O2 business

Cybersecurity:
The human challenge

Findings from an independent survey
of 5000 IT managers across 26 countries

A Sophos white paper October 2020

SOPHOS

Introduction

The role of skilled professionals in cybersecurity has never been more critical. While advances in automation and technology have played an important part in strengthening organizations' cyber defenses, truly effective security programs still require the addition of human experts.

The continued importance of security professionals has been driven in large part by the evolution of cyberattacks. Behind every cyberthreat is a cybercriminal, and today's advanced attacks often combine the latest technology with hands-on live hacking. Protecting against these human-led attacks requires human expertise.

This comprehensive study provides brand new insights into the state of cybersecurity skills and resources across the globe. It reveals the realities facing IT teams when it comes to the human-led delivery of cybersecurity and explores how organizations are responding to the challenges they face.

The study also exposes unique insights into the relationship between an organization falling victim to ransomware and their day-to-day cybersecurity practices.

About the survey

Sophos commissioned specialist research house Vanson Bourne to survey 5,000 IT managers from 26 countries during January and February 2020. Sophos had no role in the selection of respondents and all responses were provided anonymously.

COUNTRY	# RESPONDENTS
Australia	200
Belgium	100
Brazil	200
Canada	200
China	200
Colombia	200
Czech Republic	100
France	300
Germany	300

COUNTRY	# RESPONDENTS
India	300
Italy	200
Japan	200
Malaysia	100
Mexico	200
Netherlands	200
Nigeria	100
Philippines	100
Poland	100

COUNTRY	# RESPONDENTS
Singapore	200
South Africa	200
Spain	200
Sweden	100
Turkey	100
UAE	100
UK	300
U.S.	500

Within each country, 50% of respondents were from organizations of between 100 and 1,000 employees, while 50% were from organizations of between 1,001 and 5,000 employees. Respondents came from a range of sectors, both public and private.

SECTOR	# RESPONDENTS
IT, technology and telecoms	979
Retail, distribution and transport	666
Manufacturing and production	648
Financial services	547
Public sector	498
Business and professional services	480
Construction and property	272
Energy, oil/gas and utilities	204
Media, leisure and entertainment	164
Other	542

Executive summary

IT teams are showing progress in many battles

- **IT teams are on top of patching.** Three quarters of IT teams apply patches to desktops, servers, applications, and internet-facing assets within a week of release. Servers and internet-facing assets are patched most quickly, with 39% of respondents patching them within 24 hours.
- **Prevention is prioritized.** On average, IT teams dedicate nearly half their time (45%) to prevention, with 30% of time spent on detection and the remaining 25% on response.
- **IT managers are keeping up to date with cybersecurity.** The majority say that they (72%) and their teams (72%) are up to date with or ahead of cybersecurity threats. Just 11% think they are significantly behind.

Improving cybersecurity requires people – who are in short supply

- **There is an urgent need for human-led threat hunting.** 48% of respondents have already incorporated human-led threat hunts in their security procedures and a further 48% plan to implement it within a year.
- **The cybersecurity skills shortage is directly impacting protection.** Over a quarter (27%) of managers said their ability to find and retain skilled IT security professionals is the single biggest challenge to their ability to deliver IT security, while 54% say it is a major challenge.

Organizations are changing the way they deliver security

- **Outsourcing IT security is rising fast.** Currently 65% outsource some or all of their IT security efforts. This is set to rise to 72% by 2022. The percentage of organizations that exclusively uses in-house staffing will drop from 34% to 26%.
- **Improving operational efficiency is a key priority.** Four in ten (39%) respondents said that improving operational efficiency and scalability is one of their biggest priorities for the IT team this year.

Ransomware victims display different behaviors and attitudes to those who haven't been hit

- **Ransomware victims are more exposed to infection from third parties.** 29% of organizations hit by ransomware in the last year allow five or more suppliers to connect directly to their network – compared with just 13% of those that weren't hit by ransomware.
- **Ransomware damages professional confidence.** IT managers whose organizations were hit by ransomware are nearly three times more likely to feel 'significantly behind' on cyberthreats than those that weren't (17% vs. 6%).
- **Being hit accelerates implementation of human-led threat hunting.** 43% of ransomware victims plan to implement human-led hunting within six months, compared with 33% of those that didn't suffer an attack.
- **Victims have learnt the importance of skilled security professionals.** Over one third (35%) of ransomware victims said recruiting and retaining skilled IT security professionals is their single biggest challenge when it comes to cybersecurity, compared with just 19% who hadn't been hit.

IT teams are showing progress in many battles

Let's start with good news: IT teams are managing to stay on top of many aspects of cybersecurity. They are successfully keeping multiple plates spinning at once, and in doing so protecting their organizations against myriad threats.

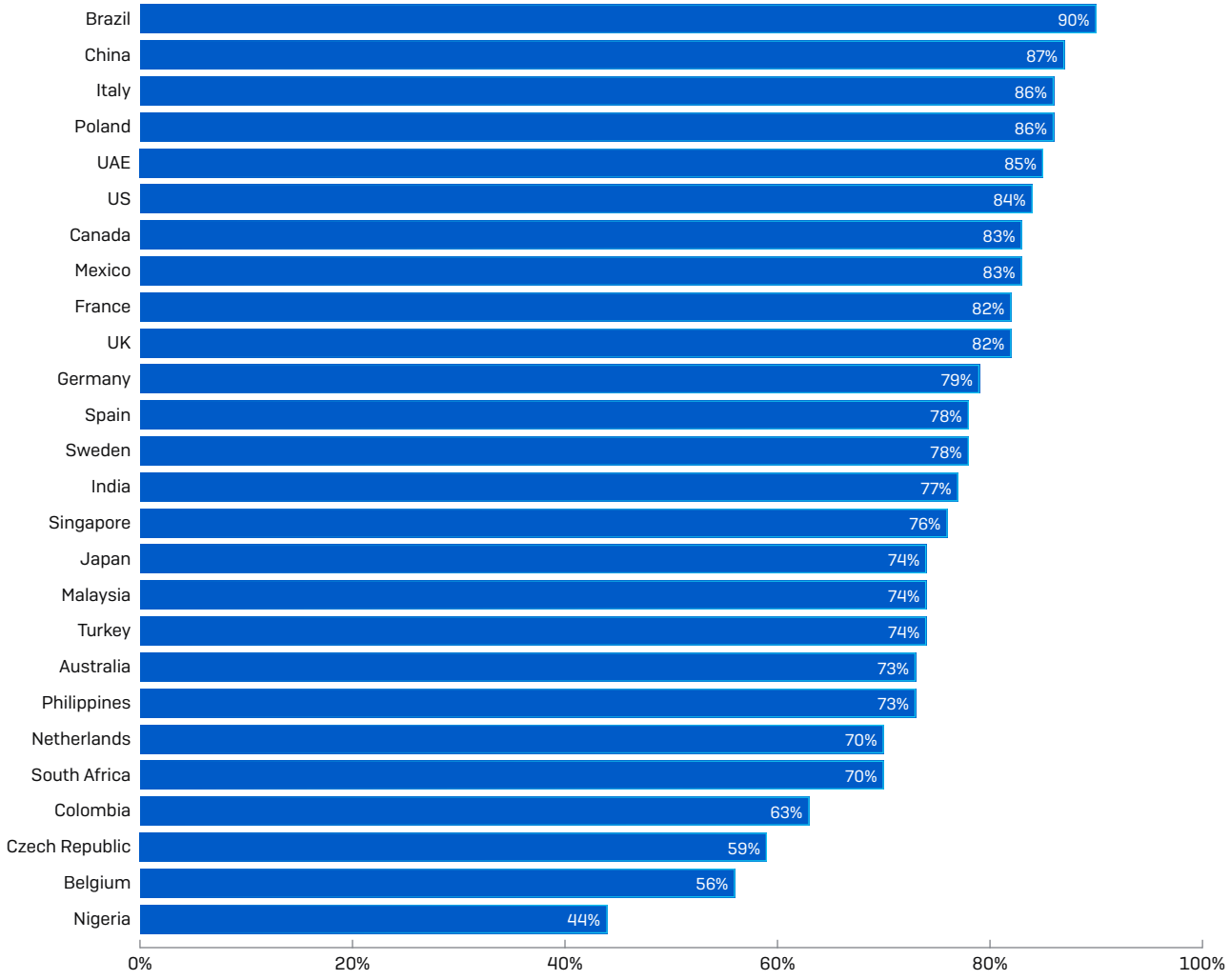
IT teams are on top of patching

"Patch early. Patch often." is a common mantra from security experts and it's one that IT teams have taken to heart. Survey respondents are alert to the need to patch quickly, with many applying patches within 24 hours of release, and three quarters doing so within a week of release. Servers and internet-facing assets are patched most quickly, with 39% of respondents patching them within 24 hours.

	PATCHED WITHIN 24 HOURS	PATCHED WITHIN A WEEK	PATCHED WITHIN A MONTH
Desktops	36%	41%	14%
Servers	39%	38%	14%
Applications	36%	40%	15%
Internet-facing assets	39%	38%	14%

However, 22% admit to taking over a week to apply desktop patches, with respondents in Nigeria, Belgium and the Czech Republic taking the longest time to patch.

Percentage of respondents that apply patches to desktops within a week of release

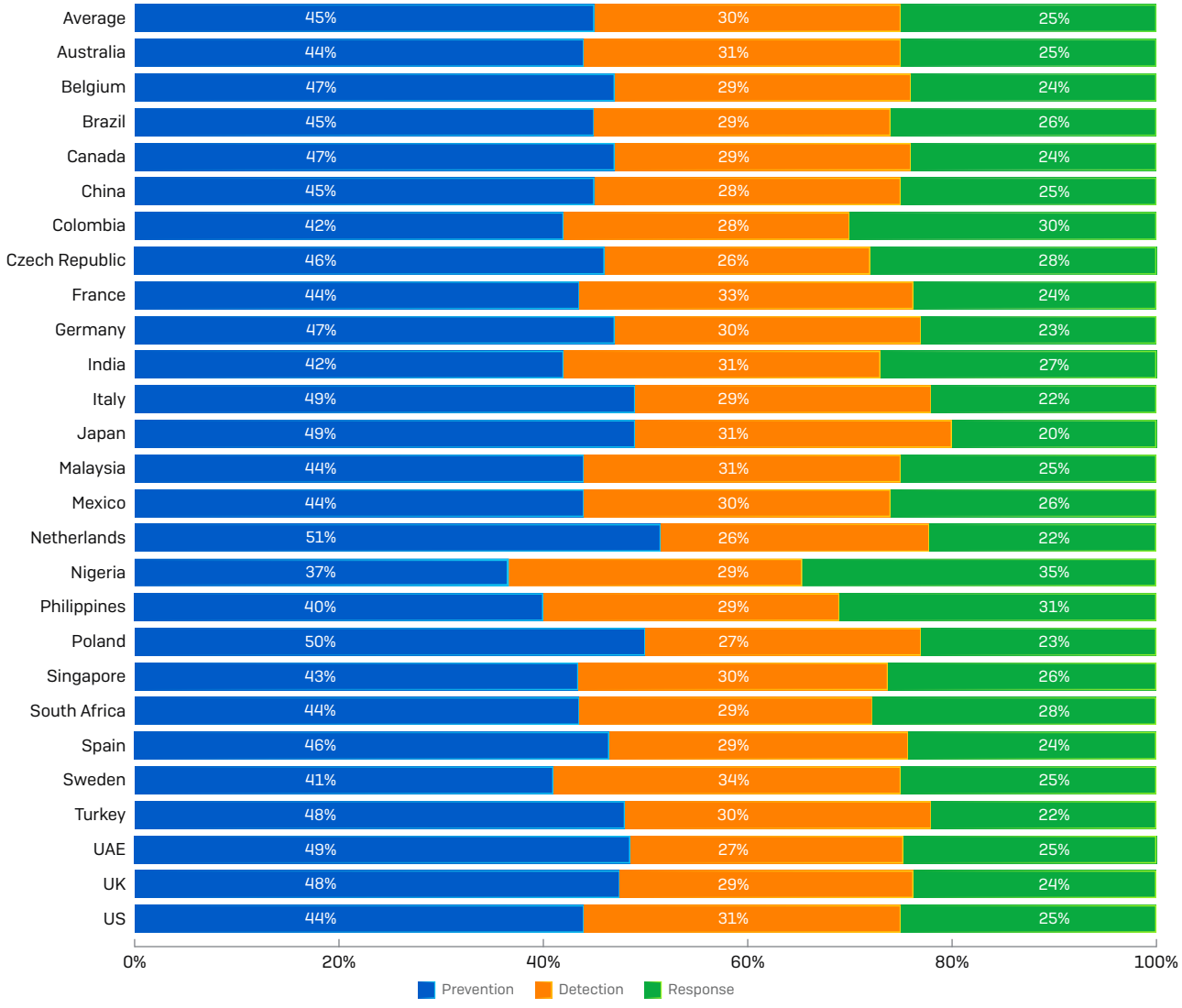


Prevention is prioritized

On average, IT teams dedicate nearly half their time (45%) to prevention, with 30% of time spent on detection and the remaining 25% on response. The data did reveal some regional variations: of the countries surveyed, IT teams in the Netherlands report the highest amount of time spent on prevention (51%); Swedish IT teams spend the most time on detection (34%); and Nigerian organizations report the highest percentage of time spent on response (35%).

While balancing prevention and detection is a sensible approach to cybersecurity, spending considerable time on response generally suggests failure to stop incidents. High scores for response indicate that an organization is experiencing a high number of incidents, that incidents are only being detected at a late stage, or both.

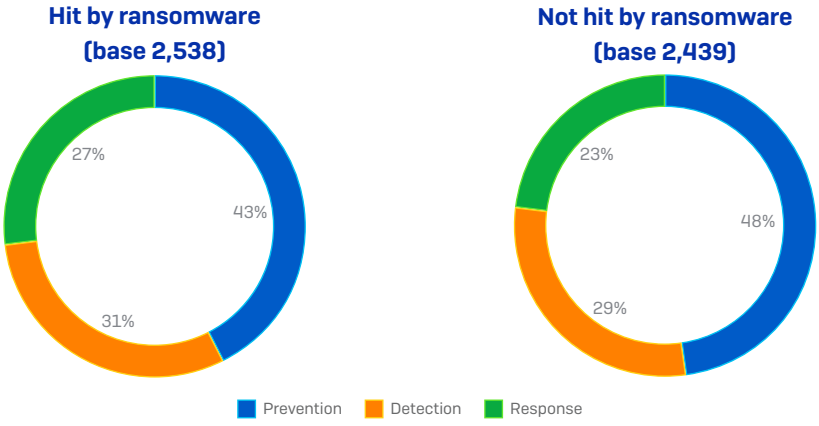
Time split between prevention, detection and response



Due to rounding, occasionally the totals do not add up to 100%

Ransomware victims spend less time on prevention and more time on response

51% of survey respondents admitted that their organization had been hit by ransomware in the preceding twelve months. Organizations that had fallen victim to ransomware put more focus on detection and response than those that hadn't. Conversely, organizations that had not been hit by ransomware spend more time on prevention than those that had fallen victim.



It may be that this increased focus on prevention has helped the organizations that weren't hit to prevent the attacks: strong defenses always start with the best protection. At the same time, ransomware victims may be more alert to the complex, multi-stage nature of advanced attacks so put greater resource into detecting and responding to the tell-tale signs that an attack is imminent.

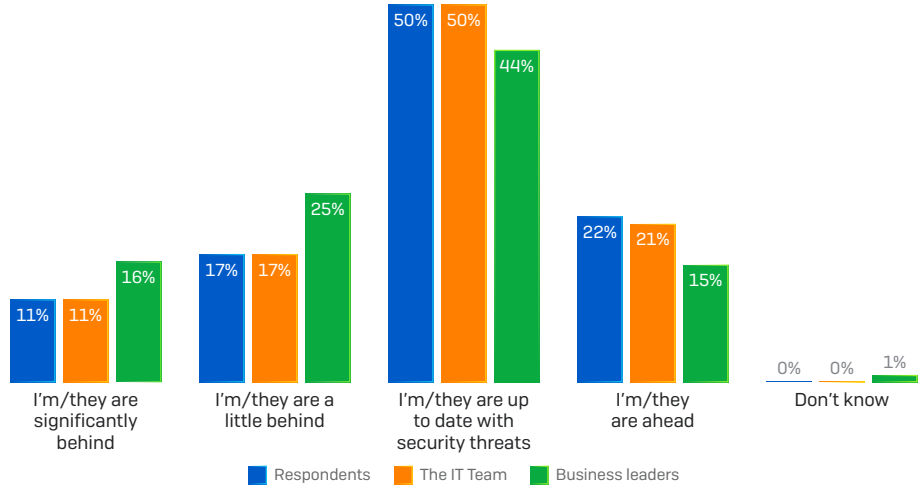
For more information on how to identify that ransomware attackers have you in their sights, read the SophosLabs article Five signs you're about to be attacked.

IT managers are keeping up to date with cybersecurity

Despite the fast-changing nature of cybersecurity threats, IT professionals think they are succeeding in staying up to date with cyberthreats. Most IT managers feel they (72%) and their teams (72%) are up to date with or ahead of cybersecurity threats. Of the 28% of IT managers who feel they are behind, 17% feel they are only a little behind, while just 11% think they are significantly behind.

These numbers mask notable regional variations: respondents in Poland, Mexico and Turkey were most likely to say they felt ahead of cyberthreats (39%, 34% and 31% respectively), while those in Nigeria (60%), Sweden (57%), and Germany (49%) were most likely to say they are behind. It's worth noting that these data points are the respondents' perceptions (and therefore there is likely a cultural impact) and not an actual measure of how up-to-date people are.

How up to date respondents feel people in their organization are with cybersecurity threats



While IT managers are generally confident that they and their team are up to date, 41% of IT managers feel their business leaders are behind (25% a little behind, 16% significantly behind). In many ways this gap is understandable – business leaders rarely specialize in cybersecurity – however it highlights the challenge IT teams face in getting leadership to understand cybersecurity risks and associated investment requests.

Ransomware attacks damage the confidence of IT professionals

Diving into the data we see that ransomware attacks inflict considerable damage on the confidence of IT managers and their teams, over and above any business impact.

Nearly three times as many IT managers whose organizations were hit by ransomware last year feel they are 'significantly behind' on cyberthreats, compared with IT managers whose organizations weren't hit (17% vs. 6%). This lower confidence carries through to the IT manager's perception of both the IT team and business leaders, as illustrated in the below table.

	IS SIGNIFICANTLY BEHIND ON CYBERTHREATS (%)	IS UP TO DATE ON CYBERTHREATS (%)
IT Managers (respondents)		
Hit by ransomware	17%	43%
Not hit by ransomware	6%	57%
IT Teams (respondent perception)		
Hit by ransomware	15%	43%
Not hit by ransomware	6%	58%
Business leaders (respondent perception)		
Hit by ransomware	20%	39%
Not hit by ransomware	11%	49%

Again, it's important to remember that these responses are the perception of the survey respondent rather than a measure of how up to date they actually are. It may be that being hit by ransomware is a reality check and, as a result of their experiences, ransomware victims have a far more accurate understanding of the situation.

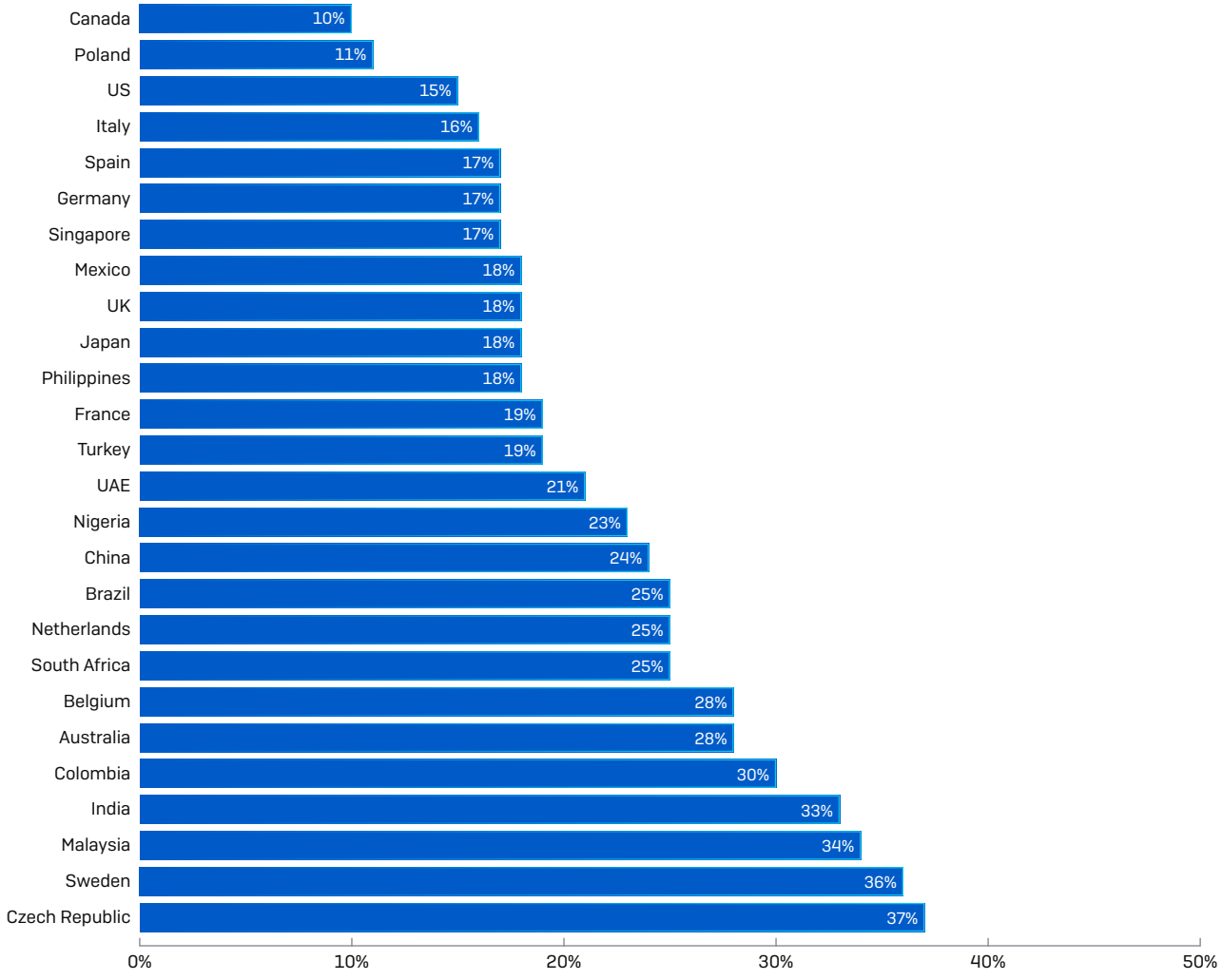
Improving cybersecurity requires people – who are in short supply

Although IT teams are winning many battles, the war is far from won. Despite the best efforts of IT leaders and their teams, cyberthreats remain an ever-present challenge – to the extent that just over half of all respondents (51%) said minimizing the risk of a cyberattack is a priority focus area for the coming 12 months. The reasons for this become clear when we look at the wide range of security challenges IT teams face.

IT teams are up against a constant barrage of cyberattacks, with threats coming from multiple directions and with varying targets. As previously mentioned, 51% of respondents were hit by ransomware in the last year and the criminals succeeded in encrypting data in 73% of these attacks*. Cloud security is also a challenge with 70% of organizations that host data or workloads in the public cloud experiencing a security incident in the last year**.

Another challenge IT teams face is securing third party organizations that can connect directly to their network, such as accounting services or IT providers. On average, respondents report having three suppliers who can connect to their systems. However, one in five respondents (21%) – rising to a third (or more) in the Czech Republic, India, Malaysia and Sweden – lets five or more suppliers connect. Conversely, in Canada and Poland just one in ten respondents reported having five or more suppliers with remote access.

Percentage of organizations with five or more suppliers that can connect directly to the network



Enabling third party suppliers to connect to the network inherently introduces security risk, as well as business benefits. The more suppliers that can connect, the greater the challenge and workload for IT teams.

Ransomware victims are more exposed to infection from third parties

Of those organizations hit by ransomware in the last year, 29% allow five or more suppliers to connect directly to their network – compared to 13% for those that weren't hit. With third party suppliers cited as the entry method by 9% of the attack victims, this is clearly as major vector of attack.

While there are many strong business reasons for enabling outside organizations to connect to your network, the clear takeaway is that securing your supply chain should be a key priority for everyone adopting this approach. Strong cybersecurity needs to be an essential criterion for anyone looking to connect to your network.

There is an urgent need for human-led threat hunting

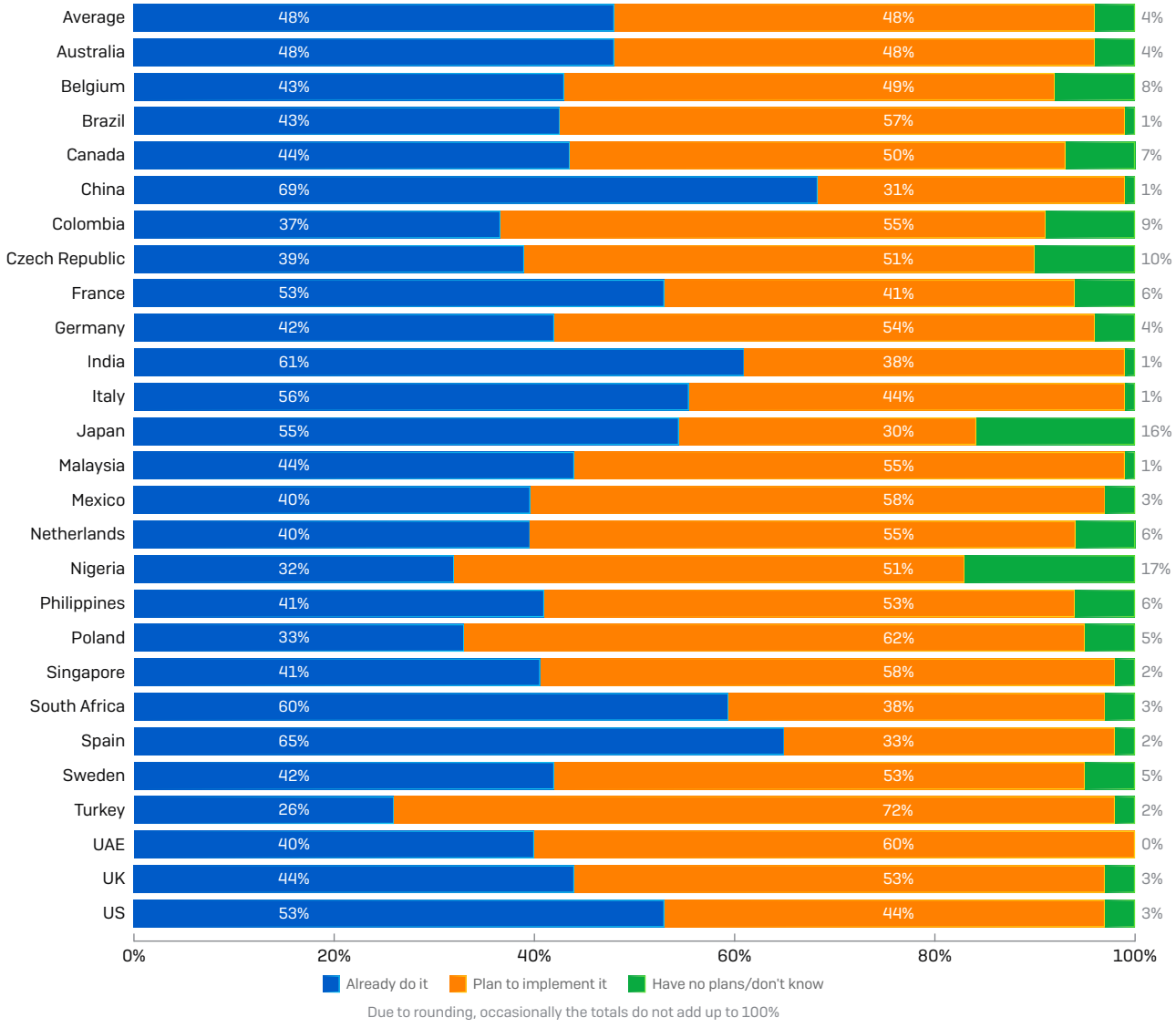
The most devastating cyberthreats generally involve human-led attacks, often exploiting legitimate tools and processes such as PowerShell. Hands-on live hacking enables attackers to modify their tactics, techniques, and procedures (TTPs) on the fly to bypass security products and protocols. Once inside a victim's network attackers can move laterally, exfiltrate data, install malware and backdoors for future attacks, and deploy ransomware.

While technology, particularly intelligent automated technology, has an important role to play, expert operators are still required. Stopping human-led attacks requires human-led threat hunting.

Virtually all the survey respondents appreciate the need for this approach: 48% already incorporate human-led threat hunts in their security procedures to identify attacker activity that may not be detected by security tools (e.g. SIEM, endpoint protection, firewall, etc.). A further 48% plan to implement it. Respondents are also alert to the urgency of deploying human-led hunting, with virtually all (99.6%) respondents who want to implement it looking to do so within the next year.

The status of human-led threat hunting varies significantly by geography. 69% of respondents from China have already implemented this approach, closely followed by Spain (65%), India (61%) and South Africa (60%). Conversely, Turkey has been slowest to adopt human-led hunting with just 26% of respondents already doing it, with Nigeria (32%) and Poland (33%) only slightly ahead.

Plans to incorporate human-led threat hunts

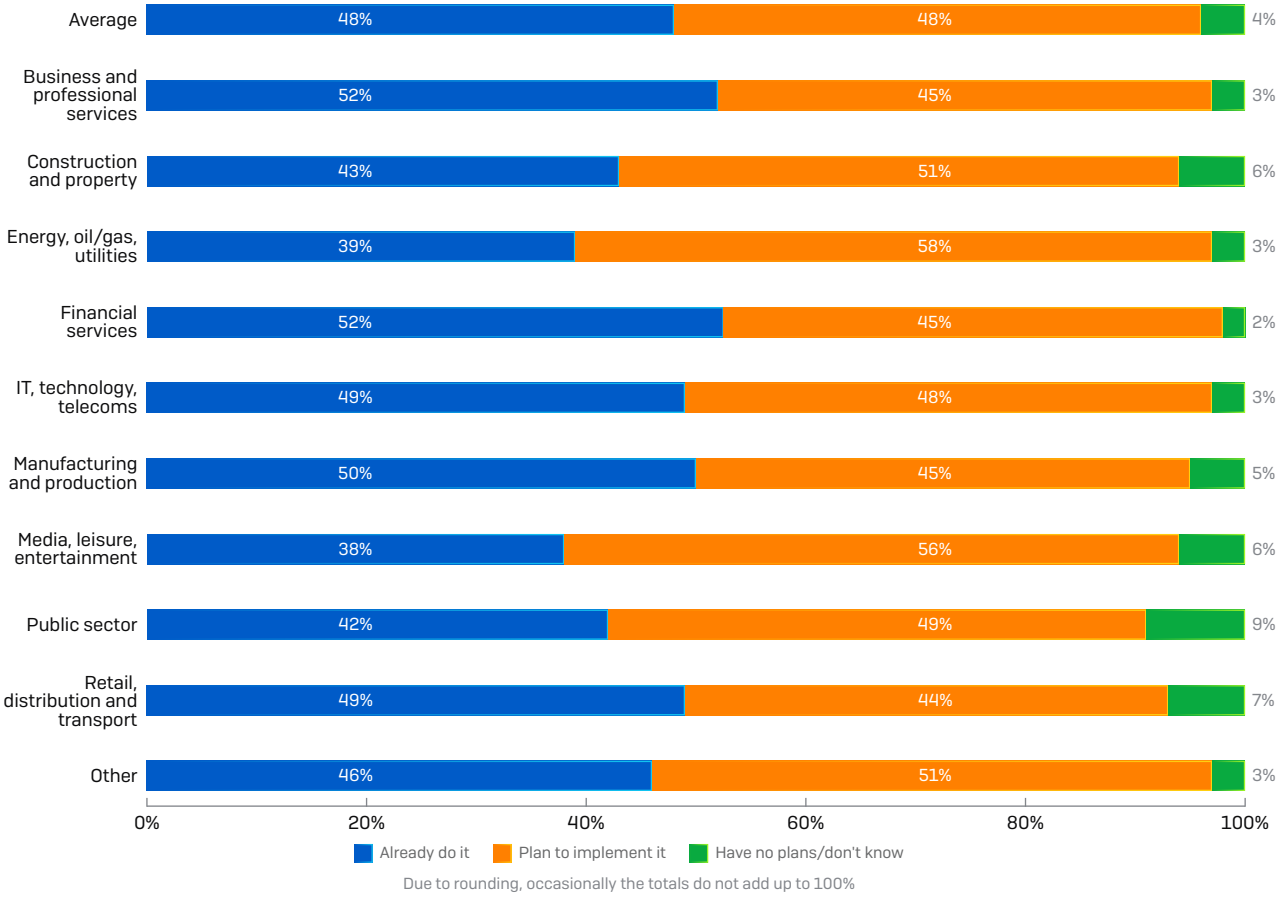


Due to rounding, occasionally the totals do not add up to 100%

The survey also revealed different levels of readiness by industry. Business and professional services and financial services are leading the implementation of human-led hunting with 52% of respondents in each industry saying that their organization is already using this approach.

In contrast respondents in both media, leisure and entertainment (38%), and the energy, oil/gas and utilities sectors (39%) are less likely to report that they are currently doing human-led threat hunting. Given the energy sector is a potential target for nation-state attacks, its vulnerability to human-led threats is concerning.

Plans to incorporate human-led threat hunts by industry

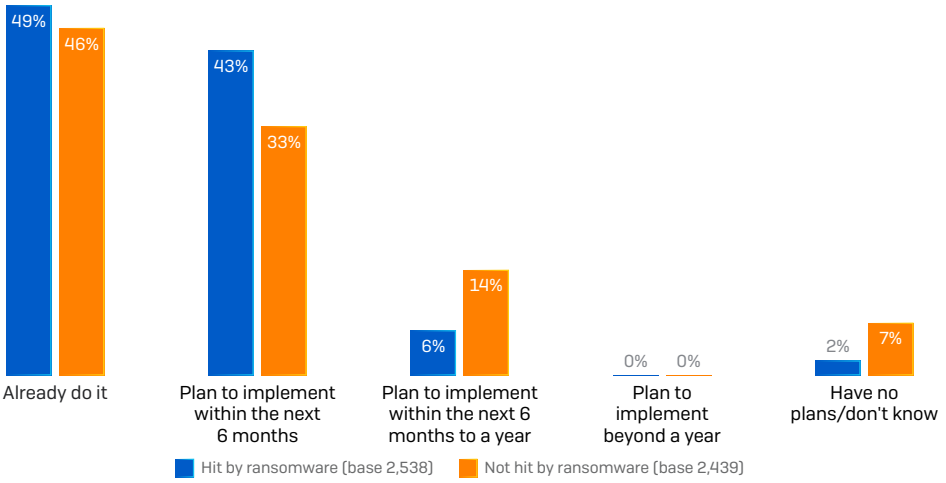


Due to rounding, occasionally the totals do not add up to 100%

Being hit by ransomware accelerates implementation of human-led threat hunting

Being hit by ransomware has little overall impact on an organization's desire to incorporate human-led threat hunts however it does drive urgency in implementation. 43% of ransomware victims plan to implement human-led threat hunting within six months, compared with 33% for those that didn't suffer an attack. This data suggests that ransomware victims are highly motivated to avoid a repeat incident.

Impact of a recent ransomware experience on the implementation of human-led threat hunting



The cybersecurity skills shortage is directly impacting protection

81% of survey respondents said their ability to find and retain skilled IT security professionals is a major challenge to their organization's ability to deliver IT security: 54% said it is a significant challenge while over a quarter (27%) report it is their single biggest challenge.

Every country reported challenges with recruiting skilled IT staff. In Italy (94%), India (93%), and Brazil and Colombia (both 92%), over nine in ten respondents said that their ability to find and retain skilled staff was a major barrier to protecting the organization from cyberthreats.

Even in South Africa, the country that is least likely to report cybersecurity staff recruitment as a challenge, over six in ten (62%) respondents say that it is causing them major issues.

To what extent is recruiting and retaining skilled IT security professionals a challenge to your organization's ability to deliver IT security?

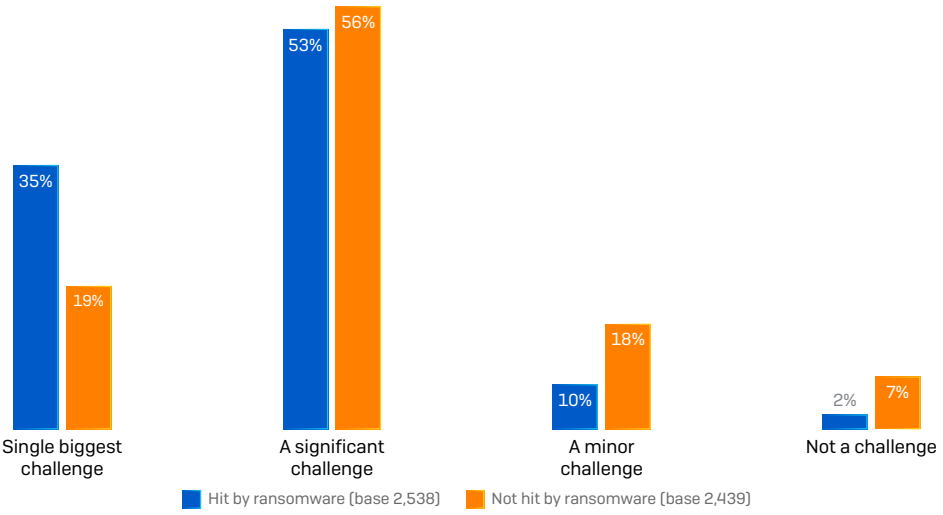
COUNTRY	IT'S OUR SINGLE BIGGEST CHALLENGE	IT'S A SIGNIFICANT CHALLENGE, BUT NOT THE BIGGEST	IT'S A MINOR CHALLENGE	IT'S NOT A CHALLENGE	DON'T KNOW
Average	27%	54%	14%	4%	0%
Australia	17%	57%	22%	5%	0%
Belgium	24%	52%	24%	0%	0%
Brazil	45%	47%	6%	3%	1%
Canada	19%	55%	18%	7%	2%
China	24%	54%	18%	4%	0%
Colombia	29%	63%	8%	1%	0%
Czech Republic	33%	47%	18%	1%	1%
France	23%	62%	11%	4%	0%
Germany	19%	63%	14%	5%	0%
India	58%	35%	6%	1%	0%
Italy	28%	67%	5%	2%	0%
Japan	35%	44%	17%	4%	1%
Malaysia	26%	54%	16%	4%	0%
Mexico	27%	62%	6%	6%	0%
Netherlands	26%	49%	25%	0%	1%
Nigeria	32%	51%	16%	1%	0%
Philippines	40%	49%	8%	2%	1%
Poland	9%	59%	20%	12%	0%
Singapore	17%	72%	10%	2%	0%
South Africa	22%	40%	19%	19%	0%
Spain	17%	58%	17%	8%	1%
Sweden	44%	41%	13%	1%	1%
Turkey	30%	52%	9%	8%	1%
UAE	22%	62%	15%	1%	0%
UK	14%	64%	20%	2%	0%
US	26%	49%	17%	8%	0%

Ransomware victims have learnt the hard way the importance of skilled security professionals

Falling victim to a cyberattack has a major impact on attitudes to cybersecurity staffing. Over one third (35%) of respondents that had fallen victim to ransomware in the last year said that recruiting and retaining skilled IT security professionals is their single biggest challenge when it comes to cybersecurity, and a further 53% said it is a significant challenge.

Conversely, among those organizations that had not been hit by ransomware in the last year just 19% said bringing in and keeping skilled staff was their biggest challenge – a full 16% points difference.

The extent recruiting and retaining skilled IT security professionals is a challenge to the organization's ability to deliver IT security



It is likely that there are several factors behind these varying attitudes. Firstly, the consequences of limited security skills are still fresh in the minds of those who have recently suffered the financial, operational and reputational cost of being held to ransom.

In addition, ransomware victims will invariably have investigated the source of the attack. In doing so they will have identified the gaps in their defenses that enabled the attackers to penetrate their organizations and access their data. Many will likely have identified a shortage of human expertise as a contributing factor to falling victim to attack.

Recruitment is the #1 priority for IT managers

A consequence of this skills shortage is that recruiting and retaining staff took number one spot in the list of priorities for IT managers. A full 55% of respondents said it's one of their focus areas for the next 12 months, pushing minimizing the risk of a cyberattack into second position. (Note: respondents could select multiple responses to this question).

Organizations are changing the way they deliver security

IT professionals are unlikely to be surprised by the resourcing challenge. Cybersecurity recruitment has been an ongoing issue for many years and, while it's heartening that managers are prioritizing resourcing, the scale of the challenge suggests that there will not be a quick fix.

Viewed through this lens, the changes IT managers are making to the way cybersecurity is delivered and their focus on improving efficiency and scalability can be considered a direct response to the resourcing challenge.

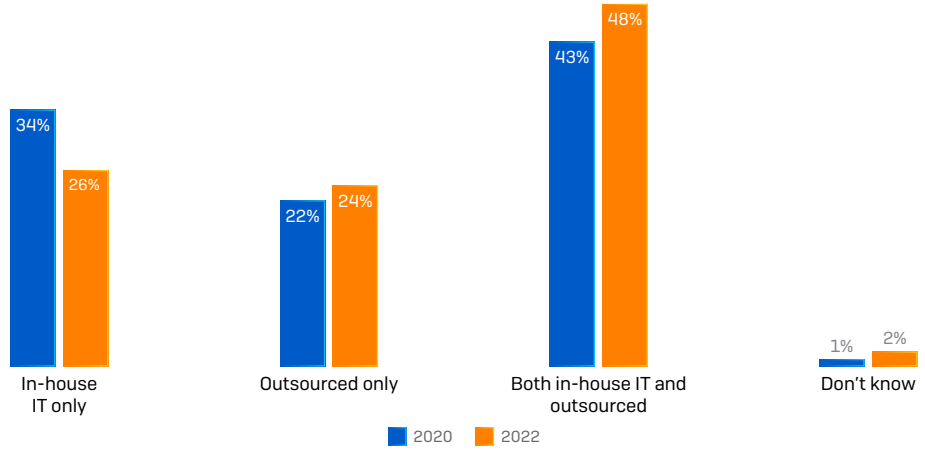
Outsourcing is growing fast

Outsourcing cybersecurity enables organizations to benefit from the expertise of security professionals without having to recruit them directly. It also often provides access to higher levels of security competency than organizations would otherwise have, thanks to the ability of security service providers to nurture and develop specialist skills.

Outsourcing IT security is already the norm, with 65% doing it in some capacity: 43% use a combination of in-house and outsourcing while 22% wholly outsource their IT security. The survey revealed regional variations. Top of the outsourcing list are China (76%), the UAE (74%), and Malaysia and Singapore (both 73%) where around three quarters of respondents already include outsourcing in their IT security delivery. At the other end of the scale, in Belgium (52%), France (54%) and Nigeria (54%) just over half of respondents are currently using third party security providers.

The global trend is for outsourcing to increase over the next two years, from the current 65% to almost three quarters (72%) in 2022. The biggest change will be in the percentage of organizations that exclusively use in-house staffing: this is set to drop from 34% to 26%. There will be increases both in the percentage that fully outsource their IT security and in those that use a combination of in-house and outsourced expertise.

How organizations deliver IT security



These global numbers mask some interesting regional variations:

- Respondents in Spain and India plan to increase in-house only IT security management – while the numbers are relatively small (from 34% to 37% in Spain, and from 33% to 34% in India) it is interesting that they plan to buck the global trend
- In the Philippines almost half of respondents (48%) plan to exclusively outsource IT security in 2022 – a huge jump from 30% today. Other countries that plan higher-than-average adoption of the outsourced-only approach are the Czech Republic, Nigeria and Sweden (all 35%) and Australia (34%)
- Over six in ten respondents plan to run a combined in-house and outsourced approach in China (67%) and Mexico (62%)

IT managers are focused on improving efficiency and scalability

Another response to the shortage of IT security expertise is to find ways to make more out of the skills that you do have. Four in ten (39%) respondents said that improving operational efficiency and scalability is one of their biggest priorities for the IT team this year. European and Japanese respondents pulled down this average, while in China, Malaysia and South Africa over half of respondents have it on their priority list.

Conclusion

These insights from 5,000 IT managers across 26 countries have shone a light on the challenges that IT teams face when it comes to managing and delivering IT security. While IT teams are winning many battles – notably with patching and staying up to date with cybersecurity threats – the war is far from won. IT professionals face challenges on myriad fronts: from ransomware and cloud security, to managing third party suppliers who can connect to the network.

In the face of the growth of human-led attacks, most organizations are turning to human-led threat hunting: by the end of 2020, 95% of respondents hope to be doing it in some capacity. At the same time, difficulties with the recruitment and retention of cybersecurity professionals is a limiting factor for the vast majority of organizations. Those organizations that have fallen victim to ransomware in the recent past are particularly alert to impact of this skills shortage on their ability to deliver effective cybersecurity.

There is a clear correlation between direct experience of ransomware and IT behaviors. Ransomware victims have greater exposure to infection from third parties than other organizations, and they also spend more time on response, indicating that they have more incidents to deal with. At the same time, their experiences have given them a greater appreciation of the importance of skilled cybersecurity professionals, and greater urgency in implementing human-led hunting.

In light of these challenges it is encouraging to see how IT teams are evolving their approaches. Use of outsourced experts looks set to further increase over the next two years, with almost three quarters of organizations outsourcing IT security in some capacity by 2022. There is also significant focus on increasing operational efficiency and scalability in many parts of the world, to enable IT teams to do more with the skilled professionals they do have.

Cybersecurity never stands still. IT teams deserve much credit for their success in staying on top of many aspects of security. Given the ongoing cybersecurity skills shortages, IT teams will need to find different ways to extend and enhance their defenses in the face of evolving threats, and in particular the increase in human-led attacks.

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