prey

Shift

STATUS OF THE

REMOTE WORK

CYBERSECURITY LANDSCAPE_

2021

30%

20%

10%

0%

Prey Inc.

Index

Shift: The Report

INTRODUCTION

These are unprecedented times. A worldwide pandemic may not be uncommon, but a worldwide pandemic in a hyperconnected, digitalized, technology-oriented time is weird, especially in the context of labor. Similar to underground music becoming mainstream, the remote work fad –that everyone believed was wishful thinking instead of a legitimate way to work– became the only productive road for millions of people and organizations around the world. We jumped on the full-remote bandwagon as soon as we could. Most of our partners and friends did it, too. But it was no easy task.

If you ask any manager about what was the hardest thing to maintain last year, the answer will always be "operations". Millions of people going remote all around the world. Millions of houses converted to makeshift offices in a matter of days. And of course, millions of endpoints reaching insecure network environments that were never meant to be used for work.

We are all aware of the evolution of risk during 2020. Although we are usually prepared for changes in cybersecurity, this year was a real maelstrom. From the consolidation of ransomware as a serious threat to the latent danger of persistent attacks like the SolarWinds hack, the "year of the pandemic" was also the year when we rethought our protection and security strategy. A year where the need for adequate countermeasures led us to invest much more –and to worry much more.

And we have reason to be worried. Our endpoints entered an unprecedented battlefield; far from our corporate environments, on insecure networks, in many cases sharing with other unsafe devices in our homes (IoT, we are looking in your direction). Because of the COVID-19 pandemic, we don't move around that much anymore, but staying home isn't necessarily the best bet. As home office becomes the standard, we have to be worried. The remote challenge is a challenge to be reckoned with.

Prey is a company with a clear mission: Minimize all concerns around mobility. In our crusade, which is now over ten years old, we have understood that it is not enough to protect devices from loss and theft if we do not look at the bigger picture. That is why we took the step further: researching cybersecurity in the remote workplace, to help you worry positively on these times of change. This shift is key for us, and we hope your organization can benefit from our analysis.

Worked on this report:

- Norman Gutiérrez, Security Researcher
- Beatriz Henríquez, Security Researcher
- Patricio Guzmán, Data Analyst
- Vicente Tiznado, Data Analyst
- Bárbara González, Design & Illustration
- Juan Ortega, Lead Marketing Manager

KEY FINDINGS

63%
Of organizations already had a policy for remote work before the pandemic

43.19%
Of office jobs will become remote permanently after the pandemic (in average)

44%
worry that employees are using BYOD devices without proper security assessment

62.7%
Believe that security threats increased in 2020

0.6%
Haven't invested in new security measures

6.22%
Of the global annual revenue was invested in average in cybersecurity in 2020

67%
State that endpoint misuse has increased with remote work

95.3%
Created or revisited their cybersecurity policy to mitigate risks

92%
Believe the pandemic has made cybersecurity a greater challenge

13.3%
Malware was their primary cause of concern before the pandemic

88.34%
Increased the number of trainings in cybersecurity in 2020

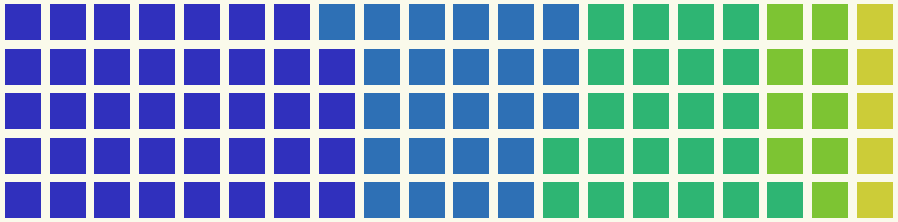
78.3%
Believe that employees don't understand the risks associated with remote work

Methodology & Key Demographics

The results shared in this report come from a comprehensive survey of 300 security and IT professionals in the United States and the United Kingdom. Conducted in December 2020, the SHIFT survey was aimed at identifying security concerns related to the remote work trend, and the evolution of such concerns as the cybersecurity landscape changed throughout the year.

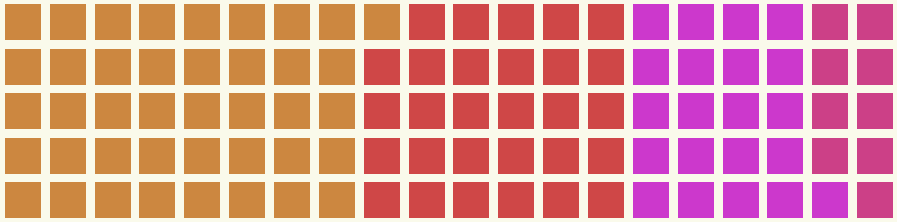
The respondents come from a variety of industries and organizations, big and small, with varying levels of seniority and responsibility to represent the security landscape broadly and accurately.

Size of the organization (in amount of employees)



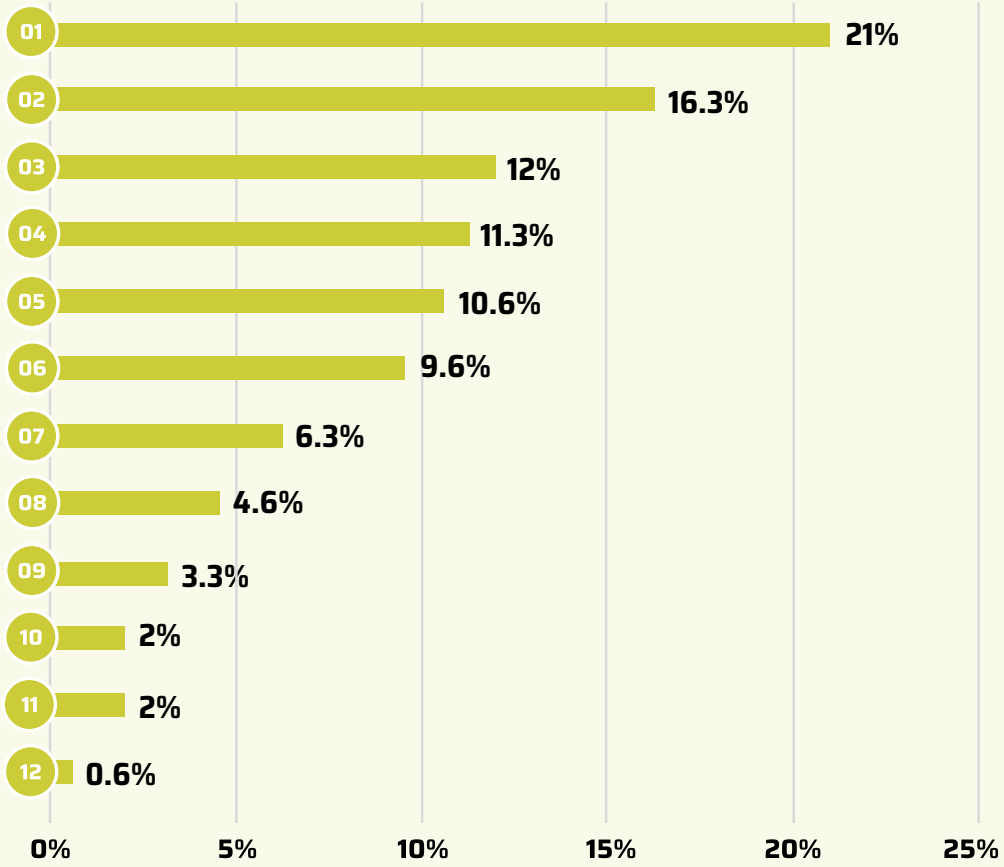
39% 500-999
24% 200-499
23% 1000-2999
9% 3000-4999
5% 5000+

Position in the organization (in seniority level)



41% CXO, senior manager of unit or department
29% Intermediate management
21% Owner, CEO, most senior level
9% Team or group supervisor

Industry or sector



01. **21%** IT, technology and telecoms.

02. **16.3** Manufacturing and production.

03. **12%** Retail, distribution and transport.

04. **11.3%** Financial services.

05. **10.6%** Other commercial sector.

06. **9.6%** Business and professional services.

07. **6.3%** Public sector (excluding public education).

08. **4.6** Construction and property.

09. **3.3%** Education (public and private).

10. **2%** Energy, oil, gas and utilities.

11. **2%** Media, leisure and entertainment.

12. **0.6%** Consumer services.

01.

REMOTE WORK

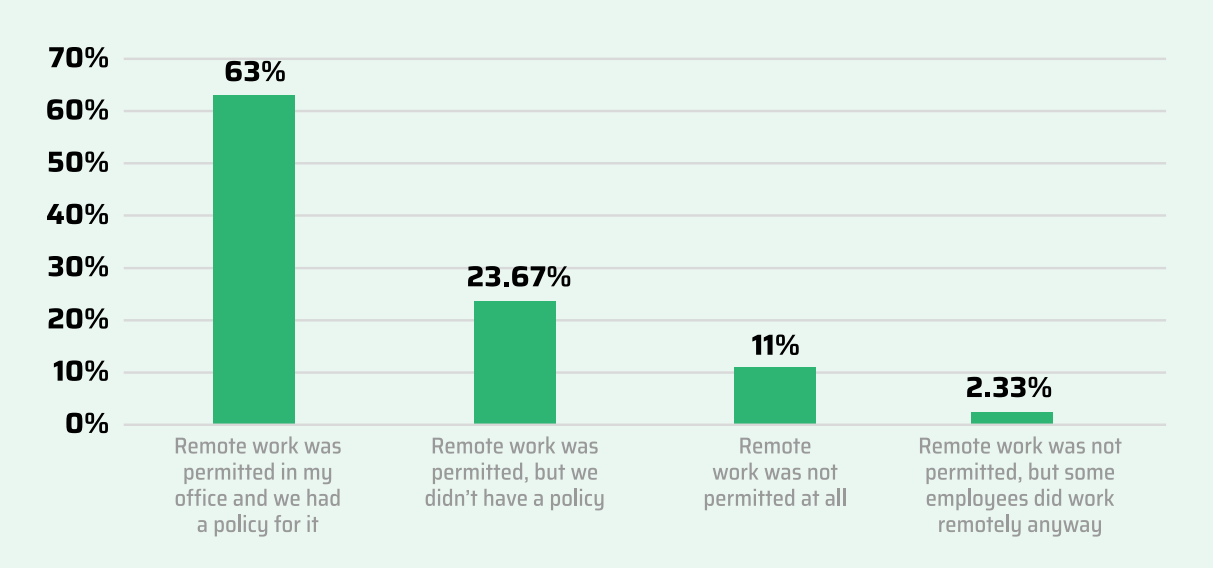
State Of The (Remote) Art
More Pandemic, More Problems
The Future Of Remote

State Of The (Remote) Art

Of all the traditions that changed with the advent of a global pandemic, the one that no one expected to change –which was ultimately the most successful– was the migration to remote work of a good number of the world's workforce1. Before the pandemic, the phrase "remote work" made most bosses and supervisors frown. All attempts to change this unquestionable way of working were received with discomfort, skepticism, and even laughter.

Despite this, many already knew remote work as a way of life. In fact, our survey proved it. Of all organizations surveyed, at least 63% had some form of remote work policy implemented, and an astounding 86.67% allowed remote work in some way or another.

This is no news, but a revelation.



We were already experiencing a shift into remote work, it just wasn't visible.

Remote work has been not only a challenge on the technical side but also a paradigm shift that defy how formal work was managed since the beginning and only started to slowly change when the Internet became ubiquitous. Most companies that have dared to make a change have been, in lieu of a more crude word, timid: relying on a hybrid model for seemingly more remote-friendly roles.

There were other companies that dared to adopt a remote-first model previous to the pandemic. Their motivators were to take advantage of talents worldwide and balance the work-life proportion for workers, and this inadvertently placed them ahead of work models worldwide in quarantine preparedness. We're talking about Basecamp, Automattic, and GitLab, to cite a few. They were the vanguard and had to swim against the current for years.

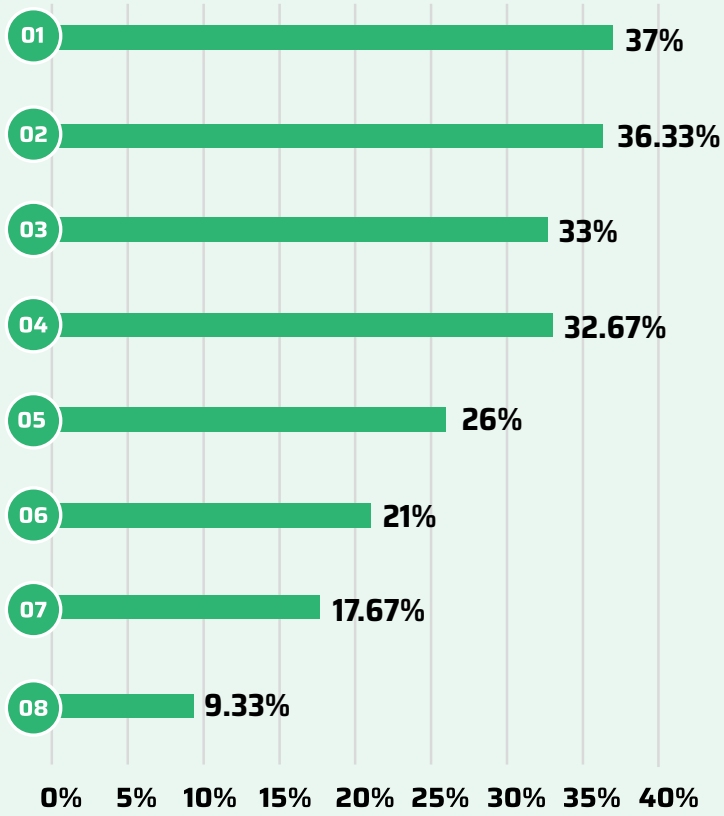
More Pandemic, More Problems

As 2020 came and offices became remote compulsorily, a new set of worries emerged. It was clear that nobody knew how to transition smoothly from our secure, functioning offices to our homes. How do we keep track of our workers' performance? Where will our meetings be?

But the real war was waged elsewhere. Our IT guys and administrators were scrambling to meet the growing demands of thousands of new home workers. And that's not all: security measures, data encryption, communication protocols, hardware management, inventory control, and even identification had to change and adapt to this new reality.

As for the concerns of our professionals, the survey reveals that the **lack of IT infrastructure to allocate sudden remote workers**, followed by **employees using third-party software, increasingly overwhelmed IT staff, and not having enough devices for everyone** were the most common. Lack of budget was a big concern too, as well as dated infrastructure and IT personnel without the necessary experience.

Note: The answers are the combination of responses ranked first, second and third in a multiple choice query.



01. **37%** Our IT infrastructure couldn't handle the number of employees who had to work remotely.

02. **36.33%** Employees using untested third-party software/tools.

03. **33%** Overwhelmed IT Staff.

04. **32.67%** Not have enough devices (e.g. laptops) to give to all employees that needed them.

05. **26%** Lack of budget for infrastructure updates.

06. **21%** Our IT staff did not have the skills needed to support totally remote work.

07. **17.67%** Our IT infrastructure was too dated.

08. **9.33%** My organization didn't experience any challenges.

There is a surprising percentage of organizations that didn't have any problems, though. Almost one out of ten is not that much, but those without problems seem to be the most prepared on the remote landscape.

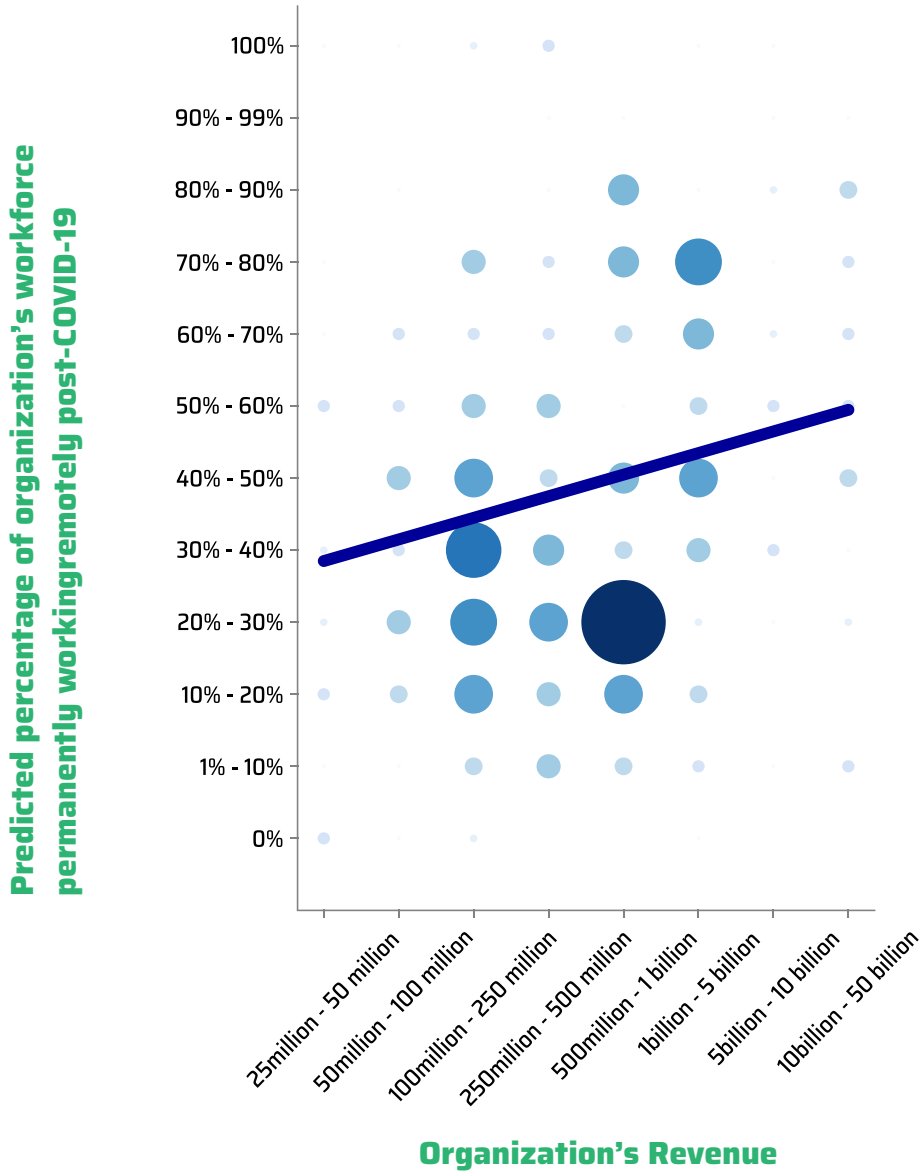
The Future of Remote

When the storm is over and the pandemic ends, the question in everyone's minds will be this one: Are we going back to normal again?

On average, **43.13%** of workers will stay remote after the pandemic ends. If we take into consideration that more than **80%** of organizations allowed remote work, the shift into this way of work is here to stay.

If not having the necessary infrastructure was one of the main reasons why remote work was not that popular before 2020, mandatory quarantines created a worldwide increasing need to leave apprehensions aside and compatibilize work with the new care needs that appeared. Pending device purchases were accelerated, policies were created and working from home practices reached companies and institutions that never expected to join. Then, the obvious happened; Companies had the real chance to verify whether remote work was a good or bad idea case by case. The logical next step is to assess and keep what they already created and saw that could work.

When the pandemic scenario transitions to a new reality, we expect that remote work will be consolidated enough to switch from work at home, to work anywhere. The scope of this shift goes farther than saving on commuting time and office resources; It should also significantly decrease air and noise pollution, decentralize population, and create better work alternatives for workers with disabilities.



02.

Cybersecurity, Before

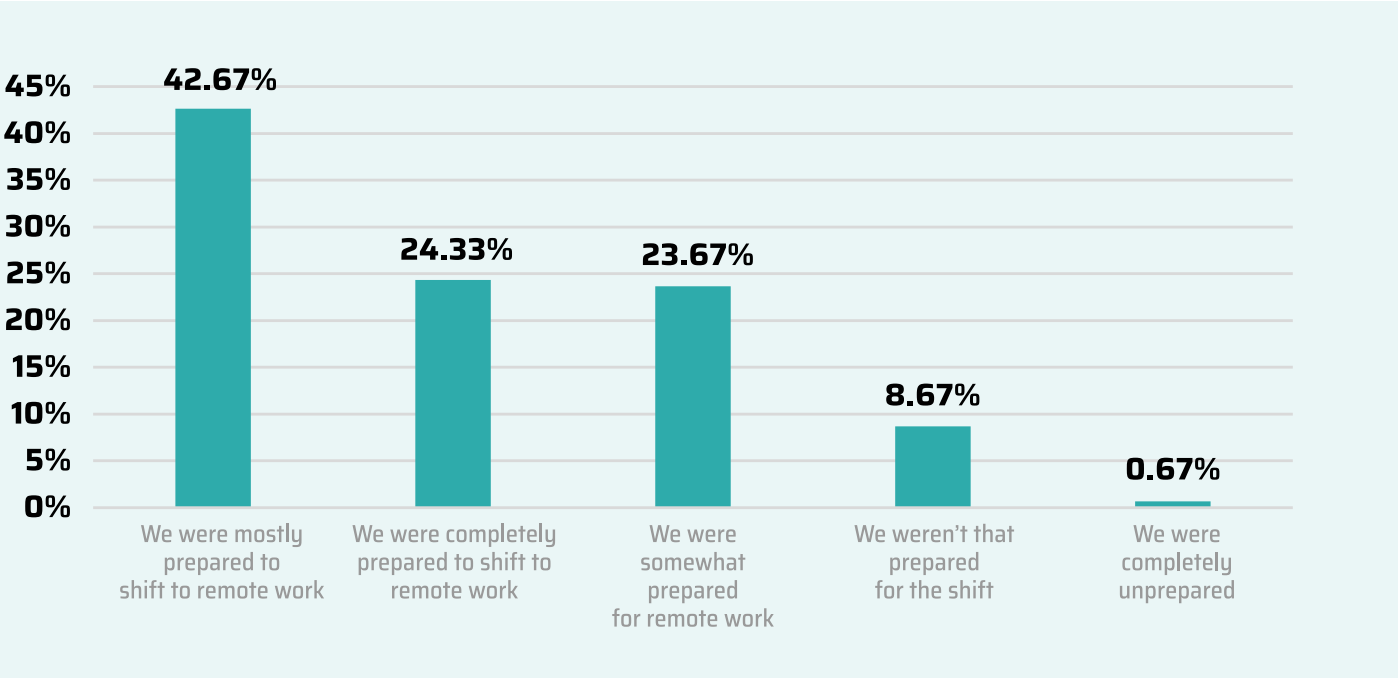
How Prepared We Were Primordial Concerns

How Prepared We Were

When COVID-19 began to spread worldwide, some of us were still skeptical about the aftermath of it.

Cybersecurity found its way in hard-control by office proxies and firewalls. At home it was usually considered a commodity, too technically advanced and strenuous to exercise at home, where data security was kept by habit recommendations and nothing else.

We asked if the organizations were prepared to shift to remote work from a cybersecurity perspective, and their response was:



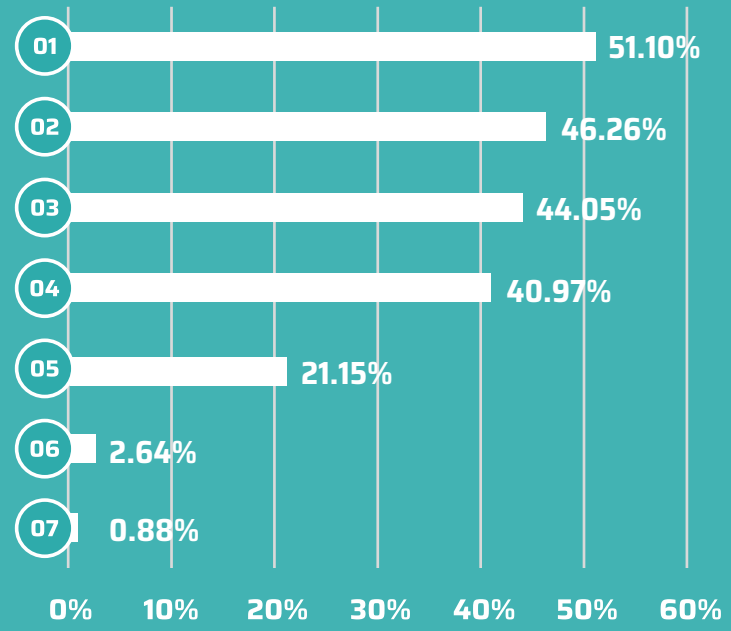
At first sight, it may sound reasonable and even positive. Almost one out of four (24.3%) were completely prepared. But turn it around: a stunning three out of four (75.7%) were unprepared for this shift, as important as it was.

From that

75 percent,

we dug deeper to understand what were the specific reasons behind this feeling of unpreparedness.

The concerns regarding threat assessment, policies and network environments are the most important for managers. This due to the fact that remote work is insecure by nature, far from the scrutiny and control of the office. We see BYOD policies as a huge concern in this regard (see “Endpoints, Full Stop”, page 19), which correlates with the investment in security (see “Levels Of Investment”, page 26)



01. **51.10%** Employees were using home/public WiFi networks.

02. **46.26%** Lack of visibility to maintain cyber security compliance within the remote environment.

03. **44.05%** Overwhelmed IT Staff.

04. **40.97%** Lack of employee security training or protocols.

05. **21.15%** We didn’t have any security systems in place to cover remote working.

06. **2.64%** Other.

07. **0.88%** Can’t say/Doesn’t know.

External Concerns

We've read the reports. We've seen the articles. And we're equally worried about it. The cybersec landscape is getting complex: APTs, malware-for-hire, and other threats are waiting for the chance to strike. Nevertheless, before the COVID-related phishing attacks and the rise of ransomware-as-a-service, that same landscape was full of terrors too. They have changed and evolved for sure, but they were always there.

A lot to unpack here. First of all, malware is still the king of the concerns of security professionals. Although certain industry analysts are pointing towards a decline in the amount of malware (due to the rise in credential theft and its benefits on breaches[2]), malware is like the flu: it will never be really gone. The same can be said for data leaks: the privacy of our data has always been a priority in most organizations.

We saw a rise in ransomware during 2018 & 2019, a plausible reason as to why they're top 3 on the list. Phishing, as well as Human Error & Misconfiguration, were some of the trends perceived by security analysts during 2019 to be important in 2020[3].

[1]The information contained in this page can be cross-referenced with the data in "Understanding The Threat", page 18.

[2,3]Verizon. 2020. 2020 Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/dbir/

The data shows the percentage of organizations that believed that any of these cyber threats were of utmost importance before the pandemic started[1]. The participants chose only three:

Malware	**41.3%**
Data leaks	**37.3%**
Ransomware attacks	**35%**
Phishing (including spear phishing, smishing etc.)	**30.7%**
Networks intrusions	**25.3%**
DDoS attack	**22.3%**
Malicious Website	**21.3%**
Human error or misconfiguration	**21.3%**
Identity theft	**20.7%**
Remote desktop attack	**18.7%**
Stolen/missing endpoints	**11%**
MitM attacks (Man-in-the-middle attacks)	**8%**
We were not worried about any cyber security threats before the COVID-19 pandemic	**2%**
Don't know	**0.3%**

03.

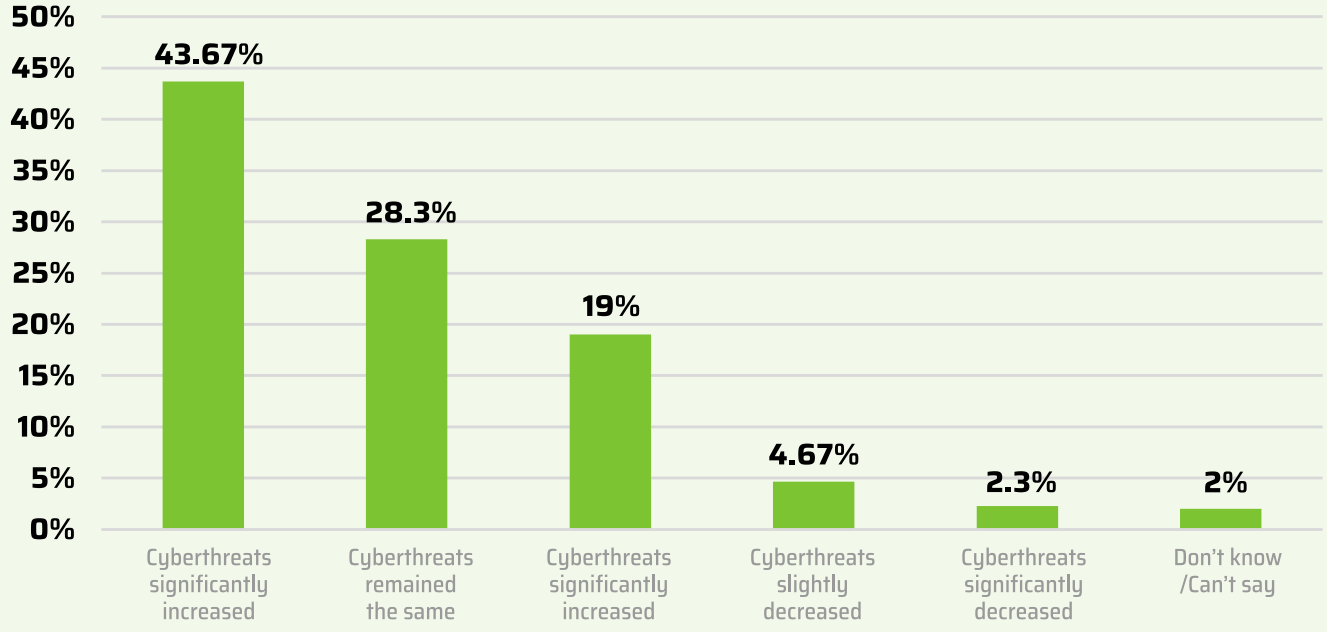
Cybersecurity, Now

A Greater Challenge
Understanding The Threat
Endpoints, Full Stop

A Greater Challenge

While society entered a time of curfews, quarantines and isolation, the cybersecurity world experienced a shift like no other. Diseases, social dissent and panic are cause for misinformation, which in turn breeds ways to deceive people. Remote work had its own challenges in security, and insecure computers and networks were ripe for exploitation.

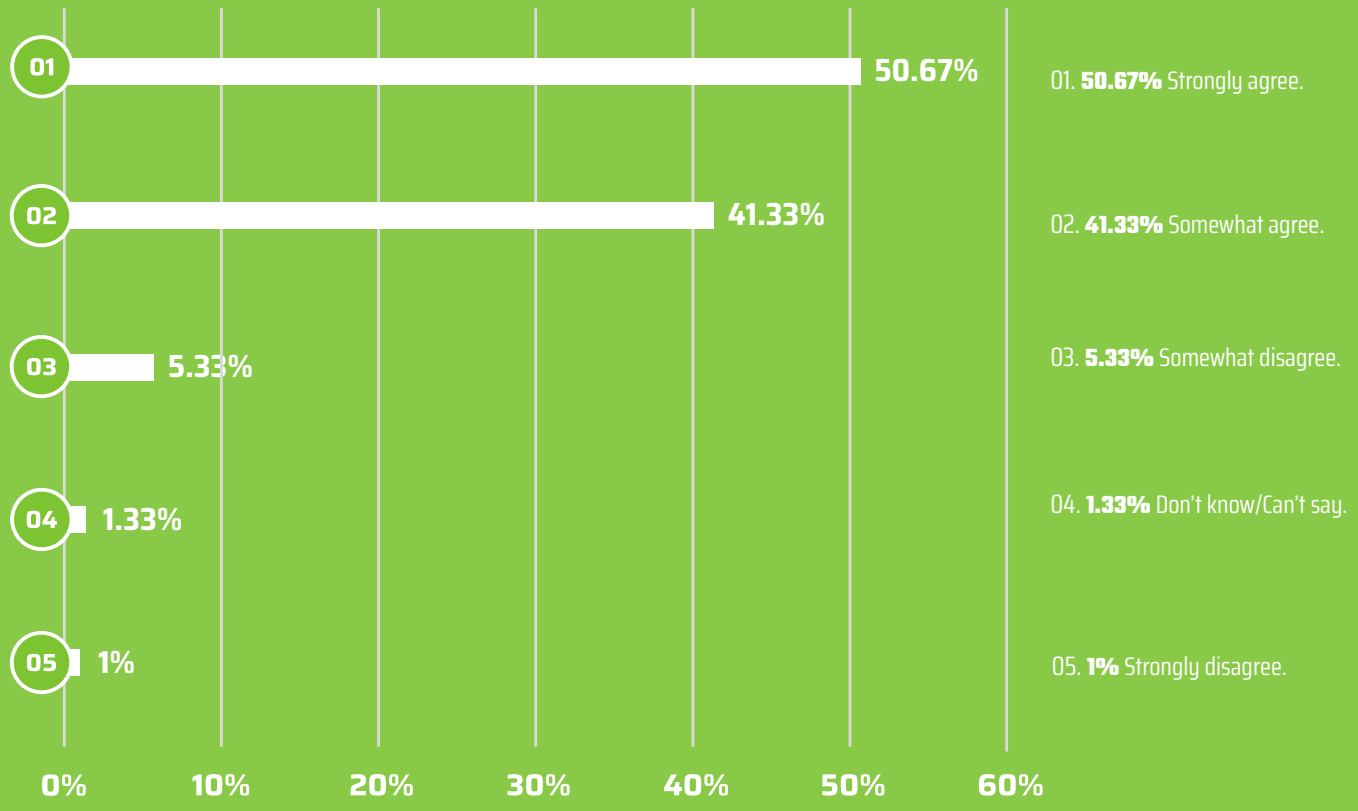
The data backs it up. Regarding the 2020 pandemic period, the surveyed organizations believe that:



62% of surveyed professionals state that threats increased after the pandemic started.

This means more than half of organizations faced a tougher scenario: new threats, increasing alerts and vulnerabilities, and in turn, a need for better cybersecurity measures.

We could observe this trend more closely: when asked if they thought the COVID-19 pandemic and remote work has made cybersecurity a greater challenge, the surveyed professionals:



This makes sense if we have in consideration that IT managers have limited power over what happens at home, and workers may or may not inform about setting changes made in the network. Remote work must happen in tandem with cybersecurity education for workers, and an often check-up of endpoints.

Understanding The Threat

As for the specific threats that worry our security professionals, the landscape has slight differences compared to the external concerns that plagued organizations before the pandemic started (see "External Concerns", page 14).

The table works exactly the same: the data shows the percentage of organizations that believe that any of these threats are of utmost importance right now. The participants chose only three, in ranking:

Data leaks are considered the most common threat that worries professionals, surpassing malware, ransomware, and phishing. As we stated earlier, data security has always been a big deal in office cybersecurity. But the top position in this list is there because of a sharp drop in other threats, not because data leaks are a sudden pandemic priority.

Another outlier, at least compared to before the pandemic started, is how identity theft and malicious websites rose in priority. These topics are somewhat intertwined. As we've discussed, the rise in attacs based on stolen credentials gave rise to protections, especially in the field of phishing and web security. However, protecting web traffic at home is very hard, an area where IT specialists have little or no control. This is a well-known pain point.

Lastly, one of the surprises is a drop in concerns about human error and misconfiguration. This may be caused by a higher number of external threats and events related to them, such as breaches and alerts. We have no doubt that human error is a serious threat to security, which is why it still is high on the list.

Threat	Pre-covid	Current	Variation
Data leaks ↑	37.3%	36.3%	-1%
Malware ↓	41.3%	36%	-5.3%
Ransomware attacks	35%	31.67%	-3.3%
Phishing (including spear phishing, smishing etc.)	30.7%	30%	-0.7%
Networks intrusions	25.3%	24.3%	-1%
Malicious Website ↑	21.3%	24%	+2.7%
DDoS attack ↓	22.3%	21.3%	-1%
Identity theft ↑	20.7%	21.3%	+0.6%
Remote desktop attack ↑	18.7%	20%	+1.3%
Human error or misconfiguration ↓	21.3%	19.67%	-1.63%
Stolen/missing endpoints	11%	11.67%	+0.67%
MitM attacks (Man-in-the-middle attacks)	8%	6.67%	-1.33%
We were not worried about any cyber security threats before the COVID-19 pandemic	2%	4.3%	+2.3%
Don't know	0.3%	1.3%	+1%

Endpoints, Full Stop

Based on our analysis so far, at least one out of ten organizations believe that endpoints are a primordial cause for concern in cybersecurity. The remote work trend emphasizes how important this is: millions of devices living in insecure environments, sometimes sharing space with vulnerable devices, and holding crucial assets and information.

But the problem is much worse:

Studies show that the misuse of endpoints goes far beyond safe, personal use and into the realm of pirate material, pornography and compromising data.

The reasons behind this "consumerisation of work devices" are still a mystery. A solid reason may be human behavior. As the lines between home and work start to blurry, so does in our devices. A user may be more inclined not to switch to a personal computer, especially when the security measures are permissive and the user has the same level of control as their personal devices.

When asked about endpoint misuse on their organizations, our respondents answered that:

Misuse slightly increased	**47.33%**
Misuse remained the same	**25.33%**
Misuse significantly increased	**19.67%**
Misuse slightly decreased	**2.67%**
Misuse significantly decreased	**2.67%**
Don't know/Can't say	**2.33%**

More than two out of three (67%) professionals state that endpoint misuse grew in some way or another in their organizations

B.Y.O.D. (Bring Your Own Device)

A reasonable number of organizations have implemented a B.Y.O.D. policy. That is, instead of providing their employees with equipment, employees themselves would use their own.

As we stated in "How Prepared We Were", a whopping 44% of professionals are worried about personal devices being used in the workplace without risk assessment. And with reason: with no control over a foreign device, any supervisor has all the right to be skeptical.

However, we cannot be blind: organizations can't cover all bases. A designer will test a feature on their personal smartphone. A sales associate will open a work email on another device. A developer will login to a SaaS internal tool with his other computer. Without the proper measures, a seemingly innocuous connection may become a liability.

04.

Solutions

Countermeasures
Employee Awareness
Policies & Training
Levels of Investment

Countermeasures

Based on the risk assessment of your organization, threat countermeasures can be quite different. The data suggests certain points in common, though.

Anti-virus/Anti malware	**70.33%**
Firewall	**68%**
VPN/Virtual Work Environment/Remote Desktop Access	**58.67%**
Endpoint Security (including device tracking/management solutions, device threat security/monitoring and device encryption)	**57.33%**
Data Encryption	**56.67**
Identity and Access Management	**54.67%**
Software Management	**50.33%**
Backup Tool	**37.33%**
Web proxy/web filtering	**33.33%**
Other	**0%**
We don't use any security controls to protect our remote working team	**0%**
Don't knowt	**1%**

Anti-virus & anti-malware solutions are ubiquitous at this point, as well as firewalls. On the other hand, the wake of VPNs, as well as Virtual Work Environments and everything related to remote desktops, can be easily traced to the need of keeping security high while millions migrated to remote jobs at home.

The same can be said for Endpoint Security, also high on our list. This is the bread and butter of the new cybersecurity landscape: a way to secure office devices while also maintaining a minimum level of security for the data in transit. Data Encryption solutions are highly appreciated too, to deliver protection to the static data on every endpoint.

Identity & Access Management seem to be a necessity for more than half of the surveyed organizations as well. Software Management sits right in the middle, a necessary evil in a remote world.

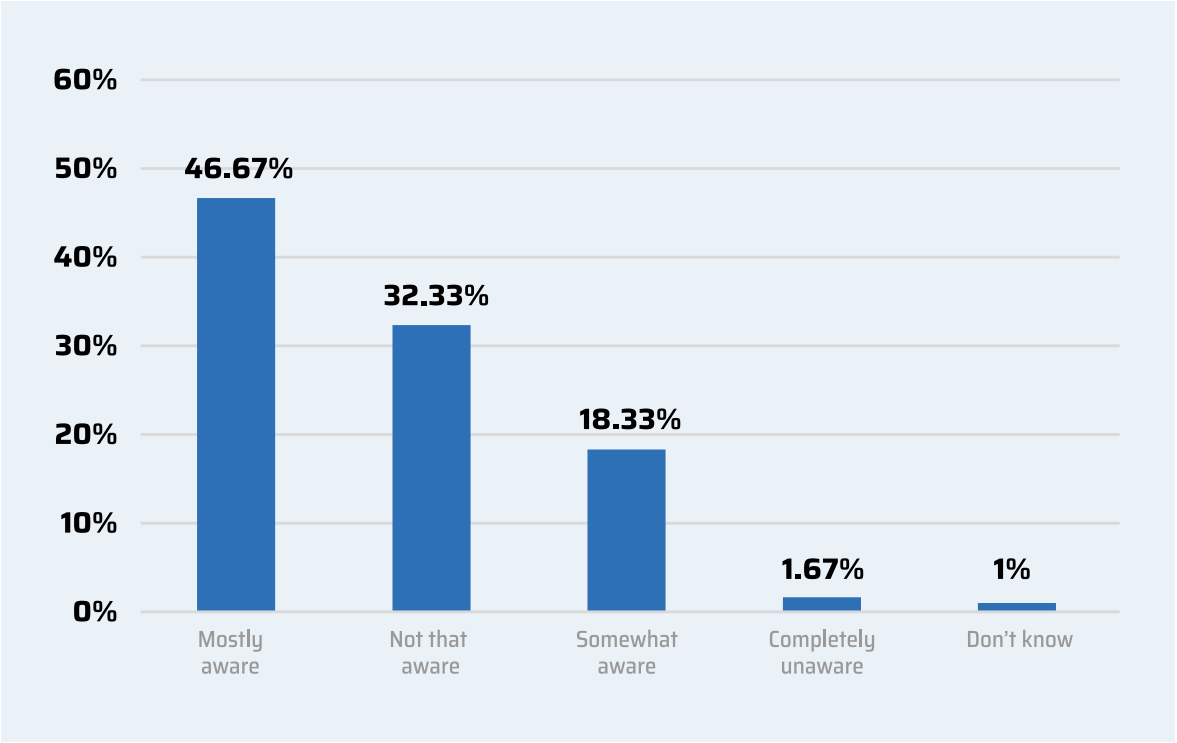
Speaking of necessary evils, Backup and Web Filtering are in dead last, only relevant to a third of our surveyed professionals. It seems logical: web filtering is easier to enforce at the office as a strict productivity measure. However, remote work isn't governed by the same rules anymore, so the priority can be modified towards more effective measures (virtual environments, endpoint security, et al).

Employee Awareness

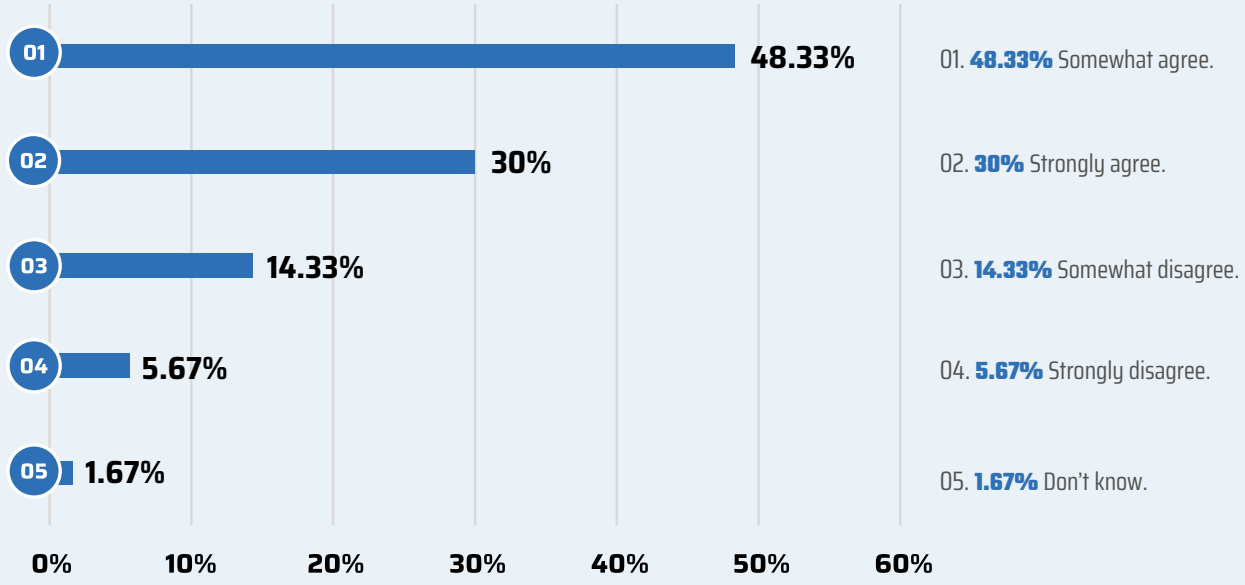
If we're talking about cybersecurity in the workplace, having threat countermeasures and highly trained security professionals is never enough. To be fully prepared, your first line of defense has to be your own personnel.

That data implies good news! As most organizations declare that their employees are mostly aware, we could only assume that enterprises are doing a good job and believe in their subordinates. However, a piece of information seems to contradict that statement.

When asked about the level of awareness of employees about cybersecurity risks, our surveyed professionals declare that they are:



When asked if the average remote working employee does not truly realize how they might put their organization's cybersecurity at risk, they:



Nearly half of our surveyed professionals somewhat agree with that statement.

A logical explanation for this discrepancy is that the employees know the causes behind cybersecurity incidents and usually know how to prevent them, but they aren't really aware of the consequences of a breach.

This may be rooted in how the education in cybersecurity is performed. For example, several companies perform phishing trials, where employees receive education on how to prevent phishing and then put their knowledge to the test in a controlled environment (i.e. a scam email sent by the IT department). Therefore, a lot of companies tell their employees about the risks of phishing but aren't very explicit about the real consequences: data exfiltration, persistent attacks, loss of business continuity, and much more.

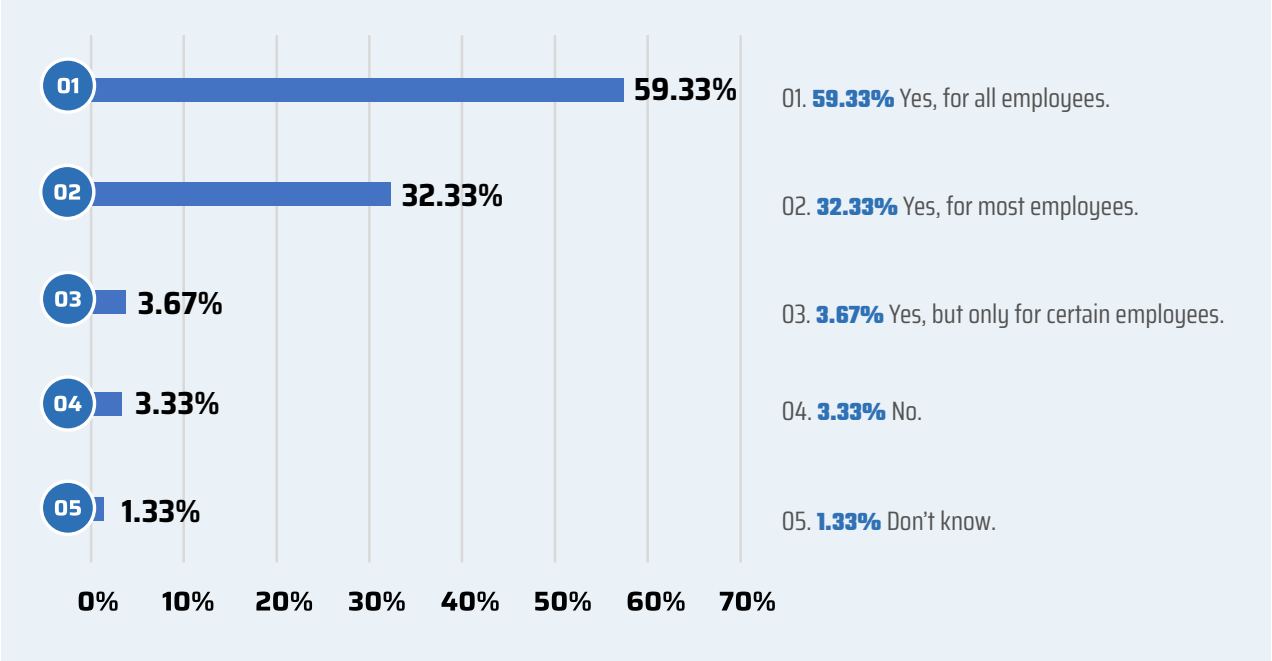
Another explanation could be the evolution of threats in the last few years, and the inability to be completely prepared for all of them. As threats like persistent mobile malware and ransomware-as-a-service become more powerful, companies may be inclined to only inform their employees about certain threats under certain conditions, such as an inminent attack. Education in cybersecurity is an investment and companies aren't always ready to make it.

Policies & Training

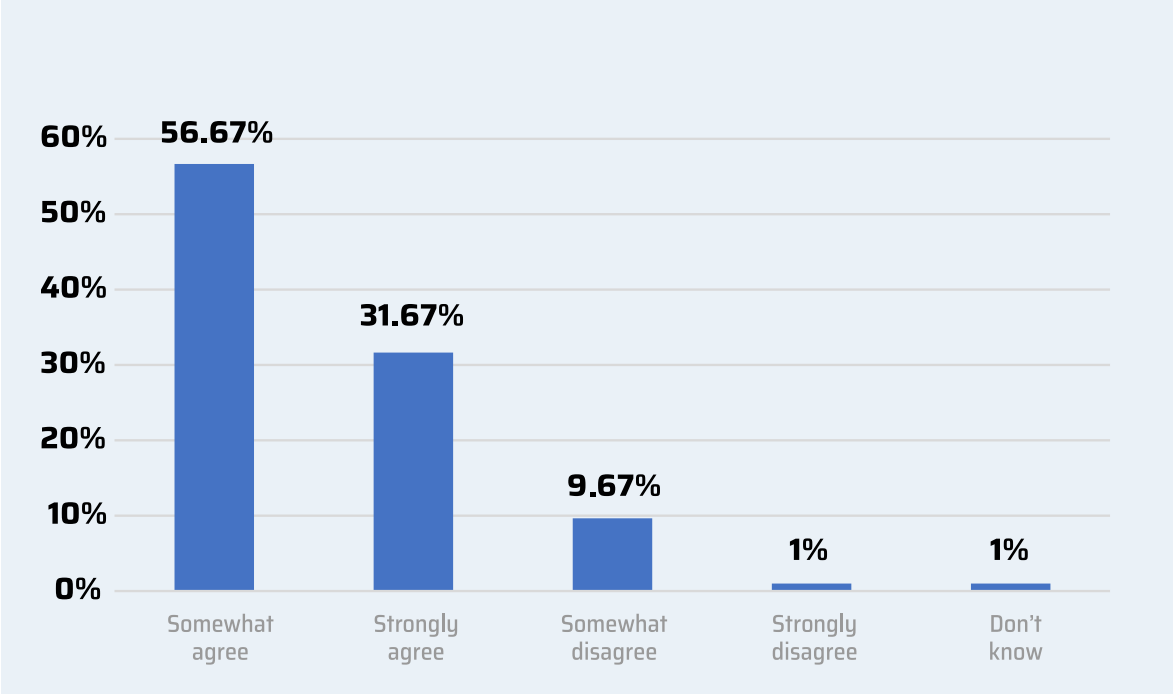
One of the ways organizations are paving the roads for safer remote environments is the implementation of policies designed to protect assets and educate employees. Comparing this to the data gathered in the previous section (see "Employee Awareness, page 23") we're glad to see this is a way that a majority of organizations define as valuable.

On the same line, continuous training and updates on potential cybersecurity issues are also helpful in reducing costs, lowering potencial chances of breaching and actively protecting employees and enterprise assets and data.

When asked if their organization created or revisited policies related to cybersecurity in the remote workplace, they responded:



Related to that, we asked if they agree to this statement: their organization increased its training efforts after the COVID-19 pandemic. Their answers:

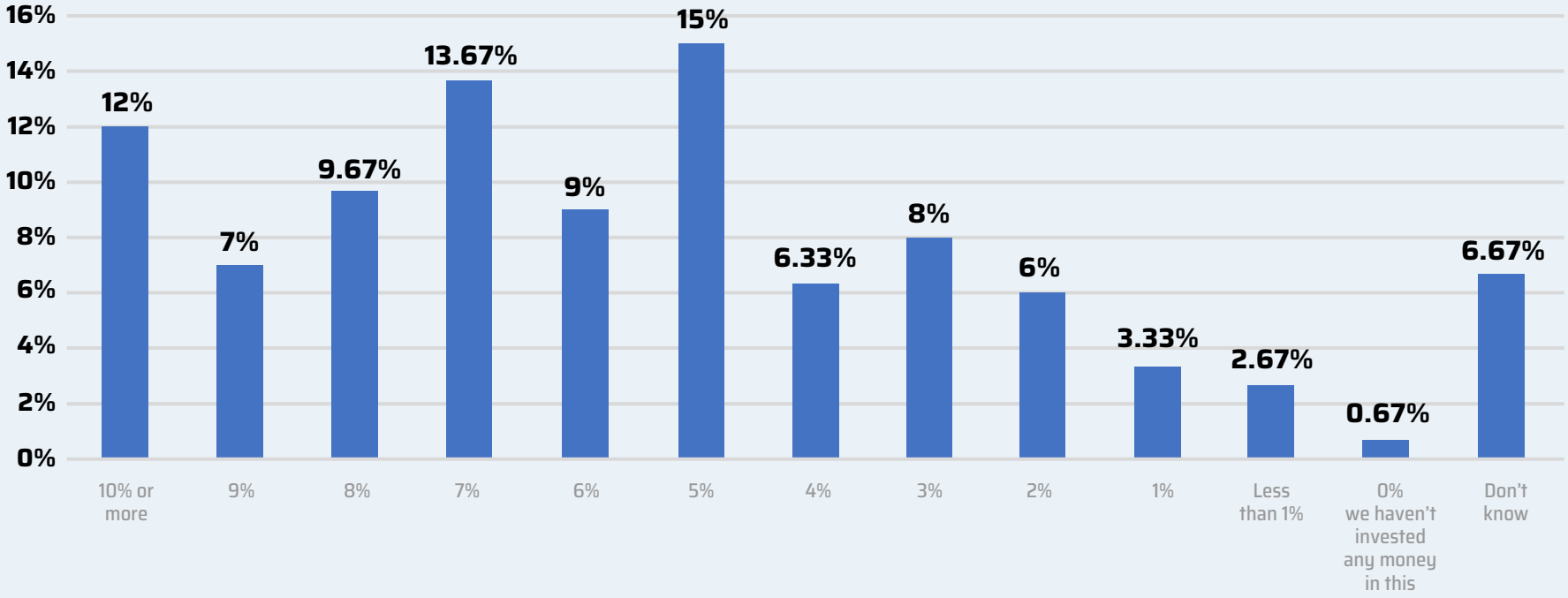


The timing of the pandemic had its positive aspects when we think about the advanced scenario in health and technology. Nowadays, remote work is not as hard to set up as it was 10 or more years ago, and that streamlines every countermeasure that needs adoption. Our data confirms the current state of mind or taking advantage of the situation to make improvements is here to stay, and it's a big opportunity to revolutionize working rituals as we know them.

Levels of Investment

At plain sight, remote work looks like a great way to save on office costs, but that should never be the case. Offices shift from physical to online and cloud-based, and that means the same security costs that were invested in securing assets should be used to benefit the new structures.

When asked about the percentage of new investment in cybersecurity at their companies, respondents said they have used, related to their global annual income:



There are multiple views to this data.

FIRSTLY, A VERY SMALL

0.6%

of companies haven't made any investment to create or improve cybersecurity policies after the pandemic began. This tells us that either it wasn't considered that relevant for their specific labors or their policies were strong enough in the first place. We know this isn't the case for most companies, and we consider these to be outliers.

IN CONTRAST, AT LEAST

12%

invested more than 10% of their global annual income in cybersecurity measures and/or remote infrastructure. Maintaining business continuity can have a huge price tag attached to it, and in a world where remote infrastructure was scarce, organizations had to spend much more.

SPEAKING ABOUT EXPENDITURES:

6.22%

in terms of global annual revenue, was the average of new investment in all of the surveyed organizations. Does it compare favorably with your own investment in cybersecurity?

05.

Wrap-Up

To recap

To recap...

A SHIFT TO REMOTE WORK WAS ALREADY IN PLACE.

With most organizations with at least a policy of remote work, and more than 40% of employees staying remote after the pandemic, it seems that the "fad" of home office is definitely here to stay.

THE LACK OF IT INFRASTRUCTURE FOR REMOTE WORKERS IS A SERIOUS PROBLEM.

The leap to remote wasn't easy at all in this regard, but at least organizations are investing 6% on average to cover the gap.

THREAT ASSESSMENT, POLICIES, AND NETWORK ENVIRONMENTS ARE BIG CONCERNS FOR IT MANAGERS.

From insecure Wifi networks to BYOD endpoints entering restricted enterprise spaces, the concerns for IT professionals regarding remote work are varied and hard to resolve.

THE COVID-19 PANDEMIC INCREASED THE AMOUNT AND SCALE OF INCIDENTS.

Most professionals agree: this pandemic has posed a greater challenge for cybersecurity (92%), and cyber threats have increased since it started (62%).

THREATS HAVE CHANGED IN 2020 TO ADAPT TO THE REMOTE WORK SITUATION.

Data leaks, endpoint vulnerabilities, identity theft, and malicious websites are new priorities in this new scenario of exploitable remote offices.

MOST ORGANIZATIONS ARE MOBILIZING THEIR TROOPS.

Countermeasures are in high demand, policies are being modified and a high percentage of organizations are increasing their investment in education and training for employees.

EMPLOYEES KNOW THE THREATS, BUT NOT THE CONSEQUENCES.

As a huge amount of employees aren't aware of the consequences of incidents and breaches, we may need to rethink the way we teach cybersecurity.

INVESTING IN CYBERSECURITY FOR REMOTE WORKERS IS MANDATORY.

As a huge amount of employees aren't aware of the consequences of incidents and breaches, we may need to rethink the way we teach cybersecurity.

About Prey

Prey is a cross-platform anti-theft and management solution for laptops, tablets and phones used to protect over 8 million devices and their data, all around the world.

Prey started back in 2009 as a solid tracking technology that helped people keep track of their laptops and phones. Nowadays, crossing the 10-year mark, Prey has evolved into a multi-platform tracking technology that offers a variety of solutions for both people and businesses: tracking, device management, data protection, and anti-theft for laptops, tablets, and smartphones.

Prey for: People | Businesses | Schools

Prey Inc. © 2021
548 Market St. #30152
San Francisco, CA 94104
USA