CROWDSTRIKE ASIA PACIFIC AND JAPAN STATE OF CYBERSECURITY REPORT

JULY 2020

Approach and methodology

Sample and data collection

Online survey

The CrowdStrike APJ survey was conducted between May 26 and June 7, 2020.

The total sample size is 2,017, which gives a confidence level of ± 2.1% at the 95% confidence level.

Research participants came from a permission-based, online panel.

All participants work in organizations of 100 or more staff (except in New Zealand where 50 to 99 staff were included) and are in managerial positions: C-Suite/executive leadership, senior management and middle management.

2,017 **fully completed surveys**

- Confidence level of ± 2.1% @ 95% confidence level
- 49 questions asked

Sample source

- Online permission-based panel

Criteria for inclusion

- Business leaders
  - C-Suite
  - Senior Management
  - Middle Management
- Organizations with 100 or more staff in each country
  - Except New Zealand where 50 to 99 staff were included

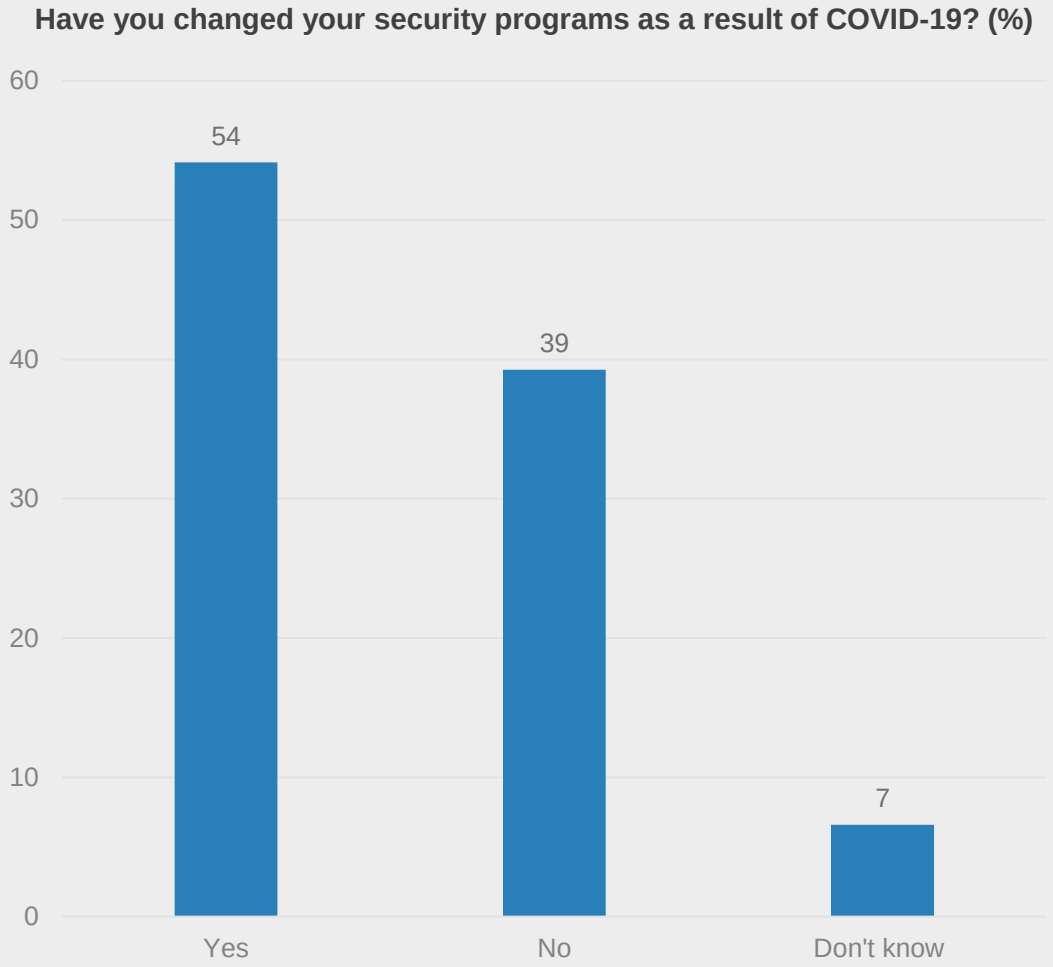
CROWDSTRIKE

StollzNow
Research & Insights Advisory

SECURITY IN RESPONSE TO COVID-19

A majority of business leaders say they have changed their security programs as a result of COVID-19

COVID-19 has caused over half (54%) of organizations to change their security programs. Yet, findings also show that almost four-in-ten (39%) have not changed their programs.



54%

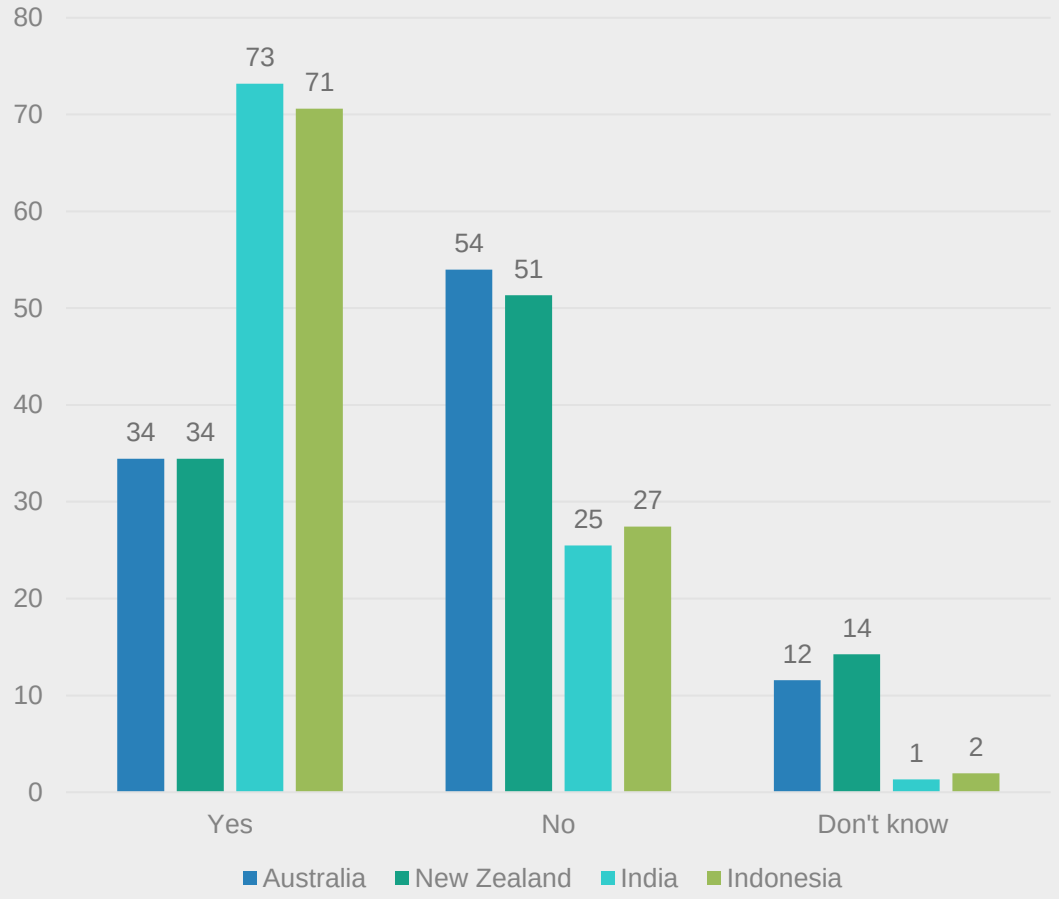
Changed security programs

Base: all research participants *n*=2,017

There are notable regional disparities in whether organizations changed their programs

While over 70% of organizations in India and Indonesia changed their security programs, over 50% of organizations in Australia and New Zealand did not.

Have you changed your security programs as a result of COVID-19? (%)



Over

70%

In India and Indonesia changed

Over

50%

In Australia and New Zealand did not change

Base: all research participants *n*=2,017

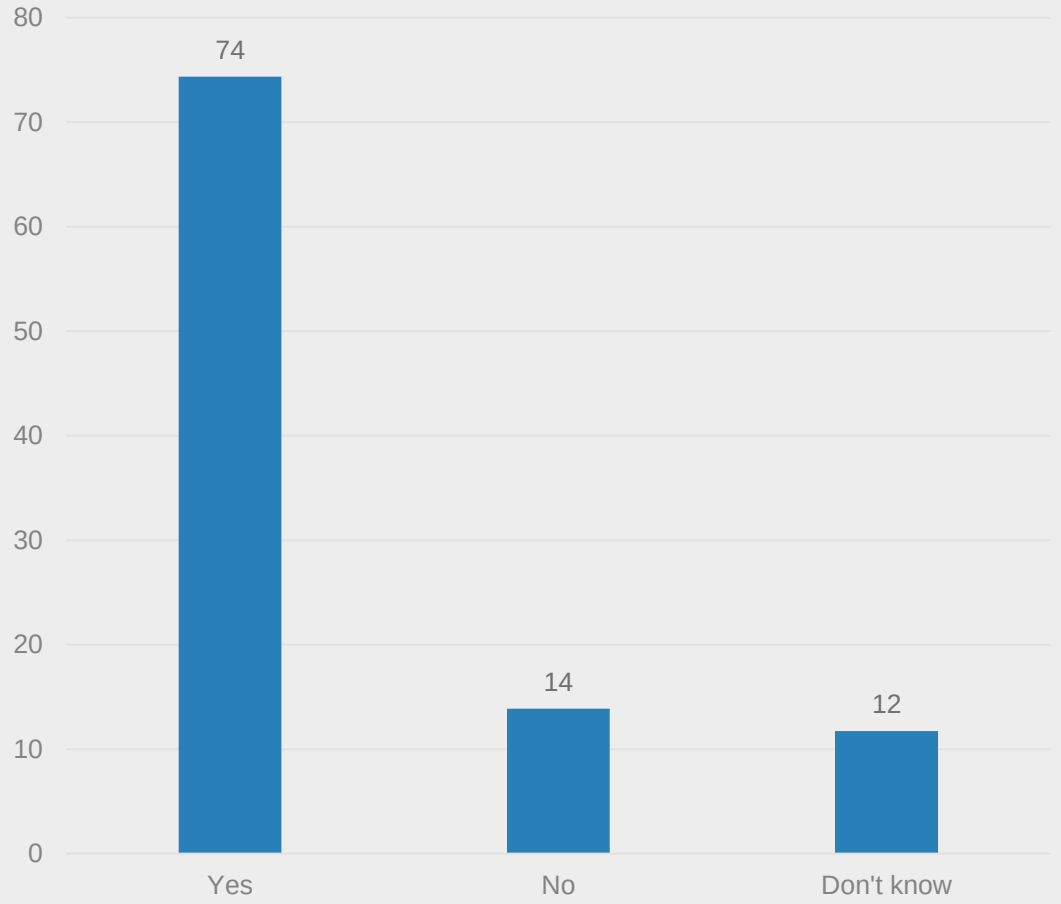
Over a quarter of respondents say their organizations don’t have a cybersecurity emergency response plan or aren’t aware if one exists

An alarming 14% do not have a cybersecurity emergency response plan. A further 12% or around one-in-ten organizations don’t know if they have a cybersecurity emergency response plan.

Only around three-quarters (74%) have a plan or know there is a plan.

All research participants are managers in larger organizations who should reasonably be expected to know about any cybersecurity plan.

Does your organization have a cybersecurity emergency response plan? (%)



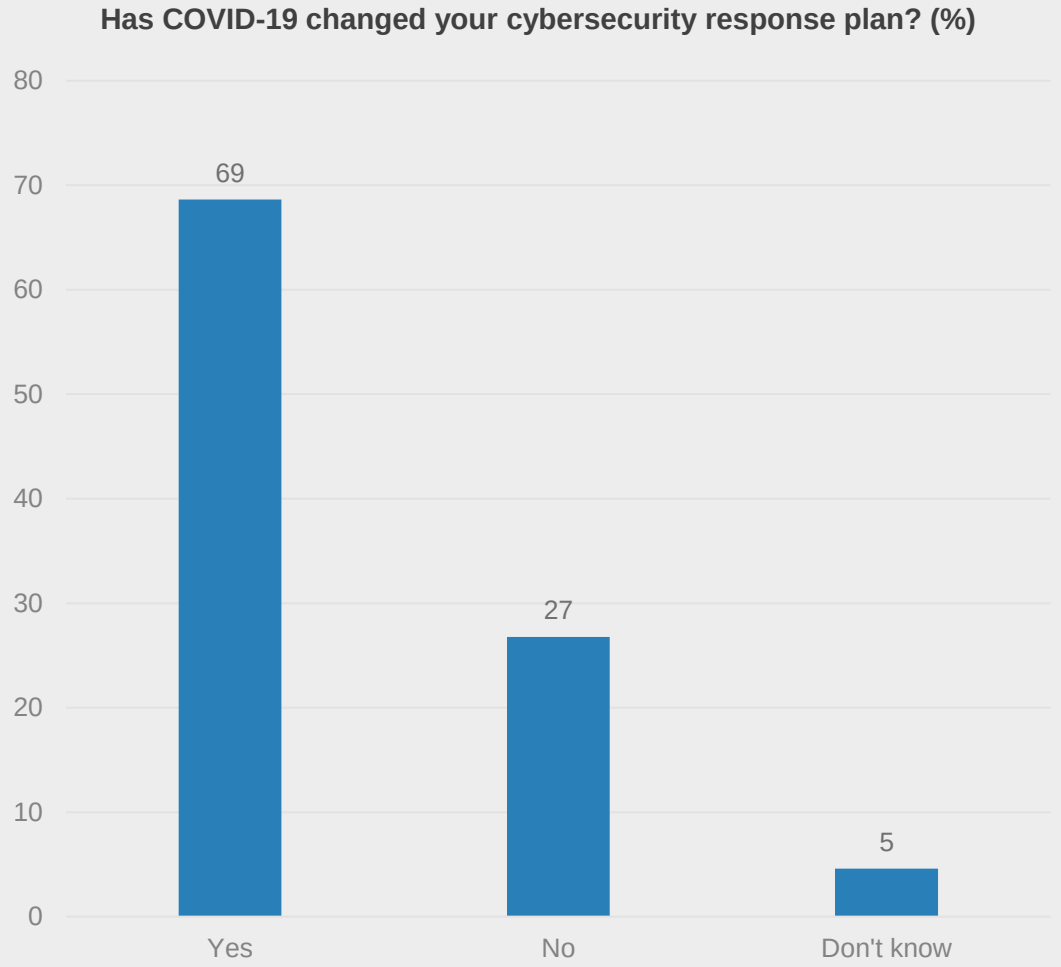
74%

Have cybersecurity plan

Base: all research participants *n*=2,017

COVID-19 has changed the cybersecurity response plan for most organizations

Those organizations that have a plan were asked whether COVID-19 has changed their cybersecurity emergency response. Almost seven in ten changed their cybersecurity response plan as a result of COVID-19.



69%

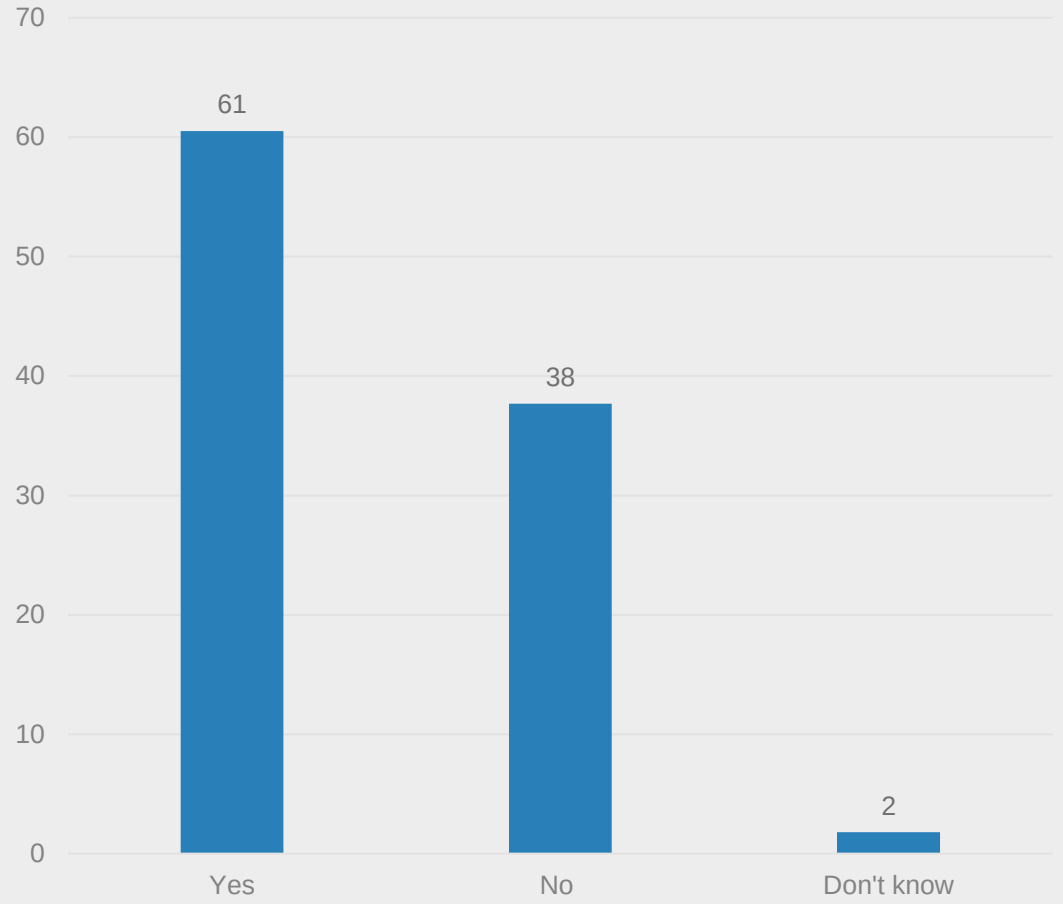
Have changed their cybersecurity response plan due to COVID-19

Base: those with a cybersecurity response plan
n=1,456

Many respondents received additional security training as a result of COVID-19

Yet, almost four in ten (38%) have not received additional training in security.

As a result of COVID-19 have you received additional training in security? (%)



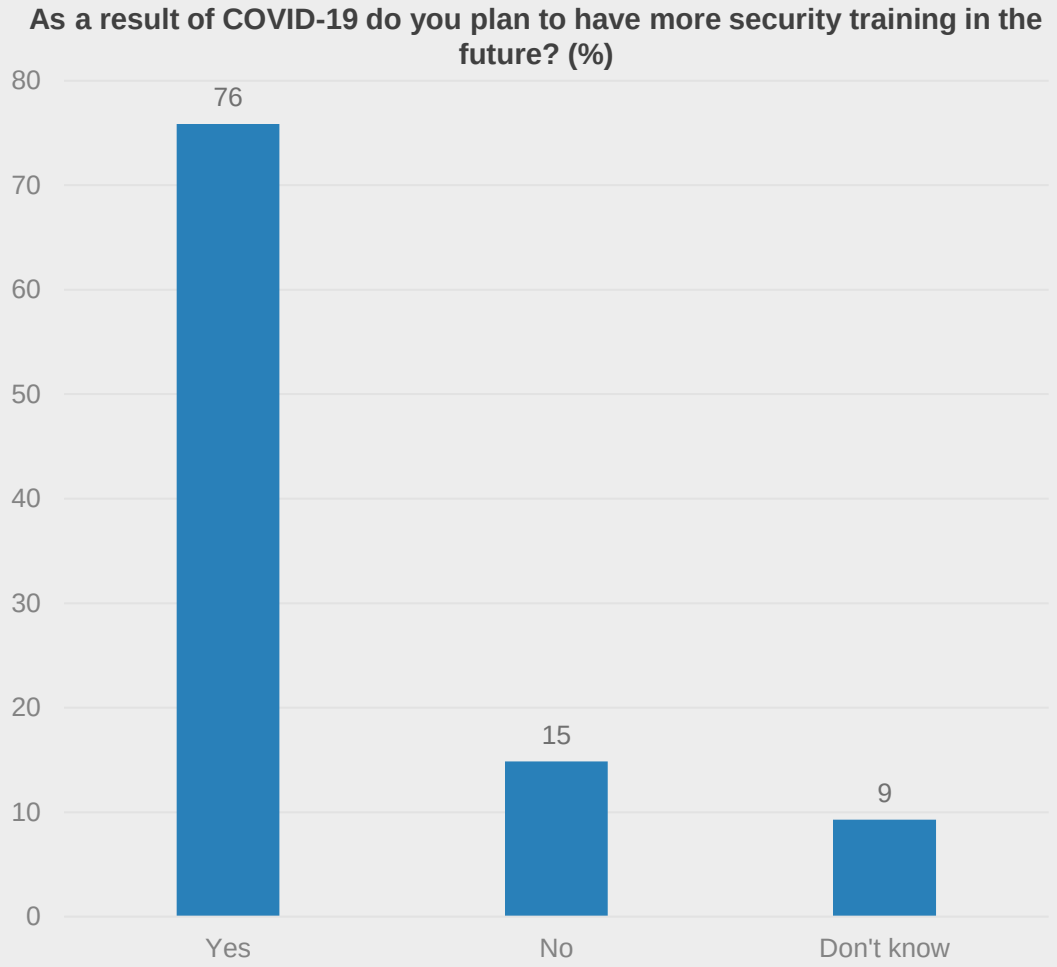
61%

Have additional training in security due to COVID-19

Base: all research participants *n*=2,017

Organizations overwhelmingly plan on having more security training in the future as a result of COVID-19

More than two-thirds (76%) plan more security training in the future as a result of COVID-19.



76%

Plan for more security training due to COVID-19

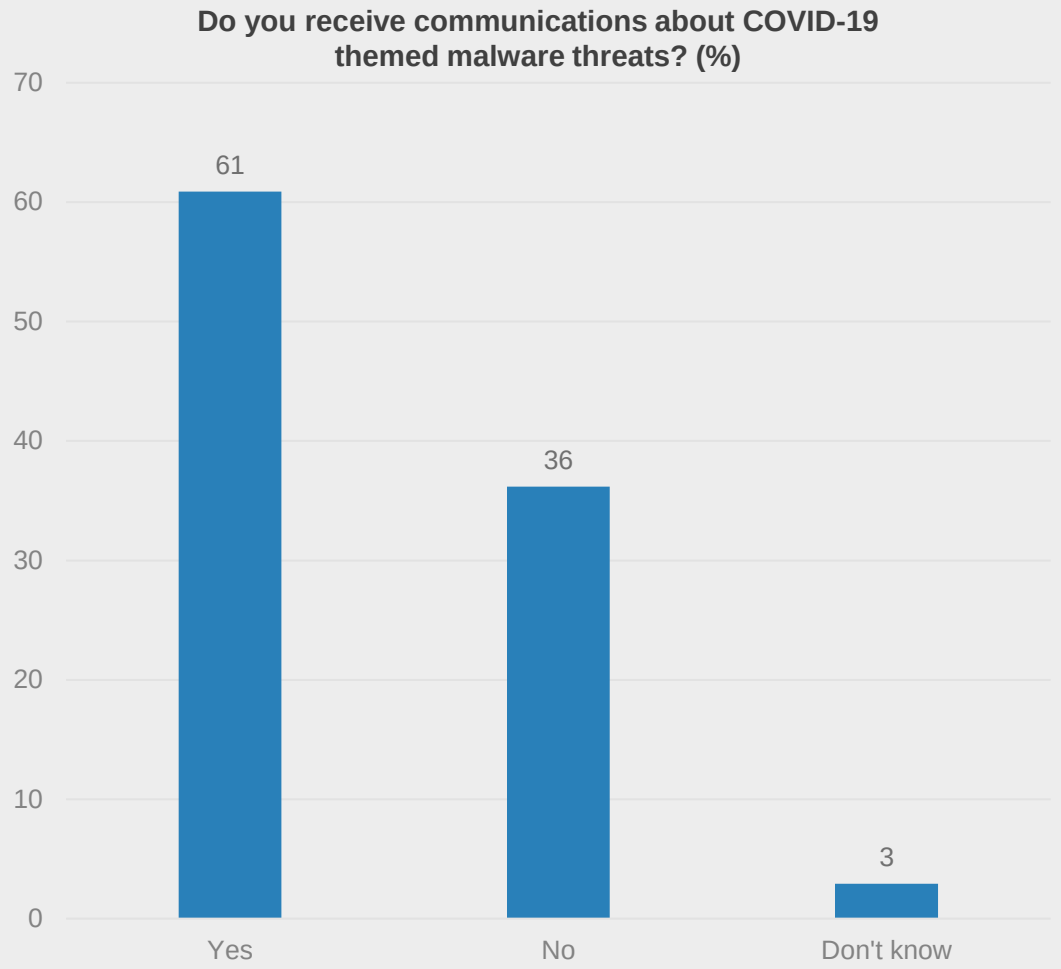
Relatively few are not planning more security training

Base: all research participants *n*=2,017

Over one-third of respondents do not receive communications about COVID-19-related malware threats

COVID-19-themed malware is common and sophisticated, frequently emulating official government advice about the pandemic. Education for all staff in any organization is an essential part of protection from malware.

Despite this, only 61% have received warnings about COVID-19-themed malware, while 36% have not received any warnings.



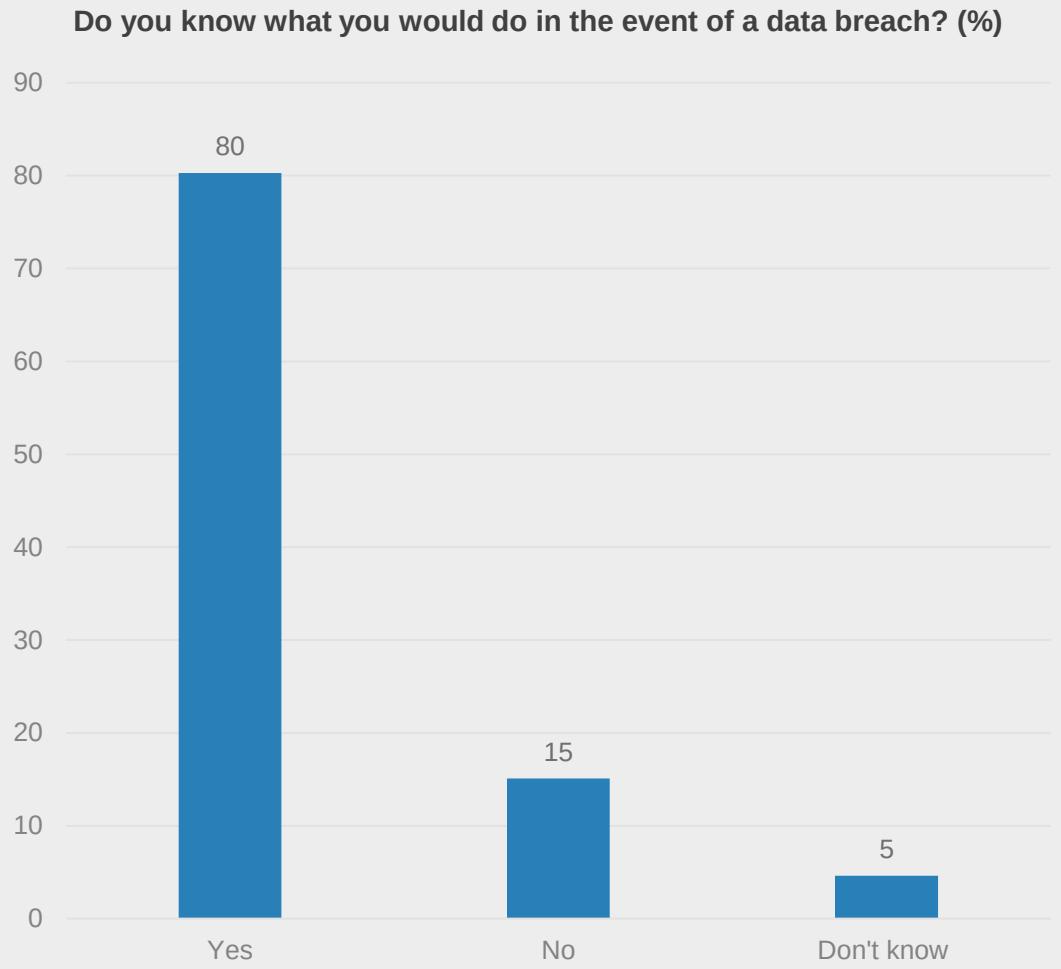
61%

Received communications about COVID-19-themed malware

Base: all research participants *n*=2,017

1 in 5 respondents do not know what to do in the event of a data breach

In a world of increasingly sophisticated cyberattacks that can bring financial and reputational ruin to organizations, it is extremely risky to have 20% of employees not know what to do in a cyberattack and possibly put the larger organization at risk.



20%

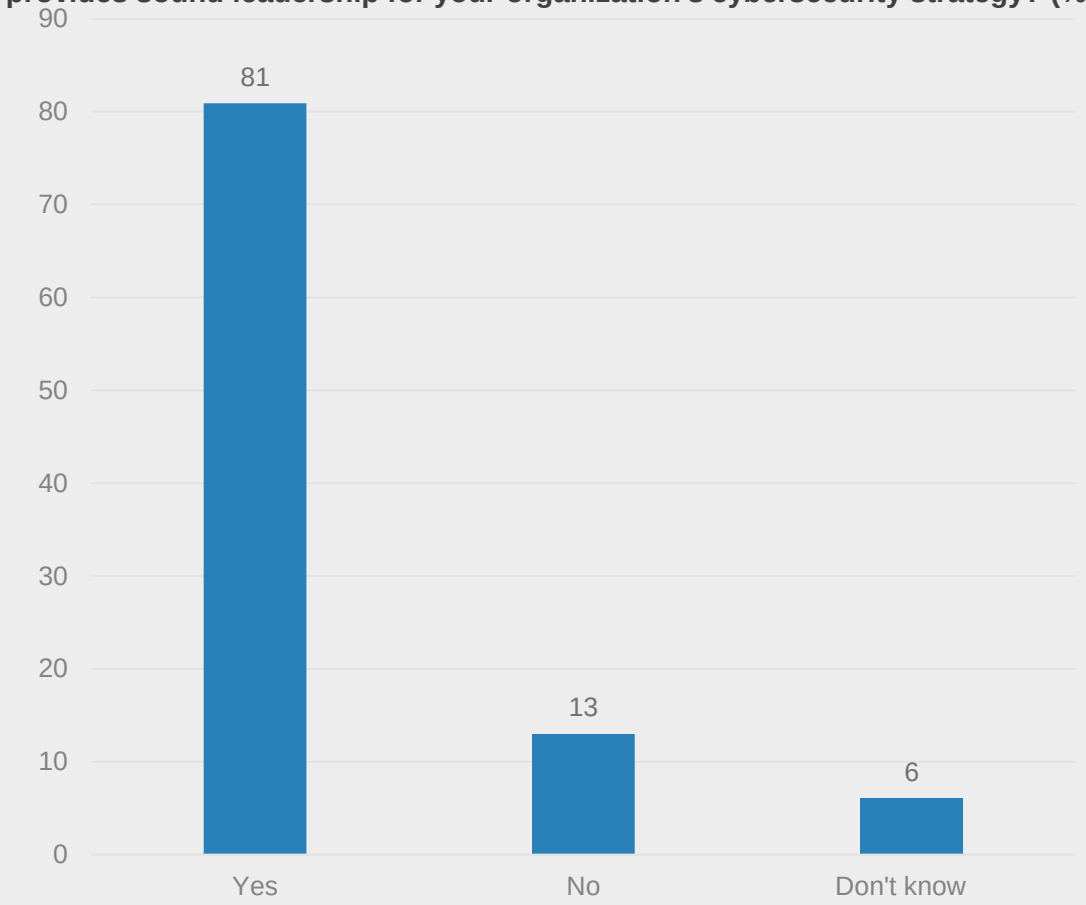
Do not know what to do in event of data breach

Base: all research participants *n*=2,017

Over 8 out of 10 respondents are confident in their company's leadership when it comes to cybersecurity strategy

81% believe that their organization's leaders have the right skills for their organization's cybersecurity strategy. Just over one in ten (13%) do not feel that leadership has the right skills.

Are you confident that your company's CEO and/or Board of Directors provides sound leadership for your organization's cybersecurity strategy? (%)



81%

Believe their leaders have the right skills in cybersecurity

Just over one in ten do not think leaders have the right skills

Base: all research participants *n*=2,017

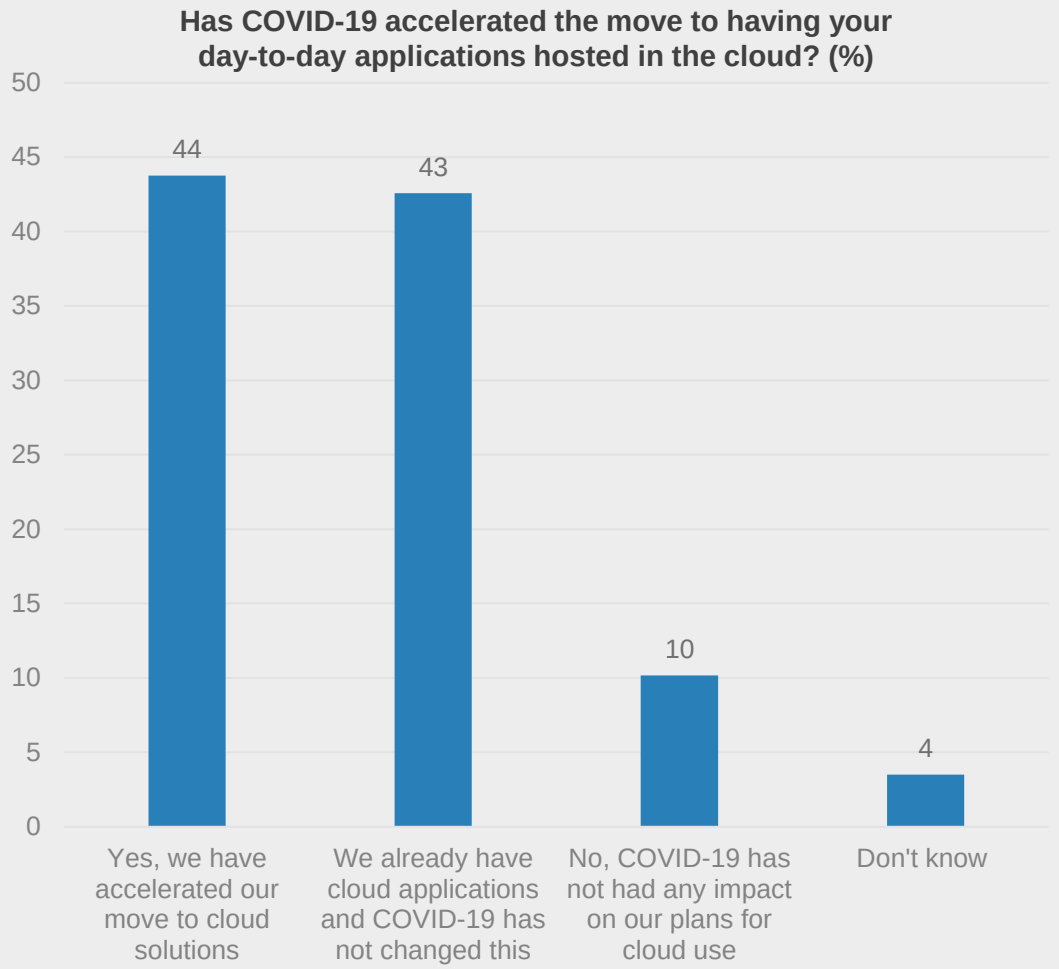
CROWDSTRIKE

StollzNow
Research & Insights Advisory

IN COVID-19 DIGITAL TRANSFORMATION AND CUSTOMER EXPERIENCE TAKE A GIANT LEAP FORWARD

COVID-19 has accelerated digital transformation for over 40% of the respondents' organizations

Almost half (44%) of the survey respondents say COVID-19 accelerated their move to cloud solutions, giving evidence of the scalability and flexibility of cloud solutions in being able to quickly accommodate the remote workforce.



44%

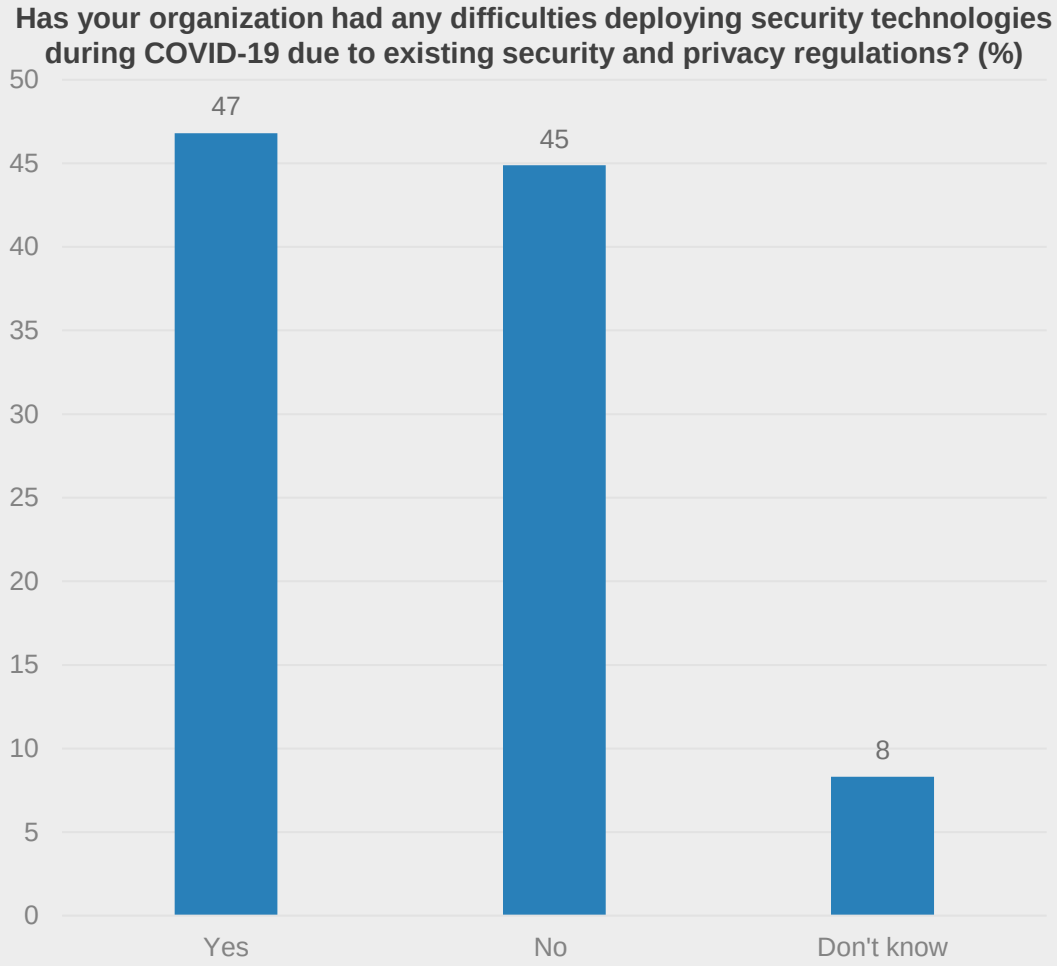
Increase to cloud solutions

COVID-19 has a massive impact on cloud

Base: all research participants *n*=2,017

Almost half of respondents have had difficulties in deploying security technologies during COVID-19

Security and privacy regulations should support security technologies but almost half (47%) report that these requirements are hampering deployment of security during COVID-19.



47%

Have difficulties

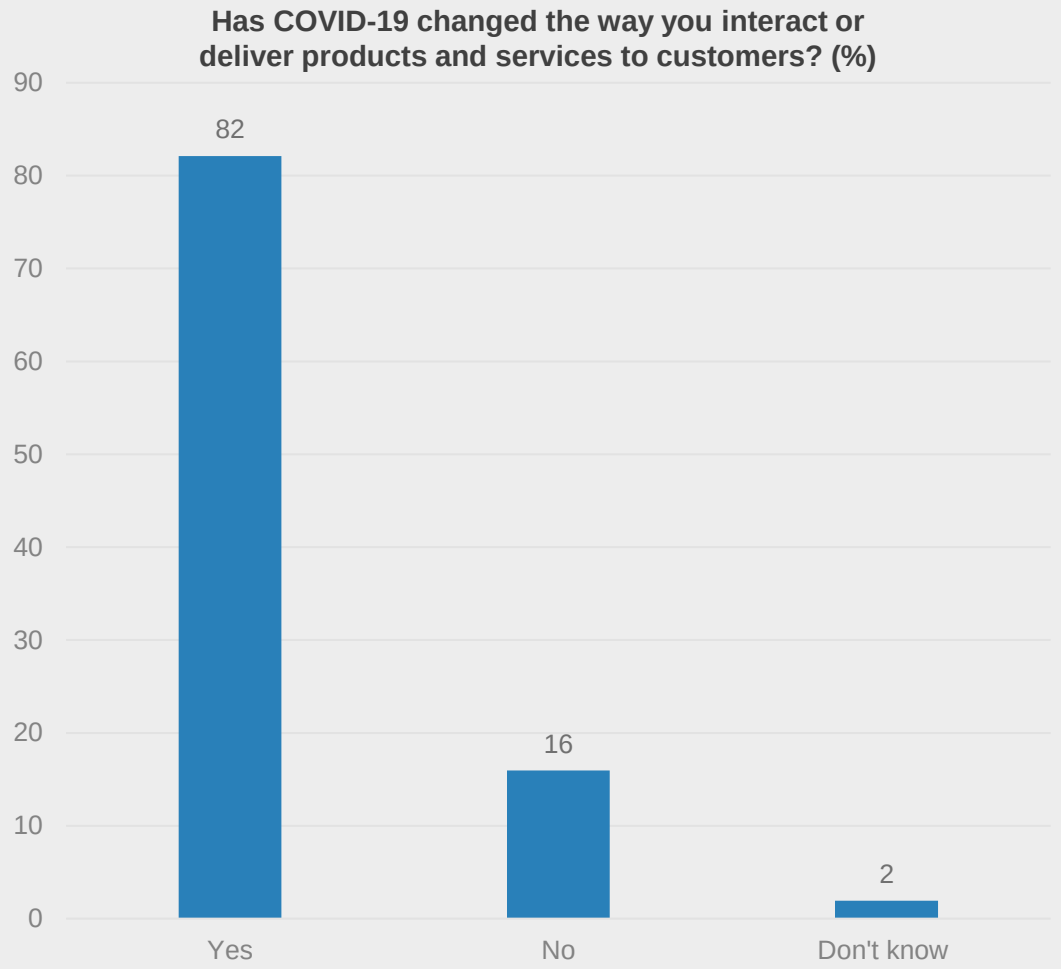
Almost half have difficulties deploying security tech during COVID-19

Base: all research participants *n*=2,017

The way respondents interact with their customers and deliver products has changed

COVID-19 hasn't just changed where we work, it has also impacted how we interact with others at the business level.

82% of organizations have changed the way they interact or deliver products or services to customers due to COVID-19. This represents a fundamental change in how a businesses services their clientele.



82%

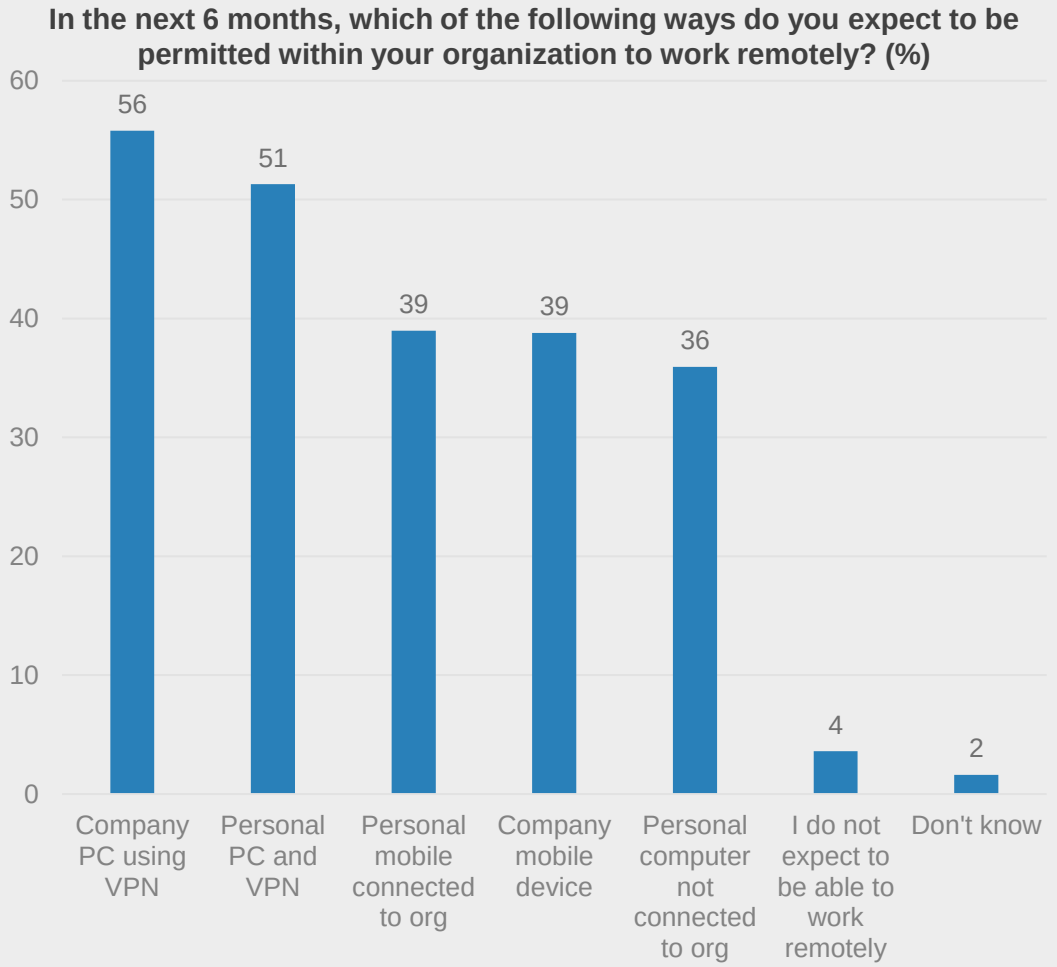
Have changed the way they interact or deliver products and services

COVID-19 has fundamentally changed the way products and services are delivered

Base: all research participants *n*=2,017

Using a VPN is an expected way of remote working with either a company PC or personal PC

Connecting to the organization's infrastructure by VPN is key to working from home in the next 6 months regardless of whether the employee is using a company-owned or personal device.



56%

Expect to use a company PC and VPN to work

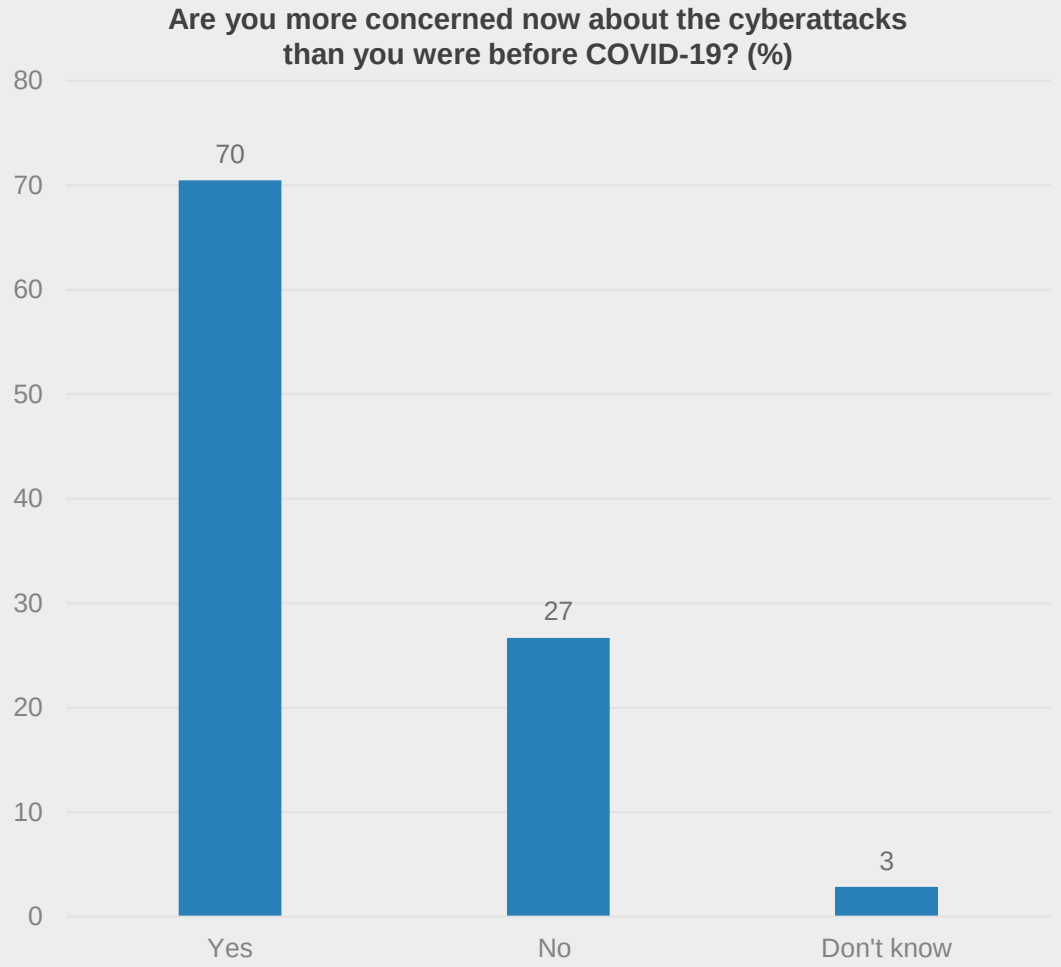
Connecting by VPN is key for security

Base: all research participants *n*=2,017

70% of survey respondents are more concerned now about cyberattacks than before the pandemic

In another example of how COVID-19 has far-reaching consequences for business, 70% are more concerned about cyberattacks now than they were at the start of the pandemic.

Only 27% are not more concerned.



70%

More concerned about cyberattacks

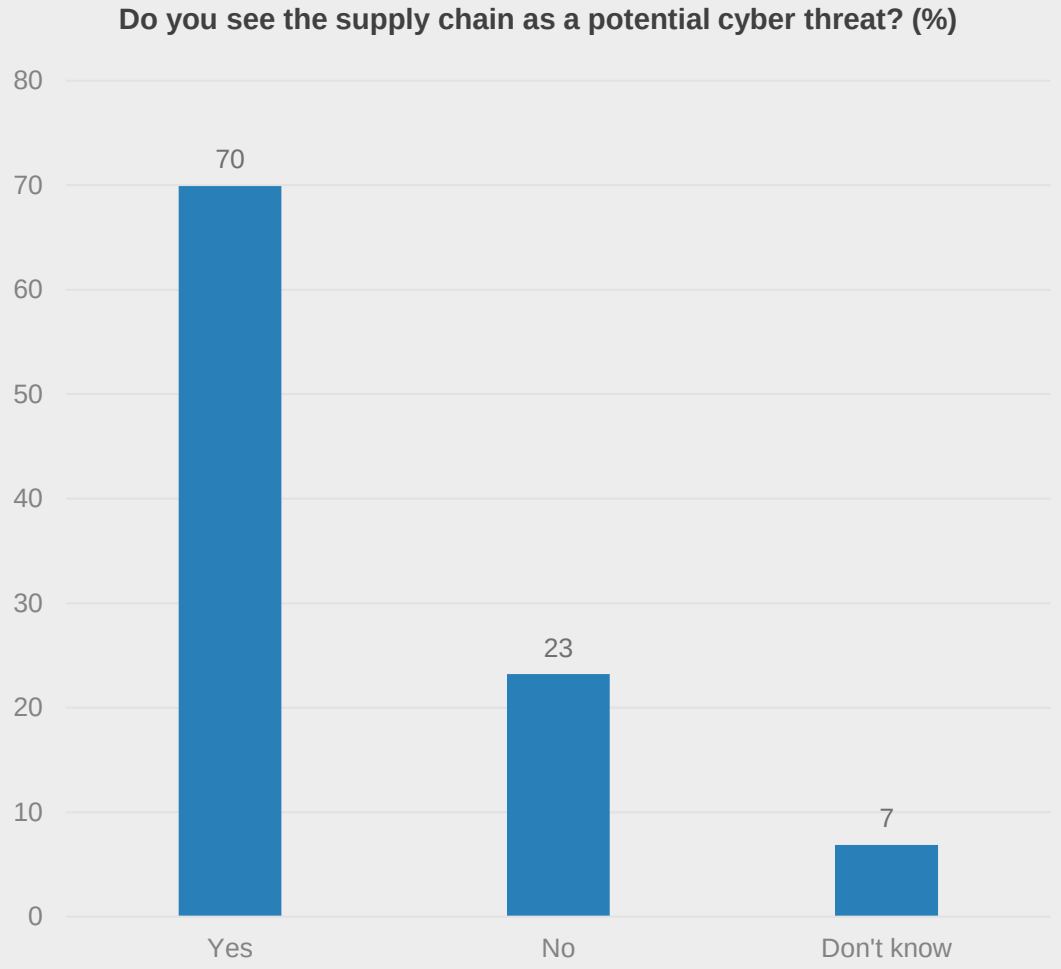
COVID-19 has significantly escalated concern about cyberattacks

Base: all research participants *n*=2,017

CHANGING SUPPLY CHAINS OPEN UP NEW CYBER RISKS

70% of respondents see the supply chain as a threat

The supply chain continues to be a source of concern when it comes to cyberattacks for over two-thirds of those surveyed. This is not surprising when you consider such notorious attacks as that of NotPetya.



70%

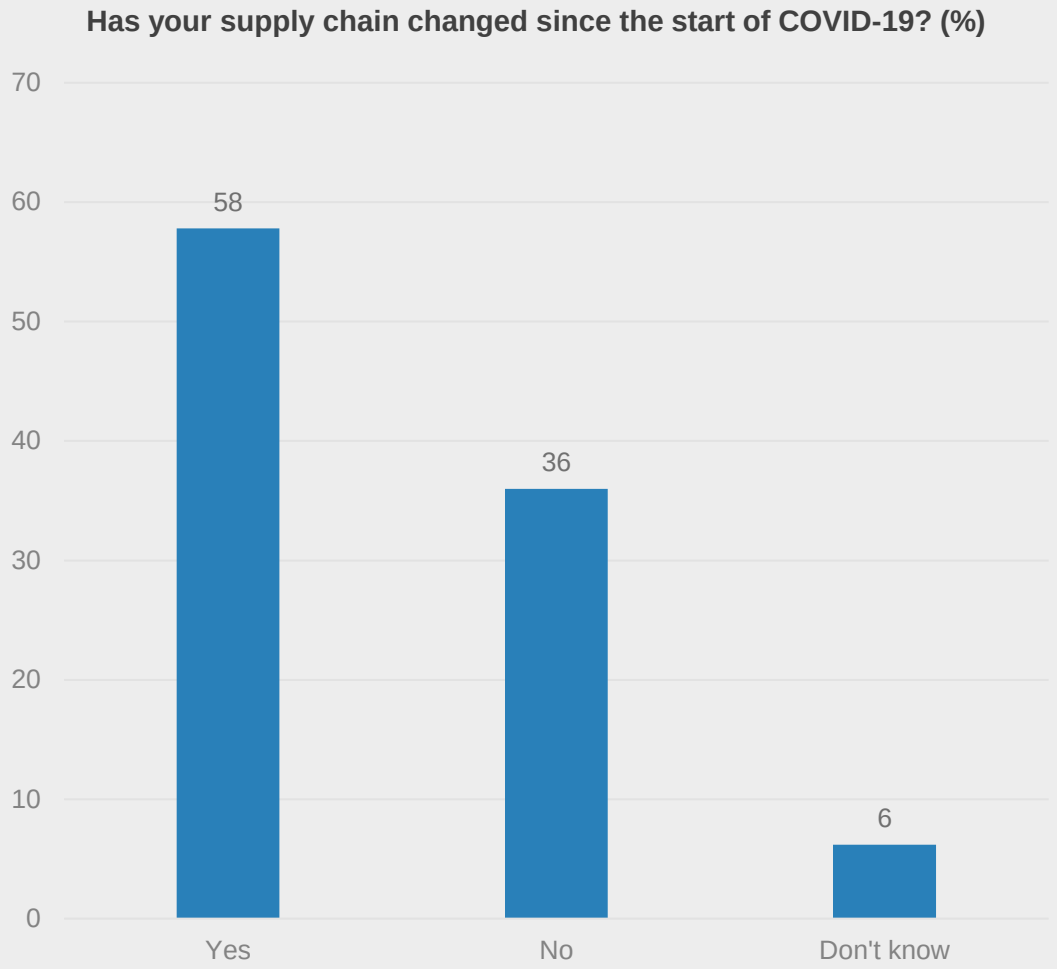
See the supply chain as a potential for a cyber threat

Over one-quarter either do not think it is a threat or "don't know"

Base: all research participants *n*=2,017

Over 50% of respondents say their supply chain has changed since COVID

58% have changed their supply chain since the start of COVID-19.



58%

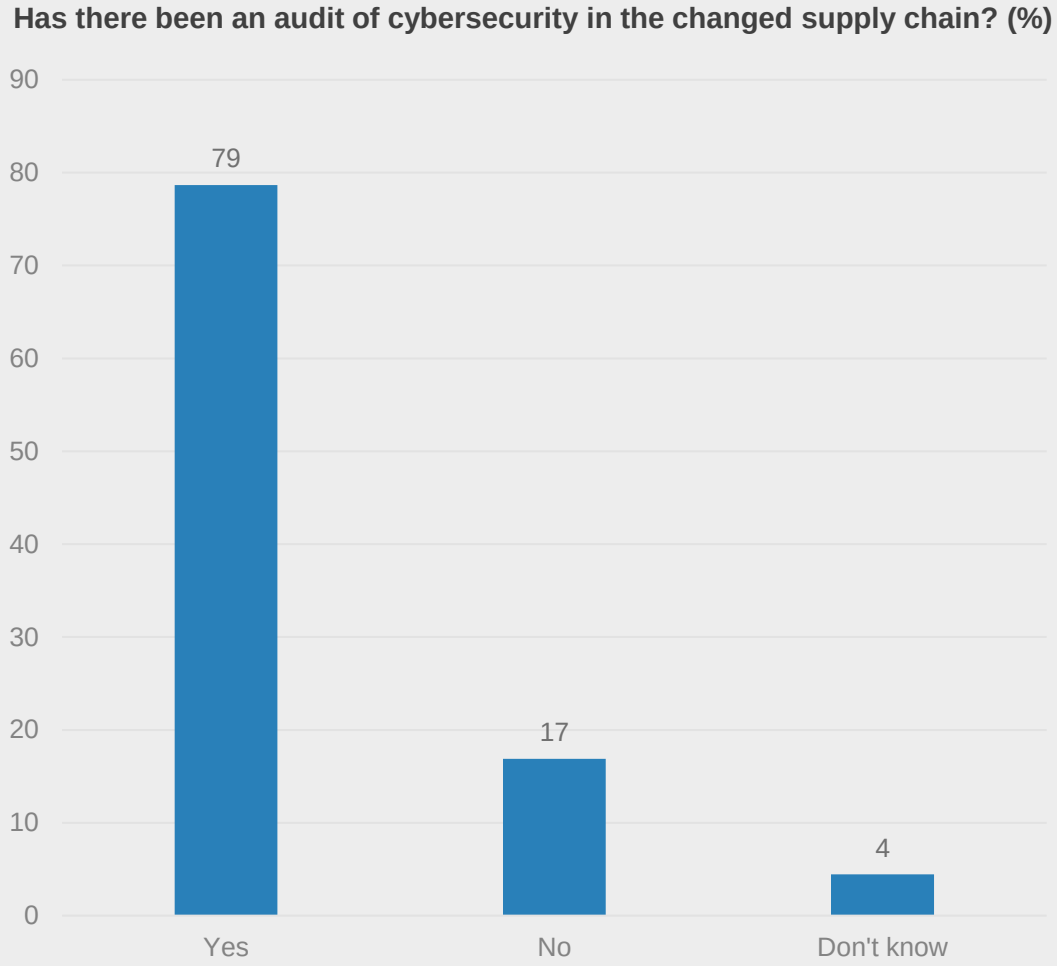
Have changed their supply chain since the start of COVID-19

Organizations have had a major change in their supply chain since the beginning of COVID-19

Base: all research participants *n*=2,017

Almost 80% say there has been a cybersecurity audit since the supply chain change

Almost one in five (17%) have not conducted an audit of cybersecurity in the changed supply chain.



17%

Have not carried out a cybersecurity audit

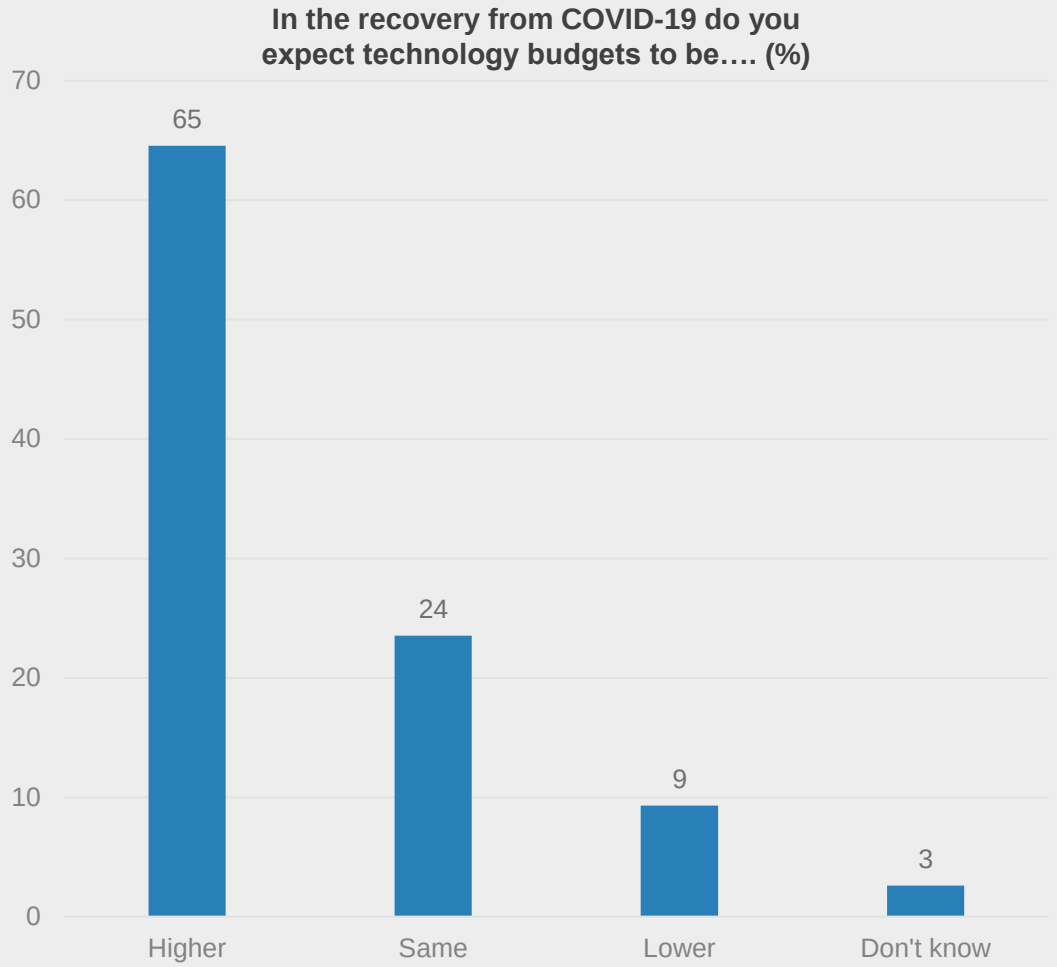
The majority of organizations have carried out an audit

Base: supply chain changed *n*=1,069

THE PATH AHEAD: HYBRID WORKING, INVESTMENT CHOICES AND MYRIAD CHALLENGES

65% expect tech budgets to increase in the COVID-19 recovery

Technology budgets are still expected to increase even with COVID-19, with 65% of managers saying they expect budgets to be higher.



65%

Expect increased tech budgets

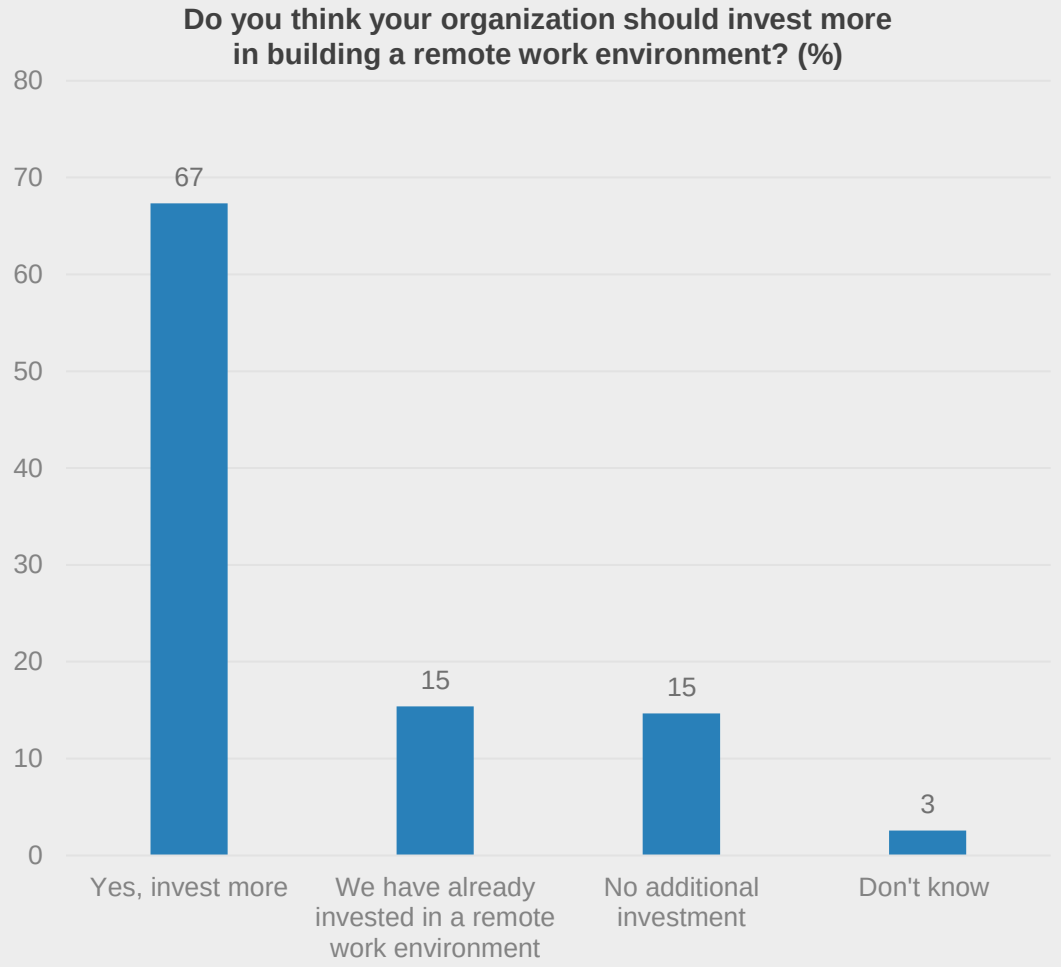
IT is the "winner" in investment post COVID-19

Base: all research participants *n*=2,017

Almost 70% of respondents believe their organizations should invest more in remote work

As the survey findings show, remote working is expected to be part of business for most organizations for at least the next six months, and organizations have ramped up their tools to accommodate current remote workers.

Despite the investment that has already taken place, 67% believe there should be more investment in remote working while only 30% believe there should be no more investment.



67%

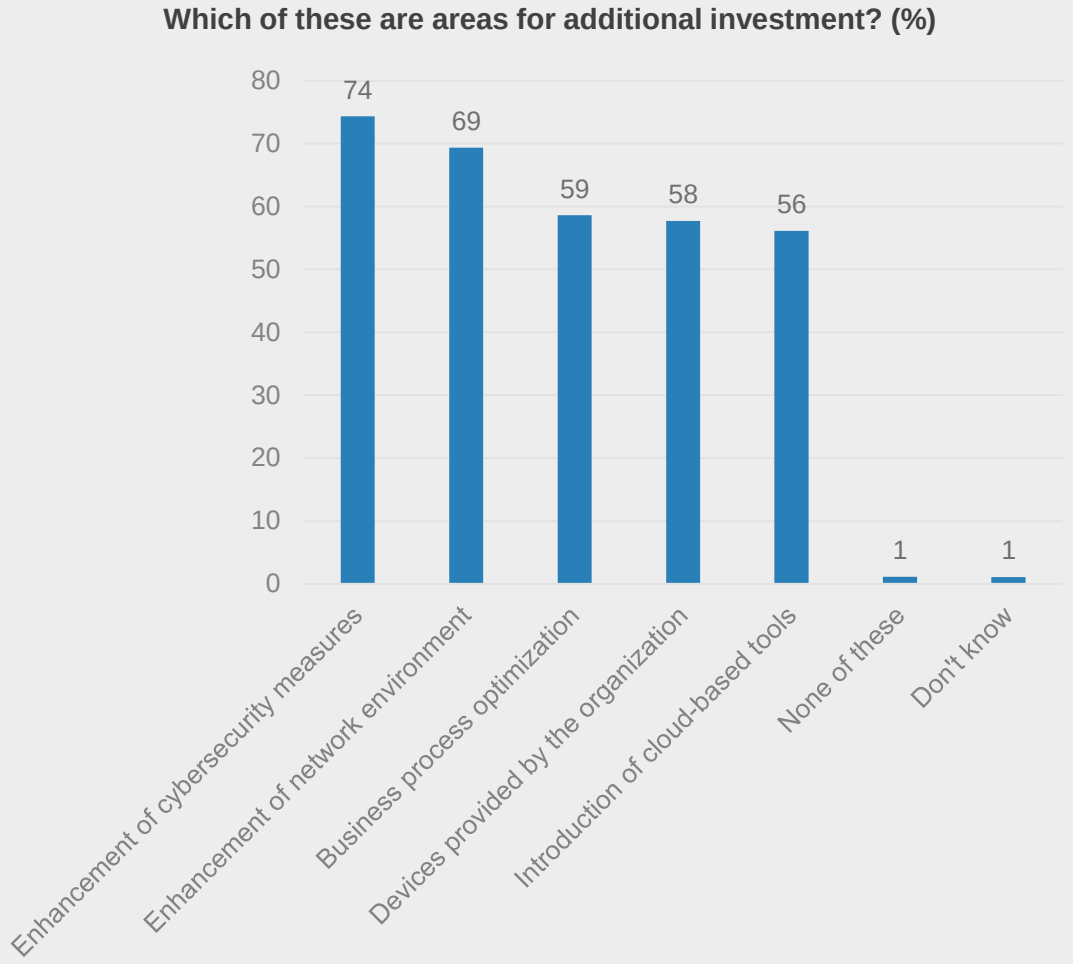
Think there should be more investment in remote working

Remote working will be part of the future

Base: all research participants *n*=2,017

74% of respondents believe cybersecurity enhancement as a top priority for additional investment

69% of business leaders also want investment in enhancement of the network environment while 59% want additional investment in business process optimization.



74%

Spend in security enhancement

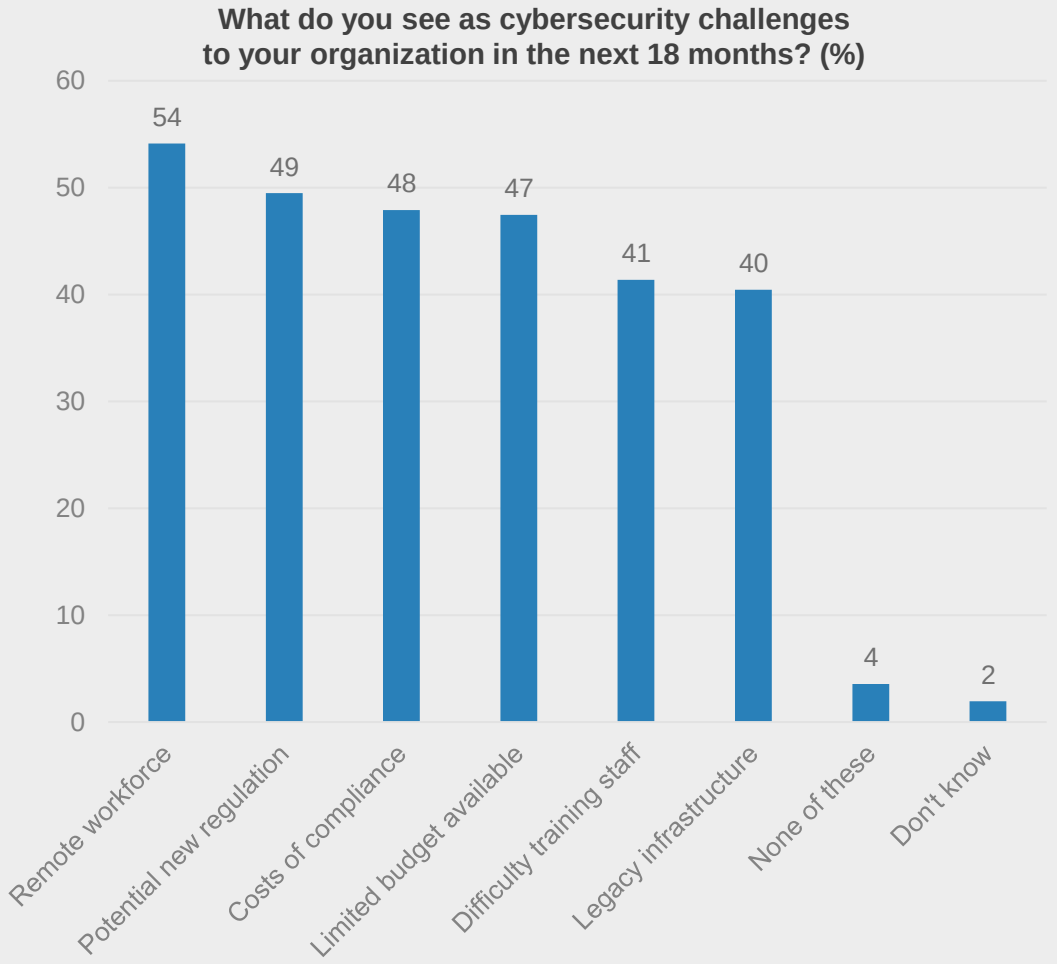
#2 area is enhancement of network environment

Base: those who think there should be more investment in remote working *n*=1,347

Over half of respondents believe that remote work will present cybersecurity challenges

Remote workforce ranked as the highest cybersecurity challenge (54%) to organizations in the next 18 months.

Other top-ranked challenges include new regulation (49%) and costs of compliance (48%), which were seen as top cybersecurity challenges in the next 18 months, with limited budgets (47%) and additional training (41%) not far behind.



54%

Remote workforce

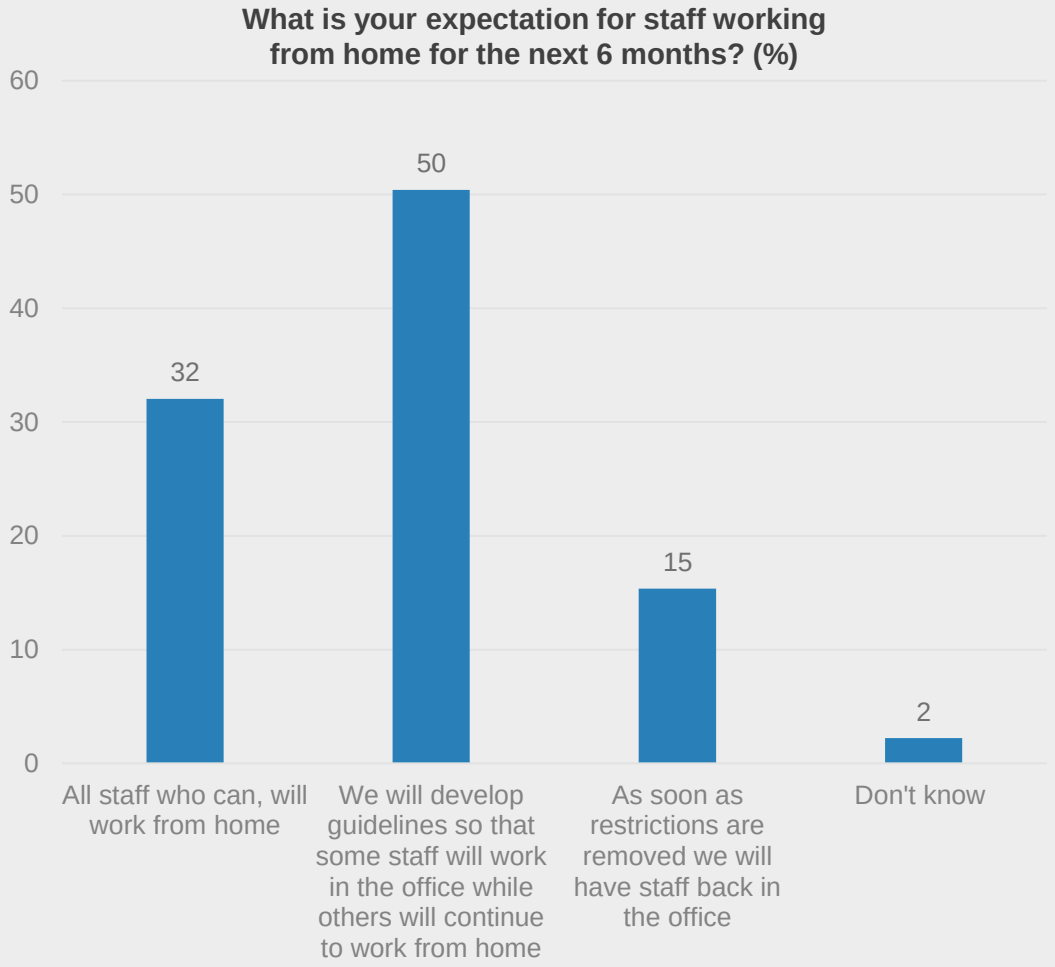
Remote workforce is the biggest challenge but only the leading one among many others

Base: all research participants *n*=2,017

The vast majority of respondents expect companies to keep some form of a work-from-home model

82% of respondents expect that either all staff that can work from home will, or that there will be a process that allows some staff to work from home.

Only 15% expect to have all staff back in the office as soon as restrictions are removed.



82%

Will have all or some of their staff working from home

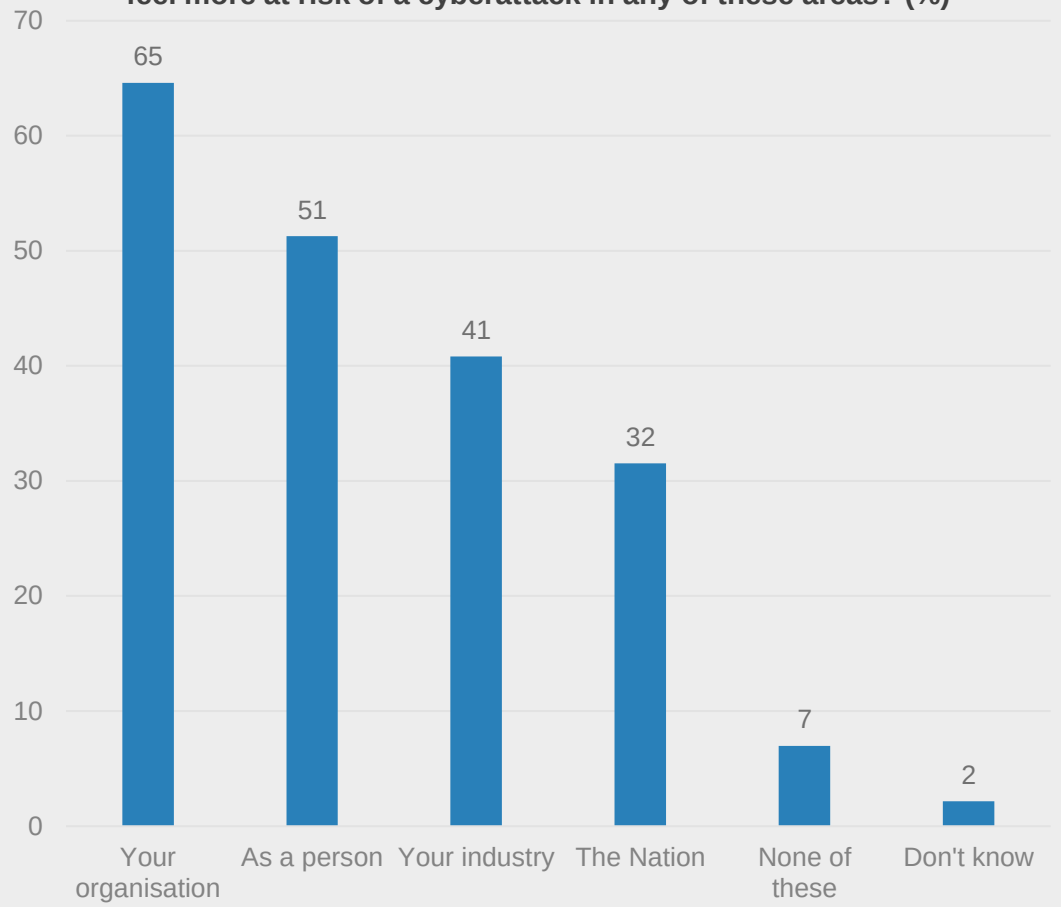
Only 15% expect to have all staff back in the office

Base: all research participants *n*=2,017

The vast majority of respondents feel vulnerable to cyberattacks in their business and personal life

Most people are concerned about themselves (51%) or their companies (65%) being more at risk from a cyberattack with the increase in remote working. Only 32% are worried about their country suffering an attack.

With the increase in remote working from home in the next 6 months, do you feel more at risk of a cyberattack in any of these areas? (%)



65%

Are worried about a cyberattack affecting their organization

Cyberattacks are expected across a range of areas but working from home is most likely felt to affect the organization

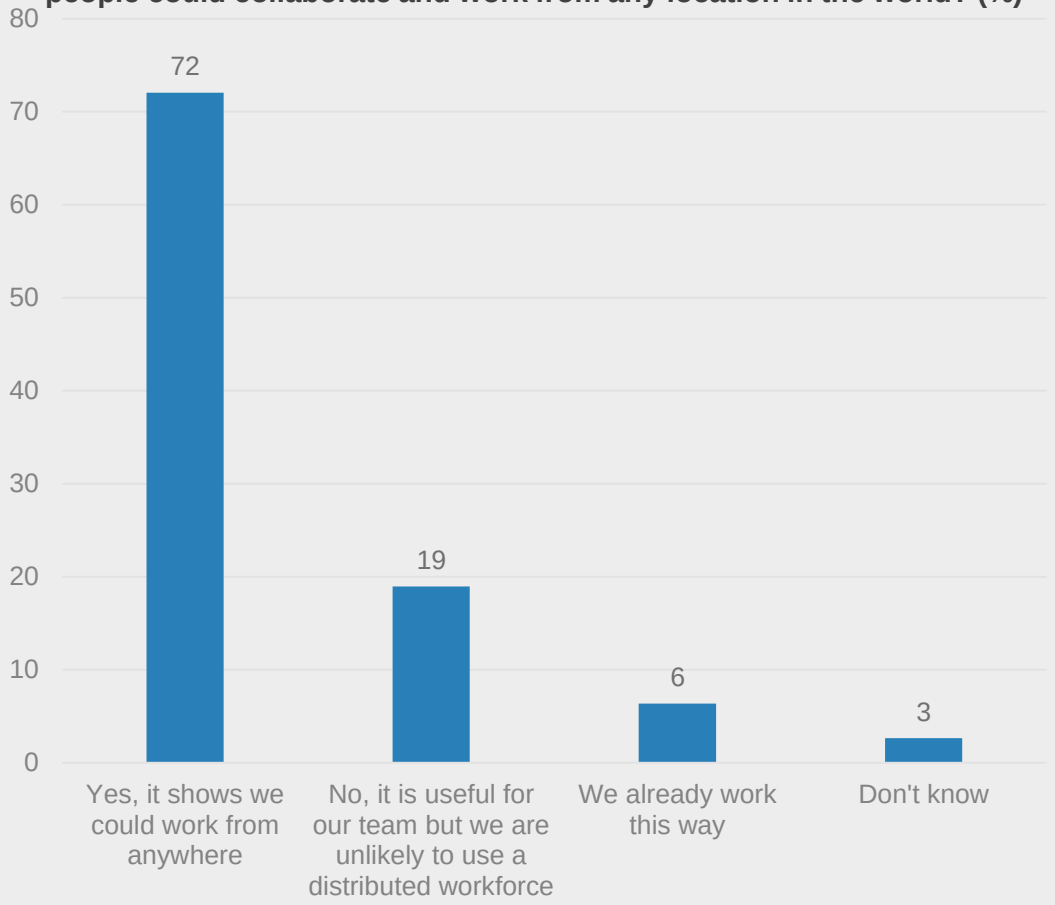
Base: all research participants *n*=2,017

The unexpected perk of COVID remote work is that it has helped to show that we can work from anywhere

Remote working has demonstrated to most organizations (72%) that they can work from anywhere.

The pandemic has created opportunities for the best teams to collaborate and work on tasks in a remote environment.

Has remote working opened new options for a distributed workforce where people could collaborate and work from any location in the world? (%)



72%

See the value of a distributed workforce

COVID-19 has shown that we can work from anywhere

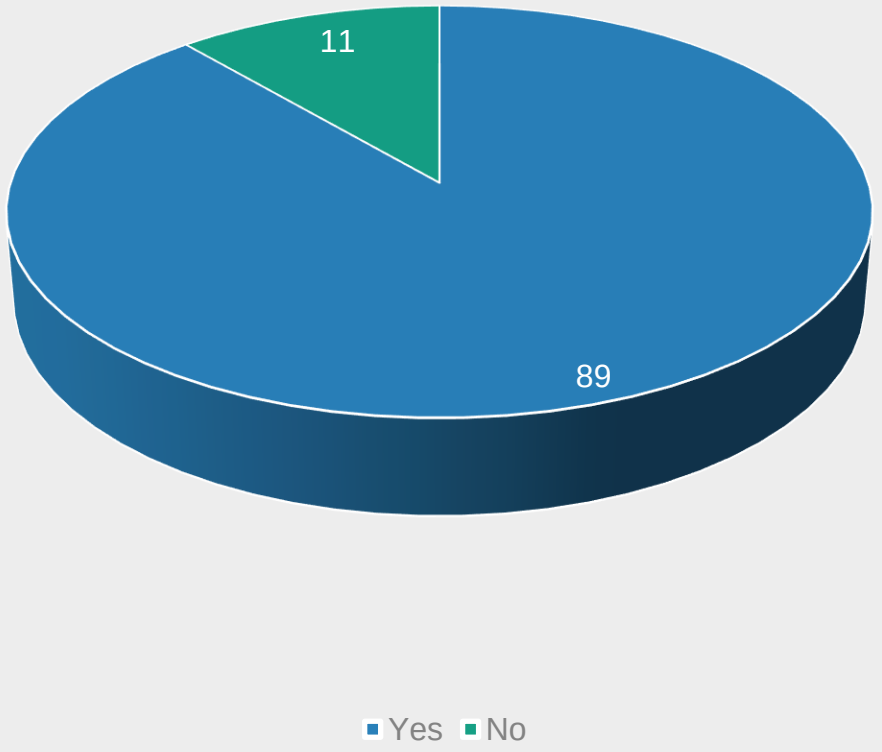
Base: all research participants *n*=2,017

89% of managers are using company security software

Most managers (89%) who are using personal devices are using mandated security software from their organizationa. However, this means that one in ten (11%) are not fully protected.

Considering the vast number of organizations represented in the research this is a huge gap in security for potentially millions of organizations.

Does your organization require any security software to be installed on personal devices before they can be used for work? (%)



11%

Not using company mandated security software on personal devices

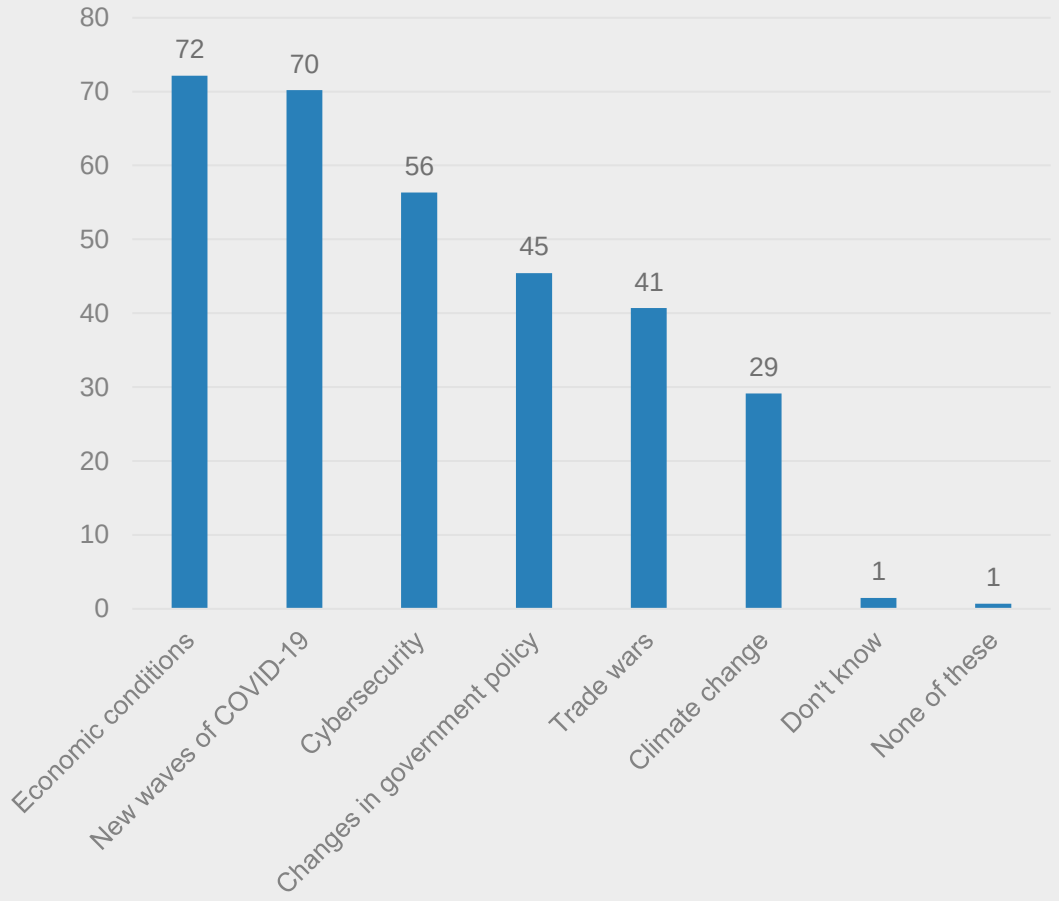
Not all organizations are protected on personal devices

Base: working from home some or all of the time and using personal device *n*=1,357

Cybersecurity is the third biggest threat in the next 6 months

Respondents believe that economic conditions (72%) and new waves of COVID-19 (70%) are the main threats in the next 6 months, with cybersecurity (56%) following in third.

Q49 Which of these do you think are threats in the next 6 months? (%)



72%

See economic conditions as a threat in the next 6 months

56%

Cybersecurity comes in at third as a threat in the next 6 months

Base: all research participants *n*=2,017