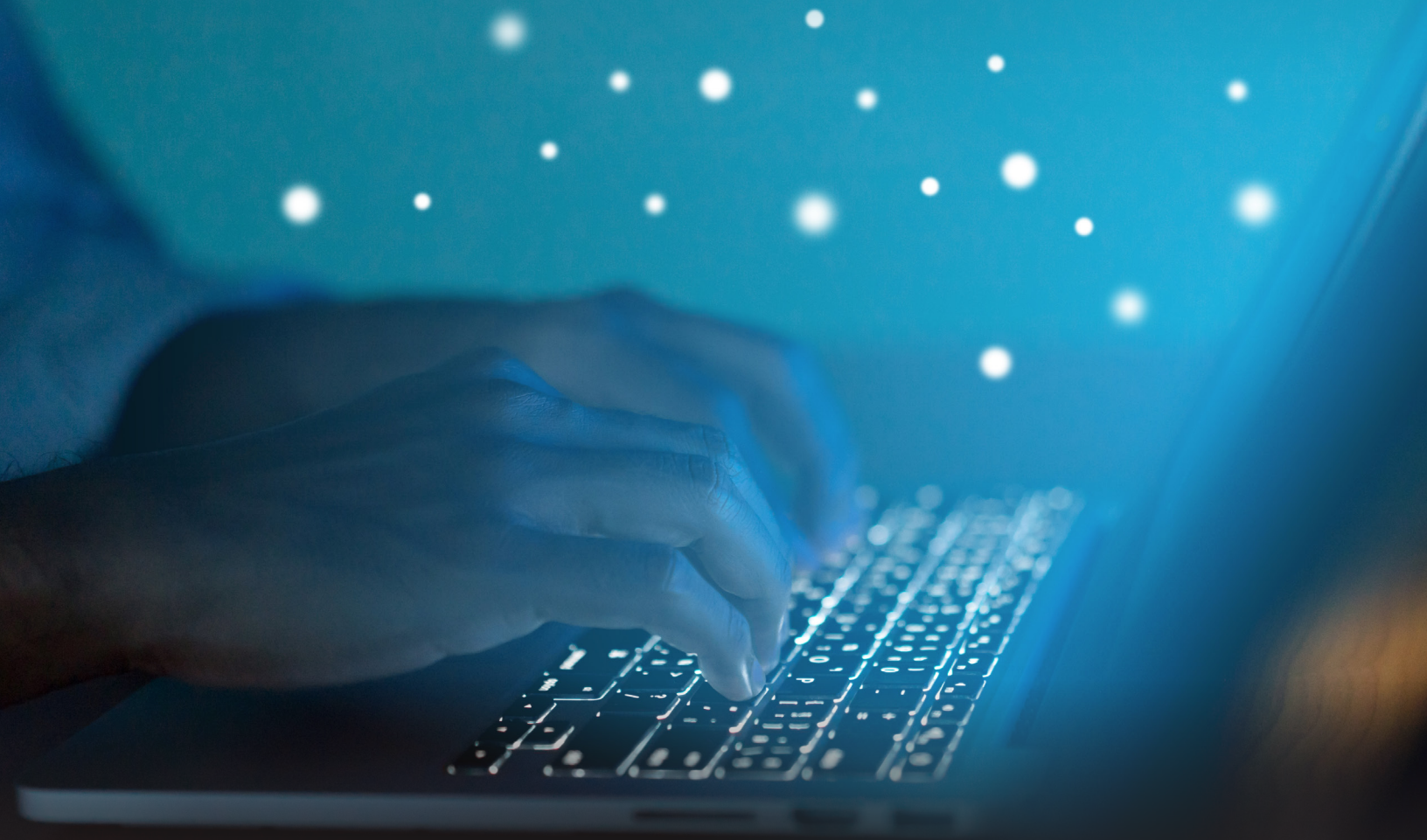
2020 SURVEY RESULTS

Using Identity and Access Governance to Mitigate Data Breach Risks



ISMG INFORMATION SECURITY MEDIA GROUP

SailPoint

Nick Holland
Director, Editorial

Using Identity and Access Governance to Mitigate Data Breach Risks

While nearly three-quarters of cybersecurity professionals would grade their organization's ability to identify and mitigate a cyberattack as above average or superior, nearly half have been subject to a spear-phishing attack and a third have suffered a malware incident in the last year. Further, over half of security professionals state that one of their biggest challenges is identifying which users and identities pose the greatest risk to their organization.

These are some of the findings of a recent survey on **Using Identity and Access Governance to Mitigate Data Breach Risks**.

This survey, sponsored by SailPoint, aims to investigate data breach risks associated with remote workers and how identity management can play a key role in threat mitigation.

In this report showcasing new research findings, you'll discover:

- Where the biggest gaps in identity management are today;
- Recent attacks and their impacts on organizations;
- Where today's organizations are focusing their investments on identity management for the coming year.

Among some of the key findings:

- Nearly three-quarters of survey participants report that their organization's ability to identify and mitigate a cyberattack is superior or above average. Twenty-one percent consider their organization is average, and just 6% consider their organization to be below average.
- Over half of survey respondents consider managing the growth in user types, applications, cloud platforms and data due to digital transformation efforts as the greatest challenge in maintaining cybersecurity across their organization.
- Nearly half of all organizations have been subject to spear-phishing attacks within the last 12 months.
- The majority of workers (61%) have access to between 6 and 15 applications in the workplace, although 15% have access to 16 or more.
- The greatest concern pertaining to identity management for security professionals is identifying which users and or identities pose the greatest risk.

Read on for full survey results, as well as expert analysis on how to put this information to use to improve your organization's ability to manage identity and access governance and data breach risks.

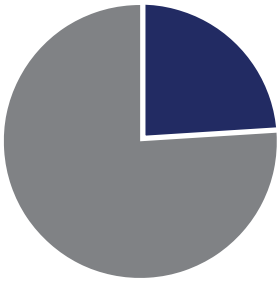
Best,

Nick Holland
Director, Editorial
Information Security Media Group
nholland@ismg.io

The survey, conducted in Summer 2020, generated more than 100 responses from cybersecurity professionals. Participating companies were those with 1,000 or more employees.

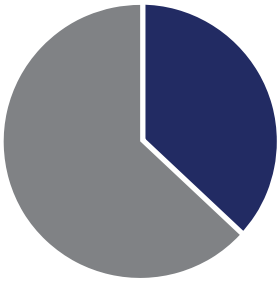
By the Numbers

Some statistics that jump out from this study:



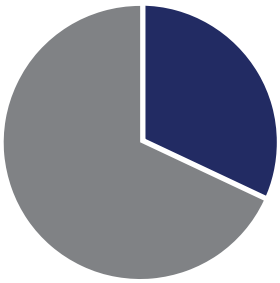
24%

of survey participants state that they have downgraded or adapted access policies to maintain operational functionality for remote employees since the COVID-19 pandemic.



37%

of survey participants state that employee credentials were compromised from a cyber incident within the past 12 months.



32%

of survey participants state that they have poor visibility into the number of applications and services that their organization is using.

Using Identity and Access Governance to Mitigate Data Breach Risks

This research showcases four key areas:

- The State of Cybersecurity Today
- The State of Identity and Access Policy
- Challenges of the Remote Workforce
- Cybersecurity Tools and Investment

The State of Cybersecurity Today

Survey results show that there is a high level of confidence among security professionals that they are managing cybersecurity risk effectively. Further, they are confident that company executives understand the necessary investment in cybersecurity tools and that employees have the ability to detect and mitigate risk.

- 73% of survey participants rate their organization's ability to identify and mitigate a cyberattack as above average or superior.
- 72% of survey participants are confident or very confident that C-level executives understand the necessary investment in cybersecurity tools to deal with evolving threats.
- 62% of survey participants are confident or very confident in their employees' ability to detect and mitigate cybersecurity threats.

The pervasiveness of cyberattacks, however, contradicts this confidence:

- 48% of respondents state that their organization has been a victim of a spear-phishing attack in the last 12 months.
- 33% state that they had been subject to a malware incident.

The State of Identity and Access Policy

Respondents are largely confident that their access policies are current and that their cybersecurity solutions can support these policies and goals.

- 71% are confident or very confident that access policies across their organization are current.
- 58% are confident or very confident that their organization's current security solutions can support cybersecurity policies and goals.

However, it appears that many are still experiencing challenges when it comes to ensuring their identity programs stay up to date with new evolving threats. Top challenges include difficulty identifying which users and identities pose the greatest risk, poor management of accounts, inconsistent access policies across business units and limited visibility into user access across the organization.

Challenges of the Remote Workforce

A comprehensive identity and access management strategy is essential for every organization. With the rapid shift to a highly remote workforce, this need is magnified. While respondents expect some workers to return to an office environment within 18 months, they still expect many workers will continue to work at home.

Top challenges in dealing with the increase in remote workers include balancing the need for security and operational functionality for remote workers (59%), educating and training employees on secure remote workplace policies and procedures (56%), and the use of personal devices and unsecured home networks for conducting company business (50%).

Of some concern: A quarter of respondents state that they have had to downgrade or adapt access policies to maintain operational functionality for remote workers.

Cybersecurity Tools and Investment

The top reason for investment in cybersecurity tools is risk reduction, with over three-quarters of respondents citing this as most important. Other significant motivators for investment include improved user and IT productivity/operational efficiency and improved compliance.

The key to managing this challenging environment will be connecting the dots between disparate systems and using automation to reduce the burden of identity management and governance on IT and security teams.

“Finding risk that is hidden and hard to spot with human eyes is key. This can be done with an AI-driven identity solution that can comb through the vast amount of identity information and surface the risky access that needs attention and remediation. IT and security teams can use their identity governance solution to also automate the provisioning of access and know that access is only granted if it adheres to the policies that have been set.”

"Finding risk that is hidden and hard to spot with human eyes is key. This can be done with an AI-driven identity solution that can comb through the vast amount of identity information and surface the risky access that needs attention and remediation. IT and security teams can use their identity governance solution to automate the provisioning of access and know that access is only granted if it adheres to the policies that have been set."

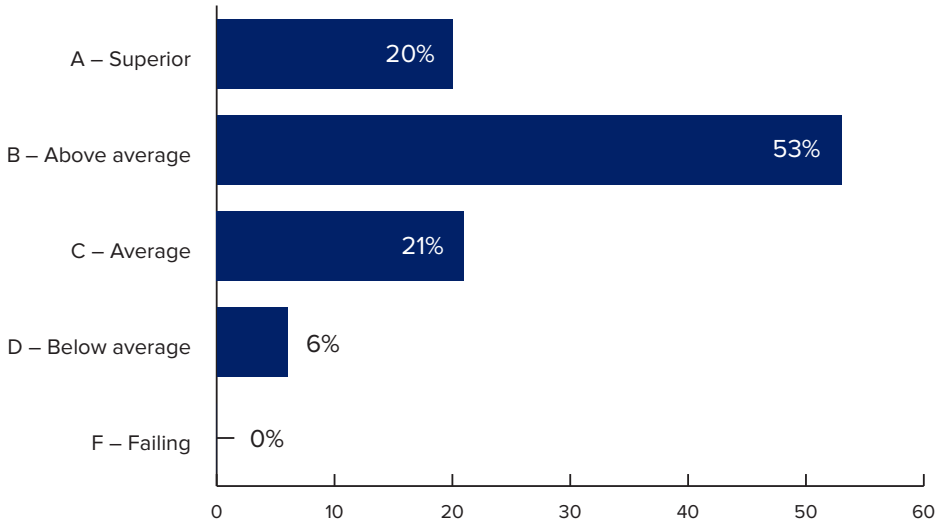
The State of Cybersecurity Today

This report begins by discussing organizational challenges that cybersecurity professionals are facing today. Among the takeaways:

- Seventy-three percent of security professionals grade their organization's ability to identify and mitigate a cyberattack as above average or superior. Yet...
- Nearly half of organizations have been the victim of a spear-phishing attack in the last 12 months.

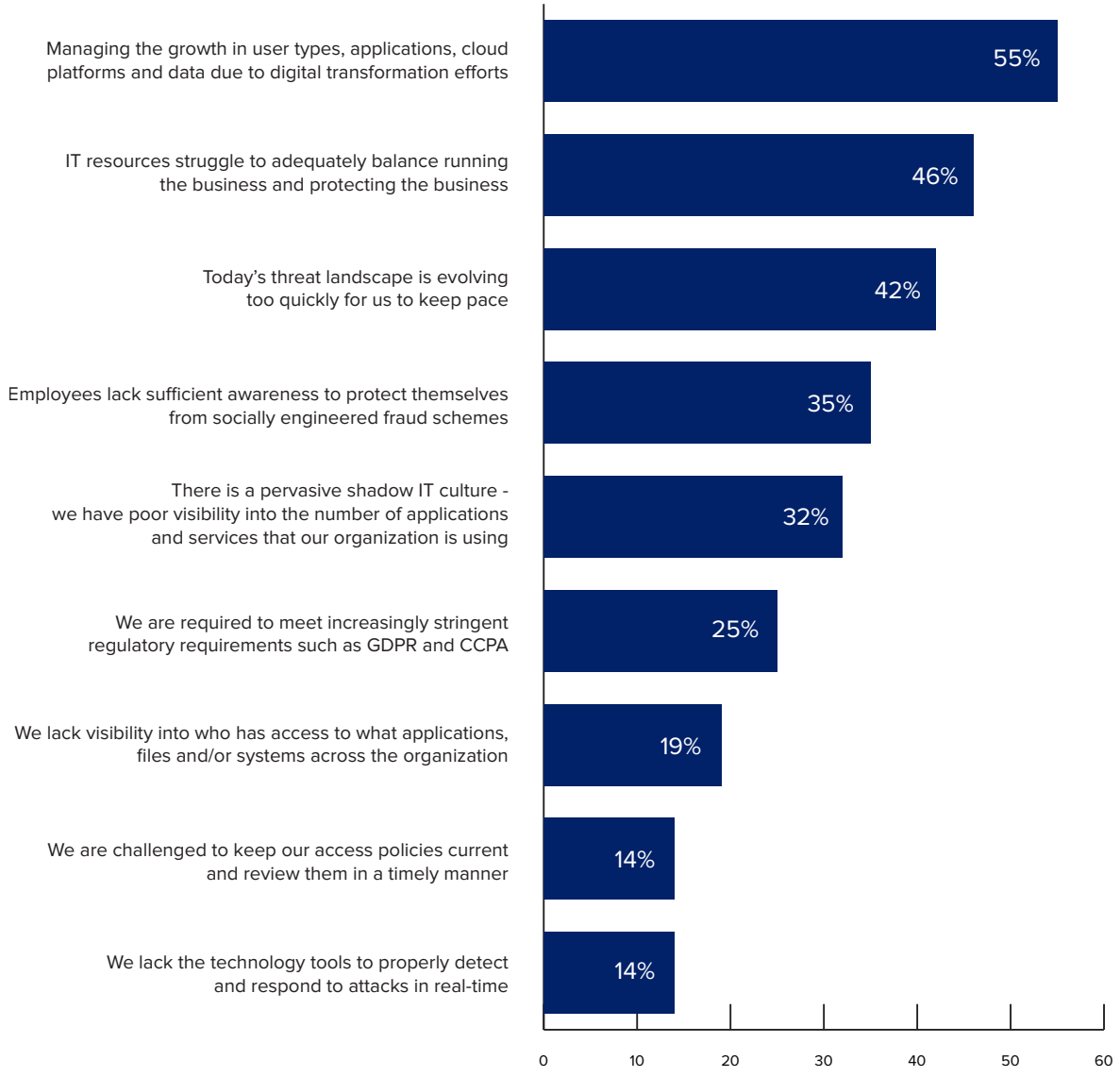
Complete results are below.

What grade would you give your organization's ability to identify and mitigate a cyberattack?



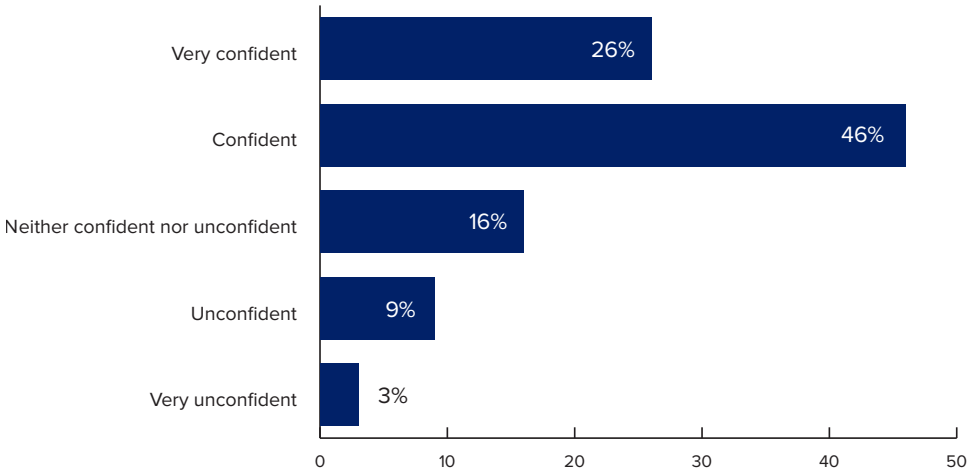
Nearly three-quarters of survey participants say their organization's ability to identify and mitigate a cyberattack is superior or above average, while 21% give their organization a ranking of "average" and just 6% consider their organization to be below average.

What do you believe are the top three challenges in maintaining cybersecurity across your organization?



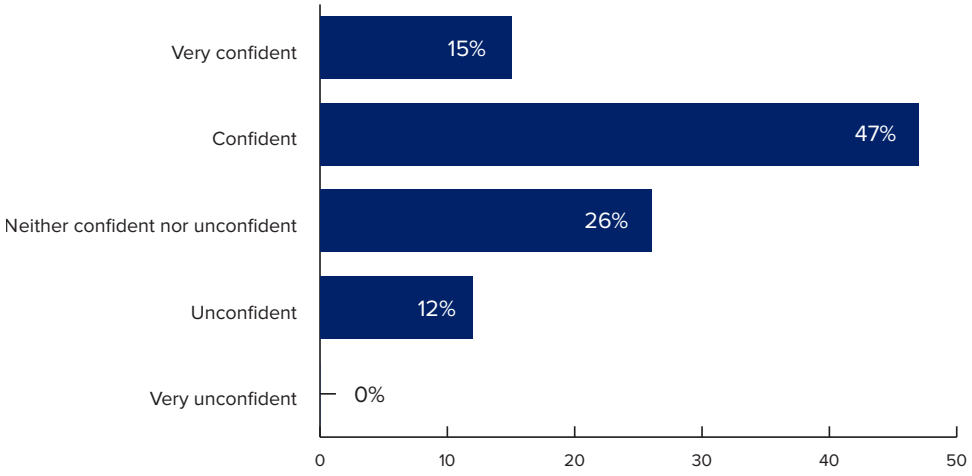
Survey participants were asked what the three greatest challenges were in maintaining cybersecurity across their organization. The greatest concern is managing the growth in user types, applications, cloud platforms and data due to digital transformation efforts. Over half of participants consider this to be one of the greatest challenges. Other areas of significant concern include IT resources struggling to adequately balance running the business and protecting the business (46%), the rapidly evolving threat landscape (42%) and employees lacking sufficient awareness to protect themselves from socially engineered fraud schemes (35%).

What degree of confidence do you have that C-level executives and/or the board of directors in your organization understand the necessary investment in cybersecurity tools to deal with the evolving threat landscape?



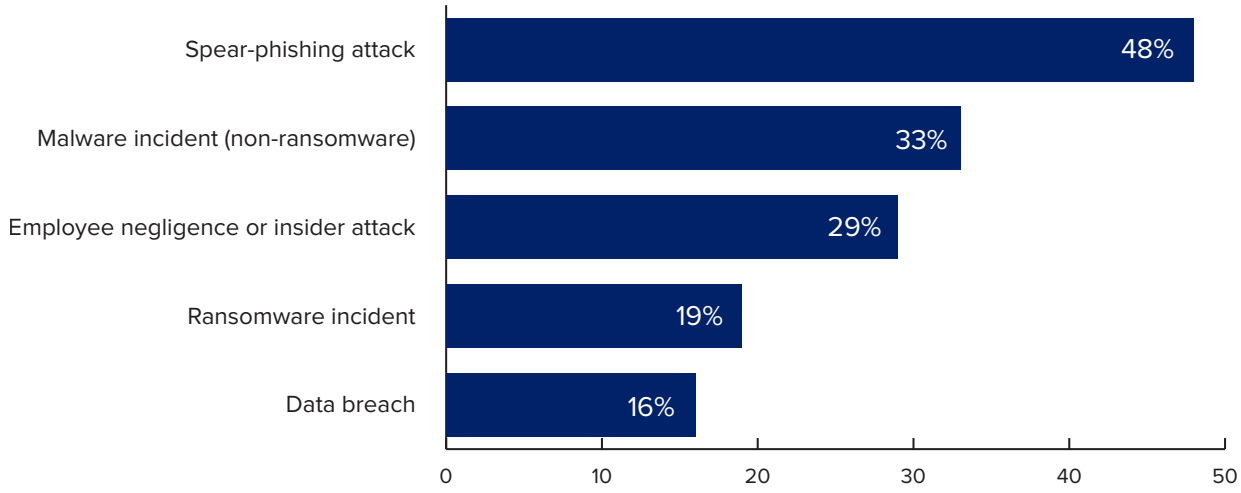
Survey participants were largely confident that C-level executives and/or the board of directors understand the requirements for investment in cybersecurity tools to deal with evolving threats. Nearly 75% of respondents are confident or very confident that senior executives and board members understand the need for cybersecurity investment, with just 12% stating that they are unconfident or very unconfident.

How would you rate your employees' ability to detect and mitigate cybersecurity threats?



While the majority of survey participants are confident or very confident that their employees are able to detect and mitigate cybersecurity threats, a significant percentage (26%) are neither confident nor unconfident, indicating some ambivalence among cybersecurity professionals on the level of faith that they have in employees being able to deal with inbound threats. Some 12% state that they are unconfident in their employees' ability to detect and mitigate cybersecurity threats.

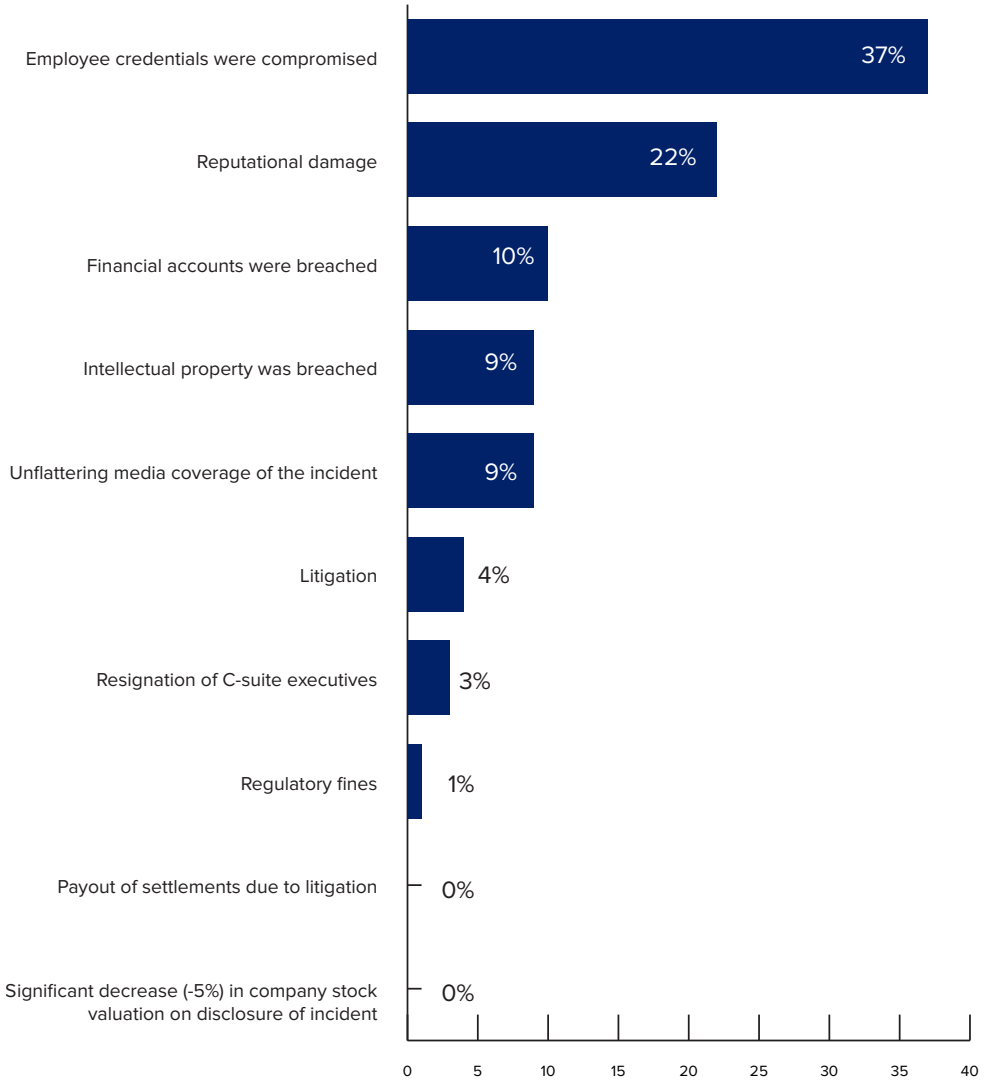
Has your organization been the victim of any of the following in the past 12 months?



Nearly half of all organizations have been subject to spear-phishing attacks within the last 12 months. Other forms of prevalent cyberattacks include malware incidents (33%), employee negligence or insider attacks (29%), ransomware incidents (19%) and data breaches (16%).

Nearly half of organizations have been subject to a spear-phishing attack within the last 12 months.

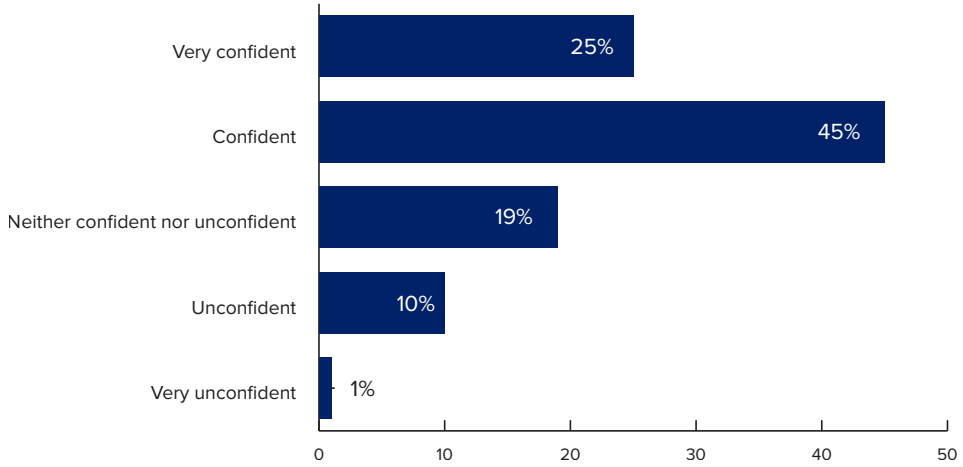
If you answered the previous question, what business impacts did your organization experience as a result? (check all that apply)



Drilling down on the answers from the previous question, survey participants were asked for details on the business impact they experienced as a result of an incident that occurred within the last 12 months. Some 37% state that employee credentials were compromised, 22% say they experienced reputational damage to their organization, 10% say they had financial accounts breached, 9% state they had intellectual property breached and a further 9% indicate that they had unflattering media coverage as a result of the incident. Three percent even stated that they had C-level executives resign as a result.

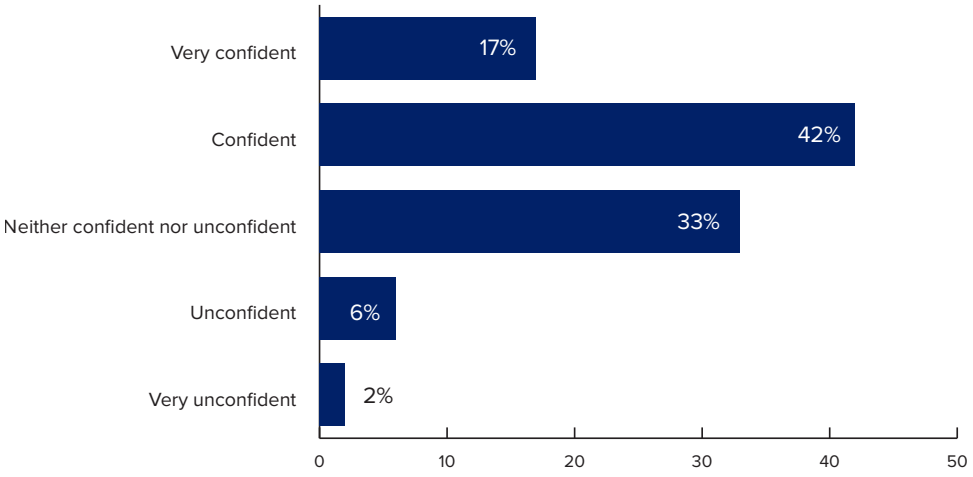
The State of Identity and Access Policy

How confident are you that access policies across your organization are current?



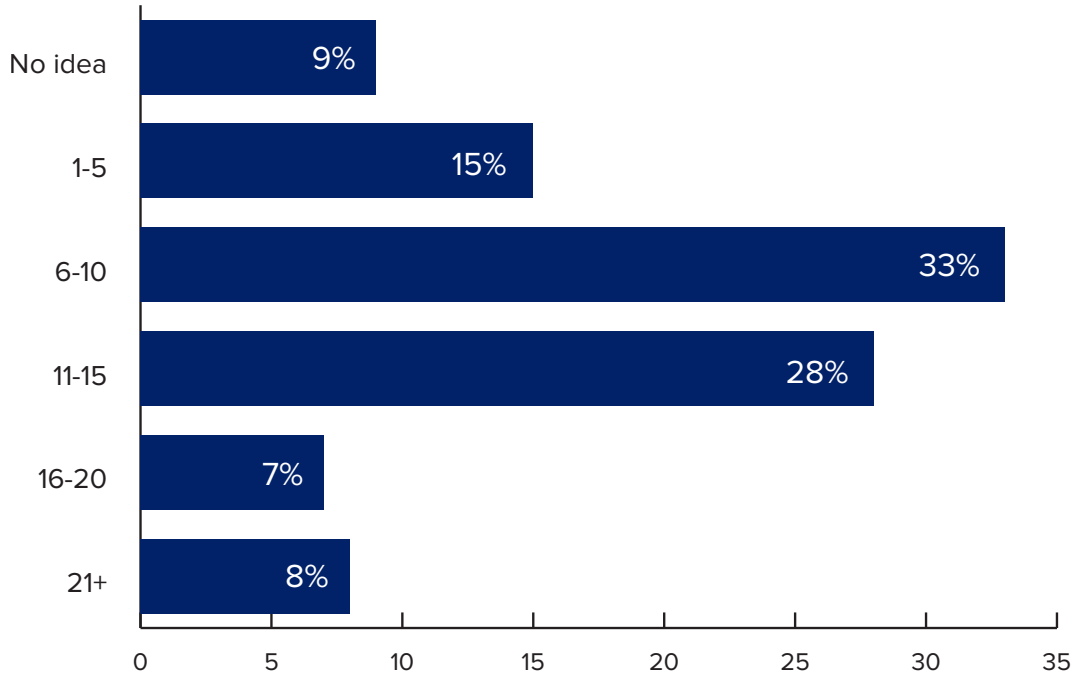
Security practitioners are largely confident that access policies across their organizations are current. Some 70% of survey participants are confident or very confident that this is the case. Nineteen percent are neither confident nor unconfident, and just 10% are unconfident.

How confident are you that your organization's current security solutions can support your cybersecurity policies and goals?



Survey participants are also confident that their organization's current security solutions can support cybersecurity policies and goals. Some 59% of respondents are confident or very confident, with a third being neither confident nor unconfident. Just 6% were unconfident, with 2% being very unconfident.

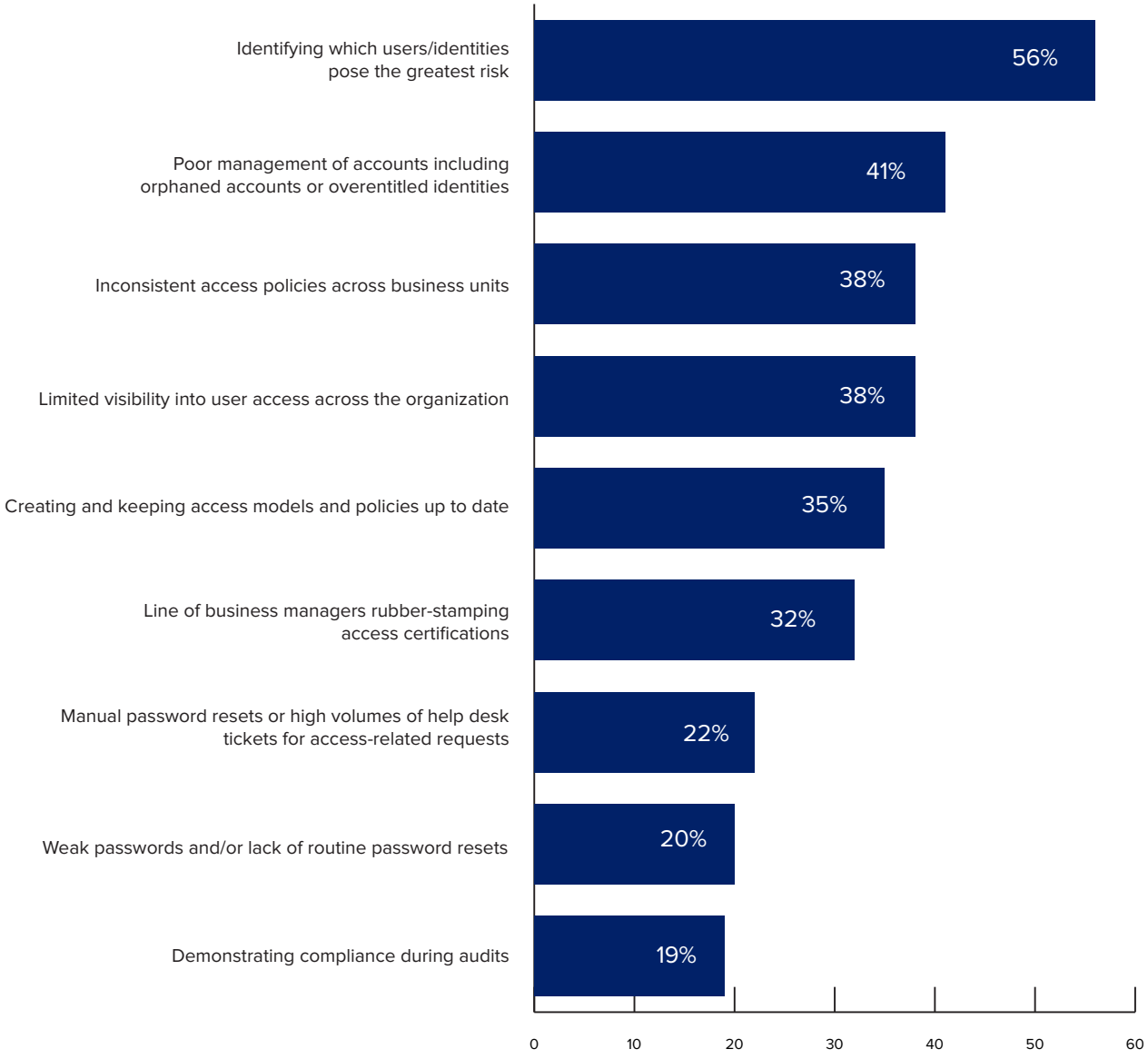
On average, how many different applications does a typical worker have access to?



The majority of workers (61%) have access to between 6 and 15 different applications in the workplace, according to responses, although 15% have access to 16 or more. Of some concern, 9% of survey participants state that they have no idea how many different applications a typical worker can access.

The majority of workers have access to between 6 and 15 applications in the workplace.

What are the top three challenges or risks you are currently facing with managing identities?



The greatest concern pertaining to identity management for security professionals is identifying which users and/or identities pose the greatest risk. Some 56% of survey participants identified this as one of the top three challenges they are facing in identity management. Another significant issue (41%) is poor management of accounts including orphaned accounts and over entitled identities, inconsistent access policies across business units (38%), limited visibility into user access across the organization (38%) and creating and keeping access models into policies up to date (35%).

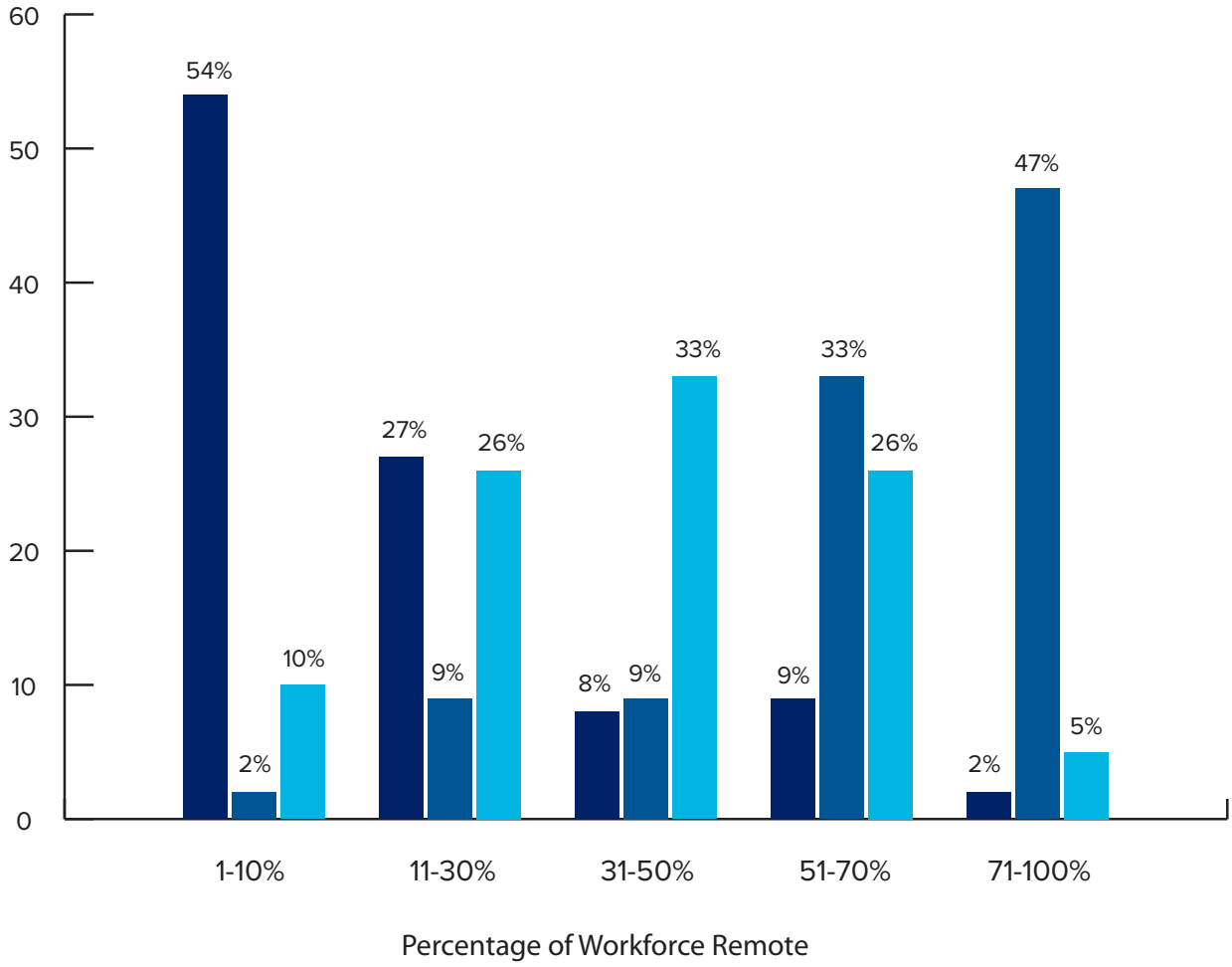
Challenges of the Remote Workforce

What percentage of your workforce...

...was remote prior to the COVID-19 pandemic?

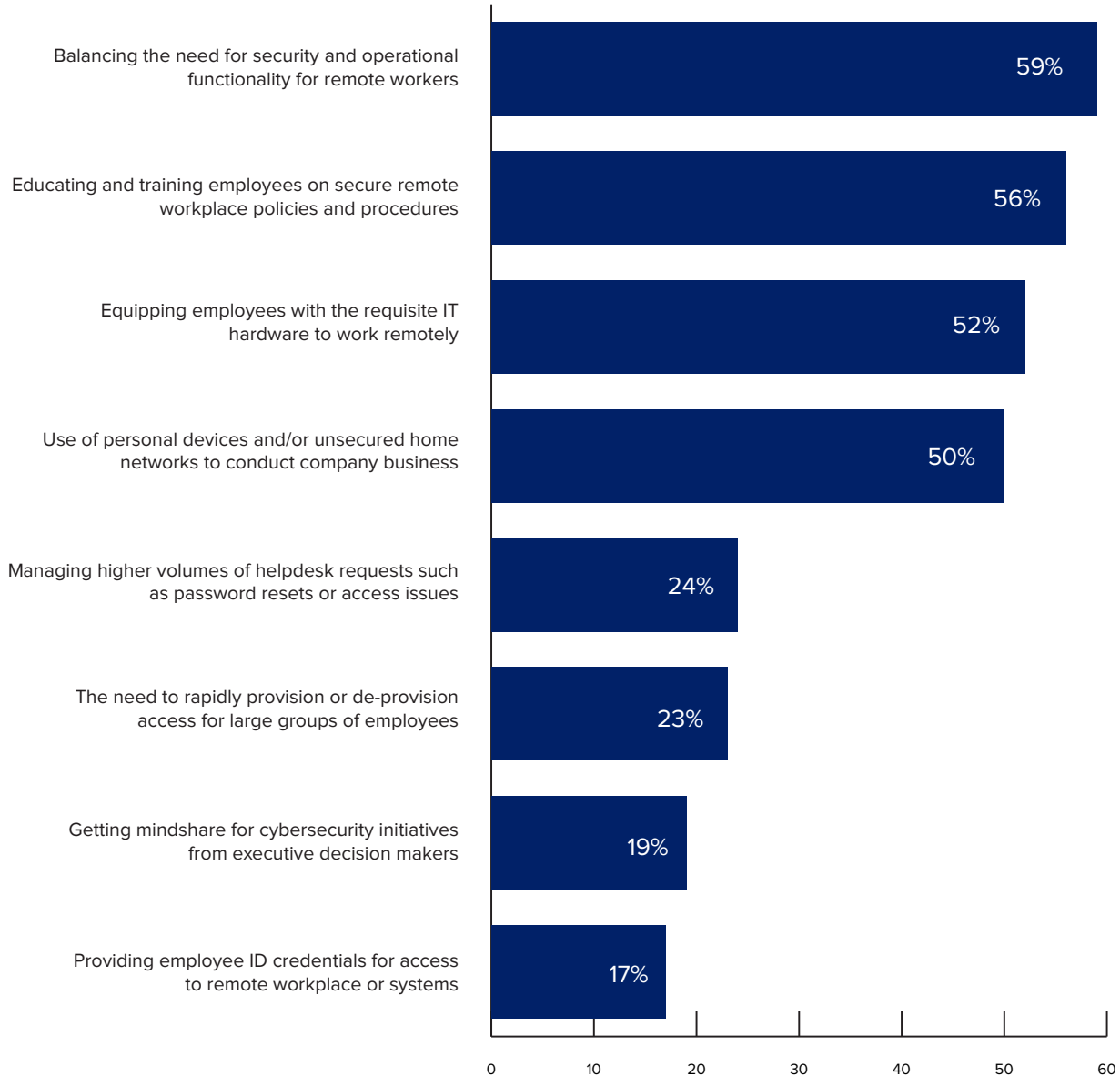
...is currently remote today?

...do you expect to remain as remote in the next 18mos?



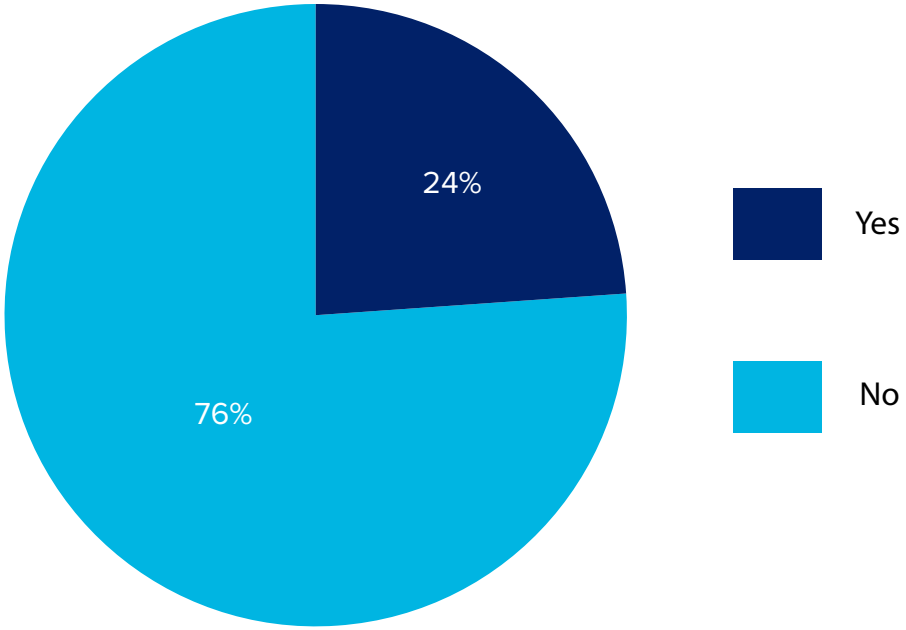
The COVID-19 pandemic led to dramatic increases in the number of employees who work remotely, and this is likely to result in some permanent changes, according to survey results. Prior to the pandemic, the vast majority of survey respondents say that under 30% of the workforce was remote. At the time the survey was conducted, 80% of participants indicated that more than 50% their workforce was remote. Eighteen months from now, 31% of respondents say, more than half of workers will still be remote.

What have been the top 3 greatest challenges with dealing with the increase in remote employees?



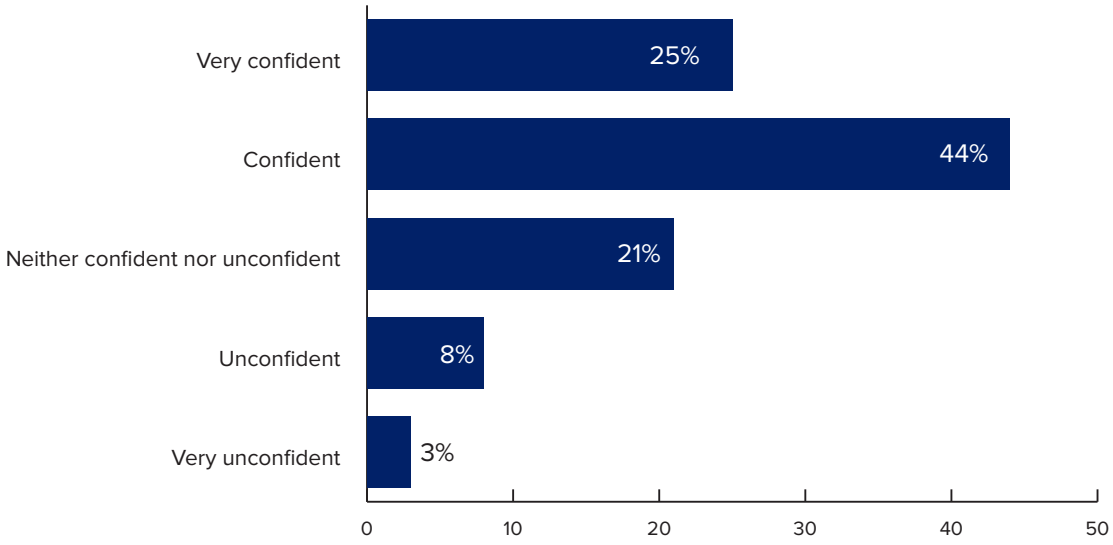
One of the most significant issues for dealing with remote employees is balancing the need for security and operational functionality. Some 59% of survey participants saw this as one of their top three greatest challenges. Other major challenges are educating and training employees on secure remote workplace policies and procedures (56%), equipping employees with the requisite hardware to work remotely (52%) and the use of personal devices and or unsecured home networks to conduct company business (50%).

Have you had to downgrade or adapt access policies in order to maintain operational functionality for remote employees?



Over three-fourths of companies have not downgraded or adapted access policies in order to maintain operational functionality for remote employees.

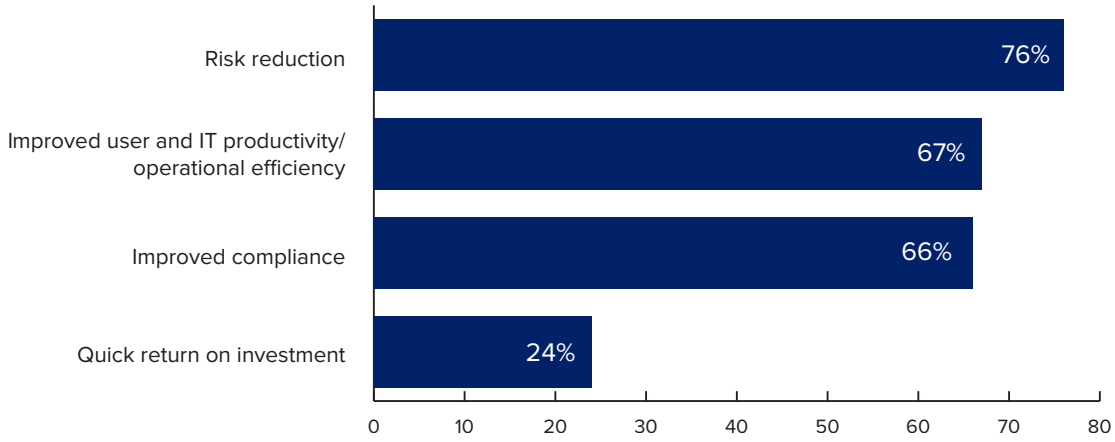
How confident do you feel about your organization's ability to control user access to file storage such as Box, SharePoint and Google Drive?



Security practitioners are largely confident in their organization's ability to control user access to file storage in the cloud. Some 69% are confident or very confident in their organization's ability to control user access to file storage, such as Box, SharePoint and Google Drive. Just 8% were unconfident and 3% very unconfident.

Cybersecurity Tools and Investment

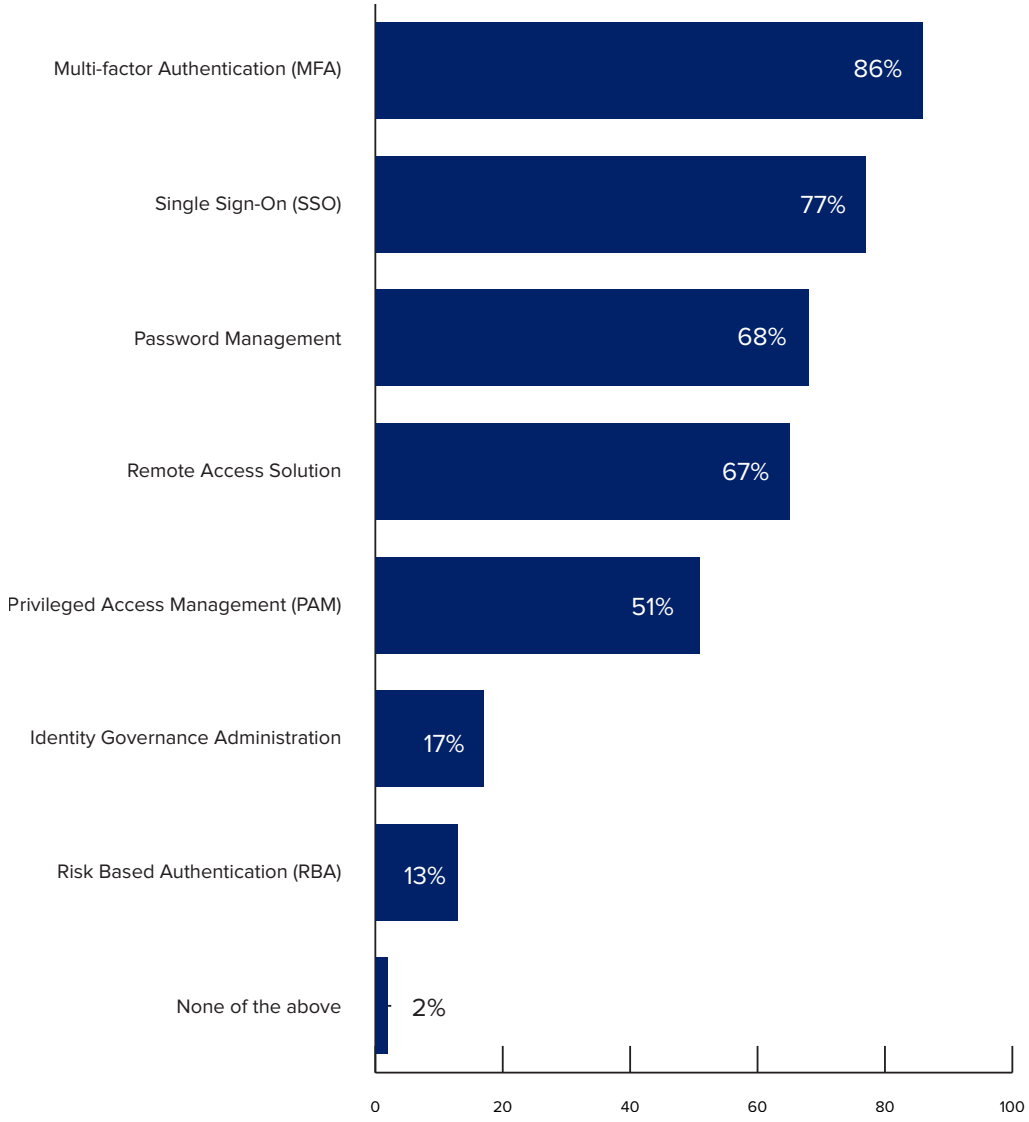
When it comes to securing a budget for cybersecurity, what business drivers are most important?



Over three-fourths of survey participants see risk reduction as the most important business driver for securing a cybersecurity budget. Some 67% also cite improved user and IT productivity/operational efficiency as an important driver for securing a budget. Compliance is also seen to be a significant driver of cybersecurity budget allocation – 66% of survey participants note improved compliance as a major driver in securing a budget.

Over three-fourths of survey participants see risk reduction as the most important business driver for securing a cybersecurity budget.

Which of the following technologies or controls are you currently using to manage identity management practices for employees?



MFA is the most commonly used technology for managing identity management for employees. Some 86% of organizations are using MFA. Other commonly used IAM tools include single sign-on (77%), password management (68%), remote access solutions (67%) and privileged access management (51%).

Conclusions and Recommendations

In reaching conclusions about the survey results, it's important to reflect upon the goals of this study, which were to help to determine:

- Where the biggest gaps in identity management are today;
- Recent attacks and their impacts on organizations;
- Where today's organizations are focusing their investments on identity management for the coming year.

Key positive insights from the survey:

- Nearly three-quarters of survey participants report that their organization's ability to identify and mitigate a cyberattack is superior or above average.
- Nearly three-quarters of respondents are confident or very confident that senior executives and board members understand the need for cybersecurity investment.
- Security practitioners are largely confident that access policies across their organizations are current.

However ...

- Over a quarter of companies have downgraded or adapted access policies in order to maintain operational functionality for remote employees.
- Nearly half of all organizations have been subject to spear-phishing attacks within the last 12 months. Other forms of prevalent cyberattacks include malware incidents (33%), employee negligence or insider attacks (29%), ransomware incidents (19%) and data breaches (16%).
- Fifty-six percent state that identifying which users/identities pose the greatest risk to their organization was one of the top three challenges they are currently facing with managing identities.

What does this mean?

There seems to be a significant disconnect between the level of confidence that security professionals have in their people, processes and culture and the reality that nearly half of organizations have been subject to cyberattacks in the past year. Further, there is a lack of clarity relating to which users and identities pose the greatest risk and the number of applications that they are using. Security professionals may be overestimating their ability to protect against inbound attacks.

This would be problematic in normal times, but as the survey indicates, the majority of employees are now working remotely, and in 18 months' time, the percentage of remote workers is not expected to reset to pre-pandemic levels. The perfect storm of a naïve remote workforce, data access on devices and networks outside of a corporate cybersecurity perimeter and a cybercriminal community seeing fertile ground for new forms of attack will make the job of security teams even more demanding.

So what's the solution?

There is no silver bullet to securing the remote worker. Rather, there are a number of steps that need to be taken to ensure that the necessary guardrails are in place to prevent security incidents from occurring. What this means is it's time for a complete reset of security expectations and a shift to focusing on identity management as the primary means of data protection, rather than a traditional firewall/VPN "castle and moat" structure.

- **Identity Really Is the New Perimeter**. Identity is the new security perimeter, but without properly governing who has access to what, you're only opening your business up to more risk. It's important to balance providing employees quick access so they can be productive with the appropriate levels of governance oversight.
- **Focus on Data Loss Prevention**. Discovering where sensitive data resides across a large hybrid environment is the first step in preventing loss. Understanding who has access and how users are able to access that information is next. Reconciling and monitoring access is then necessary to prevent accidental or intentional access or exfiltration of sensitive information. This will be more critical in industries that are more highly regulated, such as healthcare and financial services.
- **Train and Test, Often**. Employee training and testing will be imperative to ensure that they are educated and aware of inbound attacks and what to look for. In today's climate, this is more important than ever, given that there may not be someone sitting in the cubicle next to you to whom you can ask questions. Do not assume that remote workers are tech savvy – many will have worked within a secure perimeter and have not needed to focus on cybersecurity threats.
- **Authentication Is Not Enough**. Technologies that provide strong security for access to business systems will be more important than ever. MFA and single sign-on are common solutions, but only address initial entry. Utilizing the capabilities of an AI-driven identity governance solution allows organizations to define fine-grained entitlements and policies that limit the amount of information that can be accessed once within an application or system.
- **Provide Secure Networking and Collaboration Tools, or Risk Workarounds**. Monitoring usage of apps and providing secure solutions that enable business continuity are essentials steps. Providing workers with 24/7 self-service to request access and reset their own passwords enables them to keep working while reducing help desk calls and worker downtime. Employees need collaboration and communication tools more than ever to conduct business effectively – if they are handicapped then they will inevitably circumvent sanctioned channels.
- **Develop a Security Culture that Nurtures Two-Way Communication**. Employees need to know that the security team is there to help them. Being approachable and educational will encourage proactive reporting of anomalies. Employees need to remember they can "see something, say something" without judgement.

For more analysis on how to put the survey results to work, see the interview that follows with survey sponsor SailPoint.

Using Identity and Access Governance to Mitigate Data Breach Risks

Insights from Jacqueline Brinkerhoff, senior director of solutions and product marketing at SailPoint

NOTE: In preparing this report, ISMG's Nick Holland discussed the findings with Jacqueline Brinkerhoff from survey sponsor, SailPoint. Following is an excerpt of that conversation.

Key Takeaways

NICK HOLLAND: What were your first impressions of the survey findings?

JACQUELINE BRINKERHOFF: The survey is in line with what we've been seeing, especially as we've spoken with large organizations. For some, I'd say pivot is an appropriate word when it comes to how they were able to engage with the work-from-home orders. But for others, I refer to it as more like a hard left turn, since some companies were not necessarily far enough along in their digital transformation efforts to have things like their essential business apps in the cloud ready to respond to the need for their workers to access.

So some were actually forced to really accelerate their digital transformation efforts by onboarding applications almost overnight and and then figuring out how to provision that access to essential apps to their entire workforce – not only just employees or even contractors, but but extending out to partners and suppliers. This really had a big impact on their complete supply chain.

We also saw that they were trying to quickly provision access while also maintaining productivity. What was prioritized was productivity. And unfortunately, what we saw in the survey results is that security had to take a back seat in some cases to keep productivity moving forward. Organizations may have only focused on basic access management and authentication, to ensure workers are who they say they are when they're logging in. However, this has introduced a new challenge for many since they may have been provisioning access using basic identity tools that do not check against policies to see if the access was appropriate for the user's job function or role.

This has resulted in over-provisioning or over-permissioning, meaning that many workers possess more access than they really should have. With the increase in spear-phishing and malware attacks, this is concerning, especially if the workers' credentials are compromised and companies need to go back and reconcile user access to eliminate excess access and permissions to ensure that they're not leaving themselves exposed to risk.


Jacqueline Brinkerhoff

> "Identity is core and foundational to any security program."

It was not surprising to hear that many respondents are challenged with protecting the organization due to digital transformation efforts which include growth of user or identity types, explosion of new applications, adoption of cloud platforms such as AWS, Azure, and GCP, and the exponential amount of unstructured data containing sensitive information.

Unfortunately I believe we still haven't seen the security impact that the work-from-home shift is having on organizations. Industry surveys report a data breach takes approximately 200 days to detect.

The other aspect that must be considered is compliance. Audits will take place and it will be necessary to demonstrate and prove to auditors that access was appropriately granted as well as revoked, especially for workers who may have been terminated or exited the company.

Security Gaps

HOLLAND: The results that you've just talked about didn't necessarily surprise you. But what did surprise you?

BRINKERHOFF: If you look at the figures, at first blush, it could seem that these stats are at odds with one another. But then if we look deeper, it really tells an interesting story, which is that organizations are feeling like they can do a pretty good job of blocking and tackling against cybercriminals trying to penetrate and gain entry into their network. But when it comes to supporting their cybersecurity policies and goals, they seem to be lacking. They have a lot of different point solutions in their environment, but they may not necessarily all be interoperable and talking with one another, which leaves a gap in the security fabric.

But the good news is that there are organizations that have been able to confidently address this by employing identity management – specifically an AI-driven identity governance solution that can connect with all your security and IT tools so greater value can be realized from these investments.

An AI-driven approach enables organizations to gain deep intelligence and garner recommendations regarding if access is safe to grant.

Another benefit is the ability to share the identity-related information with the other IT and security tools being used to manage and protect your environment. When it comes down to it, if you look at cybercriminals, they all have different specialties and they come together to coordinate an attack. Having your IT and security investments working in silos can only protect you so much. Bringing them together and sharing information creates a much tighter security fabric and allows organizations to create automated remediation if and when a threat is detected.

Another way I like to look at this is to see identity governance as the central nervous system or brain for your IT environment. As requests come in for access, the identity governance platform can determine if it's safe to grant access and ensures access is always according to policy. It shows you how roles and policies need to get updated to keep up with the changes in your organization as well as helps you identify IT tasks that can be safely automated.

A great example of this and what we're seeing a lot of today is spear-phishing attacks. If you look at the stats, it's completely hockey-sticked over the past four months. Criminals are now starting to double down on inundating workers with malicious emails to compromise credentials and gain entry. So you may have an email security solution in place to help you scan and catch those pesky emails that cause trouble. But when you couple that with an identity governance solution, you gain a new dynamic that makes it possible to have your email security

app trigger your identity governance platform to immediately cut off a user's access and force a password reset if they happen to be a victim of a malware or spear-phishing attack. Cut off access for the user, you cut off the cyber criminal.

And this is just one example of how identity governance can work with your IT and security investments to create a strong security fabric that can catch threats early and automatically respond and remediate to them.

Top Concerns

HOLLAND: What concerns you the most about remote work, and what are the survey results telling you? And also, what do you think the results are not telling us?

BRINKERHOFF: Most organizations have traditionally started their identity efforts with single sign-on and MFA. But what organizations eventually realize is their identity program needs to go beyond that because it really requires a deep level of insight and control using policies and role-based access controls. That way, if someone is changing jobs or they're leaving the company, all of that access is immediately adjusted – whether it needs to be updated or completely revoked.

The big items that really stood out were the challenges that organizations are having with the poor management of accounts meaning not knowing where orphaned accounts and over-entitled identities exist.. That's really where AI-driven identity comes into play. Let's face it, finding an orphaned account is like trying to find a needle in a haystack. These are the things that can come back to bite you, especially if you've terminated an employee and their account is still active, which happens more often than people realize. Those are the doors you have to be aware of.

AI correlates all that identity and access information to find all of those needles, if you will, and bring them to the surface. This provides your IT and security team the exact information they need to go do something about it. Access looks suspicious? Kick off an access review and certification for that worker to ensure they have just the right amount of access needed to do their job.

In cases where you've had a merger or acquisition or even a reorganization, your policies and roles should get updated to reflect the changes that have occurred. Don't just set it and forget it. The more stale you allow your policies and roles to get, the less effective they will be at protecting your organization.

> "Keeping things secure is all about ensuring the right people have access to the right resources, regardless of whether those resources are in the cloud or on premises."

Identity Governance

HOLLAND: Based on the findings, what should security professionals focus on relating to identity governance?

BRINKERHOFF: Identity is core and foundational to any security program. With cybercriminals targeting workers and software bots to gain entry, the perimeter has had to move from the network to now each individual in the organization. So you can think of identity as the new firewall. It keeps track of the access you should have and keeps you from gaining entry to things you shouldn't.

And as it keeps track of all your access activity and history of all workers, it starts to anticipate and automate access in a secure and compliant manner.

Most organizations are short-staffed when it comes to IT and security professionals. And they always have too much to do. So effectively protecting your infrastructure should include asking yourself how can we offload the redundant IT activities and give that to the identity platform to handle?

That then opens the door to leveraging your staff's creativity and intelligence to make more critical and strategic decisions. It's this type of approach that allows you to confidently address and respond to the dynamic changes that occur.

The overall benefits of an AI-driven identity platform really provide organizations a healthy balance of productivity and security - which is especially needed as organizations now find themselves managing a "work from anywhere" workforce. Identity governance provides a framework to create an efficient environment where you can provide self-service to your workers so they can request their own access and manage or reset their own passwords; taking that off the shoulders of your IT help desk. This not only saves on costs but also gives each worker the guardrails they need to be able to do their best work possible, while knowing that they only have the least amount of access needed to successfully do their jobs. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io