Acronis

Report
2020

Acronis Cyber Readiness Report

Post-pandemic cybersecurity landscape at a glance

Acronis Cyber Readiness Report 2020

Table of contents

Introduction and research methodology

The COVID-19 pandemic has crippled businesses worldwide – based on Acronis' earlier research, more than 80% of global companies admitted they were not prepared to switch to remote work, with IT infrastructure suffering. This research aims to explore in detail:

- What were the key challenges and concerns of IT leaders and managers across the world during the pandemic?
- What key IT infrastructure vulnerabilities were exposed during the pandemic?
- Has the rate of cyberattacks really skyrocketed during the pandemic? If so, what type of attacks were favored by cybercriminals?
- What cybersecurity issues will businesses across all industries face next year?
- Are employees ready to switch to permanent remote work as the new normal?
- What tech challenges and risks will they encounter when working from home?

To find the answers, Acronis conducted an independent research study, surveying 3,400 IT managers and remote workers across 17 countries. The findings provide a clear picture of how the business world coped with remote work, what the post-pandemic cyber landscape will look like, and how protection challenges will evolve from here.

ABOUT THE SURVEY METHODOLOGY

Acronis surveyed 3,400 IT managers and remote workers in order to evaluate their cyber readiness before and after the pandemic. Acronis had no role in selecting the respondents and all responses were provided anonymously. The survey was conducted during June-July 2020.

Respondents came from 17 countries across four continents: Australia, Bulgaria, Canada, France, Germany, India, Italy, Japan, Netherlands, Singapore, South Africa, Spain, Sweden, Switzerland, UAE, UK, and US.

Within each country, 50% of respondents are members of corporate IT teams and 50% are employees that currently work remotely. The respondents are from a range of sectors, both public and private.

KEY INDUSTRIES REPRESENTED:

IT/Telecom
Hospitality/Travel
Healthcare
Education
Sports/Entertainment
Others *(Manufacturing, Finance/Legal/Professional Services, etc.)*

Copyright © 2002-2020 Acronis International GmbH.

Executive summary

KEY RESEARCH FINDINGS

New cyber landscape: videoconferencing and phishing attacks

- **31% of companies around the world are attacked at least once a day. India reported significantly more attacks per day than any other country, followed by the US and the UAE.** 9% of all companies are targeted by cyberattacks at least once an hour. Exactly 50% of all respondents report encountering a cyberattack at least once a week during the past three months.
- **39% of all companies encounter videoconferencing attacks. Canada, the UK, Switzerland, and India are among the most affected.** Phishing, DDoS, and videoconferencing attacks plague companies the most, with phishing campaigns at a historic peak.
- **It's no surprise that phishing ranks highest among recent attacks. Only 2% of global companies look for a URL filtering feature in their corporate solution.** In the meantime, 43% of companies focus on an antimalware/antivirus feature.
- **69% of remote workers have started using workplace collaboration tools like Zoom and Webex** – but only 63% of IT managers reported adopting those solutions. That means 6% of remote workers are doing their own "shadow" IT, which poses a security risk.

Cost of the pandemic: lack of integrated solutions

- **72% of organizations report that their IT costs increased during the pandemic.** In particular, 27% of companies saw a significant increase during the pandemic. Only one in five companies managed to keep their IT costs unchanged.
- **92% of global companies surveyed had to adopt new technologies to work remotely.** The top solutions were: workplace collaboration tools, privacy solutions, and endpoint cybersecurity solutions. Only 7% didn't need to upgrade their existing tool set.
- **35% of global companies reported having more new devices connected to their corporate network recently.** Having most of the world's population working remotely has effectively rendered perimeter security an outdated concept.
- **The top three tech challenges identified by remote workers:** Wi-Fi connectivity, using a VPN and other security measures, and the inability to use internal networks and applications.

The future of remote work: passing trend or new reality?

- **88% of employees would like to continue working remotely to some extent:** 32% favor office work, 33% would like to do a 50/50 split, and 35% favor remote work.
- **58% of remotely working employees report feeling better equipped to work remotely now than before the pandemic.**
- **92% of employees expect their companies to invest more into digital transformation tools** to help adapt to new business realities.
- **Only 53% of global remote workers received clear communication when switching to working from home – the other half were left to fend for themselves.** A whopping 47% didn't receive enough guidance, while 16% received no guidance at all.

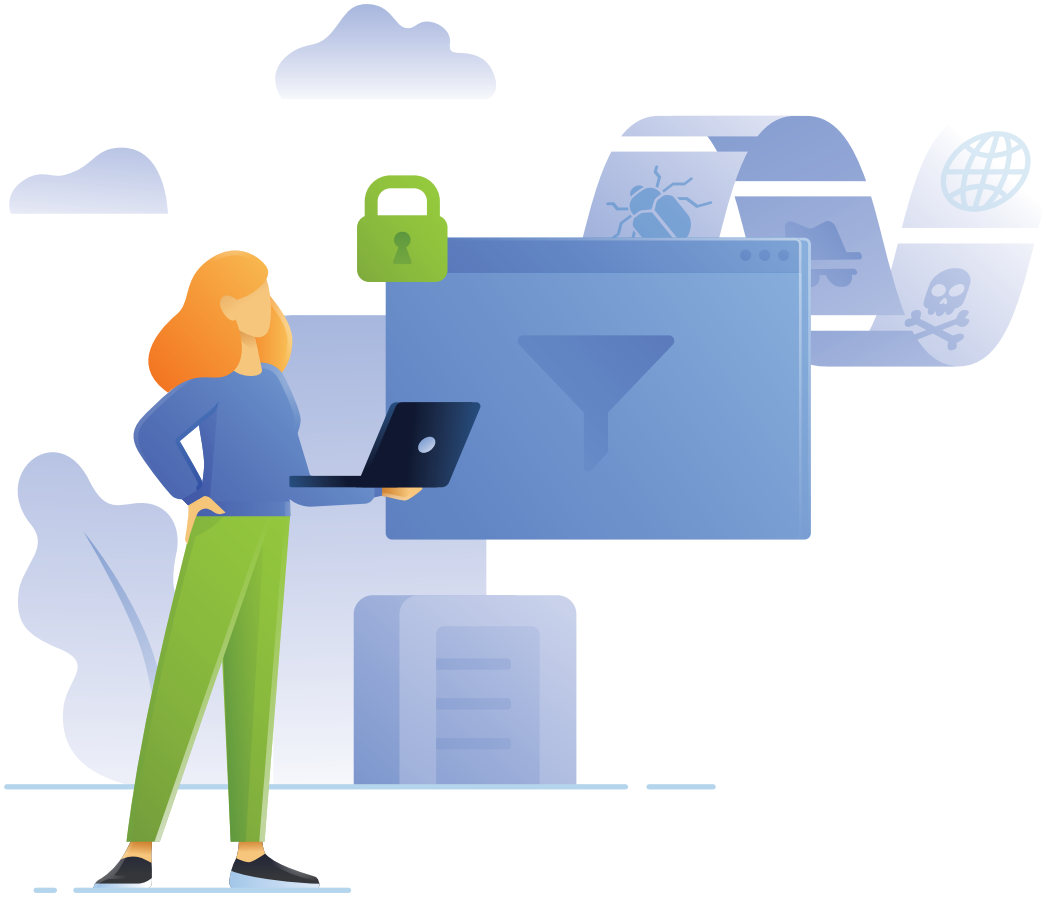
Copyright © 2002-2020 Acronis International GmbH.

Part 1

IT managers

AMONG THE SURVEY QUESTIONS

- What were the top tech challenges you encountered when managing the surge in employees working remotely due to the pandemic?
- Did you adopt any new technologies to help enable/manage/secure employees working from home?
- How have your IT infrastructure costs changed during the pandemic?
- How often has your company been targeted by a cyberattack in the past three months?
- What types of cyberattacks has your organization encountered in the past three months?
- Which features do you prioritize most when choosing/operating a corporate cyber protection solution?
- What trend have you seen regarding new devices connecting to your corporate network in the past three months?



Organizations' IT managers are struggling the most with adequately instructing employees on remote work and securing remote workers

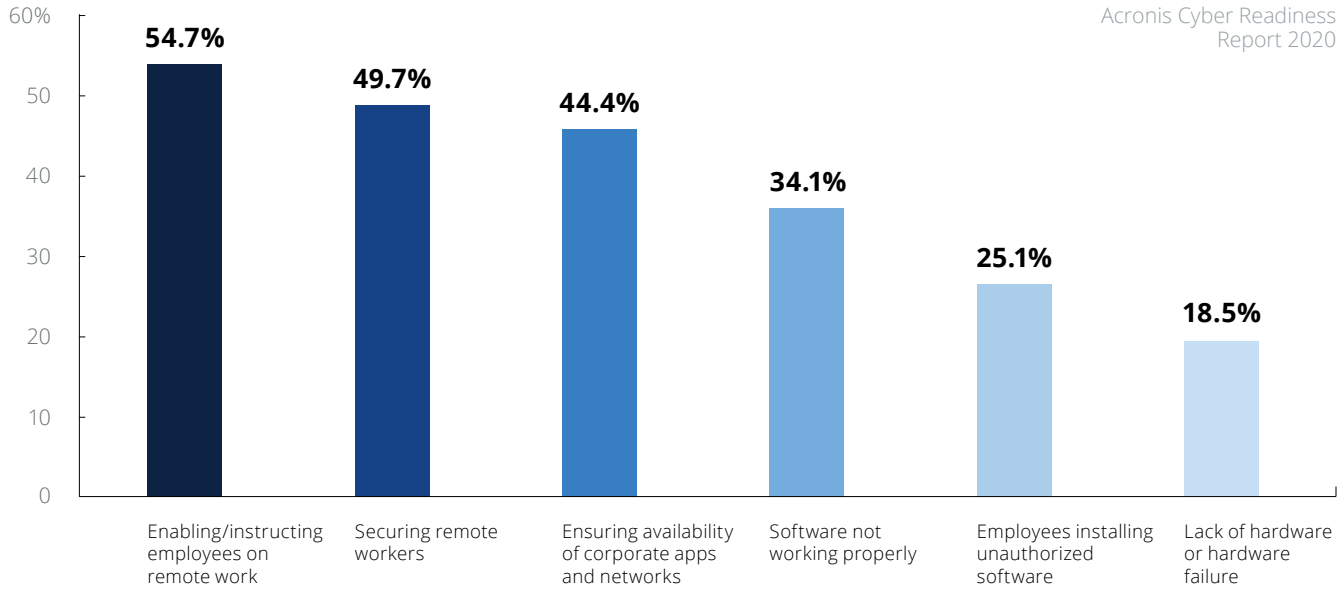
Q1. What were the top tech challenges you encountered when managing the surge in employees working remotely due to the pandemic?

Key finding: Globally, the top tech challenges for corporate IT teams were: instructing employees on remote work; securing remote workers, and ensuring the availability of internal corporate apps.

In several regions, our research detected significantly higher rates for the top-3 tech challenges compared to the global averages, particularly in Singapore, India & UAE.

Did you know?

Companies in Singapore, India & UAE reported the ***top-3 IT infrastructure challenges*** *revealed during the pandemic at significantly higher rates than those in other countries.*



Copyright © 2002-2020 Acronis International GmbH.

92% of global organizations have had to adopt new technologies in order to switch to remote work

Q2. Did you adopt any new technologies to help enable/manage/secure employees working from home?

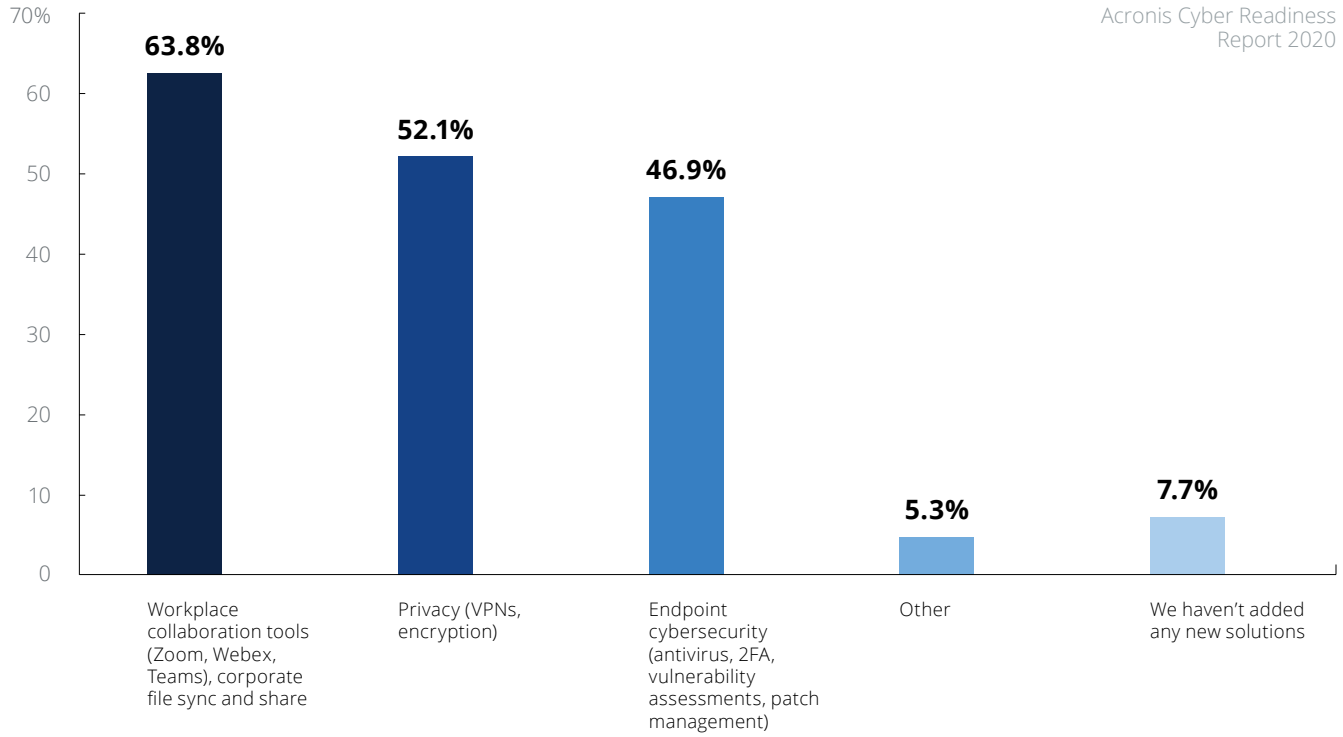
Key finding: 92.3% of global organizations surveyed have had to adopt new technologies after switching to remote work in response to the pandemic.

The top technologies and solutions companies have had to add were:

- Workplace collaboration tools (Zoom, Webex, Microsoft Teams, etc.) and corporate file sync and share solutions)
- Privacy solutions (VPNs, encryption)
- Endpoint cybersecurity solutions (antivirus, 2FA, vulnerability assessments, patch management)

Did you know?

Zoom grew from 10 million users to 200 million users "overnight" – and critical security vulnerabilities were exposed in the process. There's a better way for companies to securely use these platforms.



Copyright © 2002-2020 Acronis International GmbH.

72% of global organizations have seen their IT costs increased during the pandemic

Q3. How have your IT infrastructure costs changed during the pandemic?

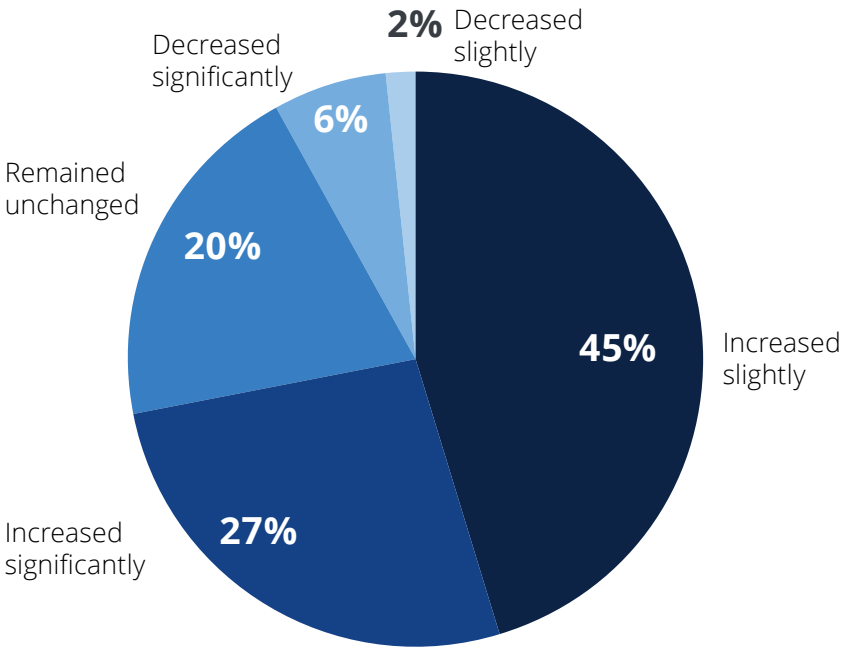
Key finding: 27% of surveyed companies report having their IT costs increase significantly during the pandemic. Only one in five companies managed to relocate funds and keep their IT costs unchanged.

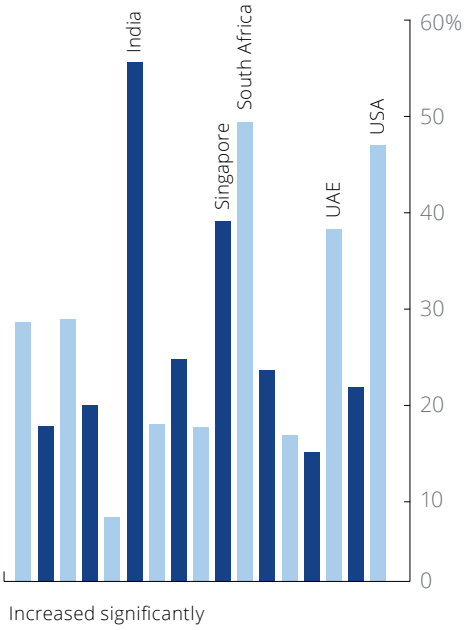
Of all companies surveyed, 8% reported having their IT infrastructure costs decrease – possibly because of layoffs around the world. Fewer employees means fewer endpoints and lower overall infrastructure costs. Companies in the US, Singapore, South Africa, India, and the UAE reported the most significant IT cost increases, followed by Germany, the Netherlands, and Sweden.

Did you know?

Only 1 out of 5 *companies managed to relocate its funds and keep the IT costs unchanged.*

Acronis Cyber Readiness Report 2020





Copyright © 2002-2020 Acronis International GmbH.

31% of global companies are attacked at least once a day. India reported nearly twice as many attacks as any other country, followed by the US and the UAE

Q4. How often has your company been targeted by a cyberattack in the past three months?

Key finding: Exactly 50% of all respondents reported encountering a cyber-attack at least once a week in the past three months – with 9% being attacked at least once an hour and 68% of all companies being attacked in the past three months.

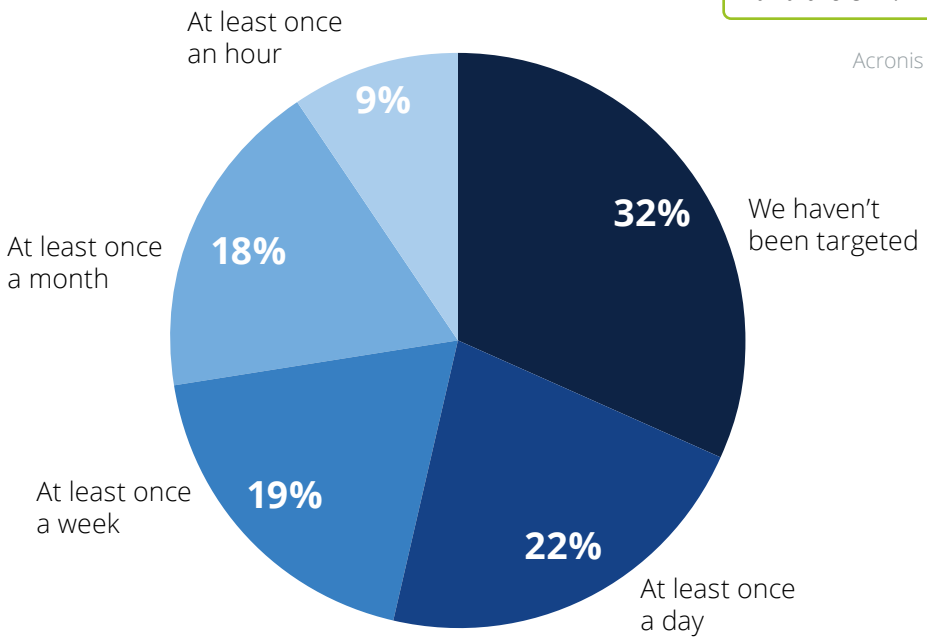
32% of global IT managers believe not having been targeted or encountering cyberattacks in the past three months. While some of those companies may have successfully blocked these attacks, most of them likely failed to detect them.

Did you know?

9% of all companies

report being targeted by cyberattacks at least once an hour in the past three months. Companies in India were far above the global average, reporting almost twice as many attacks as the next highest reporting countries, the US and the UAE.

Acronis Cyber Readiness Report 2020



Copyright © 2002-2020 Acronis International GmbH.

39% of companies have encountered videoconferencing attacks more frequently. India, Switzerland, Canada, and the UK were among the most affected.

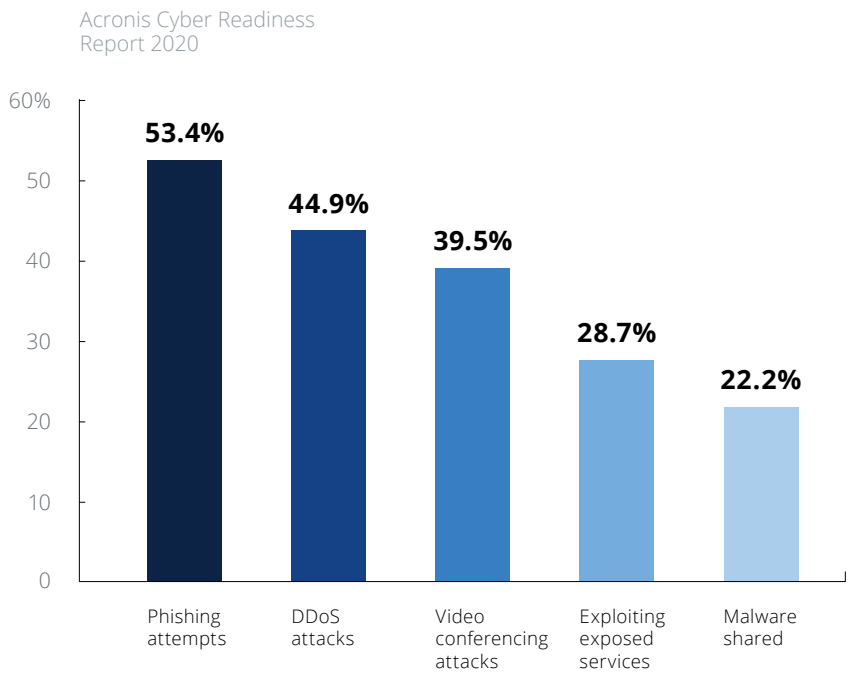
Q5. What types of cyberattacks has your organization encountered in the past three months?

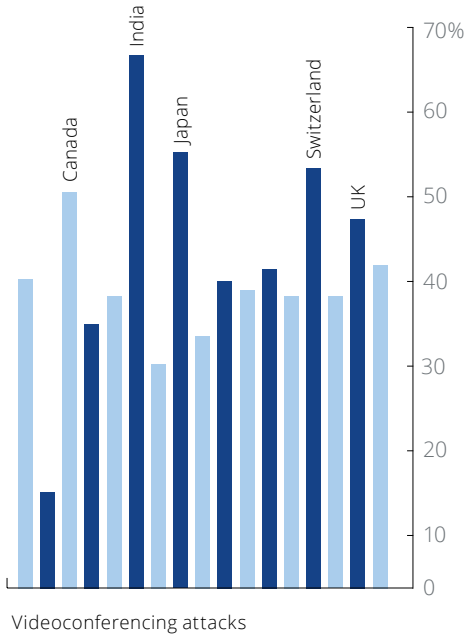
Key finding: Phishing, DDoS & Video conferencing attacks plaguing companies the most – phishing campaigns reached a peak during the pandemic.

Malware attacks - ones that were successfully detected - ranked last in the survey with 22% respondents choosing it globally, but remain a bigger issue in certain countries: Singapore, South Africa, UAE, Bulgaria & India reporting almost two times more malware attacks than the global average.

Did you know?

Zoom protection is in high demand with a new zero-day vulnerability allowing attackers to gain full control over Windows PCs. Acronis Cyber Protect defends collaboration platforms such as Zoom and Webex from exploitation and deploys a hotfix through its patch management capability.





Copyright © 2002-2020 Acronis International GmbH.

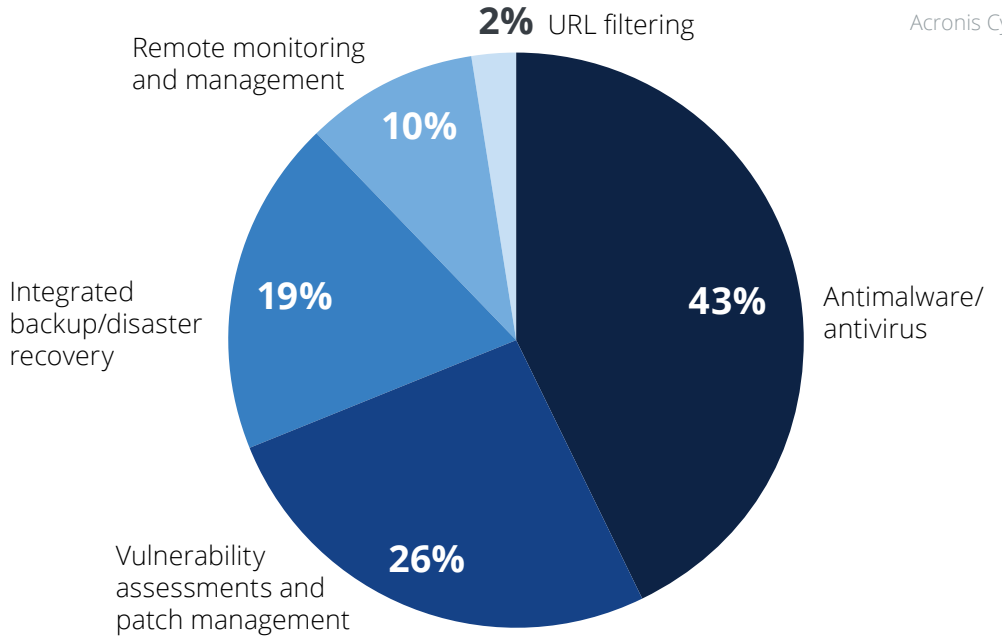
With only 2% of companies prioritizing a URL filtering feature, it's no wonder phishing attacks are at a historic peak.

Q6. Which features do you prioritize most when choosing/operating a corporate cyber protection solution?

Key finding: It's not surprising that phishing attacks ranked highest among recent attacks on global companies (see previous page), considering that only 2% of companies look for a URL filtering feature in their corporate solution. The global response is equally strange regarding malware attacks: 43% of companies choose to focus on antimalware/antivirus features, while malware attacks are the least experienced type of attack.

With 68% of global companies being attacked more frequently in the past three months, 43% of respondents have prioritized implementing an antimalware/antivirus solution. Additionally, 26% indicated that vulnerability assessments and patch management are key features in their corporate endpoint protection solution. Other key considerations reported include integrated backup/disaster recovery (19%) and remote monitoring and management (10%).

Country-level differences: Singaporean companies prioritize vulnerability assessments and patch management features more than other countries. The UK and the UAE lead globally in demand for antimalware/antivirus features. Companies in Bulgaria prioritize integrated backup/disaster recovery more than all other countries, while Japanese companies prioritize remote monitoring and management more than other countries.



Acronis Cyber Readiness Report 2020

Copyright © 2002-2020 Acronis International GmbH.

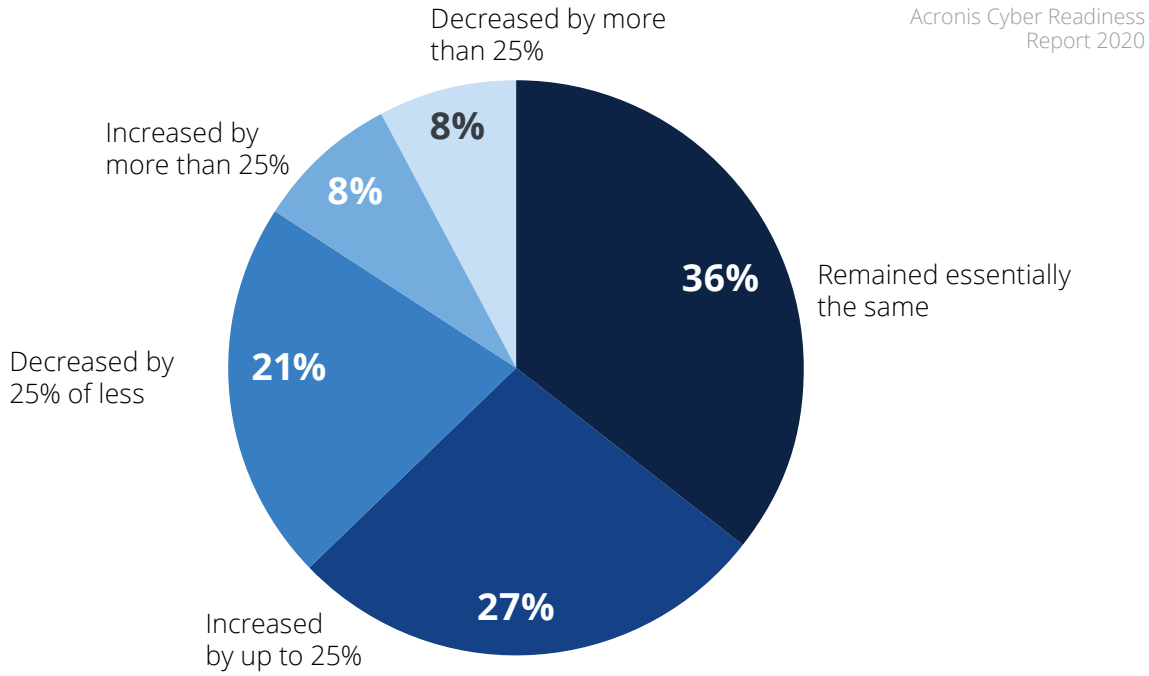
A clean split: companies report mixed results when it comes to new devices

Q7. What trend have you seen regarding new devices connecting to your corporate network in the past three months?

Key finding: 35% of companies reported more new devices connecting to their corporate network in the past three months, 36% report having the same number of new devices on their corporate network, and 29% reported having fewer new devices – most likely caused by layoffs.

With approximately 90% of the world's corporate workforce working remotely, the concept of perimeter security has rapidly become irrelevant. Furthermore, the wider adoption of some form of BYOD policy ("bring your own device") has led employees to replace their corporate desktops with personal laptops. It is fair to assume that a significant number of these devices are not properly secured – yet they are now connected to corporate networks.

Countries with the most new devices added to corporate network: the US, India, Singapore, and Sweden are all significantly ahead of the world, by up to 30%.



Copyright © 2002-2020 Acronis International GmbH.

Part 2

Remote employees

AMONG THE SURVEY QUESTIONS

- Did you receive any guidance/ announcements from your IT team when you started working remotely?
- What new tools have you started using since having to work remotely?
- What were the most technically challenging aspects for you when starting remote work?
- Have you or your family members purchased any new devices – computers or wearables – since you started working remotely?
- In terms of IT infrastructure, do you feel you are more equipped to work remotely after the pandemic than before?
- If it was guaranteed that you would have the right IT infrastructure, what working format would you consider ideal?
- Do you think your company should invest more in modern digital transformation tools to help cater to new formats of work, including remote work?

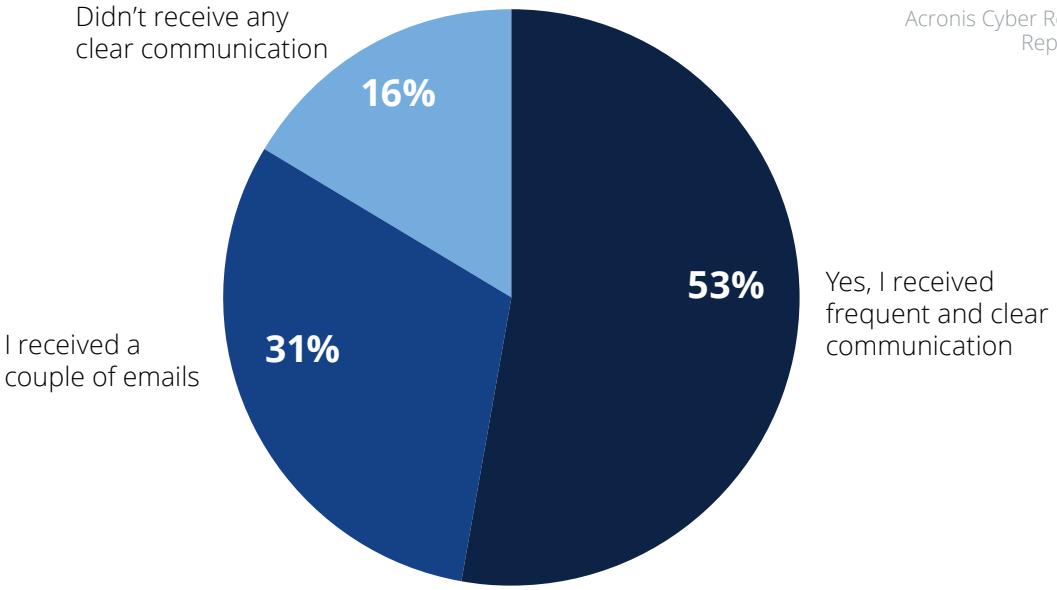
Nearly half (47%) of all global remote workers were not given adequate guidance from their IT department when switching to remote work.

Q1. Did you receive any guidance/announcements from your IT team when you started working remotely?

Key finding: A whopping 47% of remote workers received minimal or inadequate guidance when switching to work from home. A third received no clear communication at all. Workers in Japan reported both the worst rates of communication and the least IT department guidance compared to all other countries.

Did you know?

Acronis surveyed
1700+ remote workers
across the world



Acronis Cyber Readiness Report 2020

Copyright © 2002-2020 Acronis International GmbH.

69% of remote workers have started using workplace collaboration tools, like Zoom and Webex – but only 63% of IT managers reported adopting those. That means 6% of remote workers are doing their own "shadow" IT.

Q2. What new tools have you started using since having to work remotely?

Key finding: There has been notable adoption of workplace collaboration tools (69%), privacy tools (38%), and endpoint security (24%) in recent months.

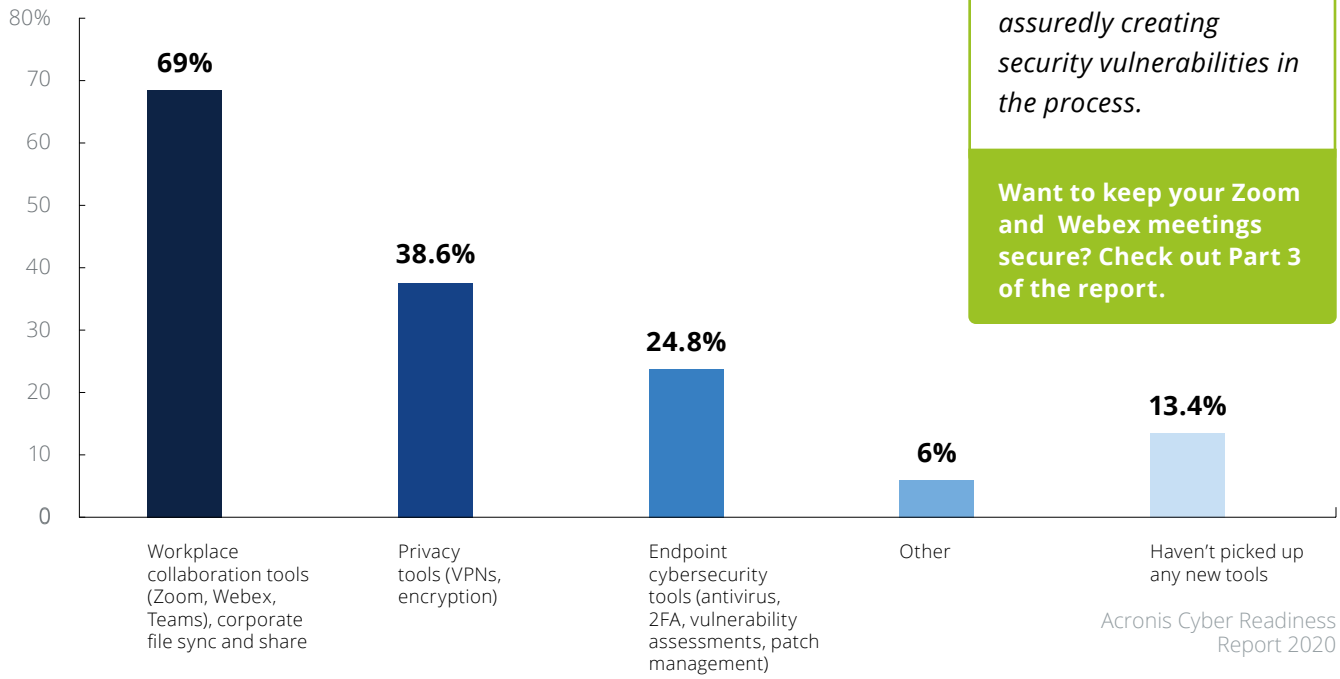
The highest levels of adoption of "workplace collaboration tools" were from remote workers in Australia, Singapore, and India. The highest levels of adoption of "privacy tools" were in Switzerland and Germany. Remote workers in India and the UAE reported the highest levels of adoption for "endpoint security" tools.

Only 13% of all global remote workers reported not having to adopt any new tools – of those, highest ranking were most likely to come from Japan and Bulgaria.

Did you know?

69% of remote workers *have started using workplace collaboration tools, like Zoom and Webex – but only 63% of IT managers reported adopting them. That suggests the remaining 6% of remote workers were installing and managing new tools themselves, almost assuredly creating security vulnerabilities in the process.*

Want to keep your Zoom and Webex meetings secure? Check out Part 3 of the report.



Acronis Cyber Readiness Report 2020

Copyright © 2002-2020 Acronis International GmbH.

The top challenges identified by remote workers: Wi-Fi connectivity, using a VPN and other security measures, and the inability to use internal networks and applications.

Q3. What were the most technically challenging aspects for you when starting remote work?

Key finding: For 37% of all respondents, Wi-Fi connectivity is the top challenge for remote workers across the world – most notably in South Africa and India.

Requiring a VPN while heavily relying on video calls – combined with entire families simultaneously working, studying, and living (i.e. streaming music and videos) at home – puts a considerable strain on a home Wi-Fi network.

"Using a VPN and other security measures" and "inability to use internal network and applications" were reported as other top challenges (30% and 25% respectively) with the highest concentrations coming from remote workers in France, India, and Sweden. The survey also showed the respondents in India, the UK, and the UAE were most likely to experience difficulties adding new devices to their corporate network, while "lack of hardware or hardware failure" proved most challenging for remote workers in Sweden, India, Spain, and Germany.

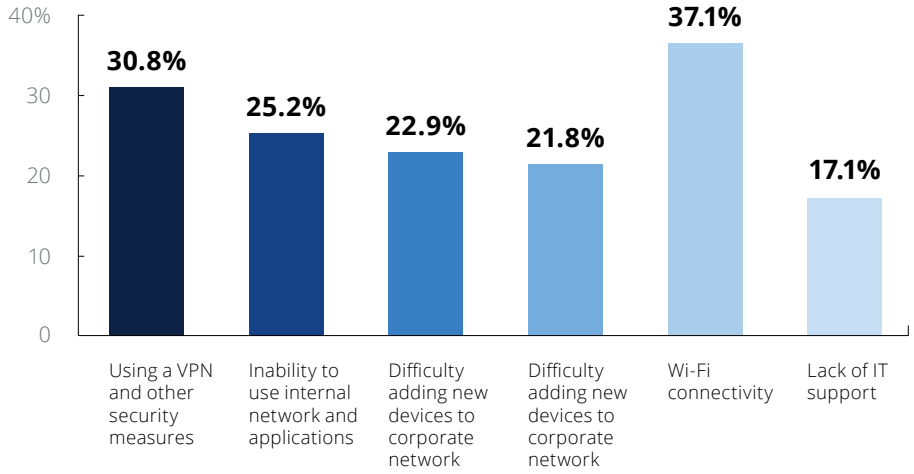
Did you know?

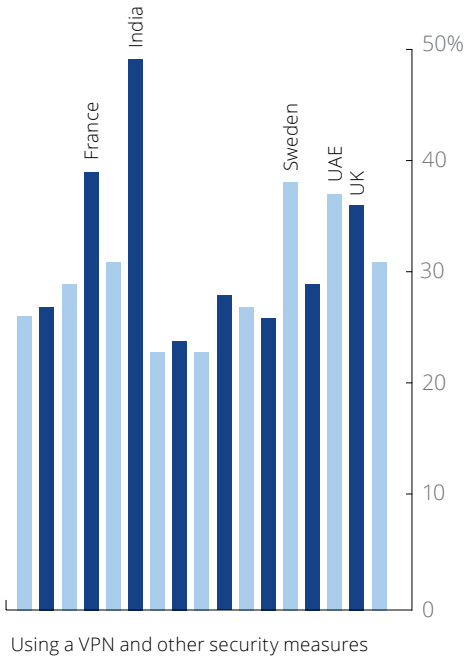
Among these top concerns,

"Lack of IT support"

ranked last, but still earned a high percentage of respondents in Japan, Bulgaria, Germany, and Australia.

Acronis Cyber Readiness Report 2020





Copyright © 2002-2020 Acronis International GmbH.

49% of global employees purchased at least one new device since they started working remotely. Remote workers in India and the UAE purchased almost twice the global average of new devices.

Q4. Have you or your family members purchased any new devices - computers or wearables - since you started working remotely?

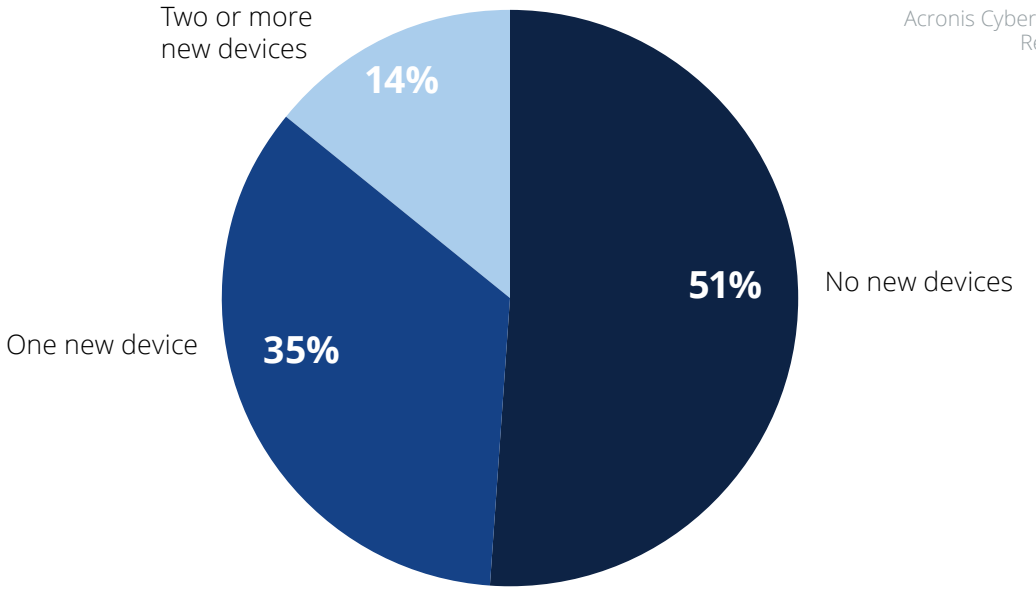
Key finding: 49% of respondents purchased at least one new device since they started working remotely. Likely, this added a new vulnerable endpoint to their home Wi-Fi and, inevitably, to their corporate network.

Considering a third of responding IT managers indicated new devices have been added to their company network since the start of remote working (see previous findings), we believe a large number of these new devices were purchased and added by employees themselves, not by their IT teams.

Conversely, 51% of remote workers have not purchased any new devices. That suggests they are still using their old, unpatched personal laptops for work. Japan ranked highest among countries with no new devices.

Did you know?

14% of remote workers purchased two or more devices, *since they began working remotely. Respondents from India and the UAE were almost twice as many as the global average to report such purchases.average.*



Acronis Cyber Readiness Report 2020

Copyright © 2002-2020 Acronis International GmbH.

58% of employees report feeling better equipped to work remotely now than before the pandemic.

Q5. In terms of IT infrastructure, do you feel you are more equipped to work remotely after the pandemic than before?

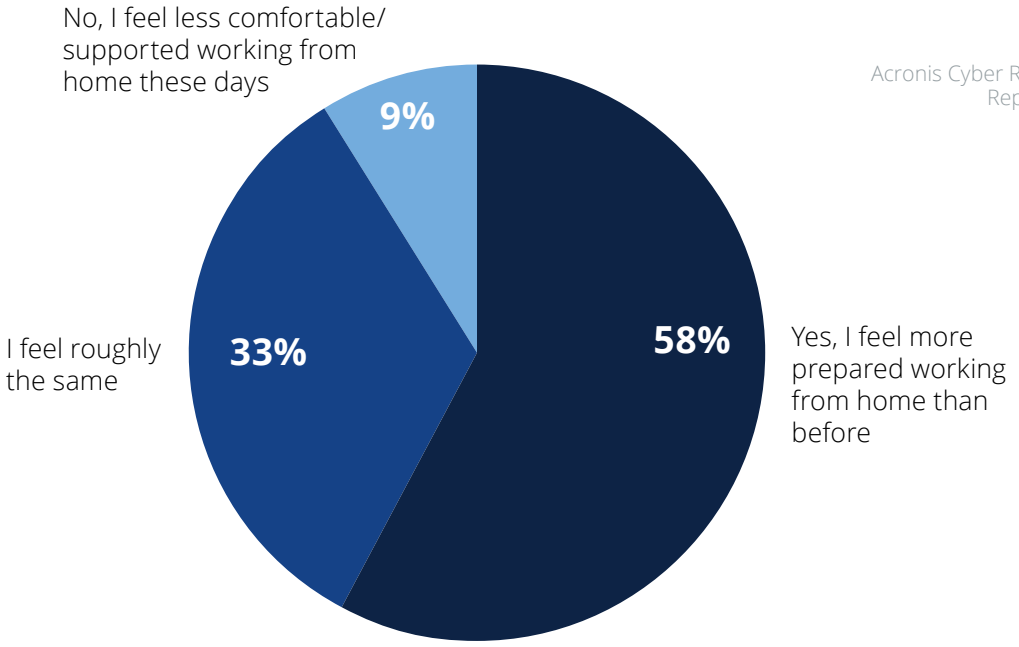
Key finding: Despite the challenges encountered by remote workers worldwide, 58% of them report feeling better equipped to work remotely now than before the pandemic.

Now equipped with workplace collaboration tools, video conferencing and VPNs enabled, remote workers are far better prepared to work from home than before. Remote workers from India, Spain, Sweden, Australia, and Bulgaria were more likely to indicate they now feel "better equipped" compared to other countries.

The next questions investigate whether these feelings will carry over to post-pandemic work arrangements.

Did you know?

Notably, in Japan, employees reported feeling less comfortable working from home - with almost twice the global average of responses - clearly correlating to the lack of IT support that ranked so high in Japan.



Acronis Cyber Readiness Report 2020

Copyright © 2002-2020 Acronis International GmbH.

Only 12% of global employees chose full office work as an ideal work arrangement. A new normal will likely emerge.

Q6. If it was guaranteed that you would have the right IT infrastructure, what working format would you consider ideal?

Key finding: 88% of employees indicated they'd like to continue working remotely to some extent. That preference is evenly split with 32% favoring a majority of in-office work, 33% favoring a 50/50 split, and 35% favoring a majority of remote work.

Not surprisingly, employees are ready for the new work format: the pandemic has provided people and businesses with an opportunity to try sustainable remote work – and many of them saw the benefits.

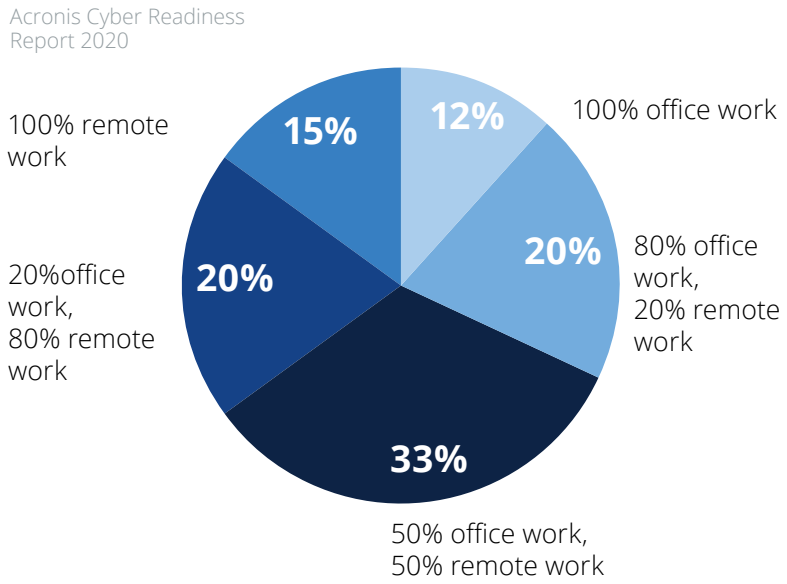
Among the 12% favoring full office work, there are the following country-level outliers: 29% of employees in India and 21% of employees in Japan.

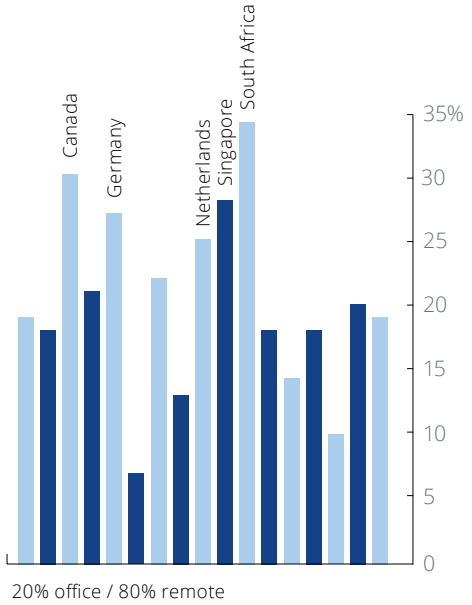
Among the 20% favoring the "80% office / 20% remote" split, there are the following country-level outliers: France - 33%, Spain – 29%, Switzerland - 28%, and the UK - 27%.

Among the 33% favoring "50% office / 50% remote" split, there are the following country-level outliers: Bulgaria – 41%, the UEA – 41%, Sweden – 40%, the Netherlands – 39%, Italy – 39%, Germany – 38%, Australia – 38%.

Among the 20% favoring "20% office / 80% remote" split, there are the following country-level outliers: South Africa – 34%, Canada – 30%, Singapore – 28%.

Among the 15% favoring full remote work, there are the following country-level outliers: the US – 26%, South Africa – 25%.





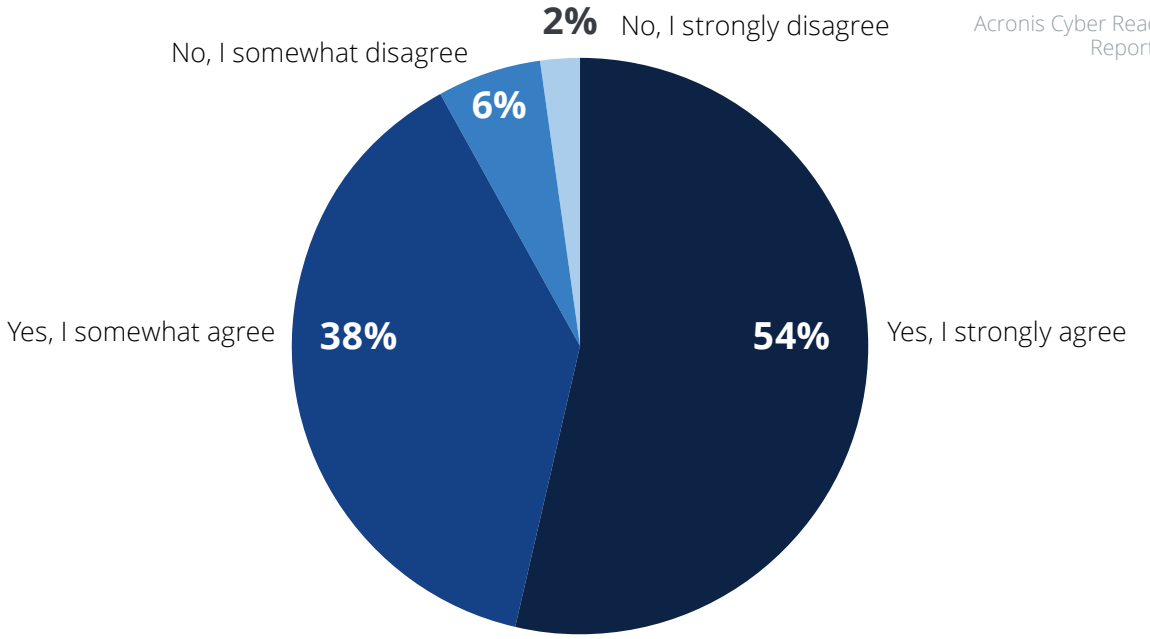
Copyright © 2002-2020 Acronis International GmbH.

92% of employees expect their companies to invest more into digital transformation tools to help adapt to new business realities.

Q7. Do you think your company should invest more in modern digital transformation tools to help cater to new formats of work, including remote work?

Key finding: 92% of global respondents want their company to undergo a continuous digital transformation in order to maintain flexibility and adaptability for the new realities of office life. Employees in India, South Africa, the UAE, France, and Japan reported favoring even higher levels of digital transformation

Employees worldwide expect an increase in digital transformation investment from their companies. The countries where this expectation is most universal are: India, South Africa, the UAE, France, and Japan.



Acronis Cyber Readiness Report 2020

Copyright © 2002-2020 Acronis International GmbH.

Part 3

Acronis CPOC Insights

Trends and predictions by Acronis Cyber Protection Operations Center (CPOC) security experts.

CURRENT ISSUES:

1. **Weak points exposed during the switch to remote work:** Three weak points were exposed during the abrupt shift to remote work. These include: 1) exposed servers (RDP, VPN, Citrix, DNS, etc.), 2) weak authentication techniques, and 3) insufficient monitoring.
2. **Corporate security protocols and tools are based on compliance rather than actual business or market needs.** Phishing remains a pressing concern – but has yet to receive a proper industry response. IT teams are only reacting to standard cyber threats, and are not adapting to address new ones.
3. **Across all industries, employees still demonstrate low awareness and willingness to follow security protocols.** The two main tasks for corporate IT teams will be communicating cybersecurity guidelines to their employees and finding a way to make sure they're followed.
4. **Missing expertise in cloud technology.** Many companies have moved workloads to the cloud but they don't have the skills in-house to manage and protect SaaS, containers or APIs, for example. As a result, badly configured cloud architectures are emerging, which will inevitably lead to data breaches.
5. **Global teams require more complex IT support and create a legislative nightmare.** The absence of a universal international cyber law leaves us exposed to foreign threats.

Did you know?

Perimeter security is out the window. #WorkFromHome will soon evolve and the next frontier - and challenge - for businesses will be #WorkFromAnywhere

The future cyberthreat landscape revolves around attacks of scale rather than attacks of sophistication. Any amateur will soon have access to malicious cyber kits.

Copyright © 2002-2020 Acronis International GmbH.

TRENDS & PREDICTIONS:

1. **Malicious Software as a Service:** For the past five years, any amateur could gain access to a malicious toolkit. – you don't need to be tech-savvy anymore to create chaos. AI/ML driven automation is helping make these tools even more powerful and increase attack frequencies. Finding a vulnerability is tricky but once it's disclosed any group of teenagers can cause mayhem and take the system down. Attribution will get tricky, making prosecution impossible.
2. **Perimeter security is out the window. #WorkFromAnywhere will soon replace #WorkFromHome.** It's not just your network that needs to be secure. The next stage is making sure you can work securely anywhere – even from an unsecure environment. People will continue to work and hire remotely, and this will be the new normal.
3. **Device security is a growing concern and a growing cost.** Inside your corporate network, data and devices are protected. But employees working from home and purchasing new devices themselves, combined with the lack of BYOD policy at many companies, leads to an exponential growth in vulnerable endpoints. These same devices will be routinely exposed to untrusted networks (hackable routers, unsecure Wi-Fi, etc.)
4. **Hacking communities and groups joining forces more often.** To capitalize on the COVID-19 pandemic, hacking communities have been joining forces and sharing resources throughout 2020.
5. **Attacks frequency increasing drastically – AI/ML can also solve the challenge of automation.** With limited human response capabilities and a skills gap on our hands, automation, artificial intelligence, and machine learning (AI/ML) become critical aspects of cyber protection.
6. **The development of 5G technology and the IoT will lead to a botnet increase – creating a surge in DDoS risks.** With the introduction of 5G networks connecting a mushrooming number of IoT devices, the speed of connectivity will lead to larger attack surfaces and increased security threats, such as DDoS attacks and cyberattacks. Organizations that rely on the internet for their business will have to adapt to the increased cyber risks posed by 5G.

Did you know?

IT teams must push harder on educating their employees about modern cyber threats.

The current industry response doesn't match the cyber security landscape – too many companies follow common protocols, leave emerging attacks unattended.

Attackers react to news instantly these days. In one recent example, the number of DNS scans tripled right after the news broke about the Microsoft DNS vulnerability.

Copyright © 2002-2020 Acronis International GmbH.

Industry breakdown – spikes detected in various verticals

SPORTS

1. Sports industry representatives reported the following as the key challenges they've encountered during the past three months: "Securing remote workers", "Software not working properly", and "Ensuring the availability of corporate apps and networks".
2. Approximately 70% of Sports industry representatives reported having their IT costs increase in the past three months.
3. The Sports industry ranks 2nd most frequently targeted industry among other verticals – almost 30% of industry representatives reported being targeted by a cyberattack at least once a day.
4. At the same time, 20% of all Sports industry representatives reported not having received any clear communication upon switching to remote work.

EDUCATION

1. IT/Telecom and Education industry representatives reported having their IT costs increase more significantly than any other vertical, with approximately 70% of Education industry representatives reporting so.
2. "Wi-Fi connectivity" was the biggest challenge for the Education industry, selected by 45% of representatives.

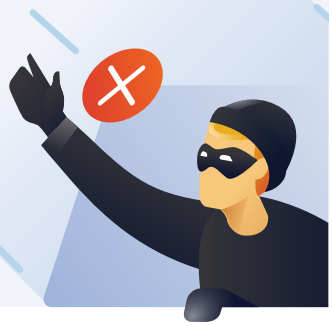
TRAVEL

1. Approximately 70% of Travel industry representatives reported having their IT costs increase in the past three months.
2. Travel industry representatives were the most heavily targeted of all – more than 45% of all respondents stated they encountered a cyberattack at least once a day in the past three months, while 12% reported facing a cyberattack at least once an hour.
3. Travel industry representatives reported a 25% or more decrease in the number of corporate devices connecting to their networks in the past three months – likely due to significant layoffs in the industry caused by the pandemic.

HEALTHCARE

1. Healthcare industry representatives reported "Securing remote workers" as the single top concern for the vertical.
2. Approximately 70% of Healthcare industry representatives reported having their IT costs increase in the past three months.
3. A whopping 68% of Healthcare industry representatives reported purchasing new devices after having switched to remote work – with 21% of respondents purchasing two or more devices.
4. Potentially as a result of those purchases, 63% of Healthcare industry representatives reported feeling better equipped to work remotely than before the pandemic.

Phishing attacks were the most encountered cyberattack across all verticals



Copyright © 2002-2020 Acronis International GmbH.

Conclusion

KEY TAKEAWAYS AND EXISTING SOLUTIONS

Remote work is here to stay and it's up to both the company and the individual to follow the best cyber protection practices available. More on cybersecurity pain points and available solutions for businesses below:

1. **Ransomware is still a pressing threat – more so, when combined with a data breach.** No business is immune and everyone is a target: 43% of cyberattacks are aimed at small businesses. Regardless of business' size, your corporate solution must have antimalware protection integrated. Acronis Active Protection, which is included in the Acronis Cyber Protect solution, has been proven by independent labs to provide a 100% detection rate and zero false positives.

2. **Zoom, Webex, and others will continue to explode in popularity – and remain a potential risk.** A recent zero-day vulnerability found in Zoom can be exploited by attackers to execute commands on a victim's Windows computer to gain remote access. This attack doesn't trigger a security warning. Luckily, Acronis Cyber Protect provides extended protection for applications such as Zoom, Webex, and Microsoft Teams, preventing exploitation and keeping the software up-to-date with patch management.

3. **Twitter accounts hijacked is only the beginning.** Elon Musk, Barack Obama, and 43 other high-profile users were used to push Bitcoin scam messages – stealing at least US$116,000 and the private account data of several users. A URL filtering feature, included in Acronis Cyber Protect, can prevent users from accessing fraudulent websites often used in such schemes. The solution's vulnerability assessment feature can also detect unpatched systems on your device and automatically deploy the required hotfixes.

Copyright © 2002-2020 Acronis International GmbH.

Acronis Cyber Protect 15

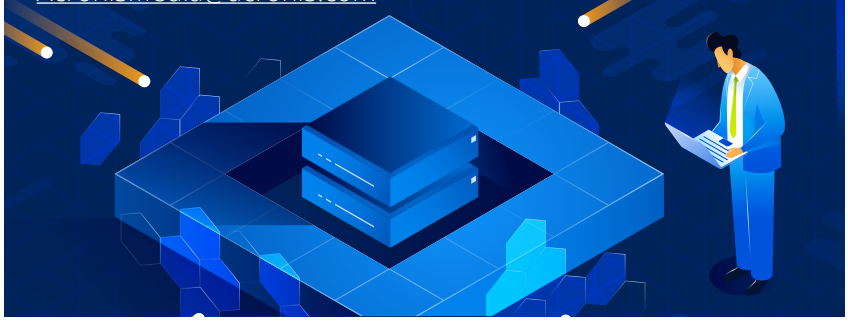
Acronis Cyber Protect 15 was developed to suit the needs of businesses operating in the post-pandemic reality. Its unique integration of data protection and cybersecurity is purpose-built to empower any organization facing strained IT workloads with infrastructure and endpoint protection that's effective in a world where perimeter security is pointless. The Acronis Cyber Protect 15 solution will be available to all businesses in September 2020. Learn more at www.acronis.com/en-us/cloud/cyber-protect

> *"The cyberthreat landscape has changed dramatically during the past few years, and in the last six months in particular. Traditional stand-alone antivirus and backup solutions are unable to protect against modern cyberthreats,"* said Serguei "SB" Beloussov, founder and CEO of Acronis.

> *"Organizations that modernize their stack with integrated data protection and cybersecurity not only gain greater security, they lower their costs, and improve efficiencies. The automation and streamlined management of Acronis Cyber Protect 15 means any business can decrease their risk, avoid downtime, and increase their IT team's productivity."*

With Acronis Cyber Protect 15's unique integration of data protection and next-generation cybersecurity capabilities – including AI-based behavioral detection that stops zero-day attacks, URL filtering, vulnerability assessments, videoconference protection, and automated patch management – organizations protect against modern cyberthreats while ensuring they can recover their data and systems in the shortest time possible.

For more info on any findings featured in the report, you can reach us via email on:
AcronisMedia@acronis.com



Did you know?

Recognized by Frost & Sullivan: Acronis Cyber Protect earns "2020 North American New Product Innovation Award"

AV-TEST independent lab reports: Acronis Cyber Protect scores perfectly, with a 100% detection rate and zero false positives.

Credits for comments – Acronis Cyber Protection Operations Centre team:

Kevin Reed,
Acronis CISO

Candid Wuest,
Acronis VP of Cyber Protect Research

Martin Brough,
Acronis Cybersecurity Expert

Topher Tebow,
Acronis Cybersecurity Analyst

Oleg Ishanov,
Acronis Director of Threat Research

Ravikant Tiwari, Acronis Senior Security Researcher

Copyright © 2002-2020 Acronis International GmbH.

Acronis

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions. With award-winning AI-based antimalware and blockchain-based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on-premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,500 employees in 33 locations in 18 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, including 100% of the Fortune 1000, and top-tier professional sports teams. Acronis products are available through 50,000 partners and service providers in over 150 countries in more than 40 languages. For more information, visit www.acronis.com