Acronis

Report
2021

Acronis Cyber Readiness Report 2021

Comprehensive cybersecurity landscape overview

Acronis
Cyber Readiness Report 2021

Table of contents

Introduction & Survey methodology

The COVID-19 pandemic has crippled businesses worldwide – based on Acronis' research from last year, 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 new challenges do IT leaders and managers struggle with the most.
- What key IT infrastructure vulnerabilities caused the most damage across all industries in the past year.
- How many cyberattacks do large businesses, SMBs, and consumers truly face on a daily basis.
- What types of attacks cybercriminals favor – and which they will focus on next year.
- How ready are employees to switch to permanent remote work – compared to last year.

To find the answers, Acronis conducted an independent research study, surveying 3,600 IT managers and remote workers across 18 countries. The findings provide a clear picture of modern cybersecurity needs, how the business world will cope with remote work further, the changed cyber landscape – and how it will evolve from here.

About the survey methodology

Acronis surveyed 3,600 IT managers and remote workers across 18 countries in order to evaluate their cyber readiness during the second year into the pandemic. Acronis had no role in selecting the respondents, all responses were provided anonymously. The survey was conducted during September-October 2021.

Respondents came from 18 countries across four continents: Australia, Bulgaria, Canada, France, Germany, India, Israel, 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
- Healthcare
- Finance
- Education
- Others (Manufacturing, Hospitality/Travel, Legal/ Professional services, etc.)

Executive summary

Key research findings

- Nearly half (47%) of IT managers report not using multi-factor authentication. They either see no value in it or consider it too complex.
- 53% of companies have a false sense of security when it comes to supply chain attacks – making them an easy target. Respondents do not truly understand the nature of supply chain attacks, just using "known, trusted software" as protection.
- Three out of ten companies report facing a cyber-attack at least once a day, similar to last year. Companies are getting better at detection overall.
- Only 20% of companies reported that they didn't get attacked – as opposed to 32% last year: attacks are increasing in frequency.
- Record-high levels of phishing attacks persist after a year – with malware attacks rising even higher in 2021: 36.5% of all attacks in 2021, up from 22.2% last year.
- With phishing attacks topping the charts, the demand for a URL filtering feature grew 10 times since last year – 20% of global companies now recognize the danger of phishing for businesses worldwide.
- A standalone antivirus solution is not enough, nor is a standalone backup: the demand for integrated backup/disaster recovery has more than doubled – 47.9% in 2021, up from 19% last year.
- Demand for remote monitoring and management tools grew over three times – 35.7% in 2021, up from 10% last year. Remote work has finally been recognized as the long-term default format of work.
- One in four remote workers struggled with the lack of IT support in 2021 – among the key challenges they faced this year. The top three tech challenges identified by remote workers: Wi-Fi Connectivity, Using a VPN and other security measures, Lack of IT support.
- One out of four remote employees is not using multi-factor authentication – making them an easy phishing target.
- On average, one out of five remote employees gets heavily targeted by phishing attacks – receiving well over 20 phishing emails per month.

IT managers

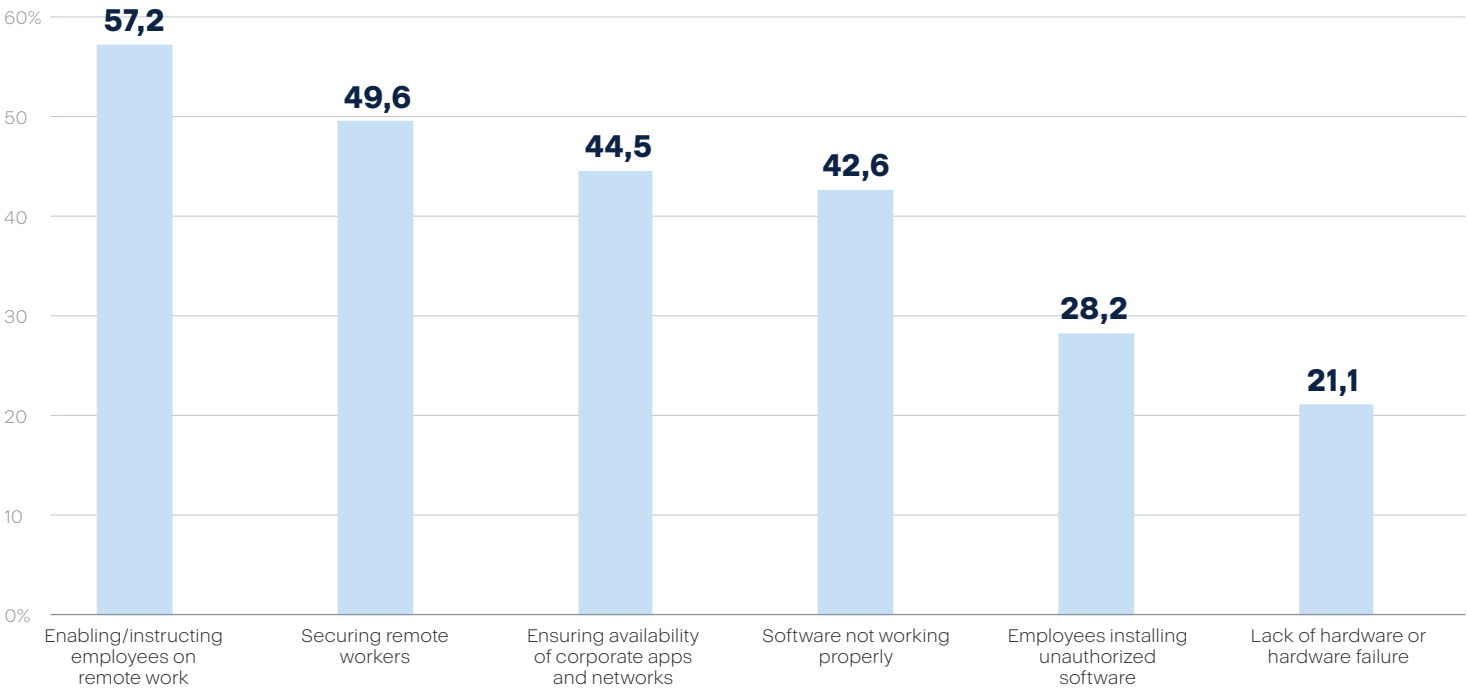
Despite the globally recognized attacks on trusted software vendors, like Kaseya or SolarWinds, over half of IT leaders believe that using “known, trusted software” is sufficient protection – making them an easy target.

Part 1

Companies are struggling more with software complexity and hardware shortage this year – the transition process has not been as smooth as initially claimed.

#1

What were the top tech challenges you encountered supporting increased remote work in the past year?



Key finding

With an overall similar picture to last year's results, we see signs of two apparent issues: software complexity is a tough enemy to beat and too many companies are experiencing a hardware shortage this year.

Globally, the top tech challenges for corporate IT teams remain: Instructing employees on remote work; Securing remote workers, and Ensuring the availability of internal corporate apps.

Notably, "Software not working properly" grew from 34.1% to 42.6% globally: most companies reportedly rolled out new services last year, but a large portion of them are still fine-tuning. Adopting new technology proved harder than expected.

Hardware shortages also became a more apparent issue this year, up from 18.5% last year to 21% in 2021: employees of giant IT companies globally report having to wait three to six months for corporate laptops due to chip shortages.

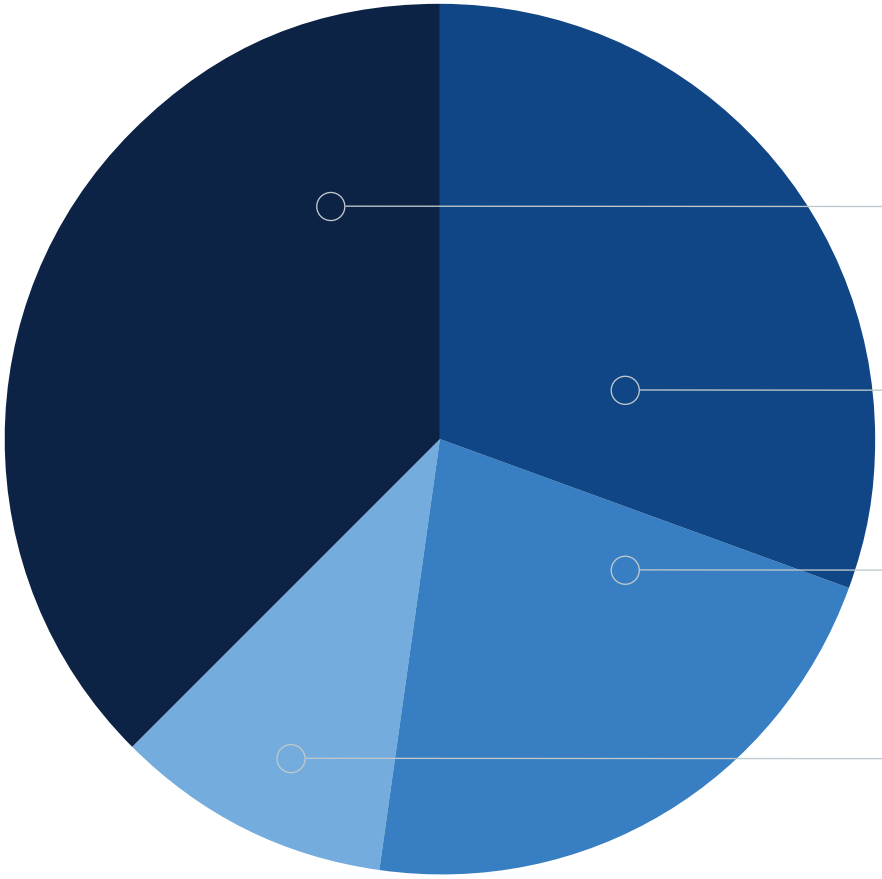
Did you know?

Instructing remote employees is still a top issue for 68% of companies in both UAE and Singapore. One in three companies in India, France and South Africa suffers from lack of hardware – opposed to one in ten companies in Sweden, lowest among all countries.

47% of IT managers don't normally use multi-factor authentication – either seeing no value in it or considering it too complex.

Do you use multi-factor authentication?

#2



37,7%
On some accounts

30,6
On most accounts

21,6
On all accounts

10,1
No

Key finding

A new question asked of the respondents this year – to determine the frequency of use of multi-factor authentication (MFA) by members of corporate IT teams.

While some accounts don't offer MFA at all, it turns out that a staggering 47% of global IT managers don't use it on a daily basis. Among the top reasons, we suspect those IT managers either: see no value in MFA, presume it unimportant or find it too difficult or time-consuming to implement.

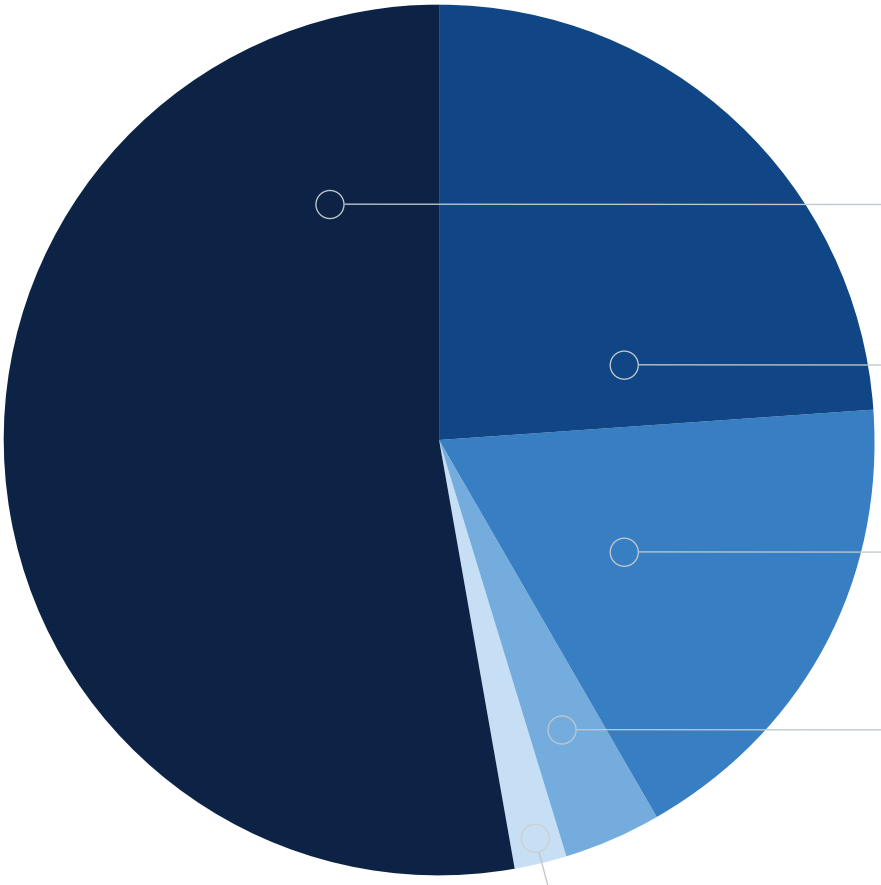
Did you know?

Colonial Pipeline was one of the cases where old VPN passwords were leaked – making it one of the incidents that could've been avoided with MFA.

53% of companies have a false sense of security when it comes to supply chain attacks – making them an easy target.

How do you protect against software supply chain attacks?

#3



53%
We only use known, trusted software

23,8
We use AV/EDR scanning

17,8
We outsource this protection to an external provider

3,5
We don't currently, but plan to within the next year

1,9
I don't know

Key finding

Another new question we asked this year, procuring interesting results. Only 24% of global IT managers confirmed that they were using AV/EDR scanning – while 18% outsource their protection to an external provider. However, 53% exhibit either a false sense of security or do not truly understand the nature of supply chain attacks – claiming to use "known, trusted software" only.

The most well-knownrecent cases of such thinking putting businesses in danger were SolarWinds and Kaseya – both trusted software manufacturers, both having suffered devastating attacks affecting their partners and clients globally. A supply-chain attack is, by definition, coming from a trusted network – and this year all technology vendors are becoming desired targets in the eyes of cyber criminals.

Overall, only 2% of respondents didn't know if or how their company defended against such attacks. While 98% of IT managers are aware of supply chain attacks as a credible threat - due to attacks on Kaseya and others – it would seem, the majority is still drawing the wrong conclusions, despite growing awareness.

Did you know?

Keen to know how to defend against supply chain attacks, like the SolarWinds breach?

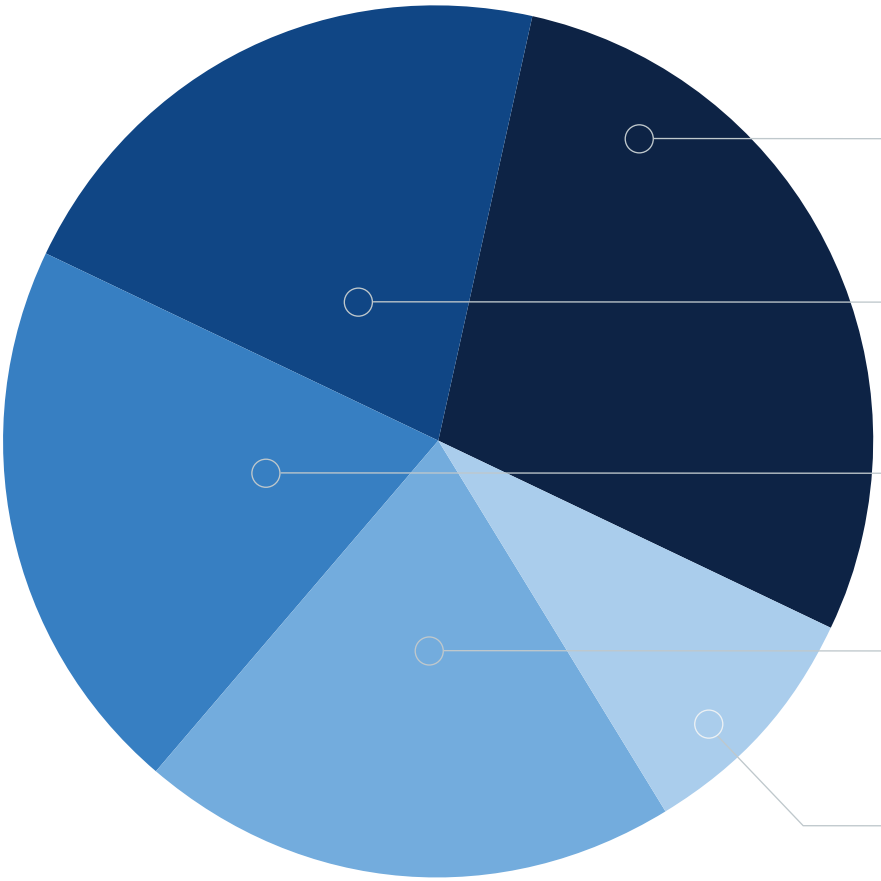
Check out this Acronis whitepaper

HERE

Three out of ten companies report being attacked at least once a day – similar to last year. Companies are getting better at detection overall.

How often was your company targeted by cyberattacks in the past year?

#4



28,6%
At least once a month

21,4
At least once a week

20,6
At least once a day

20,1
We haven't been targeted

9,3
At least once an hour

Key finding

This year, 30% of companies report being attacked at least once a day – similar to last year's level of 31%.

This year's stats are showing that only 20% or one-fifth of all companies did not report getting attacked – as opposed to 32% last year. There are two possible explanations: either attacks are increasing in volume and frequency or companies are getting better at detection – we believe both to be true.

Attackers are now using automation more frequently, learning to use artificial intelligence (AI) and machine learning (ML) in more attacks.

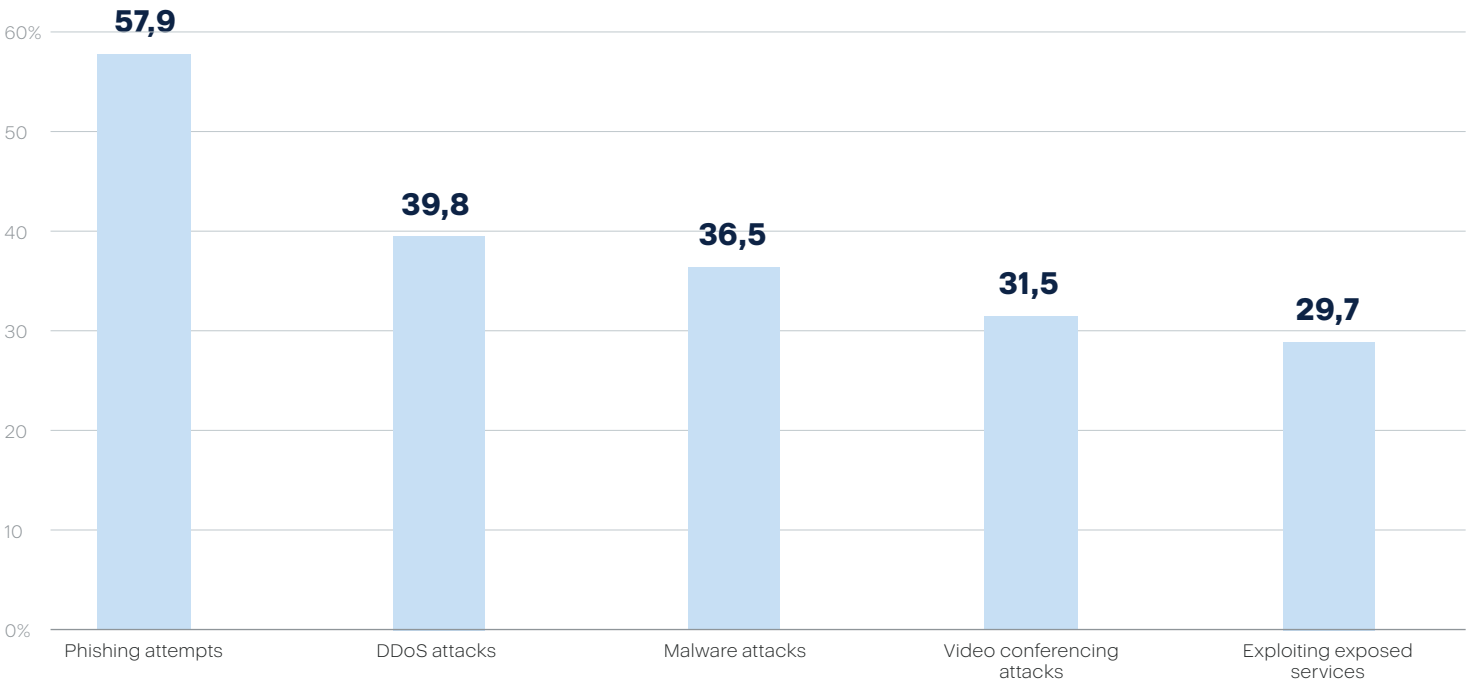
Did you know?

Half of companies in Bulgaria and India faced cyberattacks at least once a day – 27% and 16% respectively attacked each hour. One third of companies in Japan and Switzerland did not face cyberattacks last year, as reported by 35% and 29% of IT managers respectively.

Record-high levels of phishing attacks remain after a year – malware attacks rising even higher in 2021.

What cyberattack types has your organization encountered in the past year?

#5



Key finding

Phishing and malware attacks continue to rise, with phishing still the top attack type plaguing companies – and last year's peak numbers holding up even after a year.

Phishing is probably the easiest attack to carry out and one of the most efficient techniques that continues to prey on the human element – growing even further from the record high of 53.4% last year to 57.9% in 2021. Further growth iin the success rates of phishing attacks can only be countered by raising awareness and having a strong email security.

Notably, malware attacks grew most significantly, from 22.2% in 2020 to 36.5% this year. Both phishing and malware attacks are still mainly delivered via email - the more emails you send or receive, the more malware and phishing you face - but malware attacks are the ones showing the most growth. One of the possible reasons: anti-malware protection solutions used by companies are not good enough – more attacks are succeeding and cyber criminals to rely more on malware.

Did you know?

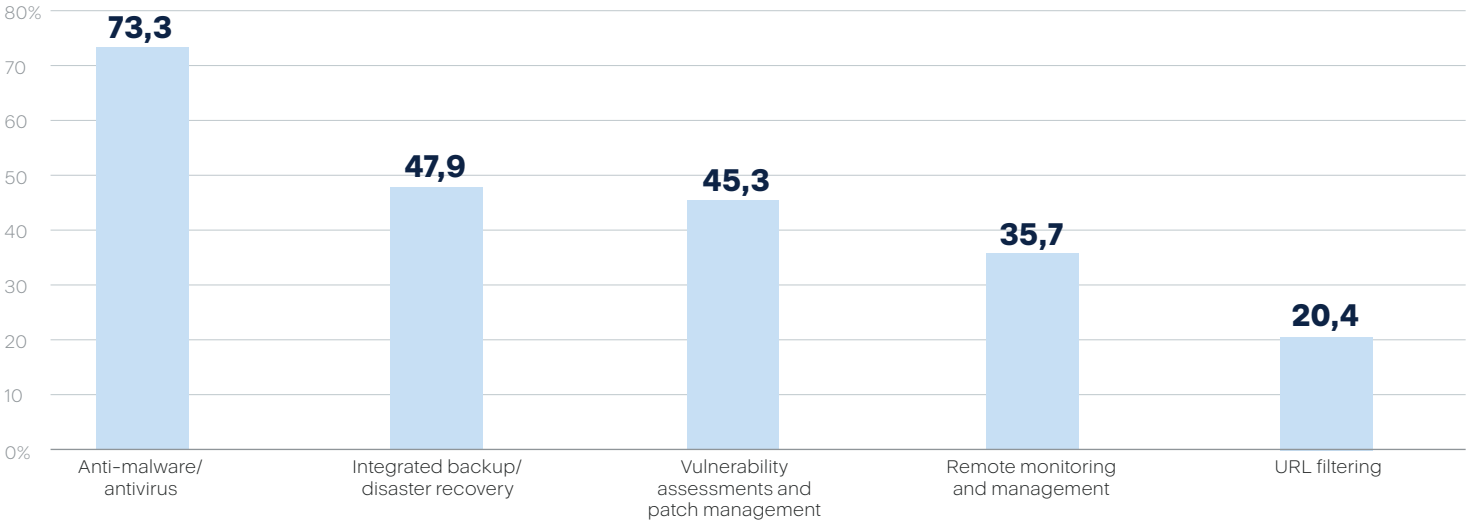
Phishing is still the most common attack type – companies in Singapore, Italy and UK facing it most frequently, as reported by 74%, 69% and 68.6% of IT managers.

Half of companies in South Africa and Singapore faced malware attacks last year, far above the global average of 36%

Demand for a URL filtering solution grew 10 times since last year – while demand for integrated backup/disaster recovery doubles.

#6

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



Key finding

With phishing attacks topping the charts, the demand for URL filtering features among companies has grown from 2% last year to 20.4% in 2021 – a positive sign that the danger of phishing is finally being recognized by businesses globally.

The demand for antivirus has also grown by 30% – from 43% last year to 73.3% in 2021. But for every step the companies are taking, cyber criminals have already taken three: an antivirus solution alone is not enough, nor is standalone backup. Companies worldwide are discovering this: we saw the demand for integrated backup/disaster recovery more than doubled – from 19% last year to 47.9% in 2021.

Not surprisingly, vulnerability assessments and patch management grew significantly: from 26% last year to 45% in 2021 – in response the cyberthreat landscape. Not only did we see increased volumes of vulnerabilities reported in key platforms in 2021, including Microsoft, Chrome and others – but more threat actors are specifically looking for vulnerabilities this year. Fueled by remote work, exposed file exchange, and more services going online, the hunt for vulnerabilities has never been bigger.

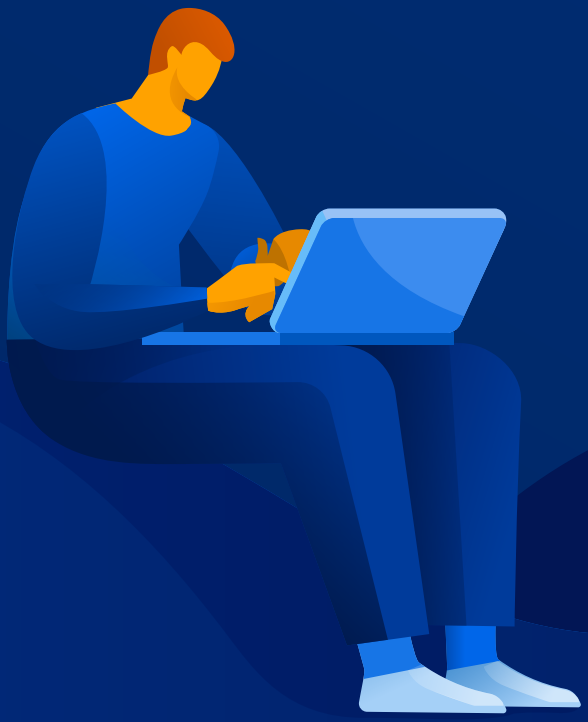
Remote monitoring and management tools are in high demand this year – up from 10% last year to 35.7% in 2021: which is no surprise given the raging pandemic and remote work becoming the default format of work.

Did you know?

A bug bounty program is an essential tool for security flaw detection. Check out the Acronis Bug Bounty program on HackerOne to learn more: offering up to $5,000 for spotting bugs in our cyber protection solutions.

Remote employees

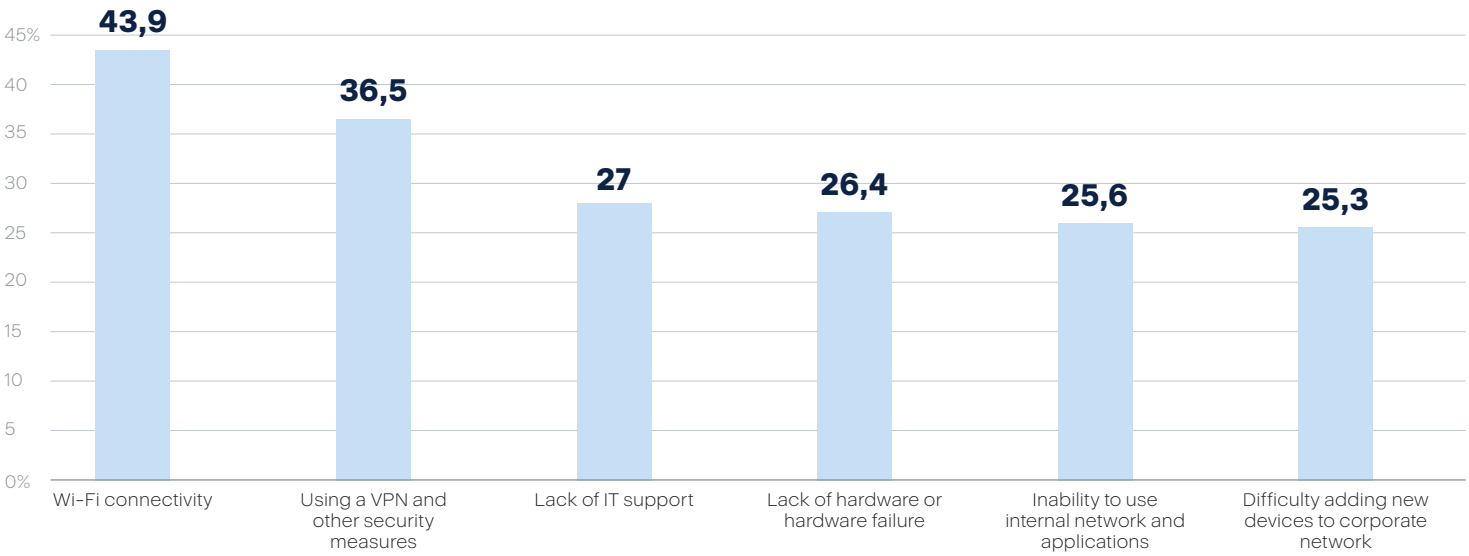
Despite the growing cyberthreats, people will continue to work and hire remotely - that's the reality all IT teams need to equip for. Finding a solution to hardware shortages, increased software complexity and growing need for IT support is a good start.



Part 2

One in four remote workers struggled with the lack of IT support in 2021 – among the top three tech challenges they faced this year.

What have been the most technically challenging aspects of working remotely?



Key finding

We detected the most significant growth of concern among remote employees over "Lack of IT support" – reported by 17.1% of respondents last year, now up to 27% in 2021, highlighting an interesting trend.

Providing IT support has become even more difficult this year – the environment has changed dramatically: physical distance has become permanent, environments have only increased in size and complexity, and addressing IT issues has become slower and more expensive.

With new tools and solutions for remote work being adopted, IT teams have more applications to manage, like cloud applications. Not all IT teams had the rights skill set for that, increasing stress and the need for experienced IT professionals.

Same as last year, enabling a VPN, relying heavily on video calls and live streaming, having whole families working and studying at home at the same time – these factors are reflecting badly on remote workers' Wi-Fi connectivity, leaving them frustrated and cutting corners on data protection procedures.

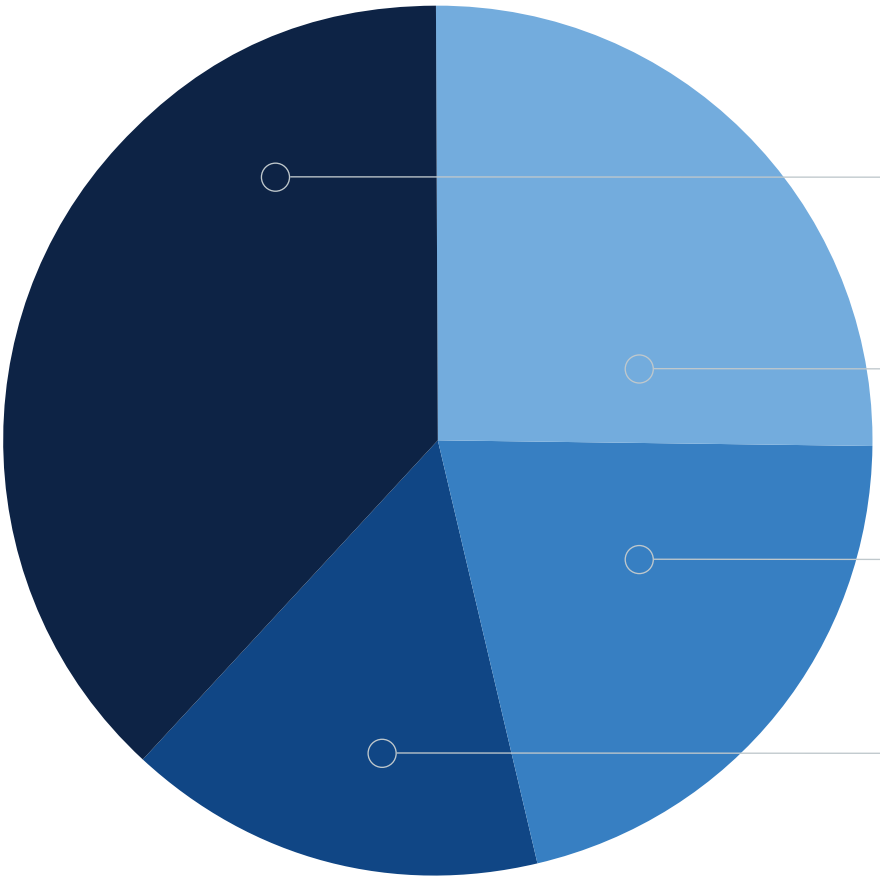
Remote monitoring and management tools are in high demand this year – up from 10% last year to 35.7% in 2021: which is no surprise given the raging pandemic and remote work becoming the default format of work, and a long-term one.

Did you know?

Wi-Fi connectivity is a top issue for two-thirds of employees in India and Israel. 58% of employees in India also suffer from lack of hardware and being unable to add new devices – two times the global average.

One out of four remote employees is not using multi-factor authentication – making them an easy phishing target.

Do you use multi-factor authentication?



38,3%
Na některých účtech

25,3%
Ne

21%
Na většině účtů

15,4%
Na všech účtech

Key finding

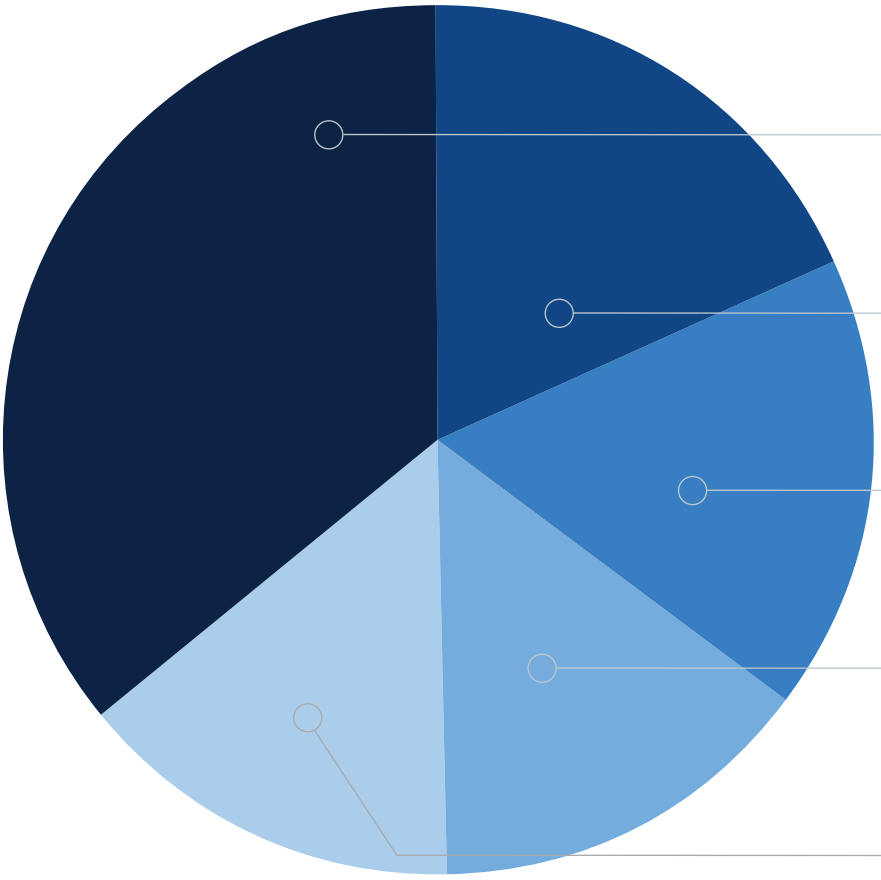
Only over a third of remote employees (36%) are using multi-factor authentication (MFA) on most or all the accounts – while 25% are not using it at all, leaving themselves exposed.

Not using MFA leaves your email, social media , and other accounts vulnerable to phishing attacks, which is still the most frequently reported type of cyberattack, having grown even more since last year – as seen in Part 1: IT managers.

The largest segment of remote workers (38%) is using MFA on some accounts only: likely forced to do so by various platforms enforcing MFA for daily operations – for example, banking service providers or cashless payment operators.

On average, one out of five remote employees gets heavily targeted by phishing attacks – receiving more than 5 phishing emails each week.

#3



36%
1-5 e-mailů

18,3%
20+ e-mailů

17%
6-10 e-mailů

14,5%
Žádné

14,2%
Nevím

Key finding

71% of respondents confirm being targeted by phishing each month – with 18%, or roughly one out of five, receiving over 20 phishing emails in a month.

The users targeted most are usually the ones using email most often: the more active you are, the better target you make. We're seeing more sophisticated phishing techniques each day, requiring 24/7 vigilance.

Learning to identify such attacks through awareness and proper training is crucial in keeping not just enterprises and organizations protected, but your personal assets as well.

Did you know? 2021 is the year sophisticated phishing techniques establish their presence – third-party phishing, impersonation, personalized messages banking on loads of personal info getting leaked in frequent data breaches.

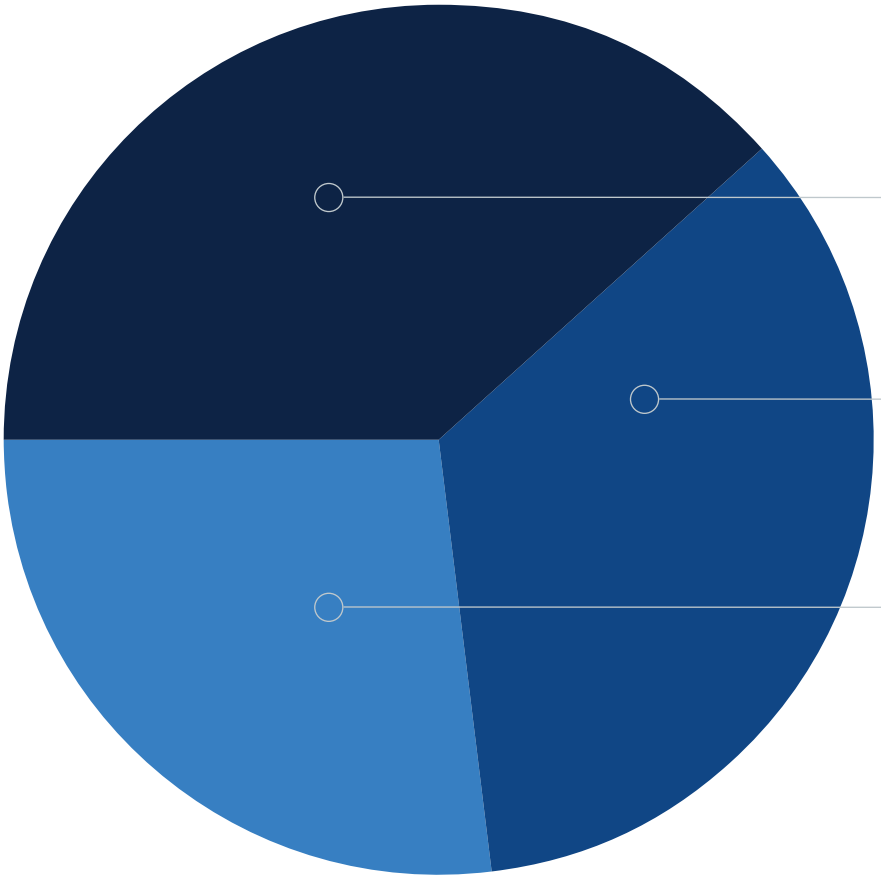
Did you know?

Employees in Bulgaria, India and UAE facing phishing attacks most often – 30%, 26% and 23% report receiving over 20 phishing emails per month.

Number of remote employees to purchase 2 or more devices nearly doubled this year, purchase confirmed by 27% of respondents.

#4

Have you or your family members purchased any new devices – computers or wearables – since having started to work remotely?



38,6%

Jedno nové zařízení

34,7%

Žádné nové zařízení

26,7%

Dvě a více zařízení

Key finding

Remote work has finally been accepted as the default work format – with 66% of employees buying extra devices for themselves, as well as their kids' remote studies.

Conversely, 35% of remote workers report not having purchased any new devices this year (down from 51% in 2020) – suggesting they are still using their old, unpatched personal laptops for work.

Acronis Cyber Protection Operations Center insights

If you are keen to learn more about cybersecurity pain points and available solutions for businesses, don't miss the chance to register for the Acronis #CyberFit Summit World Tour 2021 - kicking off in Miami, Florida on October 25 with a hybrid event.

REGISTER NOW

Trends overview from Acronis Cyber Protection Operations Center (CPOC) security experts

CPOC

1. The growing complexity of IT infrastructure

In last year's Acronis Cyber Readiness Report, we saw an increase in adoption of new services, especially SaaS in the cloud. This increases the overall complexity of the IT environment further and will most likely lead to more unplanned disruptions in the future.

Automation can help to keep up with the different configuration changes, but such scripts need to be carefully planned and monitored or they may generate even more issues.

2. Attacks outside of Windows

We have seen attackers increasingly expanding their targets. It is no longer Windows only, but Linux, MacOS, Android and iOS devices as well. Attackers are also going after virtualized environments more often, be it container in the cloud or performant VM servers, like ESXi servers, which have seen an increase in ransomware attacks.

3. Malicious Software as a Service growing further

Unfortunately, you don't need to be tech-savvy to create chaos with malware. Cybercriminal groups have further expanded their malware-as-a-service model, providing step-by-step guides on how to compromise targets and make profits. Ransomware groups now even try to recruit company insiders, getting them to execute the ransomware in exchange for a share of the profits.

Did you know?

Facebook experienced an unwanted disruption when they went offline for six hours after a faulty Border Gateway Protocol (BGP) configuration update knocked them off the Internet, including their DNS servers.

Three key weak points were exposed during last year's abrupt shift to remote work:

- Exposed servers (RDP, VPN, Citrix, DNS, etc.)
- Weak authentication techniques
- Insufficient monitoring.

4. New name, old tricks

A handful of ransomware groups have "rebranded" themselves – for example, DarkSide or DoppelPaymer, after their affiliates attacked large targets and attracted law enforcement attention. This is an attempt to make it more difficult for law enforcement agencies to make a case – don't get fooled, they are still out there attacking companies like yours.

5. Phishing still works well

Malicious emails and phishing in all variations are still at an all-time high. Despite the constant awareness campaigns, users still fall for them and enable the attacker to compromise their organization. With increased automation and personalized information from the various data breaches, these attacks are constantly growing in sophistication and efficacy.

6. Patch, patch, patch

Over 16,000 vulnerabilities have been reported so far in 2021. Many of them were critical and in-core components, such as Microsoft Exchange server, Chrome browser or Apache webserver. Keeping up with plugging these weaknesses can become a full-time job and puts additional stress on the already overloaded IT teams.

7. Remote work will not go away

Global businesses employ international teams, requiring more complex IT support and creating a legislative nightmare. The supply shortage of hardware devices increases the complexity even further. People will continue to work and hire remotely – that's the business reality most IT teams were not ready for.

Conclusion

Remote work is here to stay, so are the increased levels of sophisticated cyber-attacks – and it's up to both the company and the individual to follow the best cyber protection practices available.

Are you keen to learn more about cybersecurity pain points and available solutions for businesses?

Register now for the Acronis #CyberFit Summit World Tour 2021, kicking off in Miami, Florida on October 25-27, 2021. One platform that allows you to:

- Attend result-focused virtual sessions for free and learn from world-class experts on cyber protection.
- Enhance your MSP business' cyber protection capabilities with advice from the top channel, cybersecurity, and industry experts.
- Hear exclusive case studies of successful, profitable, and scaling MSPs and MSSPs.
- Learn how to grow your business with cybersecurity-forward services.
- Join hands-on, interactive workshops, insightful panels and breakouts, and inspiring keynotes – while enjoying IT channel networking opportunities.

Get access to the recorded sessions from the Acronis #CyberFit Summit World Tour 2021 here

For more information about the report, you can reach us via email at: AcronisMedia@acronis.com

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 powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence 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 1,700 employees in 34 locations in 19 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 25 languages. For more information, visit www.acronis.com