O2 business

The IT Security Team: 2021 and beyond

Findings from an independent survey of 5000 IT managers across 30 countries

A Sophos white paper June 2021

SOPHOS

IT teams have been at the forefront of pandemic response in almost every organization. IT has played a direct and critical role in enabling organizations to continue working despite the restrictions and limitations necessitated by COVID-19. It is thanks in large part to committed and passionate IT teams around the globe that so many organizations have been able to remain operational during the pandemic. They helped education establishments deliver learning online, enabled retailers to switch to online trading, and ensured public bodies could continue to provide essential services, just to name just a few examples.

This report, based on direct feedback from 5,400 IT managers across 30 countries, shines a spotlight on the realities that IT teams have faced in the last 12 months. It reveals the changes IT teams have experienced over the course of 2020, with particular focus on cybersecurity, and the impact of those changes on IT team members. The report also looks at the future of IT security teams, revealing expectations for IT over the next five years and helping organizations to start building their IT team of the future, today.

Key findings

Changes in IT team experiences over the course of 2020

- **IT AND cybersecurity workload grew:** 63% saw an increase in non-security workload, while 69% experienced an increase in IT security workload
- **Cyberattacks became more prevalent:** 61% report an increase in the number of cyberattacks on their organization
- **IT teams were able to enhance their cybersecurity abilities:** 70% of IT teams said they had further developed their cybersecurity skills and knowledge during this timeframe
- **Adversity brought teams together:** 52% say team morale increased over the year, with ransomware victims considerably more likely to have experienced an increase in team morale than those that weren't hit (60% vs. 47%)

The current state of play

- **IT teams need help dealing with complex attacks:** 54% say cyberattacks are now too advanced for their IT team to deal with on their own
- **IT teams feel well equipped for the challenges ahead:** 82% believe they have the tools and knowledge to investigate fully suspicious activities

The IT team of the future

- **IT security teams are set to grow in size**
  - 68% anticipate an increase in in-house IT security staff by 2023, and 76% by 2026
  - 56% expect the number of outsourced IT security staff to grow by 2023 and 64% by 2026.
- **AI technology is a key tool in future security strategies**
  - 92% expect AI to help deal with the growing number and/or complexity of threats

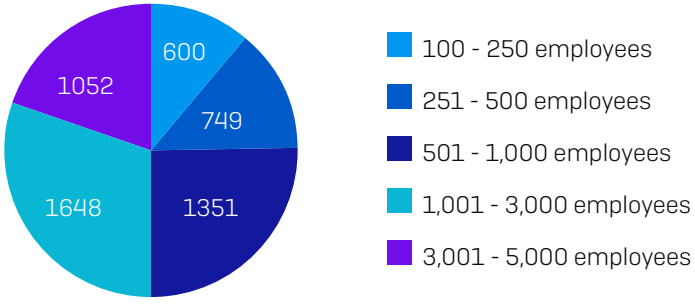
About the survey

Sophos commissioned independent research house Vanson Bourne to survey 5,400 IT decision makers across 30 countries. The survey was conducted in January and February 2021.

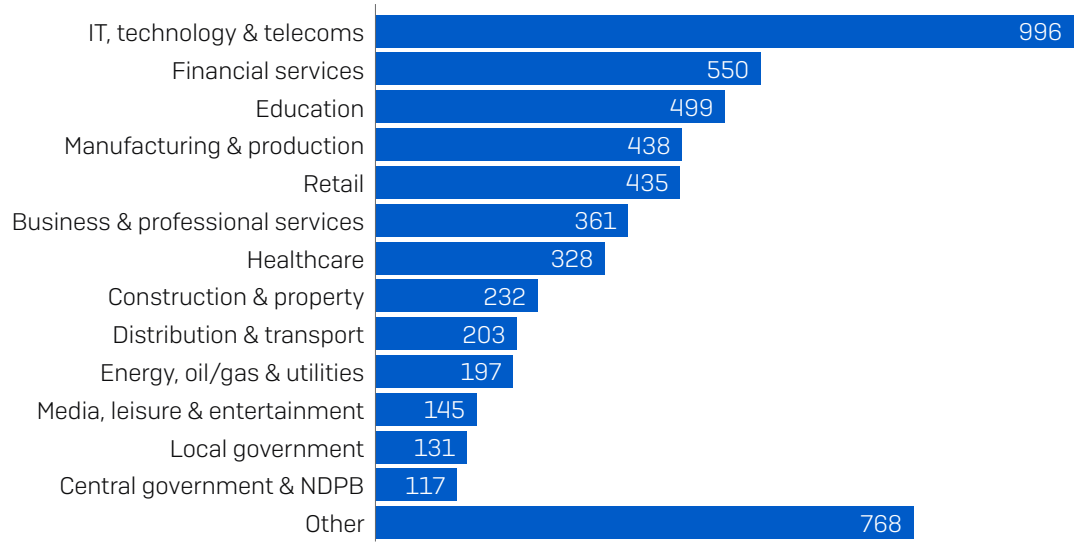
Country	# Respondents	Country	# Respondents	Country	# Respondents
Australia	250	India	300	Saudi Arabia	100
Austria	100	Israel	100	Singapore	150
Belgium	100	Italy	200	South Africa	200
Brazil	200	Japan	300	Spain	150
Canada	200	Malaysia	150	Sweden	100
Chile	200	Mexico	200	Switzerland	100
Colombia	200	Netherlands	150	Turkey	100
Czech Republic	100	Nigeria	100	UAE	100
France	200	Philippines	150	U.K.	300
Germany	300	Poland	100	U.S.	500

50% of the respondents in each country came from organizations with 100 to 1,000 employees, and 50% from organizations with 1,001 to 5,000 employees. Respondents also came from a wide range of sectors.

How many employees does your organization have globally? [5,400]



Within which sector is your organization? [5,400]



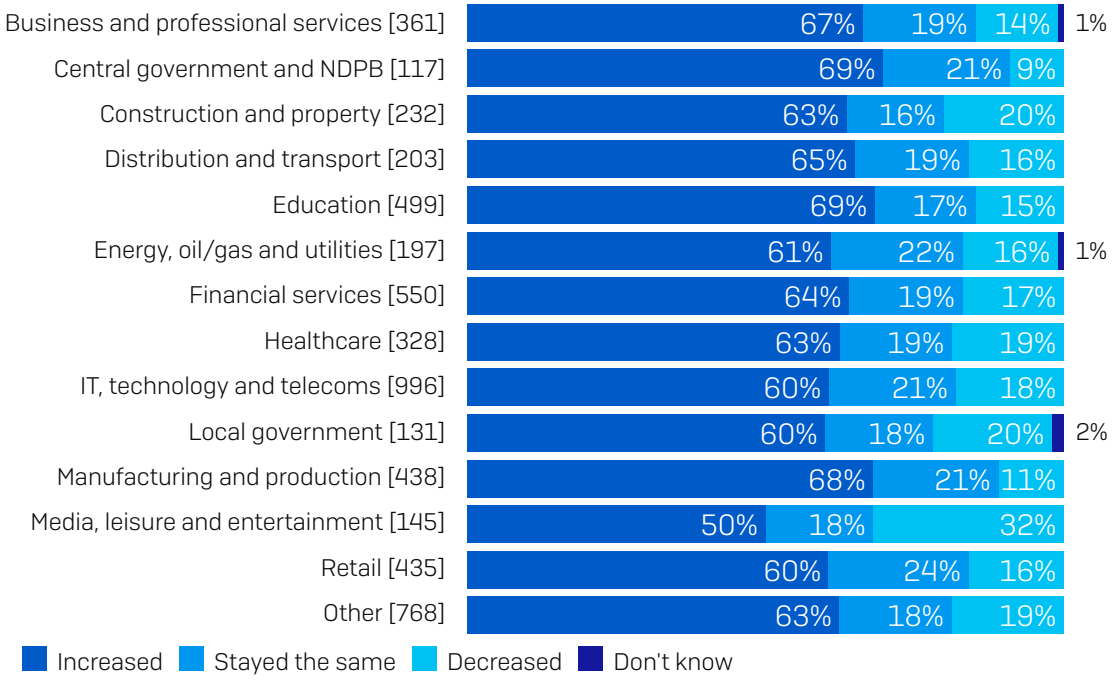
2020: A year of change

2020 was a year like no other, and IT teams were at the forefront of enabling organizations to adapt operations in response to the pandemic. Unsurprisingly, this had a considerable impact on workload.

Non-security IT workload grew...

2020 brought a lot of new work to IT teams: 63% of IT managers said their non-security workload increased over the course of 2020, with just 17% experiencing a decrease. Respondents in Turkey (84%), Austria (81%), USA (75%) were most likely to report an increase in workload.

How IT workload (non-security) changed over the course of 2020



Over the course of 2020, our IT workload (non-security) has decreased/increased/stayed the same [base sizes in chart] split by sector

Looking at the data by sector we see that IT teams in **central government and NDPB** and **education** were most impacted, with 69% of respondents reported that workload grew over the year, likely due to the central role both government and education organizations played in responding to the pandemic. Conversely, **media, leisure, and entertainment** had the highest percentage of respondents reporting a decrease (32%), likely due at least in part to the pandemic forcing many facilities to limit their services.

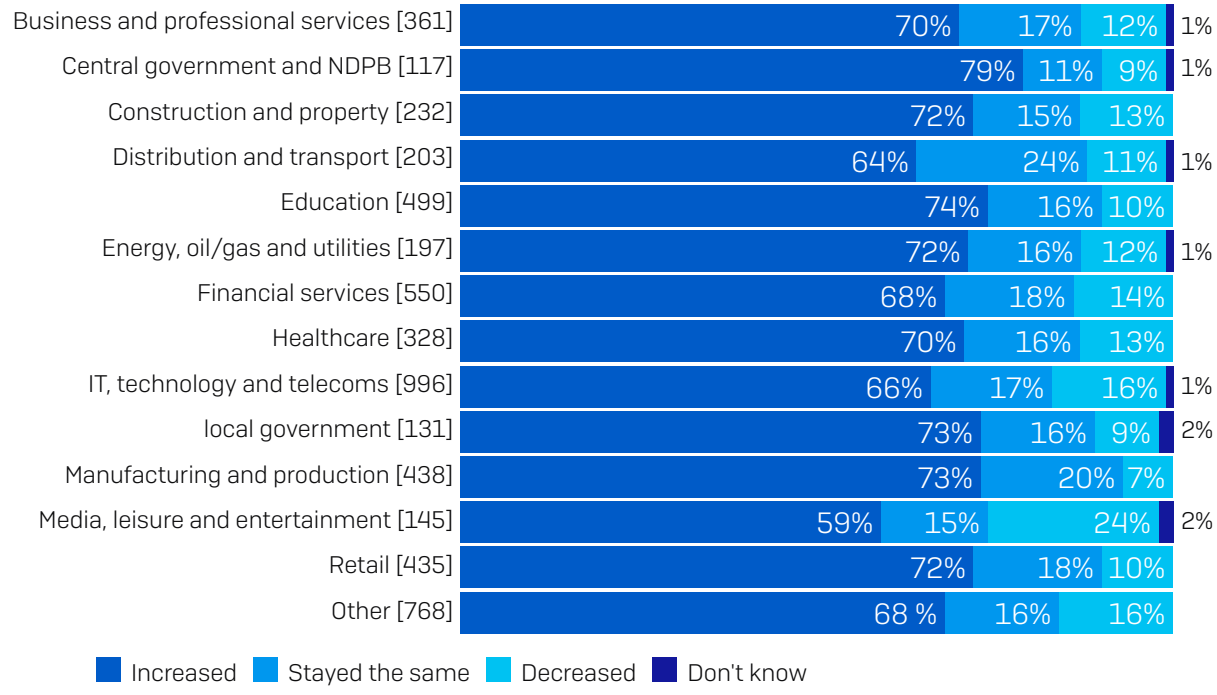
...and cybersecurity workload grew even more

How cybersecurity workload changed over the course of 2020

Over the course of 2020, our cybersecurity workload has decreased/increased/stayed the same [5,400] omitting "Don't know"

69% of respondents reported an increase in their cybersecurity workload over the previous year, 13% reported a decrease and 17% said their workload stayed the same. Turkey (82%) again reported the highest level of increase, followed by Sweden (80%), Israel, and Brazil (both 78%). At the other end of the spectrum, respondents in the UAE were most likely to report a decrease in cybersecurity workload (26%), followed by those in Switzerland (22%) and Nigeria, and the Philippines (both 19%).

How cybersecurity workload changed over the course of 2020



Over the course of 2020, our cybersecurity workload has decreased/increased/stayed the same [base sizes in chart] split by sector

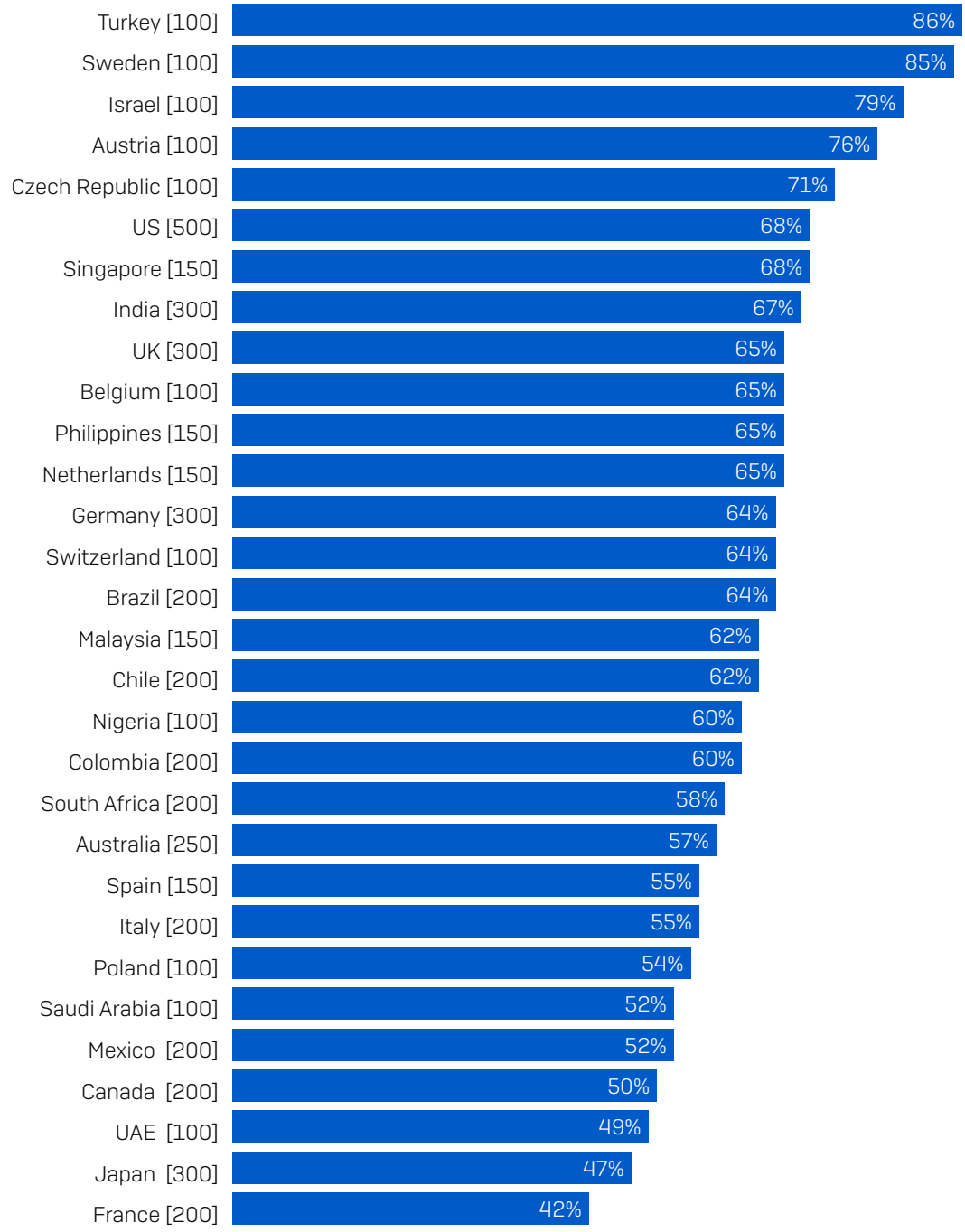
Echoing the sector trend we saw previously, IT managers in **central government and NDPB** (79%) and **education** (74%) were most likely to report an increase in cybersecurity workload over the previous year, while those in **media, leisure, and entertainment** were most likely to report a decrease (24%). Again, it is likely that this is due to these sectors being among the most heavily impacted by the pandemic, albeit in very different ways.

Cyberattacks increased in frequency

The heavier cybersecurity workload over the course of 2020 was driven, in part, by an increase in cyberattacks: over six in ten (61%) respondents reported a rise in attacks on their organization last year. Just 19% reported a decrease.

This growth occurred across all sectors, and the variance between those that experienced the largest **(central government and NDPB)** and smallest **(IT, technology and telecoms,** and **media, leisure, and entertainment)** increase was just 16 percentage points (74% vs 58%).

Percentage of respondents' organizations that experienced an increase in cyberattacks over the course of 2020



Over the course of 2020, cyberattacks have increased [base sizes in chart] omitting some answer options, split by country

However, when we look at the data by country we see a much greater variation in experiences with more than twice as many respondents in Turkey reporting an increase in attacks compared with those in France (86% vs. 42%). Very high percentages of respondents in Sweden (85%), Israel (79%), and Austria (76%) also reported an increase in cyberattacks on their organization over the course of 2020. Conversely, in France, Japan, and the UAE, fewer than half reported an increase.

Attacks are getting harder to stop

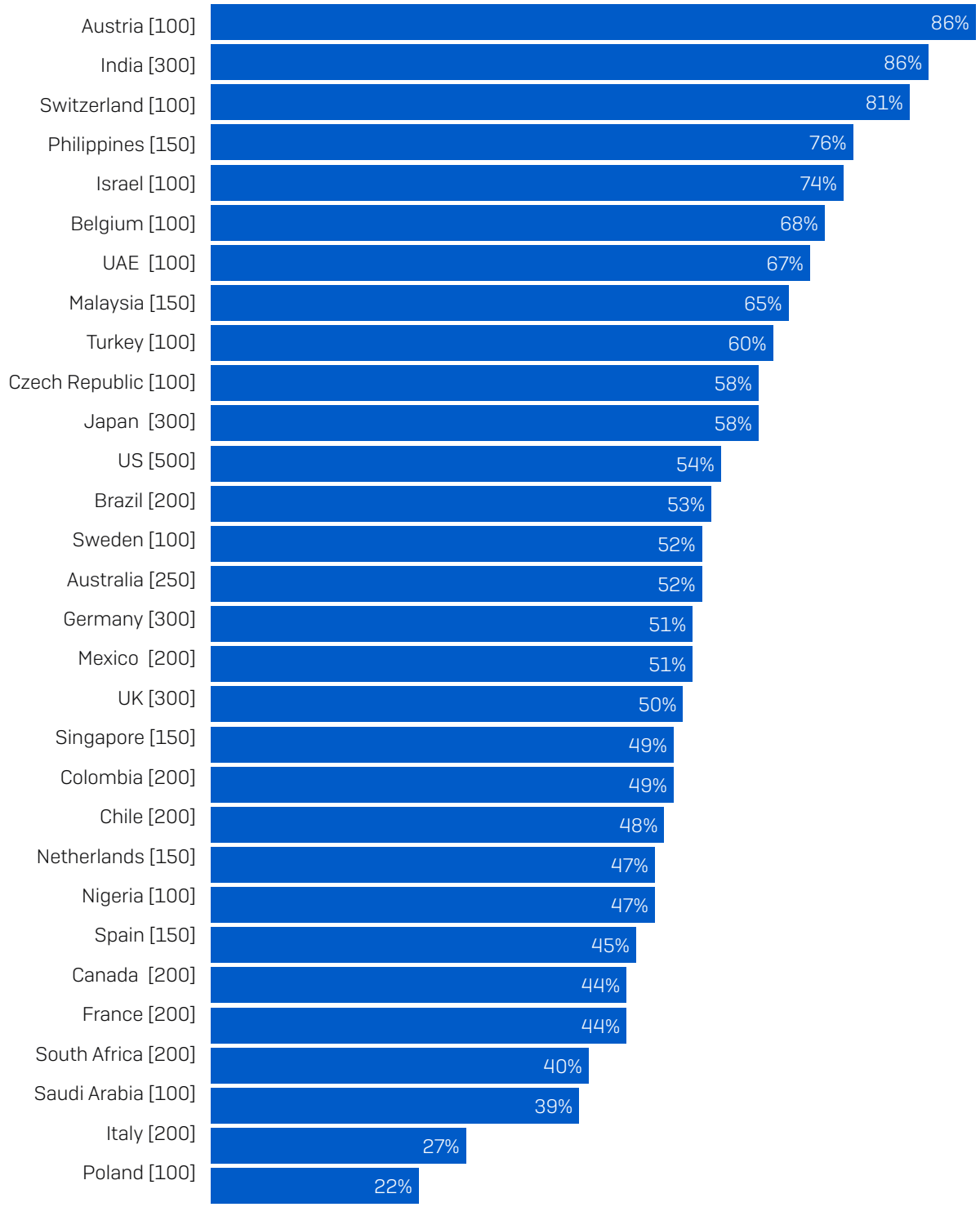
Advanced cyberattacks are complex and multi-stage, with adversaries using myriad Tactics, Techniques and Procedures (TTPs) in the course of the incident. Dealing with these attacks is challenging – and for over half of the respondents (54%), attacks are now too advanced for their IT team to deal with on their own.

Say attacks are now too advanced for their organization's IT team to deal with on their own

This challenge is most acute in the **business and professional services** sector, where 63% of respondents believe they are no longer capable of dealing with cyberattacks on their own, closely followed by **central government and NDPB** (62%) and **healthcare** (60%). Conversely, **construction and property** and **local government** were least likely (47%) to agree. In the case of local government, this is a surprising finding, because, as reported in the State of Ransomware 2021, this sector is the most likely to have their data encrypted in a ransomware attack.

Among the countries surveyed, we see considerable variation in levels of confidence in dealing with complex attacks.

Respondents that think cyberattacls are now too advanced for their IT team to deal with on their own



Respondents that agree cyberattacks are now too advanced for their organization's IT team to deal with on their own [base sizes in chart] omitting some answer options, split by country

Those based in Austria and India reported least confidence in dealing with attacks, with 86% saying they are now too complex for their IT team to deal with on their own, followed by those in Switzerland (81%), the Philippines (76%), and Israel (74%).

Recognizing the complexity of attacks and identifying when outside expertise is needed is a key step in defending against today's advanced cyberattacks. SophosLabs and the Sophos Managed Threat Response teams have seen a steady increase in the number of attacks that combine automation with hands-on live hacking in an effort to bypass an organization's defenses. Stopping these sophisticated attacks requires skilled defenders and organizations are wise to acknowledge when these skills need to be outsourced.

At the other end of the spectrum, Poland reports the least challenge in dealing with cyberattacks in-house, with only 22% of respondents saying that attacks are too advanced for their IT team to handle, closely followed by Italy (27%). This confidence in the face of the growing number of attacks may be due to investment in recruiting and developing skilled professionals who are able to stay ahead of adversaries. However it may also reflect misguided confidence in the face of today's advanced attacks. With adversaries constantly evolving their approaches, it is important to be realistic about the level of expertise needed to stop them.

Response times are down

Given the widespread increases in workload over the course of 2020, together with the challenges of adapting to the pandemic, it is perhaps unsurprising that a significant majority of respondents (61%) reported an increase in response time to IT cases over this period. 20% said response time decreased over this period, while for 19% it remained the same.

Changes in response time to IT cases over the course of 2020

Over the course of 2020, our response time to IT cases has deecreased/increased stayed the same [5,400] omitting "Don't know"

Increased response time was most widespread in the **education** sector, where 65% of respondents reported a rise. The need for education establishments in most countries to pivot to online learning during 2020 created considerable work for IT teams which will have had an impact on their ability to respond quickly to tickets.

Media, leisure, and entertainment reported the greatest decrease in response time, with nearly one third (32%) saying that they were able to respond to tickets more quickly. Again, it's likely the pandemic is a major factor behind this change, with reduced organizational output freeing up IT team time for faster response.

The impact of 2020 on the IT team

It's not all bad news. When it comes to the state of IT teams, there is lot to be encouraged by. 70% of IT managers said that their team's ability to further develop their cybersecurity skills and knowledge increased over the course of 2020, with just 12% saying it decreased.

Changes in ability to further develop cybersecurity skills and knowledge over the course of 2020

Over the course of 2020, ability to further develop our cybersecurity knowledge and skills has decreased/increased/stayed the same [5,400] omitting "Don't know"
Due to rounding, the results do not add up to 100%

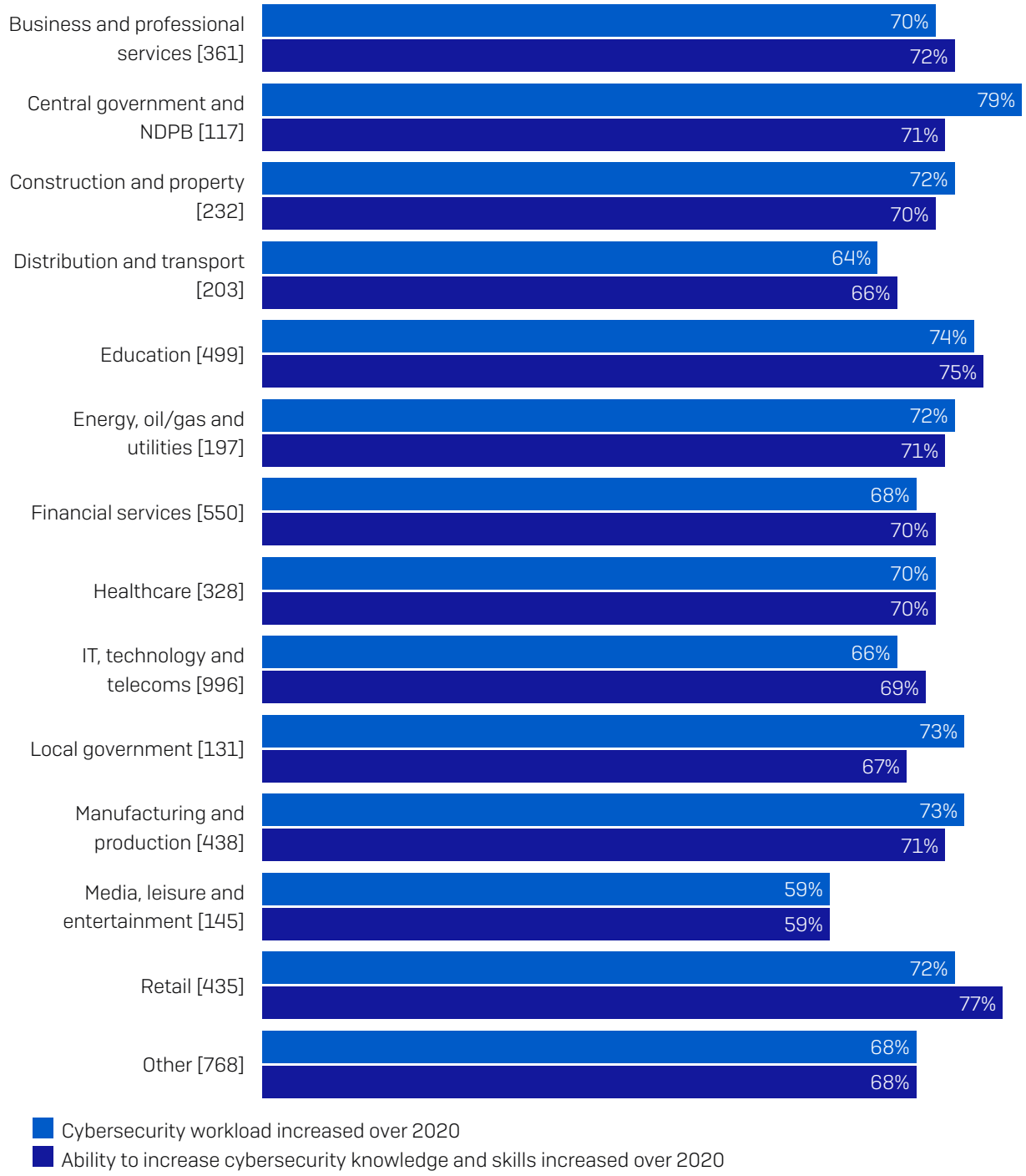
Interestingly, several sectors that were particularly affected by the pandemic reported contrasting experiences:

- **Retail** was the sector most able to increase cybersecurity skills and knowledge (77%). It is likely that that the major pivot to online retail during lockdowns provided new challenges and opportunities for IT teams in this industry.
- **Education** saw the second highest increase in cybersecurity skills and knowledge (75%). This is another sector that experienced major transformation over last year, and while the move to online teaching and learning undoubtedly presented a huge challenge for IT teams, it also created a huge learning opportunity.
- **Media, leisure, and entertainment** reported the lowest increase (59%). With this sector also noting the biggest decline in both non-security and cybersecurity workloads, it is likely that the reduced activity restricted development opportunities.

Increased workload lead to increased knowledge and skills

Overall, the data revealed a clear correlation between increased cybersecurity workload and increased ability to develop cybersecurity knowledge and skills across all sectors.

Increase in cybersecurity workload and increase in ability to develop cybersecurity knowledge and skills



Over the course of 2020, our cybersecurity workload has increased/ Over the course of 2020, our ability to increase cybersecurity knowledge and skills has increased [base sizes in chart] split by sector

Among the respondents that experienced an increase in cybersecurity workload over 2020, 84% also said their ability to develop their cybersecurity skills and knowledge increased. Similarly, over eight in ten (82%) of those that reported an increase in cyberattacks on their organization also said their ability to develop their cybersecurity skills and knowledge increased. This makes sense: while increased workload and cyberattacks add pressure, they also provide opportunities to develop new skills.

Team morale has improved

Over half the IT managers surveyed (52%) said that team morale had increased over the course of 2020. 26% said it decreased and 22% said it stayed the same.

Changes in team morale over the course of 2020

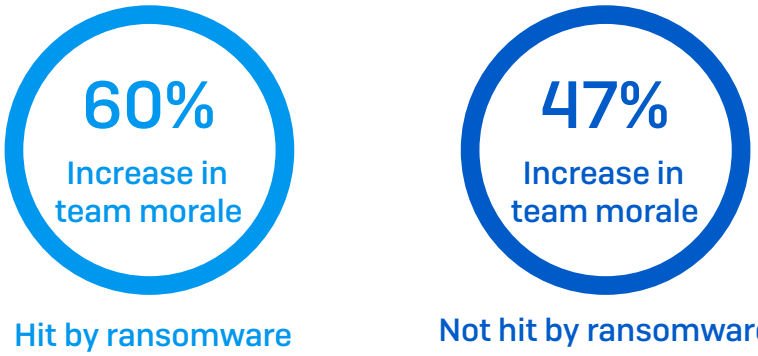
Over the course of 2020, our team morale has decreased/increased/stayed the same [5,400] omitting "Don't know"

Geographically, the biggest increases in morale were reported in Turkey (75%), Austria (71%) and India and South Africa (both 69%). At the other end of the scale, IT teams in Israel (26%), France (31%), Italy (33%) and Poland (36%) were least likely to report an improvement in team morale.

You may have noted that several countries highlighted here have also been called out in previous sections. Turkey and Austria, which had the highest proportion of respondents saying team morale had increased, were among the top four countries reporting an increase in cyberattacks. Similarly, France had the second lowest percentage of respondents reporting an increase in morale and also the lowest increases in cyberattack of all countries surveyed. This correlation between experiences of cyberattacks and team morale is one of the most striking findings in the survey.

Further demonstrating this point, 60% of respondents whose organization had been hit by a ransomware attack in the previous 12 months reported an increase in team morale, compared with 47% of those that weren't hit.

Changes in team morale over the course of 2020

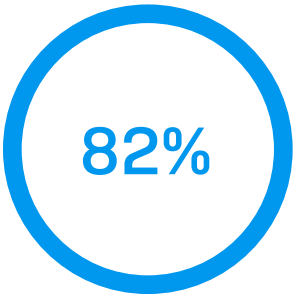


Over the course of 2020, our team morale has decreased/increased/stayed the same [5,400] omitting some answer options, split by respondents whose organization was hit by ransomware over the last year

There are a number of likely factors behind this correlation. Adversity – in this case cyberattacks – often provides opportunities for people to come together and work as a team towards a shared goal, boosting morale. Furthermore, being able to support the organization in the face of increasing attacks brings a sense of satisfaction.The highest increase in morale was reported by two sectors that were heavily impacted by the pandemic, with **education** experiencing the highest improvement (58%), closely followed by **healthcare** (57%).

At the same time, the pivotal role IT teams have played in enabling business continuity in the face of the pandemic may have resulted in greater awareness and recognition of their contribution, which also helps boost morale. If IT teams have not been duly recognized, now is the time to do so.

IT teams feel well equipped for the challenges ahead



Say they have the tools and knowledge to investigate fully suspicious activities

Respondents that agree if they detect suspicious activities in their organization, they have the tools and knowledge they need to investigate fully [5,400] omitting some answer options

In the face of the increased workload and frequency of cyberattacks during 2020, it is encouraging that 82% of IT managers say they have the tools and knowledge they need to investigate fully suspicious activities if they are detected in their organization. The opportunities provided to develop skills and knowledge during 2020 are equipping teams well for the challenges ahead. Continuing this investment in tools and training is essential if IT teams are to be able to keep up with the ongoing evolution of cyberattacks.

However, when we look at the responses to this question by sector, there are two clear outliers: **central government and NDPB** (67%) and **local government** (64%). Across the globe, the government sector has been heavily impacted by the pandemic. It has had to ensure continuity of essential services during an extended period of disruption while also providing additional support to both citizens and organizations. At the same time, public sector funding is an ongoing a challenge in many countries, which may limit the resources available. With ransomware actors focusing heavily on government organizations, it's essential that they have the resources and skills needed to investigate suspicious activities effectively.

The future IT security team

As we've seen, last year was an uphill struggle for many in IT. However, IT teams rose to the year's challenges admirably, and as a result, increased both their skills and morale. These experiences, together with wider changes in the IT landscape, such as the growth in flexible working and the use of the cloud, will have a direct impact on the IT security team of the future.

IT security teams are set to grow – fast

In the face of the growing demands on IT teams, respondents anticipate considerable growth in the size of both in-house and outsourced IT security staff, particularly in the next two years:

- 68% expect in-house staff to increase in the next two years, with 76% anticipating an increase over the next five years
- 56% expect outsourced IT staff to increase over the next two years, with 64% expecting an increase over the next five years
- Just 8% expect in-house staff numbers to be lower in five years time

IT Security Resourcing	Anticipated Change	By 2023	By 2026
In-house IT security staff	Increase	68%	76%
	Decrease	11%	8%
Outsourced IT security staff	Increase	56%	64%
	Decrease	14%	10%

How do you think the size of your organization's IT security team will change by 2023 and 2026? [5,400] excluding some answer options

Interestingly, growth in outsourced IT staff does not come at at the expense of in-house teams. Nearly half (46%) of respondents expect both in-house and outsourced IT security staff to grow by 2023, rising to 55% by 2026.

Overall, 77% of respondents anticipate growth in at least one area of resourcing (in-house or outsourced) over the next two years, rising to 85% by 2026.

AI is key

Expect AI to help address the growing number of attacks

Expect AI to help address the growing sophistication of attacks

Respondents that agree they expect AI technologies will help deal with the growing number of attacks and/or they expect AI technologies will help deal with the growing sophistication of attacks [5,400] omitting some answer options

Almost universally, IT teams are looking to AI technologies to help them combat the growth in cyberthreats. 86% expect AI technologies to help deal with the growing number of attacks, while the same percentage expecting AI technologies to help deal with the growing sophistication of attacks, with 92% selecting at least one of these options.

Build the IT security team of the future now

To build the IT team of the future you need to start now. Organizations should use these insights direct from the frontline to help set themselves up for cybersecurity success in 2023 and beyond. Based on the learnings from this report, Sophos offers five recommendations:

1. Implement tools and approaches that reduce IT security admin workload

The increase in both non-security and security workload over the last year has been very clear to see. Organizations should look to implement tools and approaches that reduce IT security workload, freeing up team teams for other activities.

- **Automate.** Take advantage of automation to reduce the burden of day-to-day tasks that suck valuable time and energy from IT professionals and divert them from strategy projects. Machines are invariably able to react faster than human operators, speeding up response time and reducing exposure.
- **Consolidate.** Simplify day-to-day admin by managing all your cybersecurity solutions via a single, unified console. Having everything in one place eliminates the need both to jump from console to console to manage security and correlate data across different systems, saving IT teams valuable time and effort. Consolidating IT security also reduces vendor management overheads.
- **Integrate.** Choose solutions that integrate and are engineered to work together. This increases both the ability to automate tasks while making it easier to conduct cross-product investigations, and delivering deeper insights into your security posture.

2. Invest in tools and training that enable IT teams to use their growing skills

IT teams have seen significant development of their skills and knowledge in the last year. Organizations would be wise to invest in the tools and training that enable them to use these new skills, and to continue learning. These resources will also help recruit new talent to the team.

3. Combine in-house and outsourced IT team expertise

Cyberthreats are already too complex for more than half of IT managers to deal with on their own – and they're only going to get even more complex. By combining both in-house and outsourced expertise in your security teams, you can get the best of both worlds: professionals with in-depth knowledge of threats and your organization. This combined structure also makes it easier to adapt and respond to changes, leveraging the best people for each situation. Organizations should look for security partners that can extend their IT team with skills and capacity not available in-house, while also providing the flexibility to adapt to their preferred operational model.

4. Set yourself up to attract the best global talent

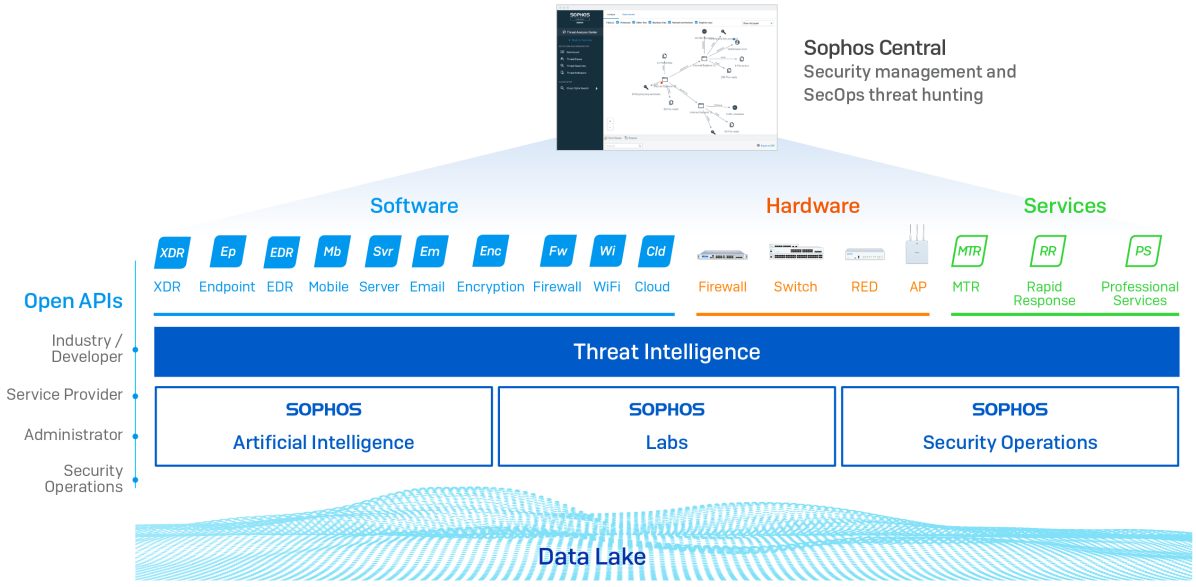
With the majority of organizations looking to expand their IT teams, competition for the best talent will be fierce. Adopting innovative technologies that can be managed from any location will help you increase your talent pool. The pandemic has taught us that almost all IT roles can be performed remotely if needed. What's more, offering high quality tools will increase your appeal to the most able candidates.

5. Build your in-house IT security team pipeline

IT security talent is already in short supply. Alongside expanding your talent pool, organizations should also look to in-house programs to nurture and build their IT team pipeline, such as apprenticeships and in-role training. While the image of a young person in a hooded top hunched over a computer in their bedroom is a stereotype, it is also a reminder that many people develop advanced cyber skills outside traditional career paths.

How Sophos can help

Sophos helps IT teams in over 500,000 organizations and 150 countries defend their organizations against cyberthreats.



The Sophos Adaptive Cybersecurity Ecosystem (ACE)

- We offer a complete portfolio of **next-gen technologies** powered by **artificial intelligence.** Our products are are engineered to work together, automating manual tasks and reducing exposure to threats – we call it Synchronized Security. Customers with our endpoint and firewall protection consistently report a reduction in day-to-day admin of at least 50%, and fewer security incidents.
- **Sophos Extended Detection and Response (XDR)** and **Sophos Endpoint Detection and Response (EDR)** give IT teams the tools they need to quickly identify and remediate threats and IT hygiene issues. Sophos EDR is the first EDR designed for security analysts and IT administrators alike, enabling IT teams to develop their expertise without adding headcount.
- All Sophos next-gen technologies are managed through the **Sophos Central** security platform – a web-based tool that enables you to employ the best security talent independent of location.
- The **Sophos Managed Threat Response (MTR)** and **Sophos Rapid Response** teams provide advanced threat hunting and incident response expertise to support in-house teams, delivered as a fully-managed service. You control how and when potential incidents are escalated, what response actions (if any) you want us to take on your behalf.
- All our protection is underpinned by the collective threat intelligence of **SophosLabs, Sophos Security Operations,** and the **Sophos AI** team, and the **Sophos Data Lake.**
- **Open APIs** enable all customers to benefit from the learnings and telemetry of our partners around the world.

To learn more about what we do and to discuss the challenges facing your team, visit our website or speak with a Sophos representative.

O2 business

SOPHOS

Published in July 2021. All information is correct at time of publication. Telefónica UK Limited Registered in England no.1743099.
Registered Office: 260 Bath Road, Slough, SL1 4DX