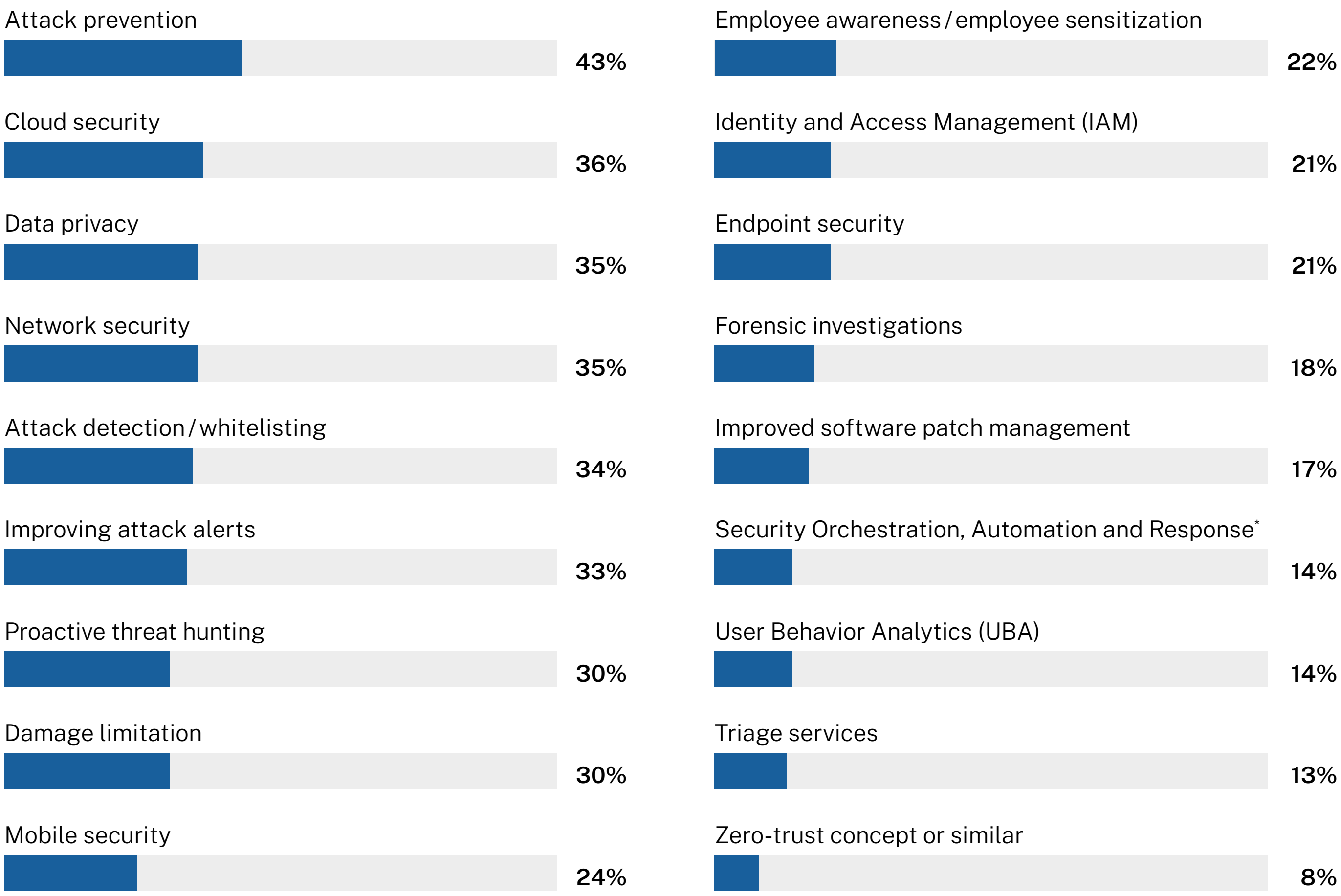
Proactive attack prevention is the top investment focus across the board, followed by cloud security, data privacy, and network security. However, investment priorities vary quite a bit by region, industry, and IT architecture.

Heavy cloud users (80% or more of IT services in the cloud), for example, are more likely to be investing in proactive threat hunting (45%), attack detection / whitelisting (40%), and improving attack alerts (36%). ▶

47%

of respondents in Latin America are investing in threat hunting, the most of any region.

Focus of cybersecurity investments, next 12 months



*(SOAR)

Security training: What's the holdup?

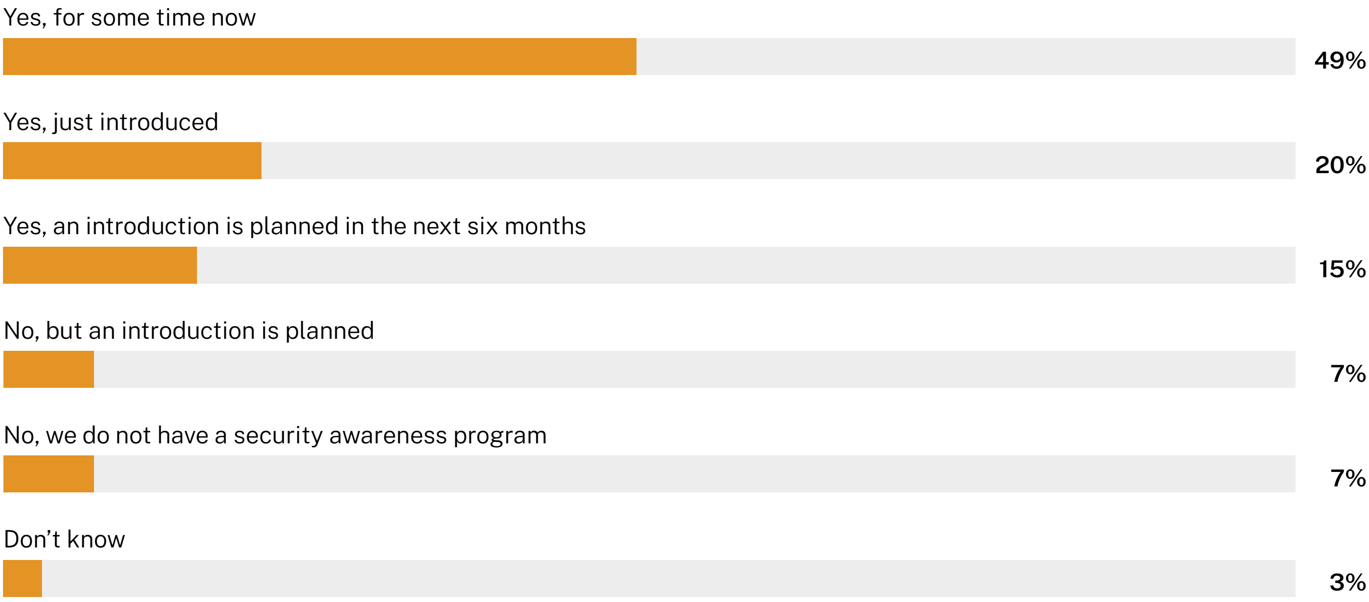
Despite the steady drumbeat around the importance of security training, it's still not ubiquitous. This is surprising, given the widespread anticipation of incidents caused by insiders, whether through negligence or malice.

Some leadership teams may not see the value of this training investment because it's impossible to eliminate insider risk completely. However, the survey shows that companies with training in place expect tangible payoffs in the form of reduced rates of espionage and other specific threats. ▸

Organizations with mandatory security training in place are less likely to expect incidents of:

- Industrial espionage (44%, versus 51% without training in place)
- Data theft / sabotage by own (former) employees (52% versus 62%)
- Theft of digital identities / theft of access data (57% versus 64%)

Does your company have mandatory IT security training or awareness programs for all users?



63%

expect risk potential to increase over the next 12 months because of employee negligence.

Noteworthy breakouts:

- Among the surveyed organizations, 29% have yet to roll out or have no plans to introduce mandatory security training programs for all employees.
- Those with most of their data (80% or more of IT services) in the cloud are more likely than others to report that they've required training for some time now (70%, versus 49% or less among other respondent segments).
- Those with a zero-trust model in place are more likely than others to report they've required training for some time now (54%, versus 40% or less among other respondents). ■

Employee awareness was No. 10 on the list of planned cybersecurity investments, with 22% citing it as a spending focus over the next 12 months.

Next Steps

Training is no magic wand — because there is no magic wand — but companies that provide security training for end users believe in its effectiveness. Look to strengthen awareness training, supported by technical controls or process improvements that reduce the chances of manual errors that, intentionally or not, increase risk.

Key Finding #3

Despite risks, cloud is a net positive for security

Take advantage of service provider features —while minding your own controls

Read On ∨

Cloud computing in all its forms represents a seismic shift for IT, and survey respondents report significant and growing usage.

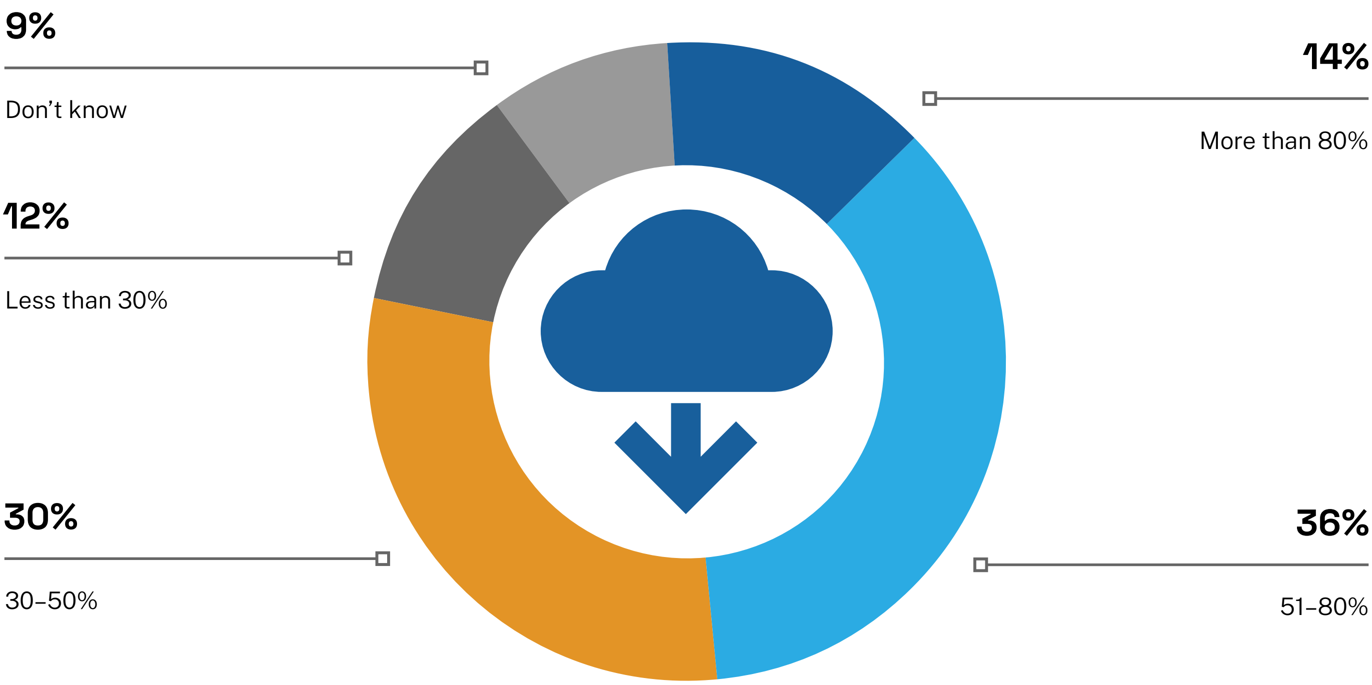
More than half of all IT services are now delivered via the cloud across the respondent base. Although organizations recognize that migrating data and infrastructure to the cloud opens or widens the attack surface, all indications are that the strengths outweigh the risks.

“Clouds are really good, homogeneous environments, and the providers are keyed into delivering good security,” says Bragdon.

Although cloud providers work continuously to improve their own security controls and extend those controls to customers, the rise of multicloud environments presents security teams with new challenges and risks. Visibility across multiple clouds is problematic, and integration points and disparate security tool sets present a new set of problems to solve for.

As the percentage of IT services in the cloud rises, so does the likelihood that a respondent’s company is using AI technology as part of its security defenses: 62% of the heavy cloud users, versus 14% of those with the lowest use of the cloud. AI and the cloud go hand-in-hand.

Share of IT services delivered via cloud

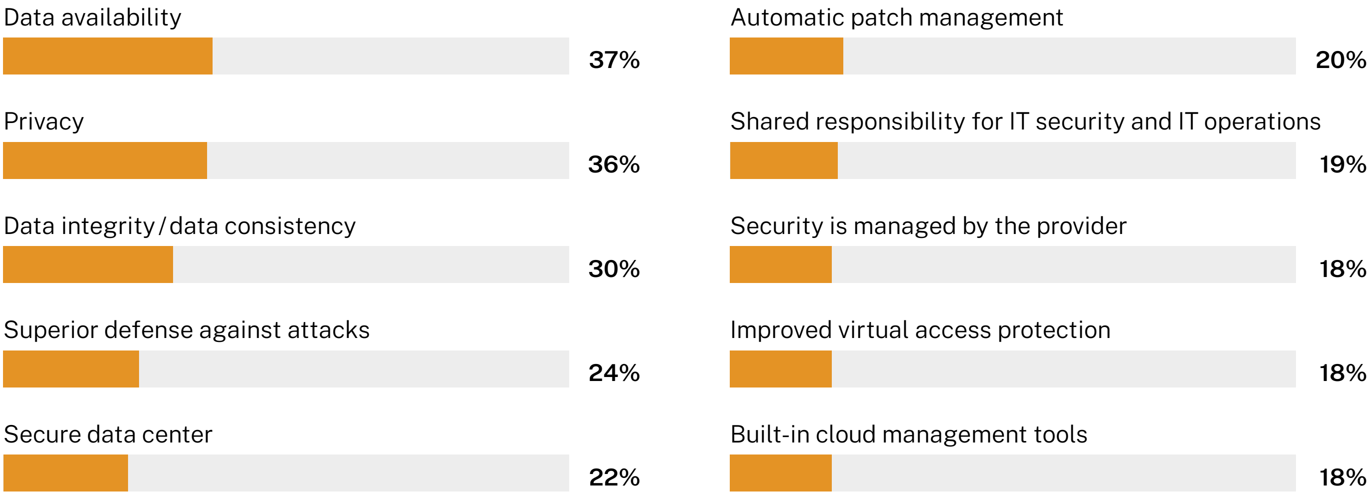


By now most IT and security leaders understand that cloud security is a shared responsibility for providers as well as their customers. The survey found significant differences, however, in perception of security advantages and risks in the cloud.

Three distinct security advantages emerged for cloud environments: improved data availability (37%), data privacy (36%), and data integrity / consistency (30%). Lower scores for other possible benefits indicate that many IT shops still believe they can do as well or better with on-premises systems and security.

Those with the most cloud experience (80% or more of IT services delivered via the cloud) are more likely to vouch for its security benefits. For example, 45% of the heavy cloud users see data integrity / data consistency as a benefit, and 42% view privacy as a positive, versus those with the lowest use of the cloud (24% citing each benefit).

Security advantages of cloud services vs. on-premises solutions



45%

of heavy cloud users view data integrity / consistency as a security benefit of the cloud.

Greater cloud usage does create some new concerns

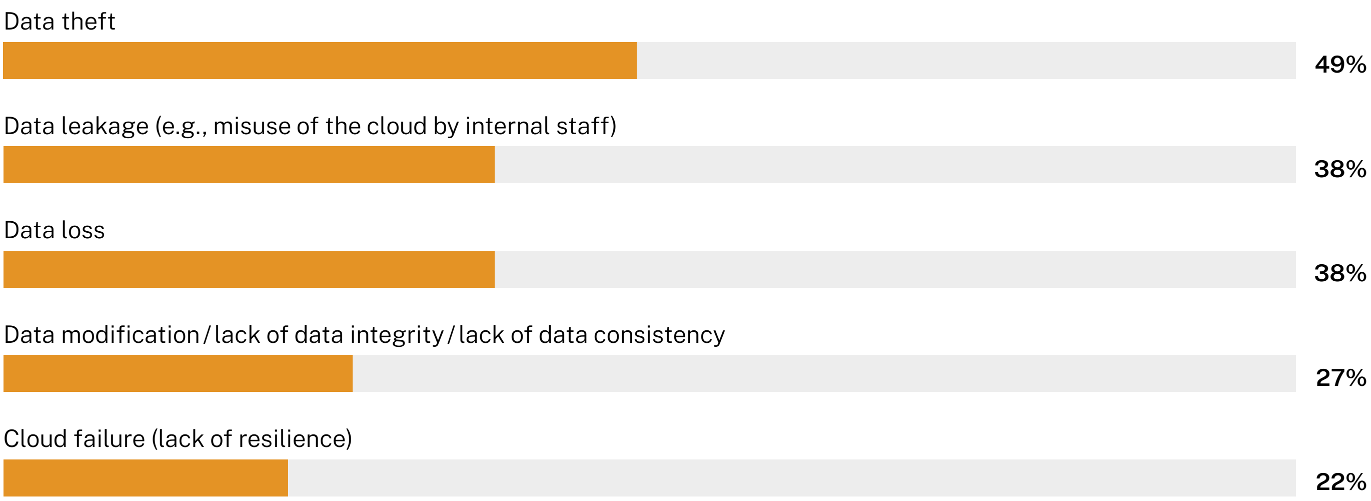
Despite the benefits, organizations still have concerns about cloud security, with data theft at the top of the list (49%). Improving password management is the top goal of technology investments related to cloud security (58%), showing further evidence of the great concern about stolen credentials and data theft.

Data theft is much more of a concern in Latin America (72%) and Africa (62%) than in other regions (43% in U.S. / Canada, 46% in Europe / Middle East, and 48% in APAC).

12%

Advanced persistent threats are more of a concern among respondents with IT security titles than among those in other roles, at 12%.

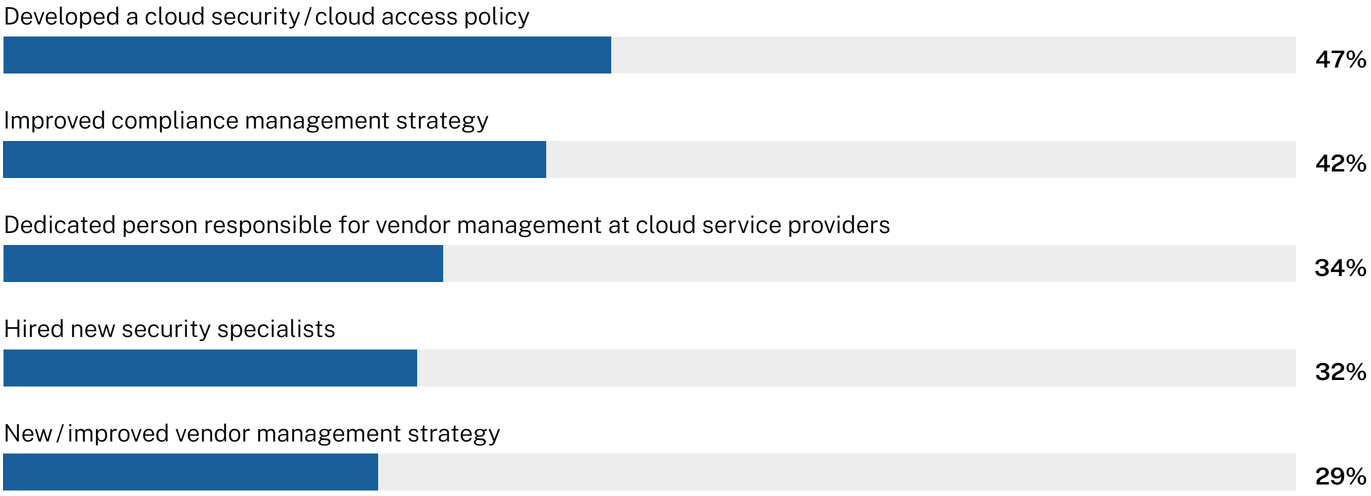
Top 5 perceived security risks associated with cloud services



Many heavy cloud users appear to have accelerated their security efforts in reaction to increasing incidents and / or damaging past attacks. Those with 80% or more of their IT services delivered in the cloud were more likely to report an increase in cybersecurity incidents in 2020, with 57% reporting an increase, versus 34% of the light cloud users. Heavy cloud users are also the most likely to report massive economic damage from a past cybersecurity event, at 31%, compared to 14% among the other respondents. ■

Cloud security is a shared responsibility between provider and customer. It's important to put a robust cloud security policy in place and support it with processes and personnel. Just 34% of organizations say they have a person dedicated to managing cloud service providers.

Top 5 precautions taken regarding cloud security



Next Steps

Top cloud providers typically offer an array of security controls and management options, but, as Bragdon notes, "Often the people negotiating the contract may not realize or care that their organization has access to all those tools." Make sure you review all cloud provider contracts and set up your cloud purchasing processes to take advantage of the available security features and functionality.

Key Finding #4

AI + zero trust is the new baseline

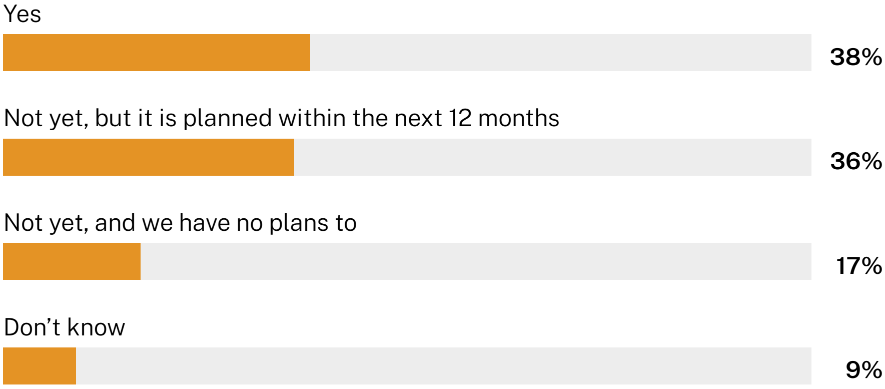
Emerging technologies and approaches will reduce the attack surface and improve detection and response

Read On

Rapid changes in a few areas, specifically AI and zero-trust security, indicate how businesses hope to hold the line against an increasing array of attacks.

AI and machine learning (ML) play increasingly vital roles in sifting through high volumes of data gathered from multiple sources to identify the most urgent threats. Deployment of AI for security purposes is expected to double this year, with respondents indicating that the cloud is the most common channel for accessing AI.

Use of AI technology as part of security defenses



It wasn’t long ago that CSOs were highly suspicious of the “AI” label’s being slapped on many security products. That skepticism was appropriate, Bragdon says.

“Ten years ago, I moderated panels at RSA where the experts were saying, ‘Machine learning is real today, but true AI is years away,’” he says.

Now products are maturing and cynicism is waning. More than one-third of the respondents (38%) use AI technology as part of security defenses today, and 36% plan to implement it in the coming year.

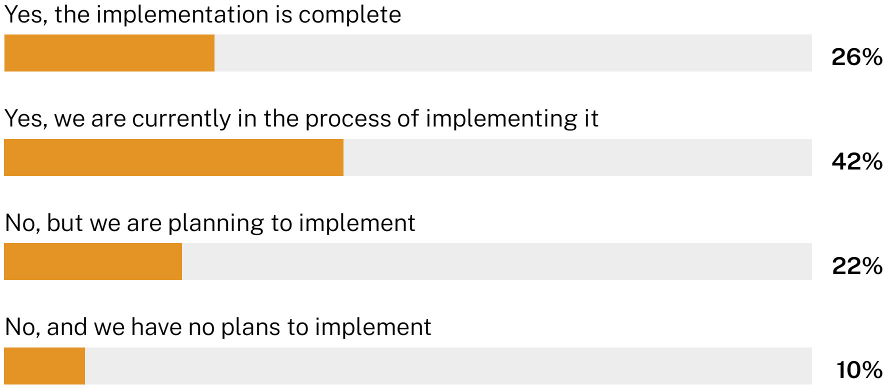
As the percentage of data in the cloud rises, so does the likelihood that a respondent’s company is using AI technology as part of security defenses: 62% of those with 80% or more of their IT services in the cloud, versus 14% of the lighter cloud users. This signals that cloud providers are integrating AI / ML-based services into their offerings and also that on-premises infrastructures could fall farther behind in this increasingly important part of the defensive arsenal.

Zero trust and identity: What's real and what's not?

As with AI, many organizations indicated that they are wading into zero trust. However, it's not clear where incremental investment is going to support this move, as key aspects associated with zero trust, such as identity and access management (IAM), did not emerge as spending priorities.

Zero-trust adoption among respondents is impressive, with 68% saying they have already adopted or are currently deploying a zero-trust model.

Implementation of a Zero Trust Model



These results continue the trajectory found in prior IDG research. In the 2020 Security Priorities study, for example, 35% of the respondents said they had deployed or were piloting zero-trust technologies and another 40% said they were actively researching the zero-trust model.

However, the data on where specific tech investment dollars are being spent raises some questions about how respondents are approaching zero trust. ▸

Among security spending plans, these categories align most closely with a zero-trust model:

- Network security (35%)
- Identity and access management (21%)
- Endpoint security (21%)
- Zero-trust concept or similar (8%)

Organizations with a security operations center (SOC) are far more likely to have implemented a zero-trust model, at 74%, compared to 30% at organizations that have no SOC.

82%

of heavy cloud users have implemented a zero-trust model.

Oddly, a zero-trust-explicit investment focus ranks very low, cited by just 8% of the respondents. IAM (a foundational zero-trust element) and endpoint protection (encompassing all those untrusted work-from-home devices) are spending priorities for just 21% of the respondents.

By comparison, network segmentation is another zero-trust principle, and network security emerged as a top-four spending priority.

Can 42% of the respondents really be "currently in the process of implementing" zero trust with so little incremental spending planned for these areas? A positive interpretation would be that organizations already have foundational pieces of zero trust well in hand. Potentially more worrisome is that companies are relabeling old efforts as "zero trust" without substantially changing their security architecture.

Bragdon leans toward the positive take. "Companies have invested heavily in IAM over the past years," he says. "They've already got some of those basic pieces in place." For example, 69% of the respondents are using MFA, which has gained significant traction as a core component of identity-based security.

Zero-trust interest is strongest among the respondents that use cloud services. Heavy cloud users (80% of IT services or more in the cloud) are the most likely to have completed implementation of a zero-trust model, at 82%. Among the organizations with less than 30% of their data in the cloud, 35% have deployed zero trust. ■

! Next Steps

It's time to jump on the AI/ML bandwagon. "There's just no way for people to keep up with the scale of data you need to monitor," says Bragdon. "Let the machines help spot the anomalies so your people can focus their time where it's really needed." Cloud services are the fastest route to AI.

Looking Forward

The pandemic has showed emphatically that trying to predict every curveball the universe might throw at us is a fool's errand.

But a few lines seem clear. Attacks will continue to escalate. Ransomware in particular will carry the banner for financially motivated incidents, at least until it becomes less effective. To combat this, organizations will keep shifting to the cloud, building zero-trust security models, and applying AI.

Although AI uptake is proceeding rapidly, it's important not to deploy the technologies in a vacuum: Only about one-third of the respondents are combining AI with SOC-style continuous monitoring and mandatory security training — despite a strong perception of reduced risk for those that institute this mix of tactics.

The survey findings also suggest there's more work to be done to fill some security holes that, left unaddressed, may dramatically increase risk. Zero-trust architectures are incomplete or, in some cases, too loosely defined. And remote-workforce policies and controls seem underdeveloped. Collaboration tools deserve closer scrutiny, especially if they operate outside the reach of some DLP controls.

In the end, it's encouraging that leadership teams are putting more money toward security, with the goal of making the business safe and resilient without restricting the agility, connectivity, and collaboration that today's organizations require.

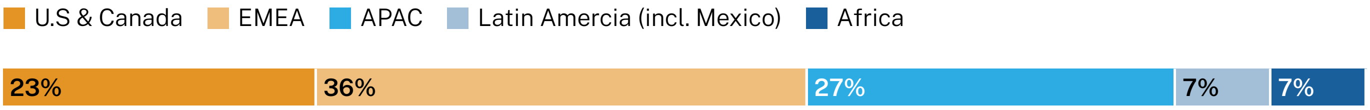
"They realize it's not about trying to eliminate the risk," Bragdon says. "No security is ever perfect. While you keep improving your preventive measures, you also have to build resilience into the business, catch incidents earlier, and contain the impact. You want to be able to take a punch and continue to operate at full speed." ■

"No security is ever perfect. While you keep improving your preventive measures, you also have to build resilience into the business, catch incidents earlier, and contain the impact."

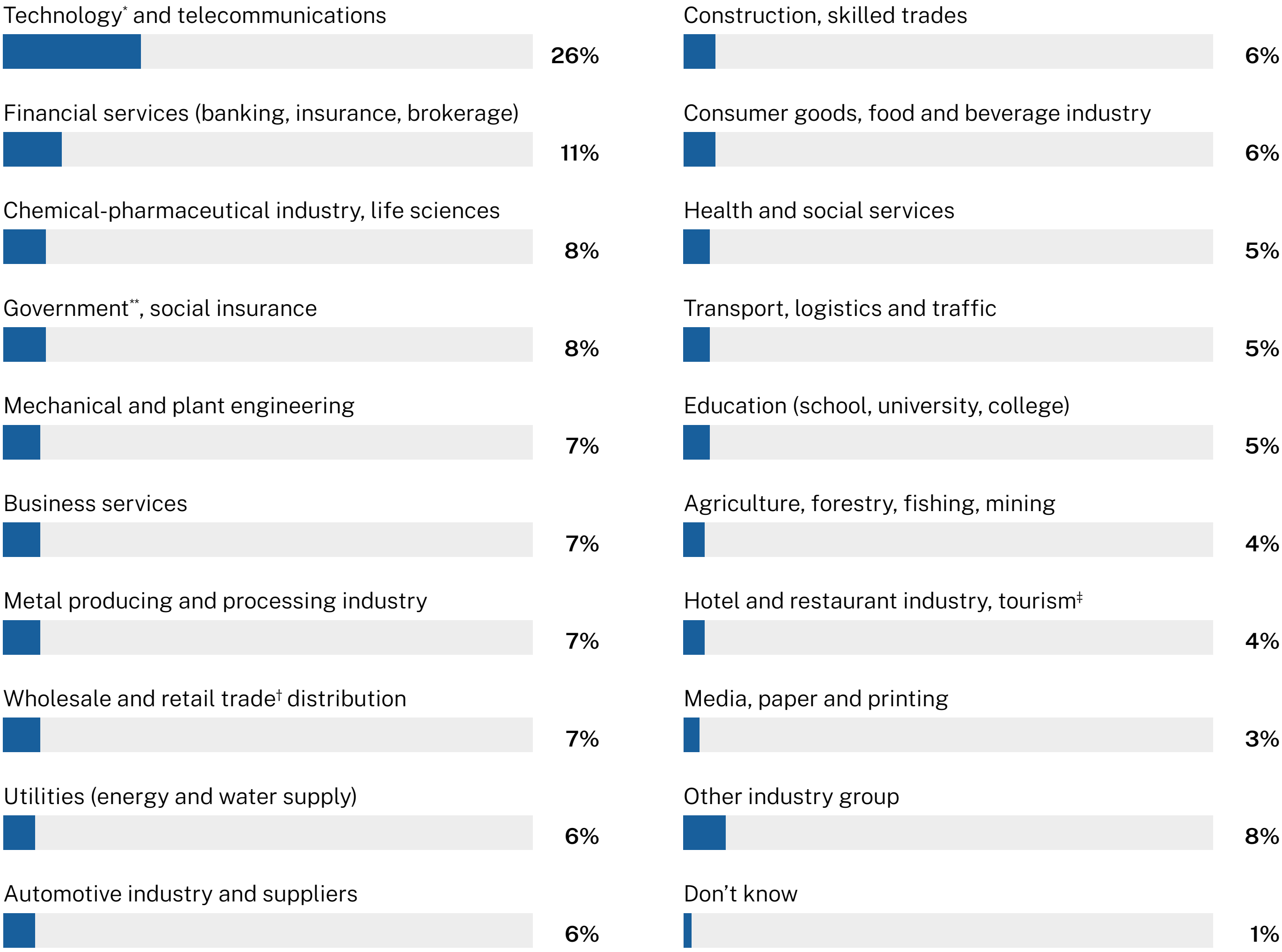
Survey Methodology

IDG's Global Intelligence Report on Cybersecurity was conducted to understand cybersecurity risk, challenges, policies, practices, and investments worldwide. Data was collected via a 26-question online survey in May and June 2021. There were 2,741 respondents in IT, security, and line-of-business positions across industries and around the world.

Global representation

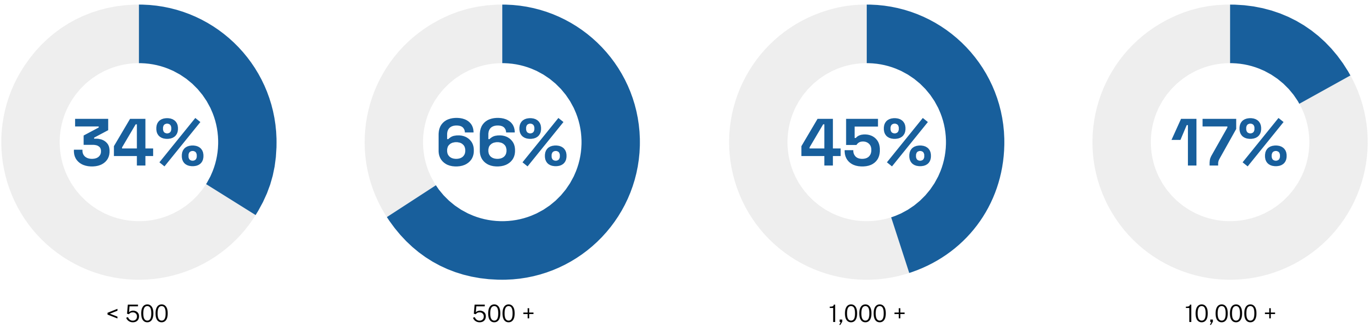


Industry

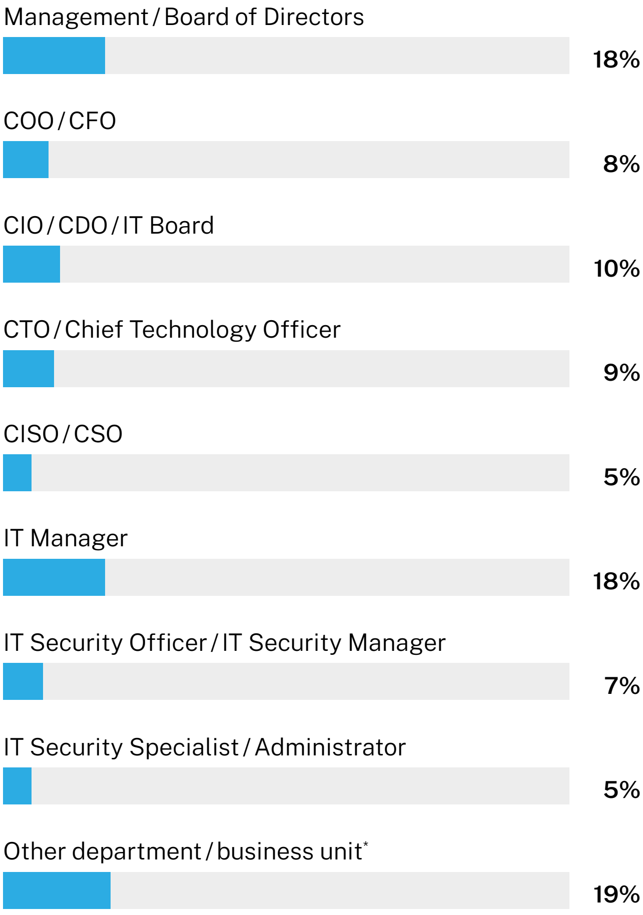


*Hardware, software, electronics ** Federal and state or local † Incl. online trade ‡ Incl. cruise lines, theme parks, casinos

Company size overview

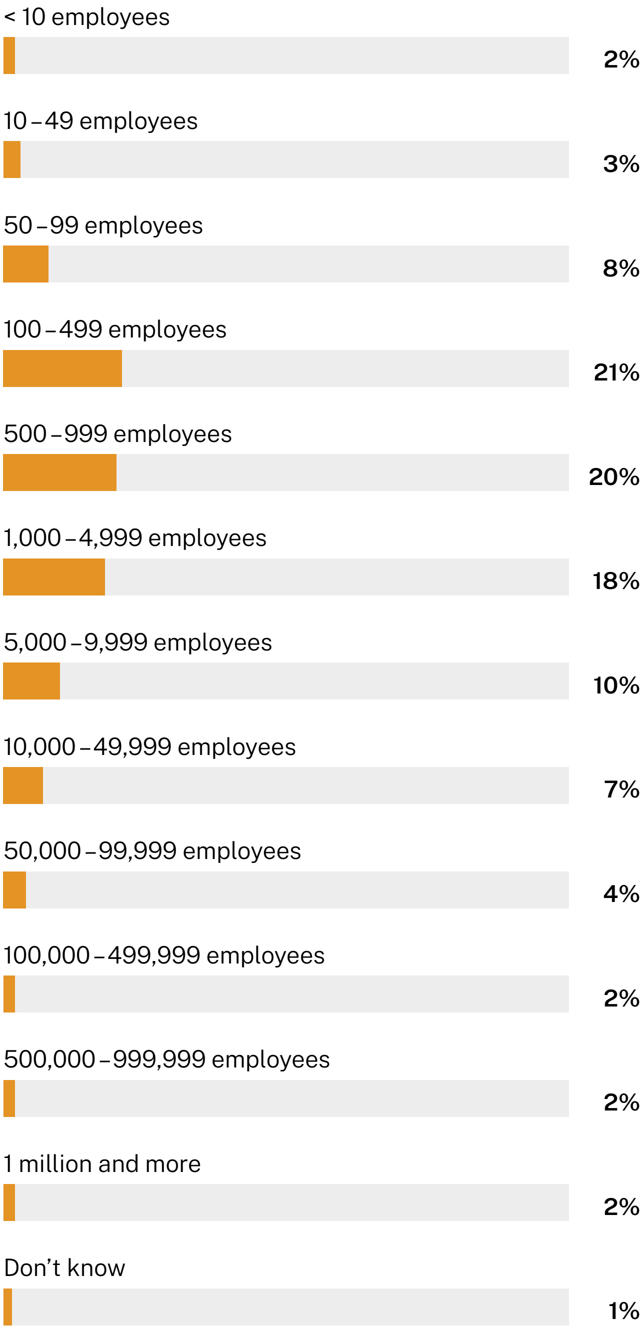


Role



*Sales, research, production, logistics, etc.

Company size



More prevention is a better cure

Adding preventative methods to existing reactionary tactics will improve your security posture.

The cybersecurity news portrays a growing and sophisticated opponent that strikes larger and more technologically advanced organizations with ease. CNA Financial, one of the largest cybersecurity insurers, paid a $40 million ransom, guaranteeing the attacks escalate. Kaseya and SolarWinds are elements of the cyber infrastructure that organizations trust for their security. If Kaseya and SolarWinds are unable to protect themselves from cyber intrusion, how can they secure their customers?

> **“If Kaseya and SolarWinds are unable to protect themselves from cyber intrusion, how can they secure their customers?”**

In the last five years, cybersecurity veered in an odd direction toward reaction and network surveillance instead of prevention. This study by IDG, sponsored by PC Matic, measures if organizations are migrating to a balance between reaction and prevention.

The study quantifies the adoption of preventative elements such as multi-factor authentication (MFA), cybersecurity training, application whitelisting (AWL), and employer-issued passwords relative to reactive methods such as endpoint detect and respond (EDR / XDR), security operations center (SOC), heuristics, threat hunting, and web filtering.

The survey found the No. 1 cybersecurity method is the SOC at 82% of respondent organizations. MFA enjoys close to 70% ▶

adoption across the world, led by high-tech companies and the financial services industry. This result is surprising given the number of recent breaches, perhaps because the study did not cover the degree to which MFA has been deployed — for example, if an organization had MFA for RDP but not for email.

Cybersecurity training is deployed in almost 70% of respondent organizations. This is great news, although cybersecurity training is less effective than other methods due to employee retention of the concepts.

If one method could be considered a panacea for ransomware, it would be AWL, an architecture that strictly allows good applications and rejects unknown applications like ransomware. Organizations employ this technology roughly at half the rate of MFA at 35%. Organizations still trust reactive technologies such as web filtering, threat hunting, and EDR / XDR more than AWL.

Trailing the prevention pack is organization-issued passwords at about 20%. It's a shame because employees are notoriously bad at choosing passwords and frequently use the same passwords at work and home. Hopefully, this simple method will get traction in the future.

SOC, MFA, and cybersecurity training are widely deployed. Other preventative methods such as AWL and organization-issued passwords are under-deployed compared to reactive measures. The best cybersecurity posture is a blend of reaction and prevention, and this study demonstrates urgent room for improvement. ■

Rob Cheng, CEO, PC Matic

Learn how organizations of all sizes are preventing ransomware with the only automated global whitelist for zero-trust cybersecurity.

Founded in 1999, PC Matic is an American cybersecurity software solution provider headquartered in Myrtle Beach, S.C. PC Matic operates remotely with employees across the United States and was originally established with the sole purpose of creating a better way to diagnose common computer problems.

As cyber threats began to evolve, PC Matic developed a holistic approach to cybersecurity — rooted in application whitelisting — widely considered the gold standard for endpoint protection and recommended by CISA, NIST, NSA, FBI, and more.

PC Matic's patented technology provides users with a cost effective and efficient way to deploy default-deny endpoint security that enhances the zero trust model, fills potential gaps left by traditional endpoint security software solutions, and provides an additional layer of protection. The PC Matic platform also features remote monitoring and management capabilities, fileless malware detection, and RDP port protection from brute-force attacks.

Create a strong and secure technology foundation

At OneNeck, we understand how difficult it is to balance the strategic responsibility of technological innovation against the need for daily operational excellence as demanded by the business. Our customers are IT leaders that are expected to juggle everything — a constant balancing act, which requires time, focus and often, additional resources. But to move forward, they need the confidence that specialized help from a skilled partner well-equipped to execute can bring — one with just the right blend of business and technology expertise.

By helping our customers create a strong and secure technology foundation, we can relieve some of the pressure due to 'transformation and modernization' overload. We understand how to navigate and manage the complexity of a hybrid IT environment, including on-premise and multi-cloud, freeing overworked IT leaders and critical staff to focus on both new and existing capabilities integral to the growth and evolution of their business.

Through advanced engineering and security best practices, we help our customers stabilize and protect their IT environments, navigate a path to IT modernization and take full advantage of new and innovative technologies in the cloud to achieve strong business growth and performance. OneNeck customers span multiple industries including healthcare, manufacturing, financial services, retail and government. ▶

"We can relieve some of the pressure due to 'transformation and modernization' overload."

They choose OneNeck because of our outstanding service and availability, our responsiveness and attention to detail, our calm and steady presence, and our personal and collaborative approach to service and support.

"Our security services include framework assessments, risk analysis and customized vCISO services."

In a world where our customers are under constant attack, our security services include framework assessments, risk analysis and customized vCISO services that analyze risk and lay the groundwork for comprehensive security strategies. We help prioritize and plan security roadmaps that are actionable and integrate across the broader IT strategy. Additionally, we help prevent, detect and respond to security threats with 24x7 response services ranging from EDR, MDR, boundary control and incident response.

OneNeck's diverse and experienced engineering team leverages ITIL based practices to manage mission-critical data centers, cloud and customer infrastructure 24/7/365. In addition, OneNeck has successfully completed SSAE 18 examinations, PCI Data Security Standard validation, ISO/IEC 27001:2013 certification validation, and HIPAA and HITECH examinations. This helps assure customers that their data is secure, available and meets their compliance requirements. ■

OneNeck IT Solutions is a wholly owned subsidiary of Telephone and Data Systems, Inc. and employs nearly 500 people throughout the U.S. OneNeck offers multi-cloud solutions, combined with managed services, professional IT services, hardware and local connectivity via top-tier data centers in Arizona, Colorado, Iowa, Minnesota, Oregon and Wisconsin. OneNeck's team of technology professionals deliver secure, modern platforms and applications for organizations embracing data-driven transformation and secure end-to-end solutions. Visit: oneneck.com

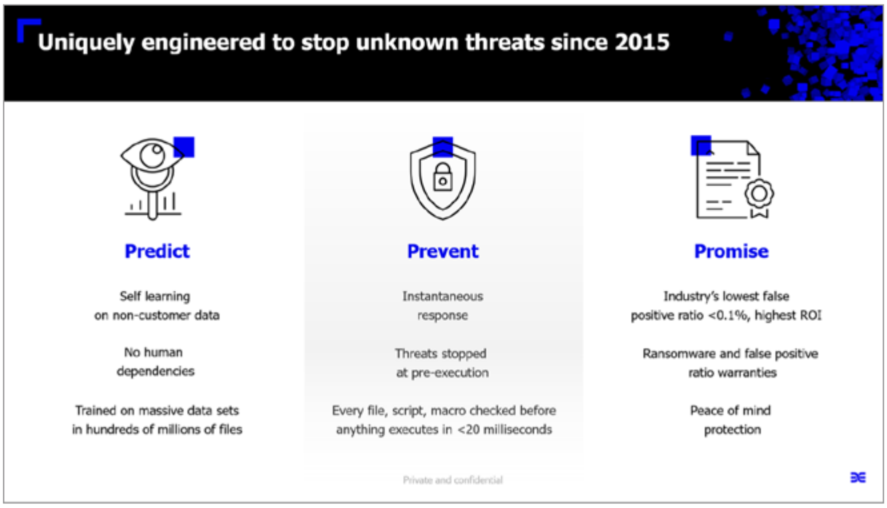
OneNeck's parent company, Telephone and Data Systems, Inc. [NYSE: TDS], a Fortune 1000® company, provides wireless; cable and wireline broadband, TV and voice; and hosted and managed services. TDS has approximately six million connections nationwide through its businesses U.S. Cellular, TDS Telecom, OneNeck IT Solutions LLC and TDS Broadband Service. Recently, TDS has been named to three Forbes lists: America's Best Employers for Diversity, Best Large Employers, and Best Employers for Women. Founded in 1969 and headquartered in Chicago, TDS employs 9,400 people. Visit: tdsinc.com

Elevate your security posture—guaranteed!

Deep Instinct is the first and only cybersecurity company to leverage a deep learning-based neutral network that learns and improves dynamically as it's fed more data. The result: we predict security risks others can't see and prevent threats pre-execution, 10 times faster than real-time, before damage is done.

We're so confident in our approach that we promise to stop 100% of ransomware and back that up with an industry-leading $3M warranty. We take that a step further by also offering a low false-positive guarantee of <.01%.

"We predict security risks others can't see."



Uniquely engineered to stop unknown threats since 2015

Predict

Self learning on non-customer data

No human dependencies

Trained on massive data sets in hundreds of millions of files

Prevent

Instantaneous response

Threats stopped at pre-execution

Every file, script, macro checked before anything executes in <20 milliseconds

Promise

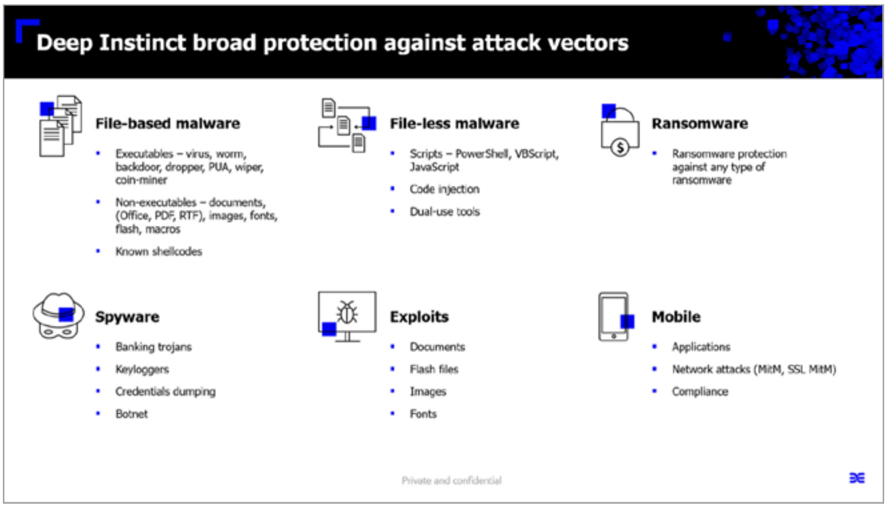
Industry's lowest false positive ratio <0.1%, highest ROI

Ransomware and false positive ratio warranties

Peace of mind protection

Private and confidential

> “The Deep Instinct advantage extends beyond just total threat protection.”



Deep Instinct broad protection against attack vectors

File-based malware

- Executables – virus, worm, backdoor, dropper, PUA, wiper, coin-miner
- Non-executables – documents, (Office, PDF, RTF), images, fonts, flash, macros
- Known shellcodes

File-less malware

- Scripts – PowerShell, VBScript, JavaScript
- Code injection
- Dual-use tools

Ransomware

- Ransomware protection against any type of ransomware

Spyware

- Banking trojans
- Keyloggers
- Credentials dumping
- Botnet

Exploits

- Documents
- Flash files
- Images
- Fonts

Mobile

- Applications
- Network attacks (MitM, SSL MitM)
- Compliance

Private and confidential

The Cybersecurity Conundrum

As the universe of threats grows in stealth and complexity, organizations are deploying machine learning (ML)-based solutions that either protect too much — flooding your team with false positives — or lack the power and precision to predict and prevent unknown, zero-day threats. Current EPP and EDR solutions alone are not enough to combat the sophisticated attacks of today.

Supercharge Your SOC

The Deep Instinct advantage extends beyond just total threat protection. The accuracy provided by our deep-learning approach means that your highly-skilled, highly-specialized security operators spend less time responding to and managing false positives, and more time focusing on the security threats that matter. Our technology makes your team smarter, faster, and more agile. ■

Deep Instinct is the most sophisticated solution for threat prevention on the market today.

- We predict security risks others can’t see.
- We prevent threats that others can’t stop.
- We promise by backing it up with a guarantee.

Regardless of your existing security posture you need Deep Instinct too.
Learn more at: deepinstinct.com