Future of Secure Remote Work Report

cisco SECURE

TABLE OF CONTENT

EXECUTIVE SUMMARY

The COVID-19 pandemic has caused businesses across the globe to transition to a remote work environment at unprecedented speed and scale. What was once "nice to have" for employees and companies became a "must have" almost overnight, with organizations all over the world shifting their entire workforce to remote working arrangements. As the transition happened, organizations had to adapt and evolve their cybersecurity approach, solutions, and policies to enable their employees to work remotely, access company resources securely, and ensure business continuity.

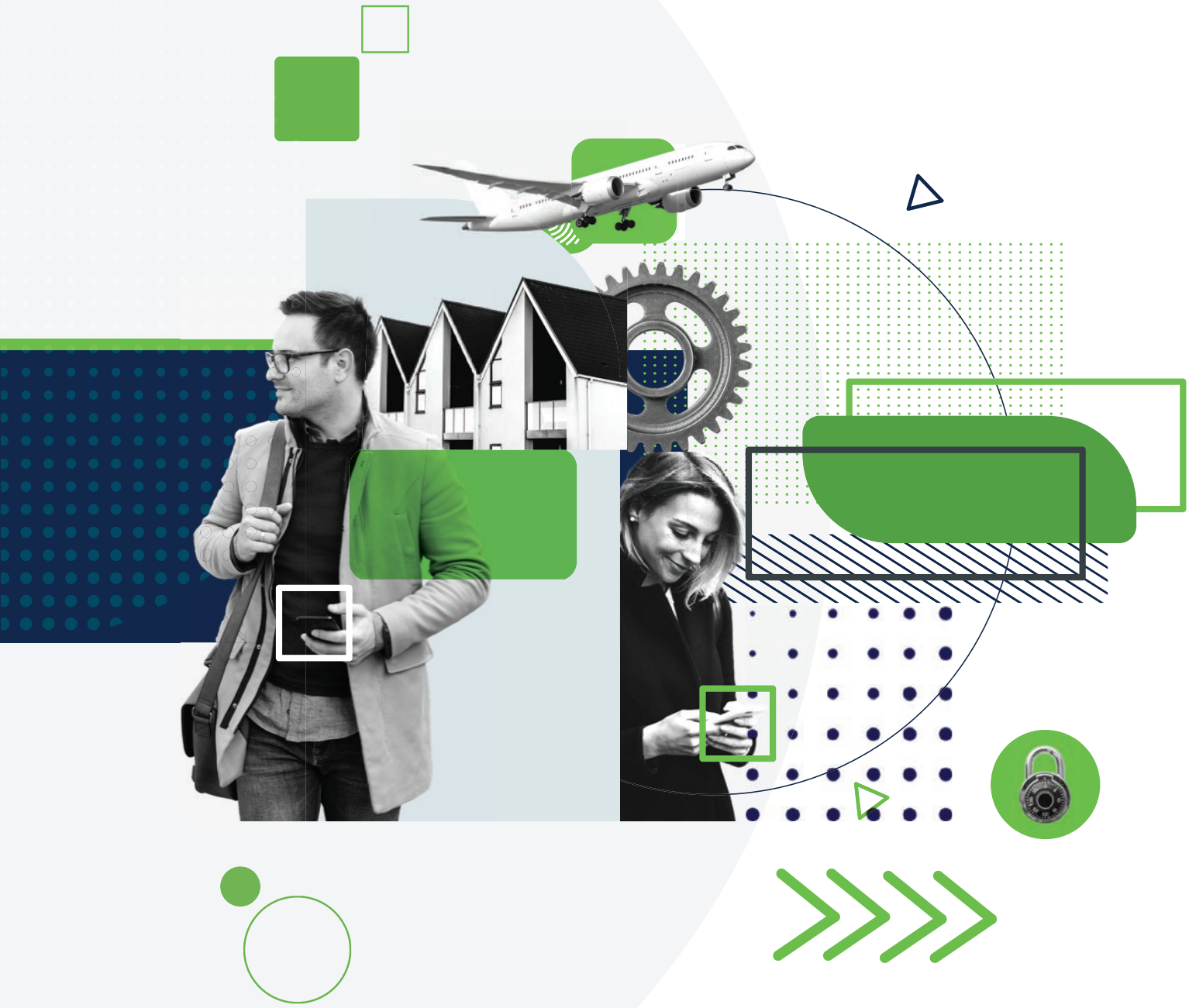
In what has been a year fraught with uncertainty, a significant trend has emerged – that of a flexible and hybrid future of work. Having worked remotely for an extended period of time, employees are now expecting that they will continue to have the flexibility and ability to work from anywhere, at any time and on any device, in a post-COVID era, even as they return to the office.

This has accelerated the need for businesses to reassess their cybersecurity posture, especially at this time when business leaders are looking to build resilient enterprises. Security can be the bridge to business resiliency as it can enable businesses to operate with flexibility by securely adapting to protect what's now and what's next. To achieve this, it is key to ensure that networking and collaborative solutions are flexible, simple to use, effective, and secure, whether delivered via on-premises data centers or in the cloud, and across all user devices – work or personal.

We wanted to understand how prepared organizations were, globally, in securing their businesses as they were forced to take their entire workforce remote due to the pandemic. More importantly, we wanted to get insights into where organizations are today in terms of the rising cybersecurity threats and alerts, the challenges they faced in this sudden transition, and how they are adapting their cybersecurity approaches to better prepare for the hybrid and flexible work environment that is here to stay. To do this, we commissioned a global research survey across 21 markets in the Americas (AMER), Asia Pacific, Japan and China (APJC), and Europe, surveying over 3000 IT decision makers from small businesses to large enterprises.

The study, titled Future of Secure Remote Work, aims to better understand the challenges that organizations faced in transitioning to remote work, while uncovering the state of their cybersecurity readiness, as well as the shifts in their priorities, policies, and investments as they prepare for a hybrid work environment that is likely here to stay.

The results are telling.



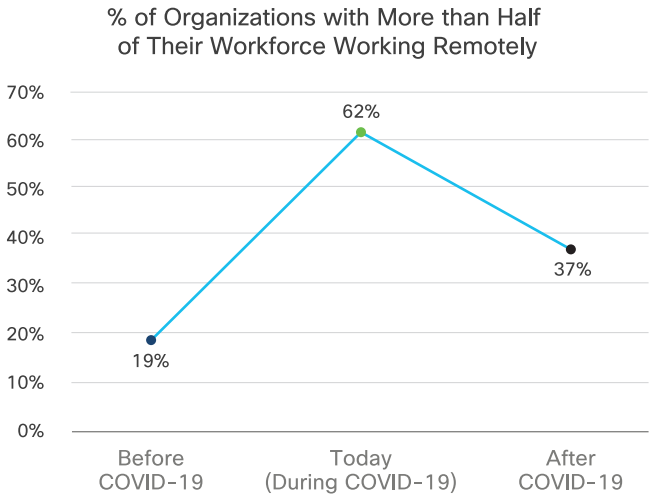
GLOBAL FINDINGS

GLOBAL FINDINGS

The Importance of Cybersecurity in a Hybrid Future of Work

Organizations are not going back to the way things were pre-COVID-19

As organizations start preparing for a post-pandemic world, one thing is clear: employees now expect to have the flexibility and ability to work remotely regardless of what the future of work entails, given the fact that we are not going back to the way things were pre-COVID-19. As observed consistently across all three regions, remote working spiked to unprecedented levels at the start of the pandemic in March, where two-thirds (62%) of respondents had ***more than half of their workforce*** work from home. Thirty-seven percent of respondents claimed that ***more than half of their workforce*** want to continue working from home post-pandemic, compared to only 19% before the disease took the world by storm.



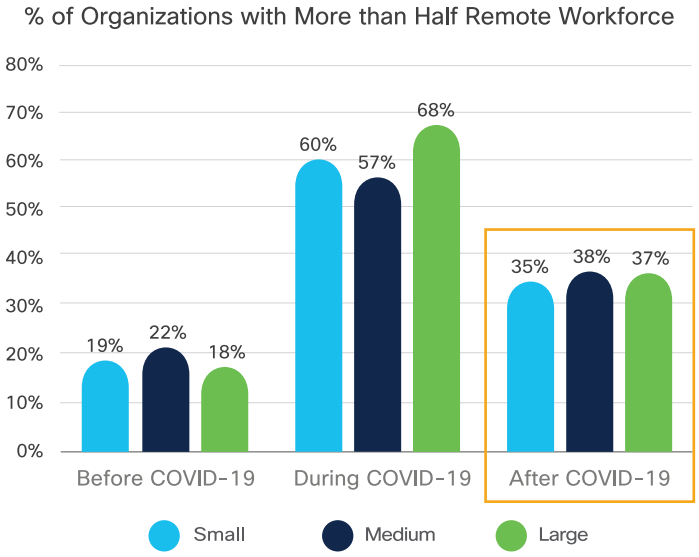
% of respondents with more than half of their workforce working remotely				
	Global	APJC	AMER	Europe
Before COVID-19	19%	19%	24%	16%
Today (During COVID-19)	62%	56%	75%	67%
After COVID-19	37%	34%	46%	34%

Organizations in AMER are leading the way with 75% of its respondents having ***more than half*** of their workforce working remotely at the moment, followed by Europe at 67% and APJC at 56%.

However, they are not going back to pre-pandemic levels anytime soon, with 46% of respondents in AMER expecting more than half of their employees to continue working remotely even after businesses have returned to normal. Likewise, 34% of respondents in both APJC and Europe noted the same.

Attitudes toward remote work are also consistent across small, medium and large organizations, where 35% of small businesses, 38% of medium businesses and 37% of large enterprises believed that ***more than half*** of their employees will be remote workers post-COVID-19.

While many businesses are likely still uncertain about what the future of work will look like, having the flexibility to securely adapt to what's now and what's next will increase their business resilience and enable them to support a more distributed workforce.



Some countries plan to embrace remote work going forward more than others

Interestingly, while most organizations plan to bring most employees back to the office after the pandemic, some countries are bucking the trend, reporting that a higher proportion of respondents claimed that ***more than half*** of their organization's workforce will continue to be remote workers in the future. These include 48% in the Philippines and 50% in the United Kingdom and the United States, as well as 53% in Brazil and India, all of which are higher than the global average of 37%.

48%
Philippines

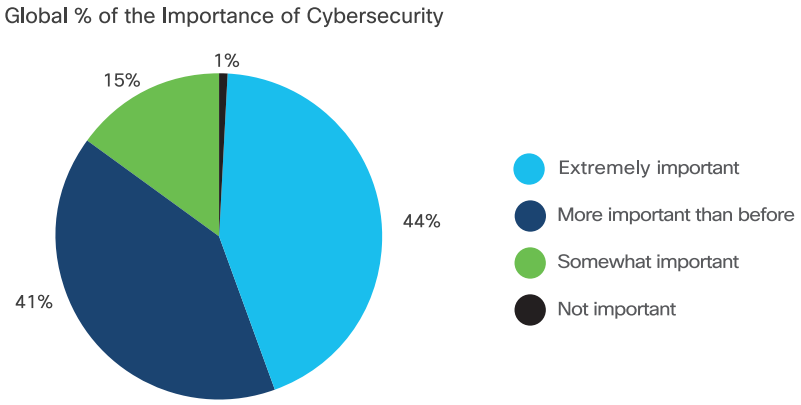
53%
Brazil
India

50%
United Kingdom
United States

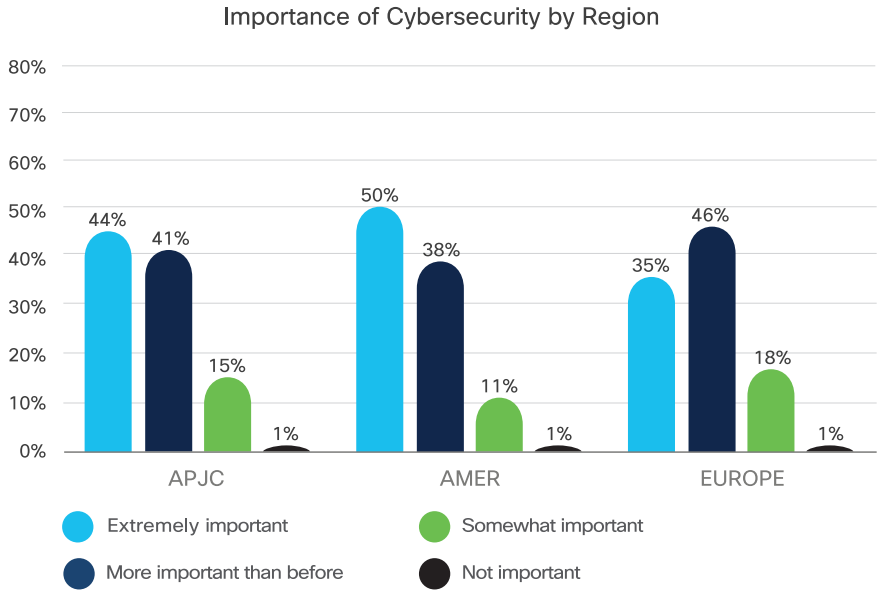
To enable this flexible and hybrid future of work trend, companies need a seamless and secure underlying infrastructure.

Cybersecurity now tops corporate priorities

The good news is cybersecurity has become a top priority for organizations. Eighty-five percent of respondents globally said that cybersecurity is ***extremely important*** or ***more important than it was before the pandemic***.



Breaking it down further, a large proportion of respondents in APJC (44%) and AMER (50%) stated that cybersecurity is ***extremely important*** to their business. Europe, on the other hand had more respondents indicating that it is ***more important than it was before at*** 46%.



This trend is also consistent across small, medium, and large businesses at **79%, 87%, and 88%,** respectively.

	Small	Medium	Large
Extremely important	36%	42%	53%
More important than before	44%	45%	35%
Somewhat important	19%	13%	11%
Not important	1%	1%	0%

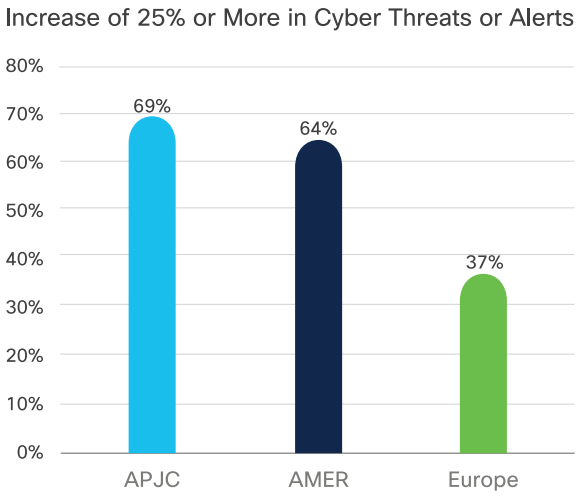
Importance of Cybersecurity by Organizational Size

A Resilient Rebound: Tackling Cybersecurity Threats and Challenges

Increasing cyber threats and alerts at varying levels

Globally, companies experienced a jump in cybersecurity threats or alerts during the pandemic as malicious actors tried to take advantage of potential security gaps, with users accessing the corporate network and cloud applications remotely. Sixty-one percent of respondents globally stated that their organizations experienced a jump of ***25% or more in cyber threats or alerts*** since the start of COVID-19. This was also experienced by 55% of small businesses, 70% of medium organizations, and 60% of large enterprises.

At 69%, more respondents in APJC experienced a jump of ***25% or more cyber threats or alerts*** since COVID-19. This was followed by 64% in AMER and 37% in Europe.



Worryingly, 8% of businesses globally did not know whether they have experienced an increase or decrease in cyber threats. This figure increases to 17% for respondents in Europe, compared to 6% in APJC and 5% in AMER. When diving deeper, the study also found some key differences between the levels of threats or alerts experienced across regions and industries.

Percentage of increase in cyber threats/alerts	Global	APJC	AMER	Europe
0% - 24%	31%	25%	31%	47%
25% - 50%	33%	35%	36%	23%
51% - 75%	23%	27%	24%	11%
76% - 100%	5%	6%	3%	2%
Don't know	8%	6%	5%	17%

25% or more threats

% of Increase in Cyber Threats or Alerts

For example, 78% of organizations in the **Architecture and Engineering** industry experienced an increase of 25% or more cyber threats or alerts, the highest across all industries. This was followed by the **Chemical Engineering and Manufacturing** sector at 72% and the **Education** sector at 70%.

Interestingly, industries that were often pegged as being of high interest to attackers, such as **Financial Services** (58%), **Software Development** (62%), and **Healthcare** (54%), defied expectations with a relatively lower proportion of organizations experiencing more alerts.

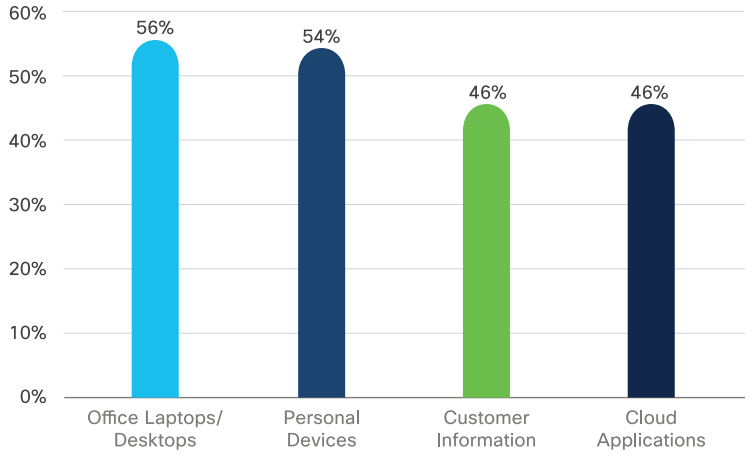
Top cybersecurity challenges reported by organizations supporting remote work

Secure access, defined as the ability to securely enable access to the enterprise network and applications for any user, from any device, at any time, is the ***top cybersecurity challenge*** faced by the largest proportion of organizations (62%) when supporting remote workers. Other concerns raised by organizations globally include data privacy (55%), which has implications for the overall security posture, and maintaining control and enforcing policies (50%).

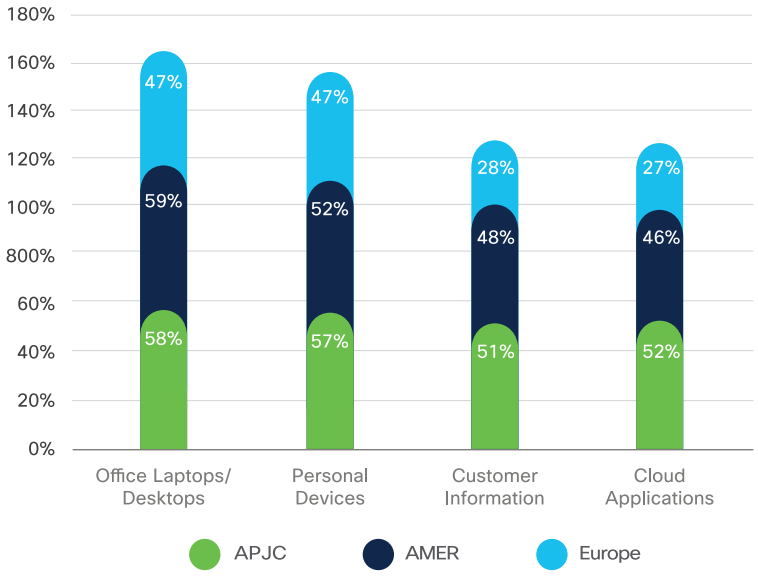
Protecting an increasing number of endpoints

Securing devices is a growing challenge for organizations now unable to rely on connecting endpoints to campus networks for visibility and pushing updates. At the same time, employees are connecting to corporate resources with more personal, unmanaged devices, creating a blind spot for security teams. One in two respondents stated that office laptops/desktops (56%) and personal devices (54%) are a challenge to protect in a remote environment. This was followed by customer information and cloud applications both at 46%.

Things that Posed a Challenge to Protect in a Remote Environment



Regional Comparison of Things that Posed a Challenge to Protect in a Remote Environment

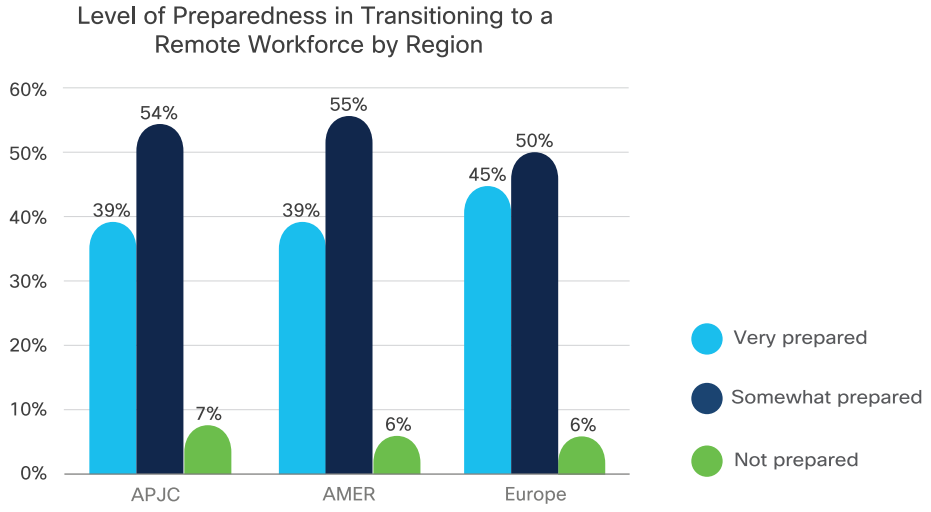


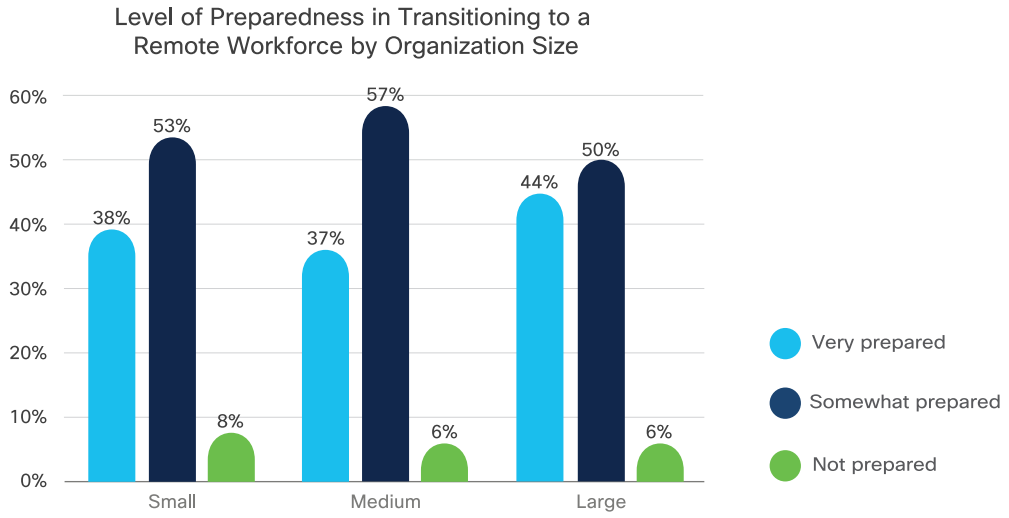
Organizations forced to accelerate digital transformation

While many organizations had begun their transitions to become cloud-first and remote-first even before the pandemic, this is a process that requires significant time and investment. The practically overnight move to a distributed workforce highlighted just how far many organizations still needed to go in their journeys. Globally, respondents reported to either be ***somewhat prepared*** (53%) or ***not prepared*** (6%) to make the accelerated transition to a remote work environment at the outset of COVID-19.

	Global	APJC	AMER	Europe
Very prepared	40%	39%	39%	45%
Somewhat prepared	53%	54%	55%	50%
Not prepared	6%	7%	6%	6%

Level of Preparedness in Transitioning to a Remote Workforce





When it comes to specific industries, organizations in the **Architecture and Engineering** (72%) industry had the highest proportion of respondents that were ***somewhat prepared***, higher than the global average of 53%, while respondents in the following industries saw the highest proportion of respondents that were ***not prepared*** to support the sudden transition compared to the global average of 6%: **Wholesale and Distribution** (15%); **Education** (14%); and **Chemical Engineering and Manufacturing**, **Non-Computer-Related Manufacturing**, and **Not-for-Profit or Charitable** (10%, respectively).

The readiness (or otherwise) of IT and security teams to support remote work potentially reflects the nature of the businesses and the ability for workers in that industry to already be spending some or all of their time operating out of the office. Firms with a bias towards knowledge work are more likely to have a larger number of remote employees than location-specific industries such as manufacturing. Companies with a larger number of telecommuting employees will naturally be more prepared to support an even bigger number of their workforce to go remote.

With 67% reporting to have been ***very prepared***, Vietnamese organizations had the highest proportion of respondents in the world that were ready to immediately transition to remote working. They were followed by the United Kingdom (59%), India (54%), and Indonesia (49%).

On the flipside, the United States, which had the highest proportion of remote workers before the pandemic (32% had more than half of their workforce remote), had a larger proportion of organizations that were only ***somewhat prepared*** (48%) compared to ***very prepared*** (46%).

Prioritizing Cybersecurity for What's Now and What's Next

Technology adoption and prioritization

The good news is, of all the technology solutions adopted to enable remote work, organizations globally ranked cybersecurity measures as the #1 priority (52% ranked it first). This was followed by collaboration tools (41% ranked it first) and professional services (27% ranked it first).

Most Widely Adopted	vs	Number 1 Priority
Collaboration Tools 73%	1	Cybersecurity Measures 52%
Cybersecurity Measures 68%	2	Collaboration Tools 41%
Cloud-Based Document Sharing 63%	3	Professional Services 27%
Distributed Data Protection 49%	4	Cloud-Based Document Sharing 22%
Professional Services 33%	5	Distributed Data Protection 19%

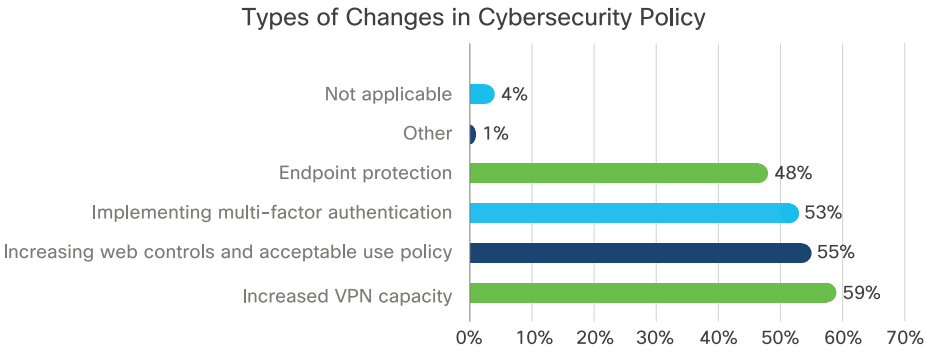
As businesses navigate the future of work, which will likely entail the adoption of various solutions from collaboration to file sharing and networking, it is critical to ensure that security is integrated across all IT tools. This will truly empower a secure and distributed workforce.

Facilitating remote working with the right protocols and policies

Ninety-six percent of organizations globally reported changes in their cybersecurity policies to support remote working. These included 93% of small businesses, 98% of medium organizations, and 97% of large organizations, indicating that organizations of all sizes found it absolutely necessary to update their policies immediately to support this change.

It seems obvious but worthy of comment that when your HR team or finance team, for example, is suddenly forced to work remotely, the protections and access granted to them as part of daily responsibilities inside the corporate network need to be replicated for a remote setting to support business continuity. Consistency of policy also becomes much more of an issue than ever before.

From this, the top policy-related changes made were increased VPN capacity (59%), increased web controls and acceptable use policy (55%), and the implementation of multi-factor authentication (MFA) (53%).



Global	APJC	AMER	Europe
Increased VPN capacity (59%)	Increasing web controls and acceptable use policy (61%)	Increased VPN capacity (64%)	Increased VPN capacity (64%)
Increasing web controls and acceptable use policy (55%)	Implementing multi-factor authentication (59%)	Increasing web controls and acceptable use policy (57%)	Implementing multi-factor authentication (38%)
Implementing multi-factor authentication (53%)	Increased VPN capacity (56%)	Implementing multi-factor authentication (51%)	Increasing web controls and acceptable use policy (34%)

Top 3 Changes in Cybersecurity Policies by Region

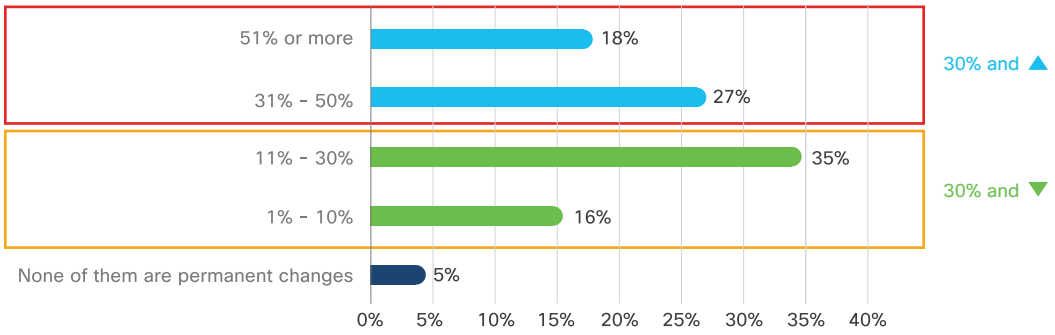
REGIONAL VARIATIONS:

- **Increasing web controls and acceptable use:**
  - Highest in APJC (61%)
  - Second in AMER (57%), similar to global (55%)
  - Third in Europe (34%)
- **Implementing multi-factor authentication:**
  - Second in APJC (59%) and Europe (38%)
  - Third in AMER (51%)
- **Increased VPN capacity:**
  - Highest in AMER and Europe (both 64%), similar to global (59%)
  - Third in APJC (56%)

Long-term changes in corporate cybersecurity policies are afoot

One of the biggest observations from the study is the fact that remote working is driving long-term changes in cybersecurity policies. This presents organizations with the unique opportunity to transform their business and security strategies to truly support the digital-first world that we are now living in, thereby enabling the level of flexibility that employees now expect with a distributed workforce.

To this end, amongst organizations that made changes to their cybersecurity policies, the vast majority (95%) indicated that some portion of these are permanent.



Proportion of Cybersecurity Policy Changes Made that Are Permanent

A deeper look across the regions reveals that more organizations in AMER (54%) and Europe (48%) said that ***more than 30%*** of their cybersecurity policy changes will be permanent, while 41% of APJC respondents indicated the same.

Magnitude of Permanent Policy Changes	Global	APJC	AMER	Europe
30% or less	50%	54%	44%	45%
More than 30%	45%	41%	54%	48%
TOTAL	**95%**	**96%**	**97%**	**93%**

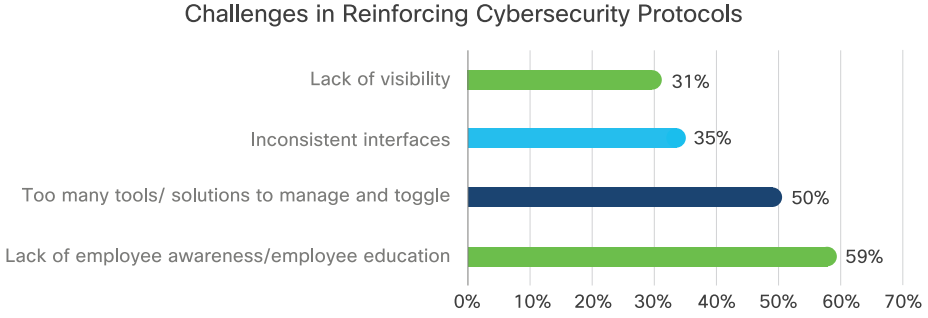
Magnitude of Permanent Cybersecurity Policy Changes According to Region

ORGANIZATIONAL SIZE (S, M, AND L) VARIATIONS:

- As expected, more large businesses (52%) are making ***more than 30%*** of their policy changes permanent compared to small and medium organizations.
- Small (55%) and medium (54%) businesses on the other hand are making ***30% or less*** of their new cybersecurity policies permanent.

Security education and culture: A must

That said, further education and better security that are simple, easy to use, and work together are needed. Fifty-nine percent of organizations globally said that the lack of employee awareness and education was the top challenge faced in reinforcing cybersecurity protocols for remote working. This was followed by too many tools/solutions to manage and toggle (50%). Similar trends were observed across APJC, AMER, and Europe.



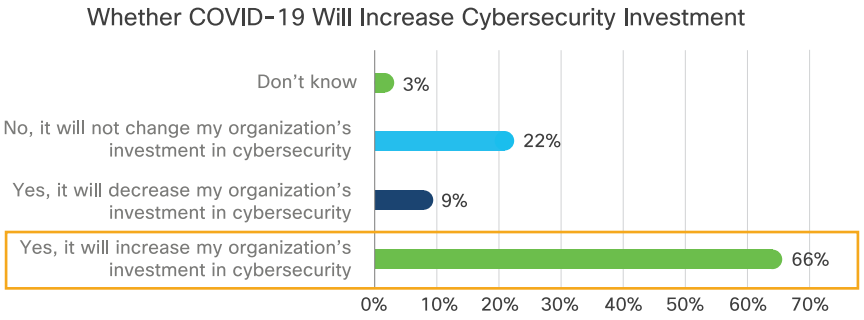
Global	APJC	AMER	Europe
Lack of employee awareness/employee education (59%)	Lack of employee awareness/employee education (61%)	Lack of employee awareness/employee education (58%)	Lack of employee awareness/employee education (54%)
Too many tools/ solutions to manage and toggle (50%)	Too many tools/ solutions to manage and toggle (53%)	Too many tools/ solutions to manage and toggle (49%)	Too many tools/ solutions to manage and toggle (43%)
Inconsistent interfaces (35%)	Inconsistent interfaces (40%)	Inconsistent interfaces (33%)	Inconsistent interfaces (22%)

Top 3 Challenges in Reinforcing Cybersecurity Protocols Across Regions

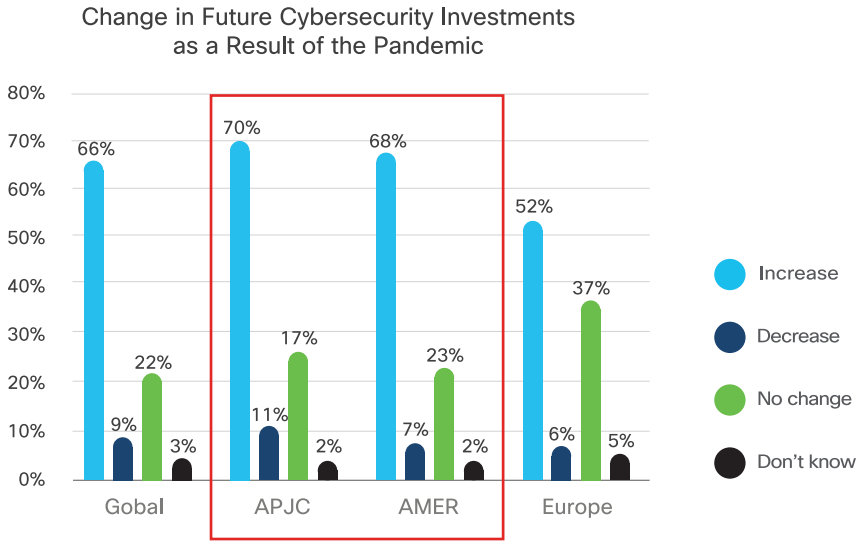
The findings show that there is an opportunity for the security industry to fundamentally change to meet this moment and increase its flexibility to support a distributed workforce where security is an enabler instead of a hindrance to collaboration. We explore more of this below.

Investments in cybersecurity on the rise

With these changes and improvements in the works, the majority of organizations globally (66%) indicated that they will likely increase their cybersecurity investments due to the COVID-19 situation.

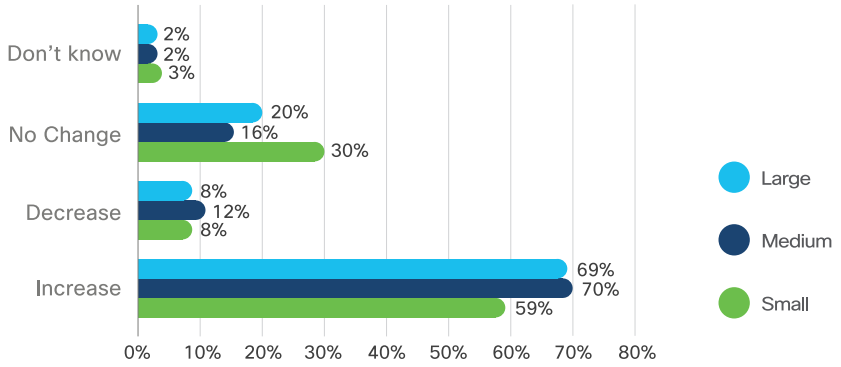


More respondents in APJC (70%) and AMER (68%) indicated that they will increase their future cybersecurity investments compared to the global average of 66%.



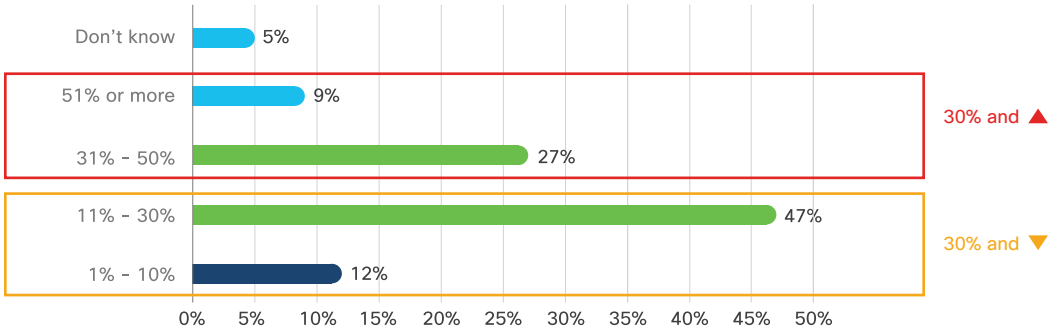
In more positive developments, organizations of all sizes are looking to increase their cybersecurity investments following the pandemic as well. Interestingly, medium-sized businesses are marginally ahead of large organizations, with 70% looking to increase spending. Small organizations are not lagging behind either, with 59% planning on doing the same.

Change in Future Cybersecurity Investments According to Organizational Size



While organizations across industries, regions, and markets are in agreement about the need to boost cybersecurity spending, the proportionality of said investments varies. For the most part, 59% of those that are planning to boost their cybersecurity investments indicated a planned increase of between ***1% to 30%***. This trend is mirrored across APJC (58%), AMER (56%), and Europe (65%).

Proportion of Increase in Cybersecurity Investments

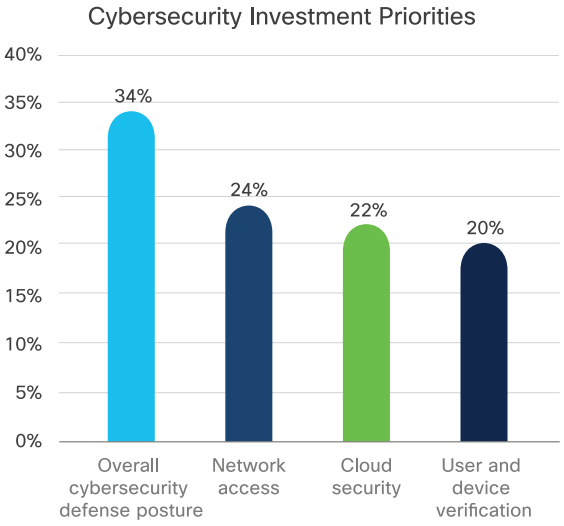


Proportion of Increased Investments	Global	APJC	AMER	Europe
30% or less	59%	58%	56%	65%
More than 30%	36%	39%	39%	23%

Organizations globally are rethinking their overall security strategy

When asked to rank their cybersecurity investments in terms of importance as they prepare for a post-COVID-19 world, overall cybersecurity defense posture — including threat protection, risk assessments, auditing, compliance and privacy, and more — is the top-ranked investment priority (34% ranked it first). It is also the top-ranked choice for 16 of the 21 markets surveyed. This indicates that the remote work environment has created strategic challenges that businesses need to address as they rethink the best ways to support the flexible and hybrid work environment that is here to stay.

Other priority investments reported by organizations include network access (24% ranked first), cloud security (22% ranked first), and user and device verification (20% ranked first).



Cybersecurity Investment Priorities Ranked 1st

REGIONAL VARIATIONS

APJC	AMER	Europe
Overall cybersecurity defense posture (35%)	Overall cybersecurity defense posture (31%)	Overall cybersecurity defense posture (33%)
Cloud security (23%)	Cloud security (25%)	Network access (29%)
Network access (23%)	Network access (22%)	User and device verification (21%)

KEY TAKEAWAYS AND RECOMMENDATION

KEY TAKEAWAYS AND RECOMMENDATIONS

#1 The future of work is dynamic: Cybersecurity must meet the needs of a distributed workforce.

The world now sees that it is possible for employees to stay connected and productive while working away from the office for prolonged periods. It is likely that many businesses will move toward a hybrid work environment that caters to both in-office and remote employees. This will offer employer and employees greater choice and flexibility from business and human capital perspectives, as well as bring more diversity into the workforce. The abrupt shift also created a series of cybersecurity challenges – keeping your business running in a very different environment or securing access at a greater scale than ever before.

Employees are connecting their office devices to their home Wi-Fi or external networks or using their personal devices to connect to corporate applications in the cloud. This is putting a sudden strain on both security and IT teams who are being tasked with quickly providing support for an unprecedented number of offsite workers and their devices – without compromising security. Policies and controls that once resided in headquarters must now follow the worker wherever and whenever they choose to require access. In addition, the opportunity for remote work comes with a sinister shadow: modern threat actors have launched more phishing attacks to trick users and steal information from them, compromise the newly remote workforce systems with malware, or exploit gaps in a company's evolving cybersecurity posture.

Businesses need to create a flexible, safe, and secure hybrid work environment with employees moving on and off network with similar levels of protection. As business and IT leaders deliver significant changes to their technology and business priorities, cybersecurity should be the bridge that enables organizations to reach their full potential.

#2 The success of a flexible hybrid workforce hinges upon preparation, collaboration, and empowerment.

One of the key issues that has emerged from the overnight shift to remote work of the last eight months is how well organizations transitioned into it. Businesses that have made incremental and continuous investments in pre-pandemic technology, such as cloud security solutions and zero-trust frameworks, have been the best prepared to support remote work. Likewise, enhancing cybersecurity measures that support such arrangements has placed organizations in a better position to face the potential increase in the number and variety of cybersecurity attacks.

In order to reap the full benefits of a flexible and hybrid workplace, however, such investments cannot be made in a vacuum. With the shift to a distributed workforce, network and security teams need to provide seamless and secure access to applications and services, anywhere and anytime. Security, networking, and collaboration can no longer be seen in silos. They must work hand in hand. Alongside these functions, leaders must put in place additional enforcement protocols and enhanced cybersecurity policies. This should also be complemented by a solid employee education program, given the fact that investment in a healthy security culture is absolutely critical.

#3 Simpler and more effective cybersecurity is critical to building business resilience.

The experience of prolonged remote working has propelled the value of cybersecurity up corporate agendas, with long-term changes in corporate cybersecurity policies likely. Additionally, many have stated that they intend to increase their cybersecurity spending in the future.

With many competing priorities for IT leaders, security cannot be an afterthought – it should be the foundation behind the success of any digitalization effort. This will ensure the security, scalability, and adaptability of these efforts. To reduce the likelihood and impact of a cybersecurity breach, organizations also need to look for ways to reduce the complexity of their cybersecurity measures. Taking a simplified approach toward more effective security ensures that it will be a business enabler, not a hinderance to what's needed now and what comes next.

Recommendations:

For businesses to enable people to work securely from anywhere, anytime, and on any device, cybersecurity should be the foundation of every IT investment. This requires a platform approach to deliver highly effective security from the network to the endpoint to the cloud. Best-of-breed point products simply do not measure up. When security must deliver less complexity, solutions must work together and offer ease of use.

To securely enable a distributed workforce and ensure the flexibility to adapt to what the future of work brings, organizations should ensure the following conditions are met:

- Verify the user's identity to establish trust: are you who you say you are?
- Enable work on any kind of device, any kind of connection, securely
- Give access to the company apps and data that workers need
- Protect users from threats once they're on the network

Future of Work: 10 Takeaways

1. Adopt a zero-trust strategy to verify the identity of all users before granting access to company-approved applications: protect the workforce, workload, and workplace.
2. Multi-factor authentication (MFA) is a natural first step in securing a distributed workforce, allowing you to verify the identities of employees attempting to access corporate assets.
3. Implement a VPN, providing a safe tunnel between users and applications so workers can stay productive and connected when they are on the road or working from home. It helps ensure only approved users get in by providing the right level of security without compromising the user experience.
4. Use DNS. Most security breaches target endpoint users, requiring a first line of defense at the DNS layer. This crucial first layer blocks domains associated with malicious behavior before they get into your network or contains malware if it is already inside.
5. Secure Office 365 email against advanced threats. With email being the #1 attack vector, protection from email threats like phishing, ransomware, business email compromise, and others is needed using an integrated, cloud-native security solution for Microsoft 365 that stops threats to Office 365 from both internal and external senders.
6. Maintain the last line of defense with secure endpoint solutions. Not only does endpoint security prevent cyber attacks, but it also rapidly detects, contains, and remediates malicious files if they evade defenses and infiltrate endpoints – before damage can be done.
7. Accelerate the strategic adoption of cloud-based security solutions to protect your workforce by delivering a seamless connection to applications in any environment from any location. Secure access service edge (SASE) is a network architecture that combines SD-WAN capabilities with cloud-native security functions such as secure web gateways, cloud access security brokers, and firewalls, all delivered from the cloud.
8. Realize greater benefits from existing products through a platform approach. This provides visibility across multiple security solutions in a unified dashboard while integrating with third-party security solutions.
9. Automate Security Operation Center (SOC) workflows such as threat investigation, hunting, and remediation to strengthen efficiency and precision, lowering operational costs. This helps security teams better support evolving business and technology needs while staying ahead of an ever-changing threat landscape.
10. Remember: People can be the strongest link in any defense. Encourage greater employee cybersecurity awareness and empowerment. Organizations need to also look at improving employee awareness on the importance of adopting security-centric practices such as learning to identify phishing attacks, practicing good password policy, and keeping software up to date. Cybersecurity training cannot be a once-a-year, compliance-based training that most employees dislike. It must be a part of the culture.

Cisco SecureX™ is a cloud-native, platform experience that connects Cisco's security and networking portfolio and your existing infrastructure. It is integrated and open for simplicity, unified in one location for visibility, and maximizes operational efficiency with automated workflows.

AMERICAS HIGHLIGHTS

AMERICAS HIGHLIGHTS

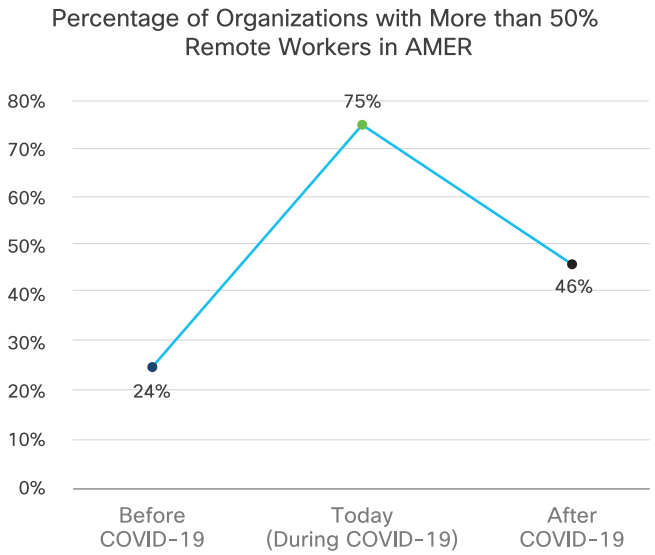
Regional Summary

The study surveyed over 600 organizations from four countries in AMER – Brazil, Canada, Mexico and the United States. Before the pandemic spurred a grand global experiment in the costs and benefits of a fully remote workforce, many people in AMER were already working outside of traditional offices. Even then, the overnight shift into a remote workforce still posed a series of cybersecurity challenges for companies. Only 39% of AMER organizations reported being ***very prepared*** for the sudden transition to a remote work environment, slightly lower than the global average of 40% and the European average of 45%. Fifty-five percent of organizations in AMER reported being ***somewhat prepared*** and 6% ***not prepared***. AMER also had more organizations that experienced a jump of ***25 percent or more*** cyber threats or alerts since the start of COVID-19 (64%) compared to the global average of 61%.

Across all regions surveyed, AMER had the highest percentage of organizations (88%) that said that cybersecurity is now ***extremely important or more important than before COVID-19***, compared to 85% in APJC and 81% in Europe. As a result, nearly all of the organizations surveyed reportedly made changes to their cybersecurity policies to support remote working (97% percent), with nearly 7 in 10 (68%) organizations projecting an increase in future cybersecurity investments due to COVID-19.

Key Findings

AMER organizations are embracing the shift to a hybrid future of work but can improve their cybersecurity readiness



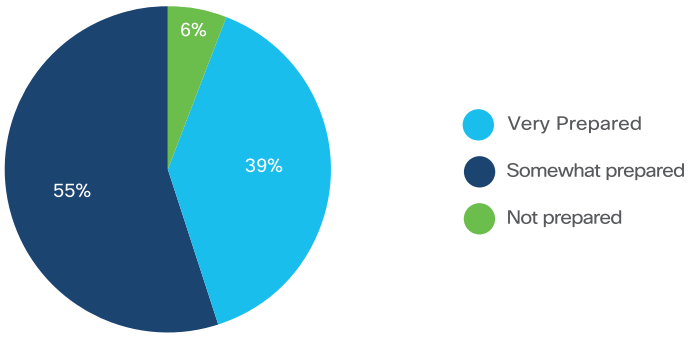
	Global	AMER
Before COVID-19	19%	24%
Today (During COVID-19)	62%	75%
After COVID-19	37%	46%

The Americas are no stranger to remote work, clocking the world's highest digital nomad record even before the pandemic. Twenty-four percent of organizations had ***more than half*** of their workforce already working remotely prior to the pandemic. This figure elevated threefold (75%) during the outbreak and is projected to go down to 46% post-COVID-19.

- Mexico recorded the highest proportion of organizations (77%) in AMER with ***more than half*** of their workforce working remotely during the pandemic. From this, a striking 40% of Mexican organizations are expecting ***more than half*** of their employees to remain remote, even in a post-pandemic world.
- Organizations in the United States (50%) and Brazil (53%) are bucking the remote working trend post-pandemic, with a higher proportion of organizations expecting ***more than half*** of their workforce to be working remotely compared to the global average of 37%.

Most organizations in the region were ***somewhat prepared*** (55%) to transition to large-scale remote work. Similar to APJC, only 39% of organizations in AMER were ***very prepared*** for the sudden shift, while a further 6% were ***not prepared***.

Level of Preparedness in Transitioning to Remote Working Amongst AMER Organizations



Level of preparedness to transition to remote working	Global	APJC	AMER	Europe
Very prepared	40%	39%	39%	45%
Somewhat prepared	53%	54%	55%	50%
Not prepared	6%	7%	6%	6%

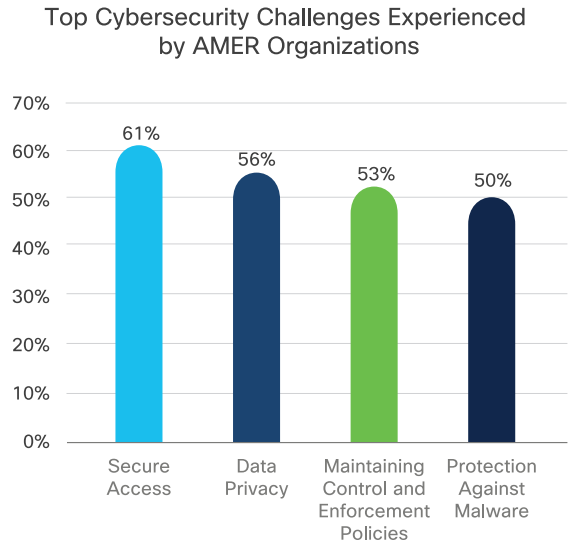
- The United States had the largest proportion of organizations that were ***very prepared*** (46%) for the sudden transition to remote working in the region (6%-7% higher than global and regional average).

Tackling cybersecurity threats and challenges in AMER

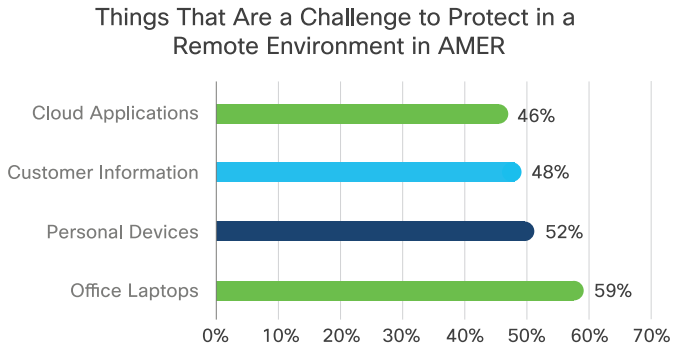
Regionally, 64% of respondents in AMER experienced a jump of ***25% or more*** in cyber threats or alerts since the start of COVID-19, slightly higher than the global average of 61%.

- This number varies across the region, with the largest proportion of respondents in Brazil (82%) experiencing a jump of ***25% or more*** in cyber threats or alerts.
- Fifty-four percent of respondents in the United States and 53% of respondents in Canada experienced a jump of 25% or more in cyber threats or alerts, lower than the regional and global averages.
- Ten percent of respondents in the United States did not know if their cyber threats or alerts have increased or decreased. This is higher than the global average of 8%, and also the highest within AMER.

As with businesses worldwide, organizations in AMER found the transition to socially distanced work hindered by cybersecurity challenges. Sixty-one percent of AMER organizations said **secure access is the top cybersecurity challenge** faced by most organizations when supporting remote workers. Other concerns raised by organizations in AMER included data privacy (56%), which has implications for the overall security posture, maintaining control and enforcement policies (53%), and protection against malware (50%).



As workers stayed home, many started using devices not as secure as those on-premises. The consequences of poorly secured networks while working from home had many businesses finding office laptops/desktops (59%) and personal devices (52%) a challenge to protect in a remote environment, followed by customer information (48%).



- The same proportion of respondents in Brazil indicated that customer information posed a challenge to protect as company laptops/desktops at 58%, higher than personal devices (53%).

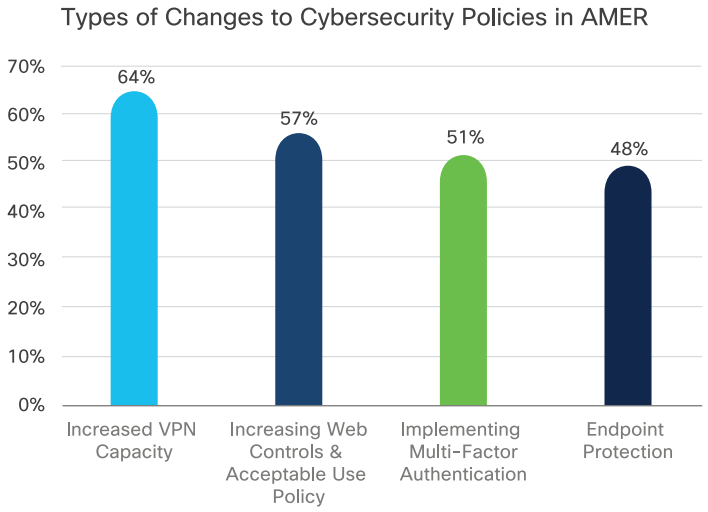
Prioritizing cybersecurity for what's now and what's next

Cybersecurity measures were clearly top of mind for organizations in AMER, with 57% of adopters ranking it as the number one priority out of all the technology solutions adopted to enable remote work; this is higher than the global average of 52% who ranked it first, with United States taking the lead at 62% (ranked it first).

Respondents in Mexico (57%) and Brazil (58%) had a higher proportion of organizations indicating that cybersecurity is ***extremely important*** compared to United States (43%) and Canada (42%), and higher than the AMER average of 50%.

Importance of cybersecurity	U.S.	Canada	Mexico	Brazil
Extremely important	43%	42%	57%	58%
More important than before	39%	42%	34%	3%
Somewhat important	17%	15%	8%	4%
Not important	1%	1%	1%	0%

Importance of Cybersecurity to the Organization According to Countries Within AMER



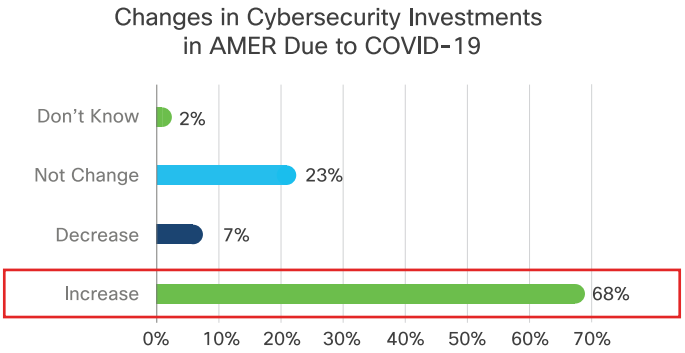
Ninety-seven percent of AMER organizations made changes to their cybersecurity policies to support their remote workforce – this is in line with global trends with an incrementally higher uptake in certain areas.

In shoring up their remote employees' defenses, the top policy-related change made was **increased VPN capacity**, which was deployed by two-thirds of AMER organizations (64%) – more than the global (59%) and APJC (56%) averages and similar to Europe (64%). This is followed by **increasing web controls and acceptable use policy** at 57%, also marginally higher than global (55%), and **implementing multi-factor authentication** (51%), 2% lower than global.

- Brazil had 7 in 10 organizations increasing its VPN capacity (71%), making it the country with the highest proportion of organizations that chose to increase VPN capacity as a top cybersecurity policy change, in the region and globally.
- While AMER singled out increasing VPN capacity as their top cybersecurity policy change made during the pandemic, 67% of organizations in Mexico also made changes in endpoint protection.

Investments in cybersecurity on the rise

As a result of the challenges around the pandemic, cybersecurity budgets for more than two-thirds (68%) of organizations in AMER are expected to increase. However, almost a quarter indicated that future investments in cybersecurity will stay the same (23%), aligned with the global average (22%).



Changes in cybersecurity investments due to COVID-19	Global	APJC	AMER	Europe
Increase	66%	70%	68%	52%
Decrease	9%	11%	7%	6%
No change	22%	17%	23%	37%
Don't know	3%	2%	2%	5%

- Brazil had the highest proportion of respondents indicating that the COVID-19 situation will result in an increase in their future cybersecurity investments (78%), compared to the global average of 66% and regional average of 68%. In fact, 48% of those that reported an increase in Brazil see investments increasing by ***more than 30%*** – highest in the AMER region.

A focus on overall cybersecurity defense posture gets the lion's share (31% ranked it first) of the region's investment as the top-ranked investment priority in AMER. Other priority investments reported by AMER organizations include cloud security (25% ranked first) and network access (22% ranked first).

COUNTRY DEEP DIVE: AMER

Brazil

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 25% • During COVID-19: 76% • After COVID-19: 53%	• Pre-COVID-19: 24% • During COVID-19: 75% • After COVID-19: 46%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 58% • More important than before: 7% • Somewhat important: 4%	• Extremely important: 50% • More important than before: 38% • Somewhat important: 11%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more : 82% • Don't know: 2%	• Increase of 25% or more: 64% • Don't know: 5%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Data privacy: 68% • Secure access: 63% • Protection against malware: 61%	• Secure access: 61% • Data privacy: 56% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Customer information AND office laptops/ desktops: 58% • Personal devices: 53% • Cloud applications: 51%	• Office laptops/desktops: 59% • Personal devices: 52% • Customer information: 48% • Cloud applications: 46%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 39% • Somewhat prepared: 55% • Not prepared: 6%	• Very prepared: 39% • Somewhat prepared: 55% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 77% • Cybersecurity measures: 73% • Cloud-based document sharing: 71%	• Collaboration tools : 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 64%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 51% • Collaboration tools: 31% • Professional services: 29%	• Cybersecurity measures: 57% • Collaboration tools: 36% • Distributed data protection: 23%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 71% • Increasing web controls and acceptable use policy: 67% • Implementing multi-factor authentication: 63%	• Increased VPN capacity: 64% • Increasing web controls and acceptable use policy: 57% • Implementing multi-factor authentication: 51%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 45% • More than 30%: 55%	• 30% or less: 44% • More than 30%: 54%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Too many tools/solutions to manage and toggle: 64% • Lack of employee awareness/employee education: 55% • Inconsistent interfaces: 33%	• Lack of employee awareness/employee education: 58% • Too many tools/solutions to manage and toggle: 49% • Inconsistent interfaces: 33%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 78% • Decrease: 9% • No change: 13%	• Increase: 68% • Decrease: 7% • No change: 23%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 52% • More than 30%: 48%	• 30% or less: 56% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 34% • Cloud security: 26% • User and device verification: 23% • Network access: 16%	• Overall cybersecurity defense posture: 31% • Cloud security: 25% • Network access AND user and device verification: 22% (TIED)	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Canada

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 20% • During COVID-19: 75% • After COVID-19: 42%	• Pre-COVID-19: 24% • During COVID-19: 75% • After COVID-19: 46%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 42% • More important than before: 42% • Somewhat important: 15%	• Extremely important: 50% • More important than before: 38% • Somewhat important: 11%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 53% • Don't know: 4%	• Increase of 25% or more: 64% • Don't know: 5%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 61% • Data privacy: 54% • Maintaining control and enforcement policies AND protection against malware: 52%	• Secure access: 61% • Data privacy: 56% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Office laptops/desktops: 56% • Customer information: 50% • Personal devices: 47% • Cloud applications: 45%	• Office laptops/desktops: 59% • Personal devices: 52% • Customer information: 48% • Cloud applications: 46%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46% (TIED)
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 39% • Somewhat prepared: 56% • Not prepared: 6%	• Very prepared: 39% • Somewhat prepared: 55% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Cloud-based document sharing: 73% • Cybersecurity measures: 71% • Collaboration tools: 68%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 64%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 59% • Cloud-based document sharing: 33% • Collaboration tools: 27%	• Cybersecurity measures: 57% • Collaboration tools: 36% • Distributed data protection: 23%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 67% • Increasing web controls and acceptable use policy: 58% • Endpoint protection: 53%	• Increased VPN capacity: 64% • Increasing web controls and acceptable use policy: 57% • Implementing multi-factor authentication: 51%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 48% • More than 30%: 50%	• 30% or less: 44% • More than 30%: 54%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 58% • Too many tools/solutions to manage and toggle: 49% • Lack of visibility: 35%	• Lack of employee awareness/employee education: 58% • Too many tools/solutions to manage and toggle: 49% • Inconsistent interfaces: 33%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 74% • Decrease: 5% • No change: 19%	• Increase: 68% • Decrease: 7% • No change: 23%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 62% • More than 30%: 32%	• 30% or less: 56% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 30% • Cloud security: 27% • Network access: 22% • User and device verification: 20%	• Overall cybersecurity defense posture: 31% • Cloud security: 25% • Network access AND user and device verification: 22%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Mexico

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 19% • During COVID-19: 77% • After COVID-19: 40%	• Pre-COVID-19: 24% • During COVID-19: 75% • After COVID-19: 46%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 57% • More important than before: 34% • Somewhat important: 8%	• Extremely important: 50% • More important than before: 38% • Somewhat important: 11%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 65% • Don't know: 6%	• Increase of 25% or more: 64% • Don't know: 5%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 62% • Data privacy: 60% • Maintaining control and enforcement policies: 59%	• Secure access: 61% • Data privacy: 56% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Office laptops/desktops: 69% • Personal devices: 58% • Cloud applications: 50% • Customer information: 48%	• Office laptops/desktops: 59% • Personal devices: 52% • Customer information: 48% • Cloud applications: 46%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46% (TIED)
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 33% • Somewhat prepared: 60% • Not prepared: 7%	• Very prepared: 39% • Somewhat prepared: 55% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	· Collaboration tools: 81% · Cybersecurity measures: 65% · Cloud-based document sharing: 64%	· Collaboration tools: 73% · Cybersecurity measures: 68% · Cloud-based document sharing: 64%	· Collaboration tools: 73% · Cybersecurity measures: 68% · Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	· Cybersecurity measures: 56% · Collaboration tools: 42% · Distributed data protection: 29%	· Cybersecurity measures: 57% · Collaboration tools: 36% · Distributed data protection: 23%	· Cybersecurity measures: 52% · Collaboration tools: 41% · Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	· Endpoint protection AND increased VPN capacity: 67% · Increasing web controls and acceptable use policy: 61%	· Increased VPN capacity: 64% · Increasing web controls and acceptable use policy: 57% · Implementing multi-factor authentication: 51%	· Increased VPN capacity: 59% · Increasing web controls and acceptable use policy: 55% · Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	· 30% or less: 46% · More than 30%: 51%	· 30% or less: 44% · More than 30%: 54%	· 30% or less: 50% · More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	· Lack of employee awareness/employee education: 63% · Too many tools/solutions to manage and toggle: 50% · Inconsistent interfaces: 34%	· Lack of employee awareness/employee education: 58% · Too many tools/solutions to manage and toggle: 49% · Inconsistent interfaces: 33%	· Lack of employee awareness/employee education: 59% · Too many tools/solutions to manage and toggle: 50% · Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 2% • Decrease: 8% • No change: 28%	• Increase: 68% • Decrease: 7% • No change: 23%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 60% • More than 30%: 36%	• 30% or less: 56% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 30% • Cloud security: 28% • User and device verification: 22% • Network access: 20%	• Overall cybersecurity defense posture: 31% • Cloud security: 25% • Network access AND user and device verification: 22%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

United States

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 32% • During COVID-19: 71% • After COVID-19: 50%	• Pre-COVID-19: 24% • During COVID-19: 75% • After COVID-19: 46%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 43% • More important than before: 39% • Somewhat important: 17%	• Extremely important: 50% • More important than before: 38% • Somewhat important: 11%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 54% • Don't know: 10%	• Increase of 25% or more: 64% • Don't know: 5%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 59% • Maintaining control and enforcement policies: 48% • Data privacy: 43%	• Secure access – 61% • Data privacy – 56% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Office laptops/desktops: 53% • Personal devices: 48% • Cloud applications: 39% • Customer information: 35%	• Office laptops/desktops: 59% • Personal devices: 52% • Customer information: 48% • Cloud applications: 46%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 46% • Somewhat prepared: 48% • Not prepared: 6%	• Very prepared: 39% • Somewhat prepared: 55% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools AND cybersecurity measures: 64% • Cloud-based document sharing: 49%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 64%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 62% • Collaboration tools: 42% • Professional services: 26%	• Cybersecurity measures: 57% • Collaboration tools: 36% • Distributed data protection: 23%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 53% • Implementing multi-factor authentication: 44% • Increasing web controls and acceptable use policy: 41%	• Increased VPN capacity: 64% • Increasing web controls and acceptable use policy: 57% • Implementing multi-factor authentication: 51%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 36% • More than 30%: 59%	• 30% or less: 44% • More than 30%: 4%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 56% • Too many tools/solutions to manage and toggle: 35% • Inconsistent interfaces: 32%	• Lack of employee awareness/employee education: 58% • Too many tools/solutions to manage and toggle: 49% • Inconsistent interfaces: 33%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 57% • Decrease: 8% • No change: 31%	• Increase: 68% • Decrease: 7% • No change: 23%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 49% • More than 30%: 40%	• 30% or less: 56% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Network access AND overall cybersecurity defense posture: 30% • User and device verification: 21% • Cloud security: 19%	• Overall cybersecurity defense posture: 31% • Cloud security: 25% • Network access AND user and device verification: 22%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

ASIA PACIFIC HIGHLIGHTS

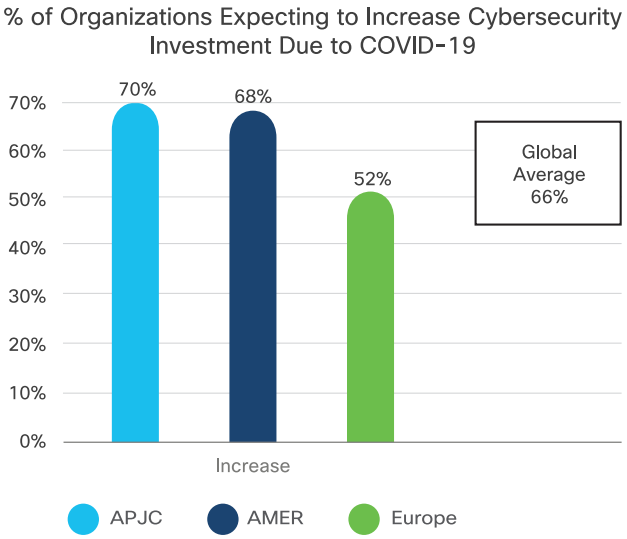
ASIA PACIFIC HIGHLIGHTS

Regional Summary

The study surveyed over 1900 organizations from 13 markets in APJC. This helped Cisco understand how organizations within the APJC region differed from their global counterparts in responding to the coronavirus crisis and, subsequently, how they adapted to support their remote workforce and their future cybersecurity plans in enabling a distributed future of work.

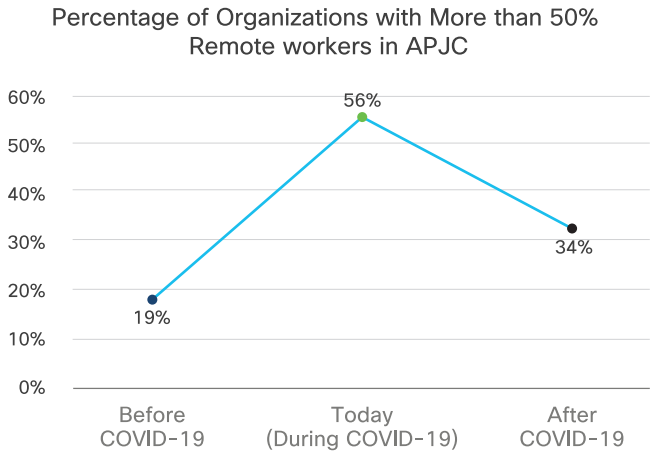
Consistent with the global average, 54% of APJC organizations stated that they were ***somewhat prepared*** in supporting the sudden transition to a remote workforce. Seven percent of organizations in the APJC region said they were ***not prepared*** for the transition, 1% less prepared compared to the global, AMER, and European averages.

While the majority of APJC organizations are still navigating the demands and constraints of their new workplace dynamics, the good news is 70% of respondents indicated that the COVID-19 situation will spur them to increase their cybersecurity investments. This makes APJC the region with the highest number of organizations that are looking to increase their cybersecurity investments amongst all three regions



Key Findings

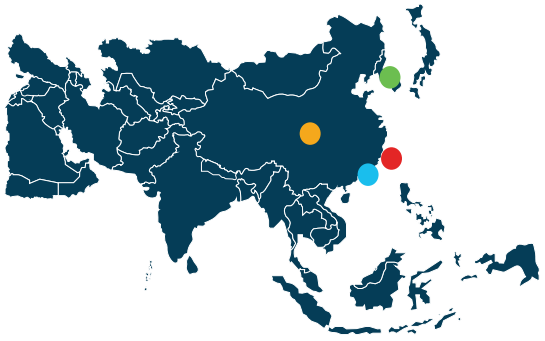
Remote worker flow consistent with global averages but certain markets bucked the trend.



	Global	APJC
Before COVID-19	19%	19%
Today (During COVID-19)	62%	56%
After COVID-19	37%	34%

While APJC is in line with global trends in the shift to a hybrid work environment, several differentiations exist:

- At the height of COVID-19, organizations in **Korea, Hong Kong and Taiwan all recorded lower numbers of remote workers** compared to the rest of the world, where only 26%, 45%, and 32% of organizations from these countries reported mobilizing ***more than half*** of their employees to work from home.
- Organizations in **China**, on the other hand, recorded an even split between remote and in-office workers at 50%.



26% Korea

32% Taiwan

45% Hong Kong

50% China

These findings may very well coincide with the fact that Taiwan never instituted any mass or nationwide lockdown measures throughout the pandemic, whereas countries that were the earliest hit, China, Korea, and Hong Kong, were able to get a firm grasp of the pandemic early on, thereby reducing the need to institutionalize remote work for a majority of their respective workforces.

Developed and developing countries defied expectations in their remote working readiness and cybersecurity prioritization

While developing countries like Vietnam, India, and Indonesia are ahead of the curve in their preparedness to transition to remote working, some of the world's most technologically advanced countries, like Japan (17%) and Korea (12%), had a higher-than-average number of organizations that were ***not prepared*** for this shift. This was also mirrored by the Philippines (12%).

APJC organizations' prioritization of cybersecurity is in line with the global average. Eighty-five percent of the region's organizations indicated that security is ***extremely important*** or ***more important than before the pandemic***. Within the region, the Philippines (93%), Singapore (89%), Thailand (87%), and Vietnam (93%) had more organizations seeing cybersecurity as a top priority compared to the regional and global averages.

Tackling cybersecurity threats and challenges in APJC

More organizations in APJC experienced a jump of ***25% or more*** in cyber threats or alerts since the start of COVID-19 compared to the global average of 61%. Within the APJC region, India (73%), Indonesia (78%), Korea (74%), Taiwan (73%), and Vietnam (91%) had more organizations experience a jump of ***25% or more*** in cyber threats and alerts compared to the regional average of 69%.

Ten percent of organizations in Malaysia and 15% of organizations in Japan did not know if their cyber threats or alerts have increased or decreased, higher than the global average of 8%. This is a cause of concern as visibility is critical when it comes to an organization's cybersecurity defense posture; you can't protect what you can't see.

Securing devices is ubiquitous when it comes to remote work with more than half of organizations in APJC stating that office laptops/ desktops (58%) and personal devices (57%) are a challenge to protect in a remote environment.

However, more APJC businesses flagged cloud applications as the third challenge to protect (52%) compared to 46% of organizations in AMER and 27% in Europe.

Global	APJC	AMER	Europe
Office laptops/ desktops (56%)	Office laptops/ desktops (58%)	Office laptops/ desktops (59%)	Personal devices (47%)
Personal devices (54%)	Personal devices (57%)	Personal devices (52%)	Office laptops/ desktops (47%)
Customer information (46%)	Cloud applications (52%)	Customer information (48%)	Customer information (28%)

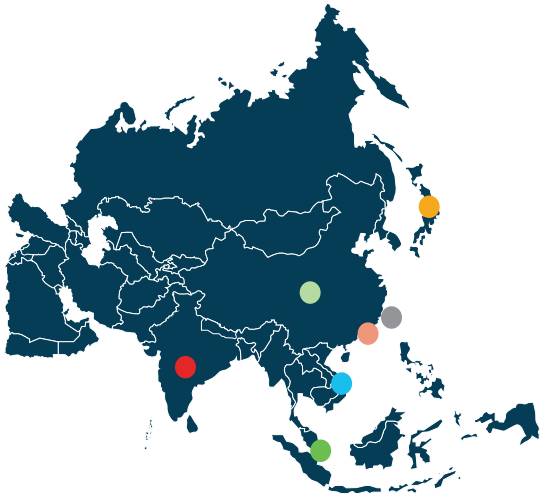
Prioritizing cybersecurity for what's now and what's next

Ninety-seven percent of organizations in APJC made changes to their cybersecurity policies in line with the global average of 96%. These changes included:

- Increasing web controls and acceptable use policy (61%), followed by implementing multi-factor authentication (59%) and increasing VPN capacity (56%).

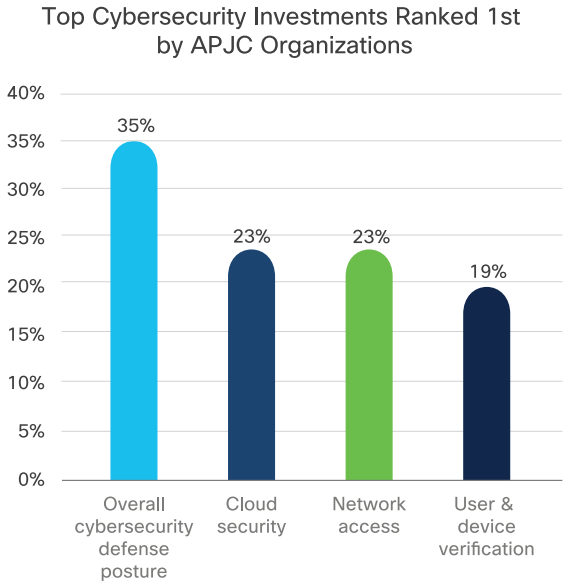
APJC organizations are the most optimistic when it comes to increasing their future cybersecurity investments to prepare for the new realities of a flexible and hybrid work environment. Seventy percent of organizations in APJC indicated that they will increase their cybersecurity investments because of COVID-19, compared to 68% in AMER and 52% in Europe.

- More than half of the APJC countries surveyed (Singapore, Vietnam, India, Japan, China, Hong Kong, and Taiwan) had more than 70% of organizations indicating possible increases in cybersecurity investments, higher than the regional average.
- Surpassing the 80% mark, Hong Kong has the highest number of organizations in the world that are expected to increase cybersecurity investments.



76% Singapore
72% China
78% Vietnam
80% Hong Kong
77% India
72% Taiwan
71% Japan

These investments will be possibly channeled into an overall cybersecurity defense posture as the most important investment (35% ranked first). Other priority investments reported by organizations included cloud security and network access (23% ranked first, respectively) and user device and verification (19% ranked first). This is similar to global trends, as organizations worldwide look to address and rethink the best ways to support the flexible and hybrid future of work that is here to stay.



COUNTRY DEEP DIVE: ASIA PACIFIC

Australia

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 22% • During COVID-19: 70% • After COVID-19: 39%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 49% • More important than before: 35% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 57% • Don't know: 7%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 53% • Verifying identity: 52% • Protection against malware: 51%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Cloud applications: 54% • Personal devices AND office laptops/desktops: 51% • Customer Information: 46%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 46% • Somewhat prepared: 50% • Not prepared: 4%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	· Cybersecurity measures: 71% · Collaboration tools: 70% · Cloud-based document sharing: 65%	· Collaboration tools: 73% · Cybersecurity measures: 68% · Cloud-based document sharing: 65%	· Collaboration tools: 73% · Cybersecurity measures: 68% · Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	· Cybersecurity measures: 60% · Collaboration tools: 36% · Professional services: 28%	· Cybersecurity measures: 50% · Collaboration tools: 41% · Professional services: 29%	· Cybersecurity measures: 52% · Collaboration tools: 41% · Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	· Increased VPN capacity: 62% · Increasing web controls and acceptable use policy AND implementing multi-factor authentication: 57% · Endpoint protection: 55%	· Increasing web controls and acceptable use policy: 61% · Implementing multi-factor authentication: 59% · Increased VPN capacity: 56%	· Increased VPN capacity: 59% · Increasing web controls and acceptable use policy: 55% · Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	· 30% or less: 48% · More than 30%: 49%	· 30% or less: 54% · More than 30%: 41%	· 30% or less: 50% · More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	· Lack of employee awareness/employee education: 57% · Too many tools/solutions to manage and toggle: 51% · Lack of visibility: 40%	· Lack of employee awareness/employee education: 61% · Too many tools/solutions to manage and toggle: 53% · Inconsistent interfaces: 40%	· Lack of employee awareness/employee education: 59% · Too many tools/solutions to manage and toggle: 50% · Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 65% • Decrease: 12% • No change: 20%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 52% • More than 30%: 43%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 39% • User and device verification, cloud security AND network access: 20%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security: 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access : 24% • Cloud security: 22% • User and device verification: 20%

China

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 16% • During COVID-19: 50% • After COVID-19: 22%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 28% • More important than before: 54% • Somewhat important: 18%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 61% • Don't know: 7%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Data privacy: 63% • Secure access: 60% • Verifying identity: 56%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Customer information: 56% • Office laptops/desktops: 53% • Personal devices: 50% • Cloud applications: 42%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 22% • Somewhat prepared: 71% • Not prepared: 6%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 76% • Cybersecurity measures: 68% • Cloud-based document sharing: 57%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 65%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Collaboration tools: 58% • Cybersecurity measures: 52% • Cloud-based document sharing: 16%	• Cybersecurity measures: 50% • Collaboration tools: 41% • Professional services: 29%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increasing web controls and acceptable use policy: 70% • Implementing multi-factor authentication: 63% • Endpoint protection: 56%	• Increasing web controls and acceptable use policy: 61% • Implementing multi-factor authentication: 59% • Increased VPN capacity: 56%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 60% • More than 30%: 36%	• 30% or less: 54% • More than 30%: 41%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Too many tools/solutions to manage and toggle: 56% • Lack of employee awareness/employee education: 48% • Inconsistent interfaces: 43%	• Lack of employee awareness/employee education: 61% • Too many tools/solutions to manage and toggle: 53% • Inconsistent interfaces: 40%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 72% • Decrease: 14% • No change: 13%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 70% • More than 30%: 25%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 43% • Cloud security: 22% • Network access: 20% • User and device verification: 15%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security; 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Hong Kong

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 9% • During COVID-19: 45% • After COVID-19: 15%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 27% • More important than before: 55% • Somewhat important: 18%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 67% • Don't know: 7%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 60% • Data privacy: 54% • Verifying identity: 52%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Office laptops/desktops: 56% • Personal devices: 55% • Customer information: 48% • Cloud applications: 43%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 32% • Somewhat prepared: 65% • Not prepared: 2%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools AND cybersecurity measures: 78% • Cloud-based document sharing: 75%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 65%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 57% • Collaboration tools: 38% • Cloud-based document sharing: 18%	• Cybersecurity measures: 50% • Collaboration tools: 41% • Professional services: 29%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 66% • Increasing web controls and acceptable use policy: 65% • Implementing multi-factor authentication: 58%	• Increasing web controls and acceptable use policy: 61% • Implementing multi-factor authentication: 59% • Increased VPN capacity: 56%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 59% • More than 30%: 40%	• 30% or less: 54% • More than 30%: 41%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 67% • Too many tools/solutions to manage and toggle: 61% • Inconsistent interfaces: 35%	• Lack of employee awareness/employee education: 61% • Too many tools/solutions to manage and toggle: 53% • Inconsistent interfaces: 40%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 80% • Decrease: 5% • No change: 13%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 74% • More than 30%: 22%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 43% • User and device verification: 23% • Cloud security: 21% • Network access: 13%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security: 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

India

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 28% • During COVID-19: 73% • After COVID-19: 53%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 56% • More important than before: 28% • Somewhat important: 13%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 73% • Don't know: 4%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 68% • Data privacy: 66% • Protection against malware: 62%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Office laptops/desktops: 66% • Personal devices: 58% • Customer information: 51% • Cloud applications: 42%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 54% • Somewhat prepared: 40% • Not prepared: 5%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Cybersecurity measures: 65% • Collaboration tools: 64% • Cloud-based document sharing: 60%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 65%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 56% • Collaboration tools: 35% • Professional services: 30%	• Cybersecurity measures: 50% • Collaboration tools: 41% • Professional services: 29%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Implementing multi-factor authentication: 66% • Increasing web controls and acceptable use policy AND increased VPN capacity: 62%	• Increasing web controls and acceptable use policy: 61% • Implementing multi-factor authentication: 59% • Increased VPN capacity: 56%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 44% • More than 30%: 54%	• 30% or less: 54% • More than 30%: 41%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Too many tools/solutions to manage and toggle: 60% • Lack of employee awareness/employee education: 55% • Inconsistent interfaces: 42%	• Lack of employee awareness/employee education - 61% • Too many tools/solutions to manage and toggle: 53% • Inconsistent interfaces: 40%	• Lack of employee awareness/employee education - 59% • Too many tools/solutions to manage and toggle - 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 77% • Decrease: 13% • No change: 7%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 51% • More than 30%: 47%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Cloud security: 31% • Network access: 25% • Overall cybersecurity defense posture: 25% • User and device verification: 19%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security: 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Indonesia

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 22% • During COVID-19: 52% • After COVID-19: 32%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 59% • More important than before: 26% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 78% • Don't know: 5%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Data privacy: 70% • Secure access: 70% • Protection against malware: 63%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Office laptops/desktops: 74% • Cloud applications: 68% • Customer information: 68% • Personal devices: 61%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 49% • Somewhat prepared: 46% • Not prepared: 5%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 73% • Cloud-based document sharing: 68% • Cybersecurity measures: 63%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 65%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 51% • Collaboration tools: 37% • Professional services: 32%	• Cybersecurity measures: 50% • Collaboration tools: 41% • Professional services: 29%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	• Increasing web controls and acceptable use policy: 76% • Endpoint protection: 62% • Implementing multi-factor authentication: 61%	• Increasing web controls and acceptable use policy: 61% • Implementing multi-factor authentication: 59% • Increased VPN capacity: 56%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 53% • More than 30%: 43%	• 30% or less: 54% • More than 30%: 41%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 74% • Inconsistent interfaces: 51% • Lack of visibility: 45%	• Lack of employee awareness/employee education: 61% • Too many tools/solutions to manage and toggle: 53% • Inconsistent interfaces: 40%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 63% • Decrease: 15% • No change: 18%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 56% • More than 30%: 40%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 35% • Network access: 28% • Cloud security: 19% • User and device verification: 18%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security: 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Japan

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 13% • During COVID-19: 65% • After COVID-19: 32%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 34% • More important than before: 44% • Somewhat important: 19%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 55% • Don't know: 15%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 68% • Data privacy: 62% • Maintaining control and enforcement policies: 46%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Office laptops/desktops: 58% • Personal devices: 48% • Cloud applications: 46% • Customer information: 42%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications:52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 19% • Somewhat prepared: 63% • Not prepared: 17%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 68% • Cybersecurity measures: 58% • Cloud-based document sharing: 56%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 65%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 57% • Collaboration tools: 56% • Cloud-based document sharing: 29%	• Cybersecurity measures: 50% • Collaboration tools: 41% • Professional services: 29%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 49% • Endpoint protection: 36% • Increasing web controls and acceptable use policy AND implementing multi-factor authentication: 35%	• Increasing web controls and acceptable use policy: 61% • Implementing multi-factor authentication: 59% • Increased VPN capacity: 56%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 54% • More than 30%: 33%	• 30% or less: 54% • More than 30%: 41%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 56% • Too many tools/solutions to manage and toggle: 47% • Inconsistent interfaces: 29%	• Lack of employee awareness/employee education: 61% • Too many tools/solutions to manage and toggle: 53% • Inconsistent interfaces: 40%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 71% • Decrease: 3% • No change: 25%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 62% • More than 30%: 29%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 39% • Network access: 28% • User and device verification: 17% • Cloud security: 16%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security: 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Korea

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 14% • During COVID-19: 26% • After COVID-19: 28%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 26% • More important than before: 50% • Somewhat important: 24%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 74% • Don't know: 3%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 50% • Data privacy: 48% • Protection against malware AND maintaining control and enforcement policies: 44%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Cloud applications: 46% • Personal devices: 45% • Office laptops/desktops: 43% • Customer information: 36%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 24% • Somewhat prepared: 64% • Not prepared: 12%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	· Cloud-based document sharing: 64% · Collaboration tools: 60% · Cybersecurity measures: 56%	· Collaboration tools: 73% · Cybersecurity measures: 68% · Cloud-based document sharing: 65%	· Collaboration tools: 73% · Cybersecurity measures: 68% · Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	· Collaboration tools: 47% · Cybersecurity measures: 44% · Cloud-based document sharing: 39%	· Cybersecurity measures: 50% · Collaboration tools: 41% · Professional services: 29%	· Cybersecurity measures: 52% · Collaboration tools: 41% · Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	· Increasing web controls and acceptable use policy: 54% · Implementing multi-factor authentication:46% · Endpoint protection: 44%	· Increasing web controls and acceptable use policy: 61% · Implementing multi-factor authentication: 59% · Increased VPN capacity: 56%	· Increased VPN capacity: 59% · Increasing web controls and acceptable use policy: 55% · Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	· 30% or less: 72% · More than 30%: 23%	· 30% or les: 54% · More than 30%: 41%	· 30% or less: 50% · More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	· Lack of employee awareness/employee education: 58% · Too many tools/solutions to manage and toggle: 50% · Inconsistent interfaces: 39%	· Lack of employee awareness/employee education: 61% · Too many tools/solutions to manage and toggle: 53% · Inconsistent interfaces: 40%	· Lack of employee awareness/employee education: 59% · Too many tools/solutions to manage and toggle: 50% · Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 68% • Decrease: 15% • No change: 17%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 73% • More than 30%: 27%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 36% • Cloud security: 23% • User and device verification AND Network access: 21%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security: 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Malaysia

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 20% • During COVID-19: 60% • After COVID-19: 35%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 32% • More important than before: 49% • Somewhat important: 18%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 62% • Don't know: 10%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 74% • Data privacy: 65% • Maintaining control and enforcement policies: 60%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Personal devices: 62% • Office laptops/desktops: 58% • Customer information:56% • Cloud applications: 55%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 36% • Somewhat prepared: 56% • Not prepared: 7%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 75% • Cybersecurity measures: 63% • Cloud-based document sharing: 62%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 65%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Collaboration tools: 46% • Cybersecurity measures: 40% • Professional services: 40%	• Cybersecurity measures: 50% • Collaboration tools: 41% • Professional services: 29%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increasing web controls and acceptable use policy: 64% • Endpoint protection: 61% • Increased VPN capacity: 60%	• Increasing web controls and acceptable use policy: 61% • Implementing multi-factor authentication: 59% • Increased VPN capacity: 56%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 54% • More than 30%: 41%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 67% • Too many tools/solutions to manage and toggle: 48% • Lack of visibility AND Inconsistent interfaces: 47%	• Lack of employee awareness/employee education: 61% • Too many tools/solutions to manage and toggle: 53% • Inconsistent interfaces: 40%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 56% • Decrease: 5% • No change: 37%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 56% • More than 30%: 39%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 34% • Network access: 28% • Cloud security: 22% • User and device verification: 16%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security: 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Philippines

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 29% • During COVID-19: 71% • After COVID-19: 48%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 64% • More important than before: 29% • Somewhat important: 7%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 66% • Don't know: 7%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access AND Maintaining control and enforcement policies: 62% • Data privacy: 56%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Office laptops/desktops: 63% • Personal devices: 58% • Customer information: 49% • Cloud applications: 46%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 41% • Somewhat prepared: 47% • Not prepared: 12%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	· Collaboration tools: 74% · Cybersecurity measures: 66% · Cloud-based document sharing: 59%	· Collaboration tools: 73% · Cybersecurity measures: 68% · Cloud-based document sharing: 65%	· Collaboration tools: 73% · Cybersecurity measures: 68% · Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	· Cybersecurity measures: 58% · Collaboration tools: 38% · Professional services: 31%	· Cybersecurity measures: 50% · Collaboration tools: 41% · Professional services: 29%	· Cybersecurity measures: 52% · Collaboration tools: 41% · Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	· Increasing web controls and acceptable use policy: 64% · Increased VPN capacity: 59% · Implementing multi-factor authentication: 54%	· Increasing web controls and acceptable use policy: 61% · Implementing multi-factor authentication: 59% · Increased VPN capacity: 56%	· Increased VPN capacity: 59% · Increasing web controls and acceptable use policy: 55% · Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	· 30% or less: 38% · More than 30%: 56%	· 30% or less: 54% · More than 30%: 41%	· 30% or less: 50% · More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	· Lack of employee awareness/employee education: 66% · Too many tools/solutions to manage and toggle: 48% · Lack of visibility: 46%	· Lack of employee awareness/employee education: 61% · Too many tools/solutions to manage and toggle: 53% · Inconsistent interfaces: 40%	· Lack of employee awareness/employee education: 59% · Too many tools/solutions to manage and toggle: 50% · Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 69% • Decrease: 14% • No change: 13%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 37% • More than 30%: 58%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 34% • Network access: 31% • Cloud security: 23% • User and device verification: 12%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security: 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Singapore

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 18% • During COVID-19: 77% • After COVID-19: 40%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely importan: 50% • More important than before: 39% • Somewhat important: 10%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 64% • Don't know: 5%	• Increase of 25% or more: 61% • Don't know: 8%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Maintaining control and enforcement policies: 58% • Secure access: 56% • Data privacy: 52%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Personal devices: 56% • Office laptops/desktops: 54% • Cloud applications: 44% • Customer information: 44%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 42% • Somewhat prepared: 54% • Not prepared: 3%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 76% • Cybersecurity measures: 75% • Cloud-based document sharing: 70%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 65%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 44% • Collaboration tools: 34% • Cloud-based document sharing: 26%	• Cybersecurity measures: 50% • Collaboration tools: 41% • Professional services: 29%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 66% • Implementing multi-factor authentication: 63% • Endpoint protection: 60%	• Increasing web controls and acceptable use policy: 61% • Implementing multi-factor authentication: 59% • Increased VPN capacity: 56%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 51% • More than 30%: 43%	• 30% or less: 54% • More than 30%: 41%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Too many tools/solutions to manage and toggle: 57% • Lack of employee awareness/employee education: 55% • Inconsistent interfaces: 47%	• Lack of employee awareness/employee education: 61% • Too many tools/solutions to manage and toggle: 53% • Inconsistent interfaces: 40%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 76% • Decrease: 8% • No change: 14%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 57% • More than 30%: 41%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 37% • Cloud security AND user and device verification: 23% • Network access: 17%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security: 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Taiwan

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 14% • During COVID-19: 32% • After COVID-19: 22%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 38% • More important than before: 47% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 73% • Don't know: 4%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 54% • Verifying identity: 50% • Protection against malware: 49%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Personal devices: 69% • Cloud applications: 62% • Office laptops/desktops: 59% • Customer information: 56%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 32% • Somewhat prepared: 58% • Not prepared: 9%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Cybersecurity measures: 78% • Collaboration tools: 77% • Cloud-based document sharing: 68%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 65%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 53% • Collaboration tools: 33% • Cloud-based document sharing: 20%	• Cybersecurity measures: 50% • Collaboration tools: 41% • Professional services: 29%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	• Implementing multi-factor authentication: 73% • Endpoint protection: 58% • Increasing web controls and acceptable use policy: 56%	• Increasing web controls and acceptable use policy: 61% • Implementing multi-factor authentication: 59% • Increased VPN capacity: 56%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 55% • More than 30%: 41%	• 30% or less: 54% • More than 30%: 41%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 58% • Too many tools/solutions to manage and toggle: 51% • Inconsistent interfaces: 39%	• Lack of employee awareness/employee education: 61% • Too many tools/solutions to manage and toggle: 53% • Inconsistent interfaces: 40%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 72% • Decrease: 11% • No change: 17%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 59% • More than 30%: 41%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 39% • Cloud security: 23% • User and device verification: 21% • Network access: 17%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security: 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Thailand

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 20% • During COVID-19: 53% • After COVID-19: 42%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 42% • More important than before: 44% • Somewhat important: 13%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 69% • Don't know: 4%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 78% • Verifying identity: 65% • Maintaining control and enforcement policies: 63%	• Secure access: 63% • Data privacy:59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Personal devices: 69% • Cloud applications: 63% • Office laptops/desktops: 58% • Customer information: 51%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 38% • Somewhat prepared: 59% • Not prepared: 3%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 80% • Cybersecurity measures: 68% • Cloud-based document sharing: 68%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 65%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 48% • Collaboration tools: 44% • Distributed data protection: 19%	• Cybersecurity measures: 50% • Collaboration tools: 41% • Professional services: 29%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services:27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Implementing multi-factor authentication: 66% • Increasing web controls and acceptable use policy AND increased VPN capacity: 55%	• Increasing web controls and acceptable use policy: 61% • Implementing multi-factor authentication: 59% • Increased VPN capacity: 56%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 52% • More than 30%: 42%	• 30% or less: 54% • More than 30%: 41%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 71% • Too many tools/solutions to manage and toggle: 46% • Lack of visibility: 35%	• Lack of employee awareness/employee education: 61% • Too many tools/solutions to manage and toggle: 53% • Inconsistent interfaces: 40%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 61% • Decrease: 16% • No change: 22%	• Increase: 70% • Decrease: 11% • No change: 17%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 56% • More than 30%: 43%	• 30% or less: 58% • More than 30%: 39%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Cloud security: 32% • Network access: 30% • Overall cybersecurity defense posture: 20% • User and device verification: 18%	• Overall cybersecurity defense posture: 35% • Network access AND cloud security: 23% • User and device verification: 19%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Vietnam

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 20% • During COVID-19: 51% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 56% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 64% • More important than before: 28% • Somewhat important: 7%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 91% • Don't know: 1%	• Increase of 25% or more: 69% • Don't know: 6%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Protection against malware: 71% • Secure access: 69% • Data privacy: 66%	• Secure access: 63% • Data privacy: 59% • Maintaining control and enforcement policies: 53%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Personal devices: 65% • Customer information: 61% • Office laptops/desktops: 60% • Cloud applications: 59%	• Office laptops/desktops: 58% • Personal devices: 57% • Cloud applications: 52% • Customer information: 51%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 67% • Somewhat prepared: 30% • Not prepared: 3%	• Very prepared: 39% • Somewhat prepared: 54% • Not prepared: 7%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	· Cybersecurity measures: 80% · Collaboration tools: 78% · Cloud-based document sharing: 76%	· Collaboration tools: 73% · Cybersecurity measures: 68% · Cloud-based document sharing: 65%	· Collaboration tools: 73% · Cybersecurity measures: 68% · Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	· Cybersecurity measures: 36% · Collaboration tools: 28% · Distributed data protection: 27%	· Cybersecurity measures:50% · Collaboration tools: 41% · Professional services: 29%	· Cybersecurity measures: 52% · Collaboration tools: 41% · Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	· Implementing multi-factor authentication: 76% · Increasing web controls and acceptable use policy: 76% · Endpoint protection: 60%	· Increasing web controls and acceptable use policy: 61% · Implementing multi-factor authentication: 59% · Increased VPN capacity: 56%	· Increased VPN capacity: 59% · Increasing web controls and acceptable use policy: 55% · Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	· 30% or less: 54% · More than 30%: 41%	· 30% or less: 54% · More than 30%: 41%	· 30% or less: 50% · More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	· Too many tools/solutions to manage and toggle: 74% · Lack of employee awareness/employee education: 62% · Inconsistent interfaces: 37%	· Lack of employee awareness/employee education: 61% · Too many tools/solutions to manage and toggle: 53% · Inconsistent interfaces: 40%	· Lack of employee awareness/employee education: 59% · Too many tools/solutions to manage and toggle: 50% · Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	· Increase: 78% · Decrease: 14% · No change: 8%	· Increase: 70% · Decrease: 11% · No change: 17%	· Increase: 66% · Decrease: 9% · No change: 22%
Proportion of increase in future cybersecurity investment	· 30% or less: 51% · More than 30%: 49%	· 30% or less: 58% · More than 30%: 39%	· 30% or less: 59% · More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	· Overall cybersecurity defense posture: 32% · User and device verification: 28% · Cloud security: 26% · Network access: 14%	· Overall cybersecurity defense posture: 35% · Network access AND cloud security: 23% · User and device verification: 19%	· Overall cybersecurity defense posture: 34% · Network access: 24% · Cloud security: 22% · User and device verification: 20%

EUROPE HIGHLIGHTS

EUROPE HIGHLIGHTS

Regional Summary

The study surveyed over 600 respondents from four countries in Europe – France, Germany, Italy, and the United Kingdom. Based on data gleaned from the respondents, COVID-19 has had a similar impact across Europe where remote work will earn, in some capacity, a permanent place in the employment mix. Thirty-four percent of organizations believe that ***more than half*** of their employees will continue working remotely post-pandemic

Contrary to their regional counterparts, organizations in Europe appear to be better prepared in supporting the sudden transition to a remote workforce. While 45% stated that they were ***very prepared*** (compared to 40% globally and 39% in APJC and AMER, respectively), 50% said they were ***somewhat prepared*** (compared to 53% globally), and 6% said they were ***not prepared*** (tied with AMER and the global averages).

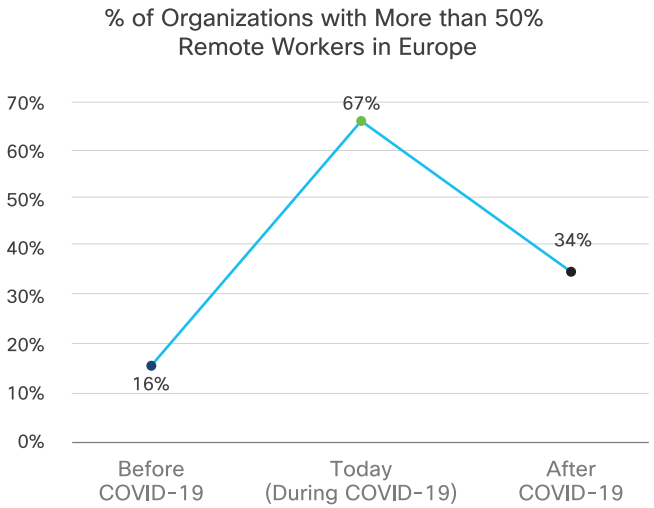
While only 37% of European respondents experienced a jump of ***25% or more*** in cyber threats or alerts, lower than the 61% global average, a worrying 17% of European respondents did not know if there was an increase or decrease in cyber threats or alerts at all. This is significantly higher than the AMER (5%) and APJC (6%) averages.

	Global	APJC	AMER	Europe
Increase in cyber alerts or attacks (25% or more)	61%	69%	64%	37%
Don't know	8%	6%	5%	17%

Just over half (52%) of organizations in Europe indicated that the COVID-19 situation will result in an increase in future cybersecurity investments. This makes Europe the region with the ***smallest proportion of organizations expecting an increase in cybersecurity investments among the three regions,*** compared to the global average of 66%. Thirty-seven percent said there will be no change to their organization's investment, the highest when compared to the AMER (23%) and APJC (17%) averages.

Key Findings

The shift to a hybrid work environment continues in Europe but at varying levels



Europe had the lowest proportion of remote workers prior to the pandemic with just 16% of organizations reporting having more than half of their workforce remote – slightly below the global average (19%). Once the pandemic hit, the proportion of organizations with ***more than half*** of their workforce remote surged to 67%, higher than the global average of 62%. Looking ahead post-COVID-19, 34% of European organizations are expecting more than half of their employees to continue working remotely, double the proportion before the outbreak.

- While respondents in France and Italy saw a four-fold increase in the proportion of organizations with ***more than half*** of their workforce being remote pre-pandemic (15% respectively) versus at the height of the pandemic (64% in France and 65% in Italy), the United Kingdom experienced the highest increase in remote workers in the world, with 85% of organizations with ***more than half*** of their workforce remote during the pandemic (up from 18% pre-pandemic). This is likely due to the country's stringent lockdown measures at the height of the outbreak.
- According to the data, more organizations in the United Kingdom (50%) are expecting ***more than half*** of their employees to continue working remotely post-COVID-19, the highest increase in remote workers of those countries surveyed in the world (ahead of the global average of 37%).
- Organizations in France (32%), Germany (24%), and Italy (33%) are also expecting to have more remote workers post-pandemic, compared to their pre-COVID-19 levels, though these numbers are lower than the global average.

32%
France

24%
Germany

33%
Italy

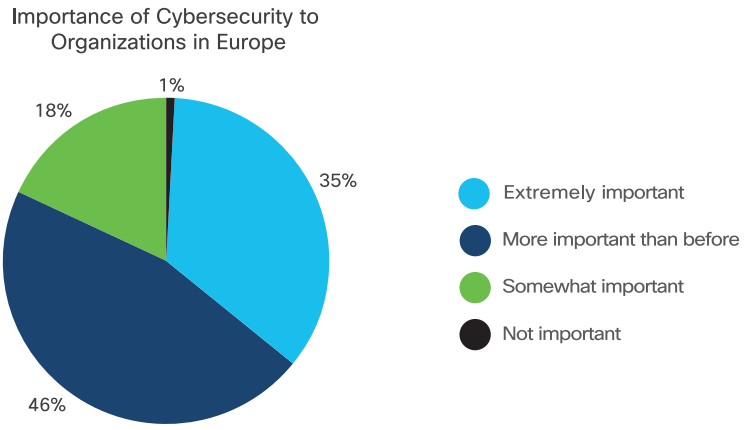
The United Kingdom had the second highest proportion of organizations that reported to be ***very prepared*** (59%) to make the accelerated transition to a remote work environment at the outset of COVID-19, in the world, after Vietnam (67%). Meanwhile, France and Italy saw the highest proportion of organizations ***not prepared*** for the transition in Europe, with a higher than global average of 9% and 8%, respectively.

Cybersecurity preparedness to transition to remote working	France	Germany	Italy	UK
Very prepared	43%	41%	35%	59%
Somewhat prepared	47%	55%	57%	39%
Not prepared	9%	4%	8%	2%

Cybersecurity Preparedness to Transition to Remote Working by Country

Cybersecurity is important but not important enough

At a time when businesses are facing an onslaught of challenges from the sudden and massive transition to remote work, Europe had the most organizations attesting to cybersecurity being ***more important than before*** at 46%, which is higher than global and APJC (41%) as well as AMER (38%) averages. Yet it still had the smallest proportion of organizations recognizing that cybersecurity is ***extremely important*** at 35%.



Importance of cybersecurity	Global	APJC	AMER	Europe
Extremely important	44%	44%	50%	35%
More important than before	41%	41%	38%	46%
Somewhat important	15%	15%	11%	18%
Not important	1%	1%	1%	1%

Importance of Cybersecurity to the Organization Regional vs. Global Average

- Delving deeper, the level of cybersecurity importance also varies within Europe itself. Forty-six percent of organizations in the United Kingdom said cybersecurity is ***extremely important***, 2% higher than the global average (44%), whereas the rest of the European countries surveyed (France, Germany, and Italy) had a higher proportion of organizations indicating that cybersecurity is ***more important than it was before***.

- Europe is also the region with the most organizations saying cybersecurity is only ***somewhat important***, at 18%, higher than the global average of 15%.

Importance of cybersecurity	France	Germany	Italy	U.K.
Extremely important	34%	32%	28%	46%
More important than before	44%	47%	57%	35%
Somewhat important	20%	19%	15%	17%
Not important	2%	1%	-	1%

Importance of Cybersecurity to the Organization by Country

Organizations in Europe experienced the smallest increase in cyber threats or alerts since the pandemic but many are not completely certain

As highlighted earlier, most European organizations reported a lower level of increase in cyber threats or alerts compared to their regional counterparts in AMER and APJC. However, they also recorded the largest proportion of organizations that are uncertain about the increase or decrease in cyber threats or alerts.

Breaking this down further, close to half of organizations in France (48%) experienced an increase of ***25% or more*** in cyber threats or alerts during the pandemic, the highest observed among the four European countries surveyed, and also higher than the regional average (37%).

On the flip side, while only 24% of U.K. organizations experienced an increase of ***25% or more*** in cyber threats or alerts, the United Kingdom recorded the largest proportion of organizations in the region that ***do not know*** whether there has been an increase or decrease (27%). This is significantly higher than the global average (8%) and regional average (17%).

Increase in cyber threats or alerts	France	Germany	Italy	U.K.
25% or more	48%	31%	43%	24%
Don't know	12%	14%	14%	27%

Increase in Cyber Threats or Alerts According to Country

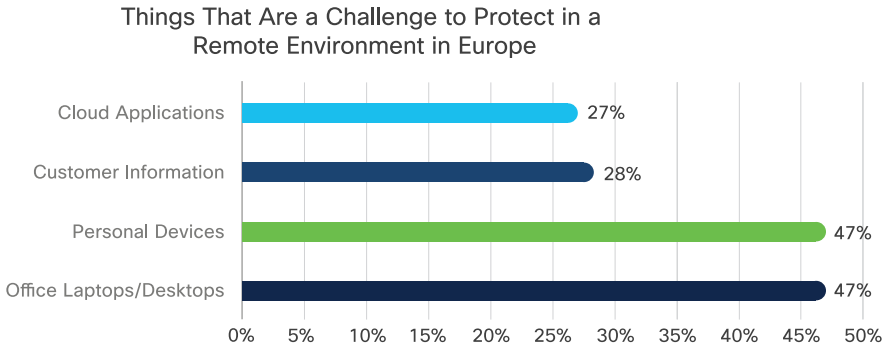
Cybersecurity challenges continue to be relentless

As more users continue to connect remotely, EU companies have seen surges in cybersecurity-related challenges. Secure access was named as the **top cybersecurity challenge** faced by the largest proportion of organizations at 57%. Other concerns include data privacy (41%), which has implications for the overall security posture, and maintaining control and enforcement policies (39%).

Endpoint security is a critical measure

Workers taking corporate devices home became the Achilles' heel to nearly half (47%) of European businesses with endpoint security threats circumventing traditional cybersecurity defenses that were not set up for remote work. This is in alignment with the global trend where 1 in 2 respondents stated that office laptops/desktops (56%) and personal devices (54%) are a top challenge in protecting a remote environment.

European organizations also found customer information (28%) and cloud applications (27%) a challenge to protect in a remote work environment. However, these figures were both significantly less than the global average (46% respectively).



- The United Kingdom is the only country in the region that had a larger proportion of organizations that found it a challenge to protect office devices (46%) than personal devices (39%).

- The same proportion (55%) of German organizations found personal devices and office laptops/desktops in a remote working environment a challenge to protect – the only market in the region with a tie. This was also 8% percent higher than the tied regional average (47%).

Supporting remote workers with the right technology priorities

As businesses went from having the majority of their meetings face-to-face to virtualizing all their communications almost overnight, Europe is on par with its global counterparts at keeping workers connected remotely yet securely. Consistent with global trends, over half (55%) of organizations that adopted these solutions ranked cybersecurity measures as its #1 priority, ahead of collaboration tools (48% ranked it first) and professional services (25% ranked it first).

- Within Europe itself, all but Germany ranked cybersecurity measures as their top priority.

Most Widely Adopted	vs	Number 1 Priority
Collaboration Tools 76%	1	Cybersecurity Measures 55%
Cybersecurity Measures 65%	2	Collaboration Tools 48%
Cloud-Based Document Sharing 56%	3	Professional Services 25%

Top IT Solutions Adoption vs. Priority Among European Organizations to Support Remote Working

- While the region ranked professional services third overall, three of the EU-surveyed countries bumped cloud sharing up into third place, except for France.

France	Germany	Italy	U.K.
Cybersecurity measures (51%)	Collaboration tools (54%)	Cybersecurity measures (58%)	Cybersecurity measures (63%)
Collaboration tools (50%)	Cybersecurity measures (46%)	Collaboration tools (44%)	Collaboration tools (43%)
Professional services (31%)	Cloud-based document sharing (31%)	Cloud-based document sharing (21%)	Cloud-based document sharing (23%)

IT Solutions Ranked #1 by Organizations in Europe

Renewing commitment to cybersecurity policies

As organizations continue to secure remote workers, the majority found it absolutely necessary to update their cybersecurity policies immediately in an effort to support this massive shift. Ninety-three percent of organizations in Europe reported changes to their cybersecurity policies – despite this being the lowest proportion among all three regions and against the global average (96%). The top policy-related change made was **increased VPN capacity** (64%), higher than the global average of 59%. Other top policy-related changes made were **implementing multi-factor authentication** (38% in Europe vs. 53% globally), **increasing web controls and acceptable use policy** (34% in Europe vs. 55% globally), and **endpoint protection** (34% in Europe vs. 48% globally).

- Interestingly, a higher proportion of organizations in France and Germany cited endpoint protection as their third cybersecurity policy change at 37% and 40%, respectively.

France	Germany	Italy	U.K.
Increased VPN capacity (63%)	Increased VPN capacity (64%)	Increased VPN capacity (66%)	Increased VPN capacity (65%)
Increasing web controls and acceptable use policy (40%)	Implementing multi-factor authentication (44%)	Implementing multi-factor authentication (40%)	Implementing multi-factor authentication (35%)
Endpoint protection (37%)	Endpoint protection (40%)	Increasing web controls and acceptable use policy (39%)	Increasing web controls and acceptable use policy (29%)

The Top Policy-Related Changes Made by Country

Simplicity and education are key to reinforcing protocols

While the pandemic forced businesses to accelerate their digital transformation and remote work plans, many employees were also learning and evolving their work habits in real time, with many working remotely for the first time. Security awareness training became more important than ever, as malicious actors recognized this potential learning gap and have continued to find new ways to capitalize on the unsuspecting.

Fifty-four percent of European organizations (vs. 59% globally) reported that the lack of employee awareness and education was the ***top challenge faced in reinforcing cybersecurity protocols*** for remote working, followed by having too many tools and solutions to manage and toggle (43% vs. 50% globally). Only 22% of European organizations reported struggling with the deployment of inconsistent interfaces (vs. 35% globally). While Europe's average is the lowest among global and regional averages, the findings show that there is an opportunity for further education and better security measures that are simple and easy to use and work well together.

Global	APJC	AMER	Europe
Lack of employee awareness/employee education (59%)	Lack of employee awareness/employee education (61%)	Lack of employee awareness/employee education (58%)	Lack of employee awareness/employee education (54%)
Too many tools/ solutions to manage and toggle (50%)	Too many tools/ solutions to manage and toggle (53%)	Too many tools/ solutions to manage and toggle (49%)	Too many tools/ solutions to manage and toggle (43%)
Inconsistent interfaces (35%)	Inconsistent interfaces (40%)	Inconsistent interfaces (33%)	Inconsistent interfaces (22%)

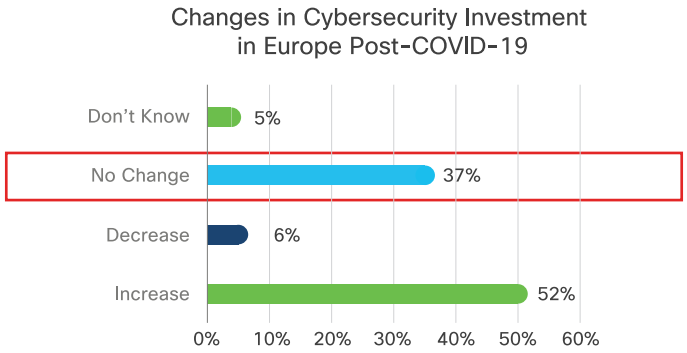
Top 3 Challenges in Reinforcing Cybersecurity Protocols by Region

- Germany bucked the trend with more organizations listing having too many tools and solutions to manage and toggle as its top challenge at 55%, higher than the regional average (43%).

Taking a measured yet proactive approach to increasing cybersecurity investments

More than half (52%) of European organizations indicated that the COVID-19 situation will result in an increase in their future cybersecurity investments. This is a step in the right direction despite it being the region recording the lowest proportion of organizations looking to boost such investments. Consequently, 37% of European organizations indicated that there will be ***no change*** to their organization's cybersecurity investment, the highest across all regions.

- France (56%), Italy (52%), and Germany (56%) had over half of organizations claiming that they will increase their cybersecurity spending following the pandemic.
- The United Kingdom, on the other hand, recorded the largest proportion of respondents indicating no change to their future investment in cybersecurity (49%) in the world. They also recorded the lowest proportion of organizations indicating an increase to their cybersecurity investment in the world at 44%.



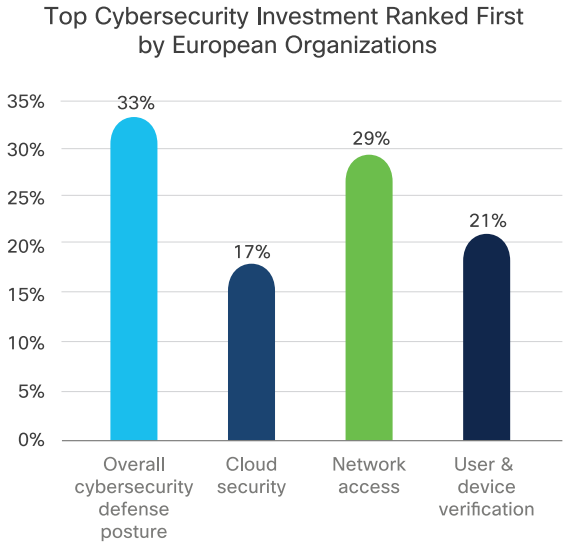
Changes in cybersecurity investments due to COVID-19	Global	APJC	AMER	Europe
Increase	66%	70%	68%	52%
Decrease	9%	11%	7%	6%
No change	22%	17%	23%	37%
Don't know	3%	2%	2%	5%

Changes in Cybersecurity Investments Regional vs. Global Averages

Pandemic spurs organizations in Europe to rethink their cybersecurity strategy

When asked to rank their cybersecurity investments in terms of importance, overall cybersecurity defense posture is the top-ranked investment priority (33% ranked it first).

It is the top-ranked choice for Italy (32% ranked it first) and United Kingdom (48% ranked it first). Other priority investments reported by European organizations include network access (29% ranked first) and user and device verification (21% ranked first). This indicates that organizations in Europe are tailoring their cybersecurity strategy toward a holistic, zero-trust approach to securely support a hybrid future of work as a result of the pandemic.



France	Germany	Italy	U.K.
Network access (33%)	Network access (32%)	Overall cybersecurity defense posture (32%)	Overall cybersecurity defense posture (48%)
Overall cybersecurity defense posture (25%)	Overall cybersecurity defense posture (28%)	Network access (32%)	User and device verification (20%)
User and device verification (22%)	User and device verification (22%)	User and device verification (21%)	Network access (17%)
Cloud security (20%)	Cloud security (18%)	Cloud security (15%)	Cloud security (15%)

Cybersecurity Investments Priorities (Ranked #1) by Country

COUNTRY DEEP DIVE: EUROPE

France

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 15% • During COVID-19: 64% • After COVID-19: 32%	• Pre-COVID-19: 16% • During COVID-19: 67% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 34% • More important than before: 44% • Somewhat important: 20%	• Extremely important: 35% • More important than before: 46% • Somewhat important: 18%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 48% • Don't know: 12%	• Increase of 25% or more: 37% • Don't know: 17%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 52% • Data privacy: 40% • Protection against malware: 36%	• Secure access: 57% • Data privacy: 41% • Maintaining control and enforcement policies: 39%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Personal devices: 49% • Office laptops/desktops: 44% • Cloud applications: 26% • Customer information: 25%	• Personal devices: 47% • Office laptops/desktops: 47% • Customer information: 28% • Cloud applications: 27%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 43% • Somewhat prepared: 47% • Not prepared: 9%	• Very prepared: 45% • Somewhat prepared: 50% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 73% • Cybersecurity measures: 66% • Cloud-based document sharing: 53%	• Collaboration tools: 76% • Cybersecurity measures: 65% • Cloud-based document sharing: 56%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 51% • Collaboration tools: 50% • Professional services: 31%	• Cybersecurity measures: 55% • Collaboration tools: 48% • Professional services: 25%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 63% • Increasing web controls and acceptable use policy: 40% • Endpoint protection: 37%	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 38% • Increasing web controls and acceptable use policy: 34%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 53% • More than 30%: 45%	• 30% or less: 45% • More than 30%: 48%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 50% • Too many tools/solutions to manage and toggle: 46% • Inconsistent interfaces: 27%	• Lack of employee awareness/employee education: 54% • Too many tools/solutions to manage and toggle: 43% • Inconsistent interfaces: 22%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 56% • Decrease: 9% • No change: 29%	• Increase: 52% • Decrease: 6% • No change: 37%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 63% • More than 30%: 27%	• 30% or less: 65% More than 30%: 23%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Network access: 33% • Overall cybersecurity defense posture: 25% • User and device verification: 22% • Cloud security: 20%	• Overall cybersecurity defense posture: 33% • Network access: 29% • User and device verification: 21% • Cloud security: 17%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Germany

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 15% • During COVID-19: 53% • After COVID-19: 24%	• Pre-COVID-19: 16% • During COVID-19: 67% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 32% • More important than before: 47% • Somewhat important: 19%	• Extremely important: 35% • More important than before: 46% • Somewhat important: 18%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 31% • Don't know: 14%	• Increase of 25% or more: 37% • Don't know: 17%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 64% • Data privacy: 54% • Maintaining control and enforcement policies: 43%	• Secure access: 57% • Data privacy: 41% • Maintaining control and enforcement policies: 39%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Personal devices AND Office laptops/desktops: 55% (TIED) • Cloud applications: 42% • Customer information: 31%	• Personal devices: 47% • Office laptops/desktops: 47% • Customer information: 28% • Cloud applications: 27%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46% (TIED)
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 41% • Somewhat prepared: 55% • Not prepared: 4%	• Very prepared: 45% • Somewhat prepared: 50% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 72% • Cybersecurity measures: 62% • Cloud-based document sharing: 53%	• Collaboration tools: 76% • Cybersecurity measures: 65% • Cloud-based document sharing: 56%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Collaboration tools: 54% • Cybersecurity measures: 46% • Cloud-based document sharing: 31%	• Cybersecurity measures: 55% • Collaboration tools: 48% • Professional services: 25%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 44% • Endpoint protection: 40%	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 38% • Increasing web controls and acceptable use policy: 34%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 57% • More than 30%: 38%	• 30% or less: 45% • More than 30%: 48%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Too many tools/solutions to manage and toggle: 55% • Lack of employee awareness/employee education: 49% • Inconsistent interfaces: 23%	• Lack of employee awareness/employee education: 54% • Too many tools/solutions to manage and toggle: 43% • Inconsistent interfaces: 22%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 56% • Decrease: 6% • No change: 34%	• Increase: 52% • Decrease: 6% • No change: 37%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 77% • More than 30%: 16%	• 30% or less: 65% More than 30%: 23%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Network access: 32% • Overall cybersecurity defense posture: 28% • User and device verification: 22% • Cloud security: 18%	• Overall cybersecurity defense posture: 33% • Network access: 29% • User and device verification: 21% • Cloud security: 17%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Italy

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 15% • During COVID-19: 65% • After COVID-19: 33%	• Pre-COVID-19: 16% • During COVID-19: 67% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 28% • More important than before: 57% • Somewhat important: 15%	• Extremely important: 35% • More important than before: 46% • Somewhat important: 18%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 43% • Don't know: 14%	• Increase of 25% or more: 37% • Don't know: 17%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 68% • Maintaining control and enforcement policies: 49% • Data privacy: 47%	• Secure access: 57% • Data privacy: 41% • Maintaining control and enforcement policies: 39%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Personal devices: 46% • Office laptops/desktops: 42% • Customer information: 30% • Cloud applications: 21%	• Personal devices: 47% • Office laptops/desktops: 47% • Customer information: 28% • Cloud applications: 27%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46% (TIED)
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 35% • Somewhat prepared: 57% • Not prepared: 8%	• Very prepared: 45% • Somewhat prepared: 50% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 79% • Cybersecurity measures: 68% • Cloud-based document sharing: 62%	• Collaboration tools: 76% • Cybersecurity measures: 65% • Cloud-based document sharing: 56%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document Sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 58% • Collaboration tools: 44% • Cloud-based document sharing: 21%	• Cybersecurity measures: 55% • Collaboration tools: 48% • Professional service: 25%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 66% • Implementing multi-factor authentication: 40% • Increasing web controls and acceptable use policy: 39%	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 38% • Increasing web controls and acceptable use policy: 34%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 39% • More than 30%: 46%	• 30% or less: 45% • More than 30%: 48%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 63% • Too many tools/solutions to manage and toggle: 41% • Lack of visibility / Inconsistent interfaces: 15%	• Lack of employee awareness/employee education: 54% • Too many tools/solutions to manage and toggle: 43% • Inconsistent interfaces: 22%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 52% • Decrease: 6% • No change: 37%	• Increase: 52% • Decrease: 6% • No change: 37	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 63% • More than 30%: 26%	• 30% or less: 65% More than 30%: 23%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 32% • Network access: 32% • User and device verification: 21% • Cloud security: 15%	• Overall cybersecurity defense posture: 33% • Network access: 29% • User and device verification: 21% • Cloud security: 17%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

United Kingdom

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organizations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 18% • During COVID-19: 85% • After COVID-19: 50%	• Pre-COVID-19: 16% • During COVID-19: 67% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organizations	• Extremely important: 46% • More important than before: 35% • Somewhat important: 17%	• Extremely important: 35% • More important than before: 46% • Somewhat important: 18%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 24% • Don't know: 27%	• Increase of 25% or more: 37% • Don't know: 17%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 43% • Maintaining control and enforcement policies: 31% • Protection against malware: 27%	• Secure access: 57% • Data privacy: 41% • Maintaining control and enforcement policies: 39%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Office laptops/desktops: 46% • Personal devices: 39% • Customer information: 27% • Cloud applications: 20%	• Personal devices: 47% • Office laptops/desktops: 47% • Customer information: 28% • Cloud applications: 27%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46% (TIED)
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 59% • Somewhat prepared: 39% • Not prepared: 2%	• Very prepared: 45% • Somewhat prepared: 50% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritizing Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 79% • Cybersecurity measures: 65% • Cloud-based document sharing: 57%	• Collaboration tools: 76% • Cybersecurity measures: 65% • Cloud-based document sharing: 56%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organizations that ranked it first)	• Cybersecurity measures: 63% • Collaboration tools: 43% • Cloud-based document sharing: 23%	• Cybersecurity measures: 55% • Collaboration tools: 48% • Professional services: 25%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 65% • Implementing multi-factor authentication: 35% • Increasing web controls and acceptable use policy: 29%	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 38% • Increasing web controls and acceptable use policy: 34%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 30% • More than 30%: 64%	• 30% or less: 45% • More than 30%: 48%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 57% • Too many tools/solutions to manage and toggle: 29% • Inconsistent interfaces: 21%	• Lack of employee awareness/employee education: 54% • Too many tools/solutions to manage and toggle: 43% • Inconsistent interfaces: 22%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 44% • Decrease: 1% • No change: 49%	• Increase: 52% • Decrease: 6% • No change: 37%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 57% • More than 30%: 21%	• 30% or less: 65% More than 30%: 23%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 48% • User and device verification: 20% • Network access: 17% • Cloud security: 15%	• Overall cybersecurity defense posture: 33% • Network access: 29% • User and device verification: 21% • Cloud security: 17%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 65% • Implementing multi-factor authentication: 35% • Increasing web controls and acceptable use policy: 29%	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 38% • Increasing web controls and acceptable use policy: 34%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 30% • More than 30%: 64%	• 30% or less: 45% • More than 30%: 48%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 57% • Too many tools/solutions to manage and toggle: 29% • Inconsistent interfaces: 21%	• Lack of employee awareness/employee education: 54% • Too many tools/solutions to manage and toggle: 43% • Inconsistent interfaces: 22%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organization's future investment in cybersecurity due to COVID-19	• Increase: 44% • Decrease: 1% • No change: 49%	• Increase: 52% • Decrease: 6% • No change: 37%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 57% • More than 30%: 21%	• 30% or less: 65% More than 30%: 23%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organizations that ranked it first)	• Overall cybersecurity defense posture: 48% • User and device verification: 20% • Network access: 17% • Cloud security: 15%	• Overall cybersecurity defense posture: 33% • Network access: 29% • User and device verification: 21% • Cloud security: 17%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

ABOUT THE FUTURE OF SECURE REMOTE WORK REPORT

In February to March 2020, organizations sought to protect their workforce by mandating and enabling their employees to work from home. While necessary for protecting people and communities, this experience physically separated security professionals from their own teams, from the employees who depended on them, and from the critical systems they were responsible for. The remote work arrangement also placed greater strain on existing digital policies and business continuity planning during an already stressful time.

That's not to say that we couldn't find ways to adapt to this new way of working. In the spirit of this reality, more than 3000 IT decision makers from small to large organizations were surveyed from June 16 to September 4, 2020, across a spectrum of 30 industries, including financial services, healthcare, architecture, transportation, etc., to understand how they have been impacted by the COVID-19 crisis from a cybersecurity perspective.

3196 respondents in **21** markets

AMER:
- Brazil
- Canada
- Mexico
- United States

EUROPE:
- France
- Germany
- Italy
- United Kingdom

APJC:
- Australia
- China
- Hong Kong
- India
- Indonesia
- Japan
- Korea
- Malaysia
- Philippines
- Singapore
- Taiwan
- Thailand
- Vietnam

Industries:
- Accounting
- Architecture
- Business Consulting
- Chemical Engineering or Manufacturing
- Construction
- Education
- Financial Services
- Government
- Healthcare
- Manufacturing:
- Non-computer Related
- Retail
- Software Development
- Telecommunications
- Transportation
- Wholesale and Distribution
- Non-Profit/ Charitable

Audience:
Professionals responsible for their company's IT

These organizations include:
- small (between 1 and 249 employees),
- medium (between 250 and 999 employees), and
- large businesses (1000 employees or more).

Objectives:

- To explore the **challenges** of moving some or all of an organization's workforce to a **remote environment** almost overnight and the **readiness** of organizations around the world in securing their businesses in a remote work arrangement

- To understand how businesses adapted to this sudden transition including the shifts in their cybersecurity priorities, policies and investments

- To enable businesses to understand and prepare for a hybrid work environment by securely adapting to protect what's now and what's next.

Research Parameters

#1 The rise of remote workers during COVID-19 and the importance of cybersecurity to support them

1) Number of people working remotely before, during and after COVID-19
2) Importance of cybersecurity in today's COVID-19 and remote working landscape

#2 Addressing cybersecurity preparedness, threats, and challenges

1) How prepared are organizations with their cybersecurity features/solutions when (suddenly) transitioning to remote working
2) Types of cybersecurity challenges encountered during mass remote working and their gravity in order of importance
3) Most challenging things to protect during remote working

#3 Technology priorities and adoption to support remote working

1) Type of technologies adopted
2) Rank and order of importance of technologies adopted

#4 Movements in cybersecurity policies and enforcement protocols to support remote workers

1) Type of changes made
2) Proportion of changes in cybersecurity policies
3) Challenges in enforcing cybersecurity protocols

#5 Cybersecurity investments, today and beyond

1) Whether COVID-19 will change organization's future cybersecurity investment
2) Percentage of increase, decrease, or no change in investment
3) Rank of future cybersecurity investment in order of importance

Future of Secure Remote Work Report

cisco SECURE