SOPHOS
Cybersecurity evolved.

The State of Ransomware 2021

Sophos' annual ransomware survey delivers fresh new insights into the experiences of mid-sized organizations across the globe. It explores the prevalence of attacks, as well as the impact of those attacks on victims, including year-on-year trends. This year, for the first time, the survey also reveals the actual ransom payments made by victims, as well as the proportion of data victims were able to recover after they had paid.

A Sophos Whitepaper. April 2021

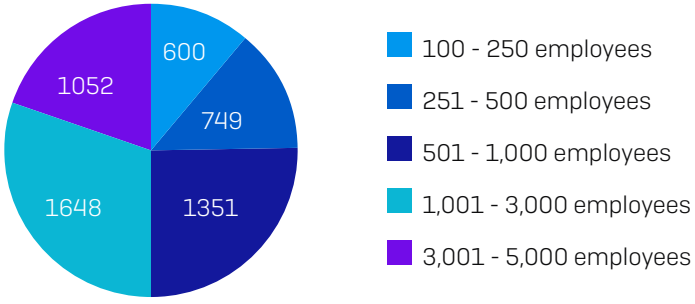
About the survey

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.

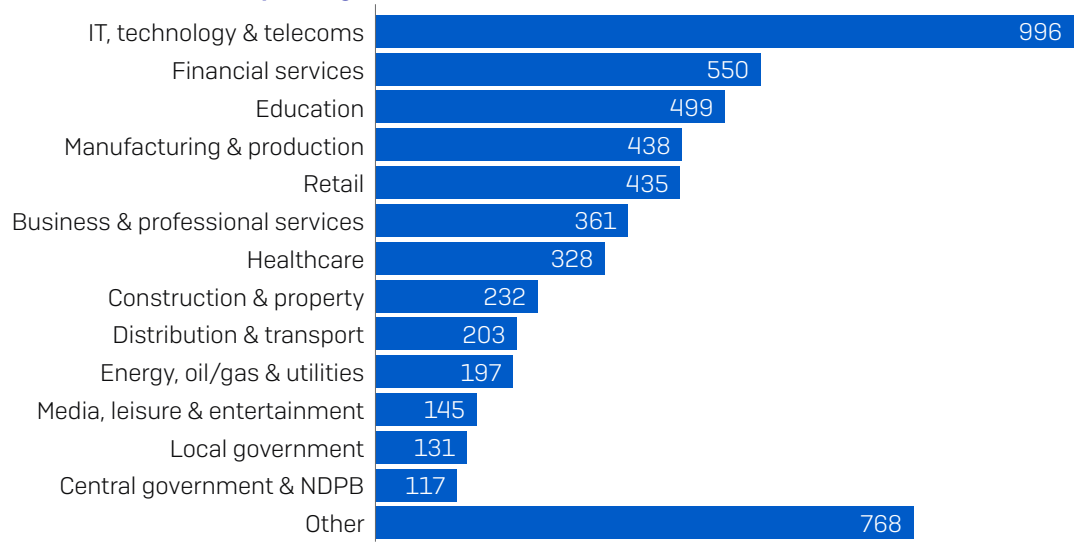
COUNTRY	# RESPONDENTS	COUNTRY	# RESPONDENTS	COUNTRY	# RESPONDENTS
Australia	250	India	300	Saudi Arabia	100
Austria	100	Israel	100	Singapore	150
Belgium	100	Italy	200	South Africa	200
Brazil	200	Japan	300	Spain	150
Canada	200	Malaysia	150	Sweden	100
Chile	200	Mexico	200	Switzerland	100
Colombia	200	Netherlands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

As in previous years, 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?



Within which sector is your organization?



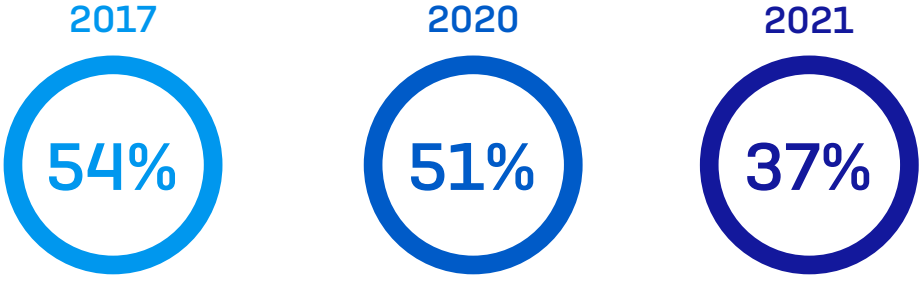
Key findings

- **37%** of respondents' organizations **were hit by ransomware in the last year**
- **54%** that were hit by ransomware in the last year said the **cybercriminals succeeded in encrypting their data** in the most significant attack
- **96%** of those whose data was encrypted **got their data back** in the most significant ransomware attack
- The **average ransom paid** by mid-sized organizations was **US$170,404**
- However, on average, only **65% of the encrypted data was restored** after the ransom was paid
- The **average bill for rectifying a ransomware attack**, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. was **US$1.85 million**
- **Extortion-style attacks** where data was not encrypted but the victim was still held to ransom **have more than doubled** since last year, up from 3% to 7%
- Having **trained IT staff who are able to stop attacks** is the most common reason some organizations are confident they will not be hit by ransomware in the future

The prevalence of ransomware

Ransomware remains a major threat

37% of organizations – over a third of the 5,400 surveyed – were hit by ransomware last year, defined as **multiple computers being impacted by a ransomware attack, but not necessarily encrypted**. While this is a high number, the good news is that it is a significant reduction on last year, when 51% said they'd been hit.

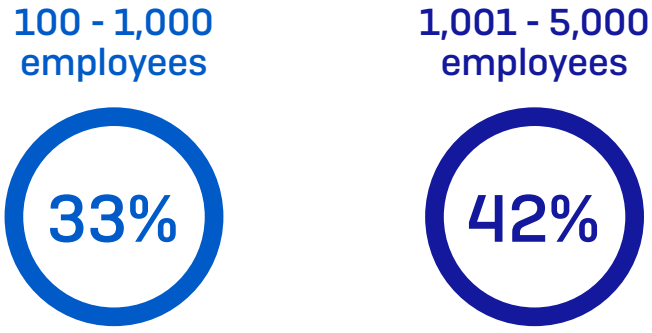


In the last year, has your organization been hit by ransomware? Yes [2021=5,400; 2020=5,000; 2017=2,700] omitting some answer options, split by year

Changes in attacker behaviors observed by SophosLabs and the Sophos Managed Threat Response teams indicate that the reduction in the number of attacks could be due in part to evolving attack approaches. For instance, many attackers have moved from larger scale, generic, automated attacks to more targeted attacks that include human operated, hands-on-keyboard hacking. While the overall number of attacks is lower, our experience shows that the potential for damage from these targeted attacks is much higher.

Larger organizations are more likely to be hit

Looking at the number of ransomware incidents by organization size, we see that larger organizations reported a greater prevalence of attacks, with 42% of the 1,001-5,000 employee group admitting to having been hit, compared with 33% of the smaller companies.

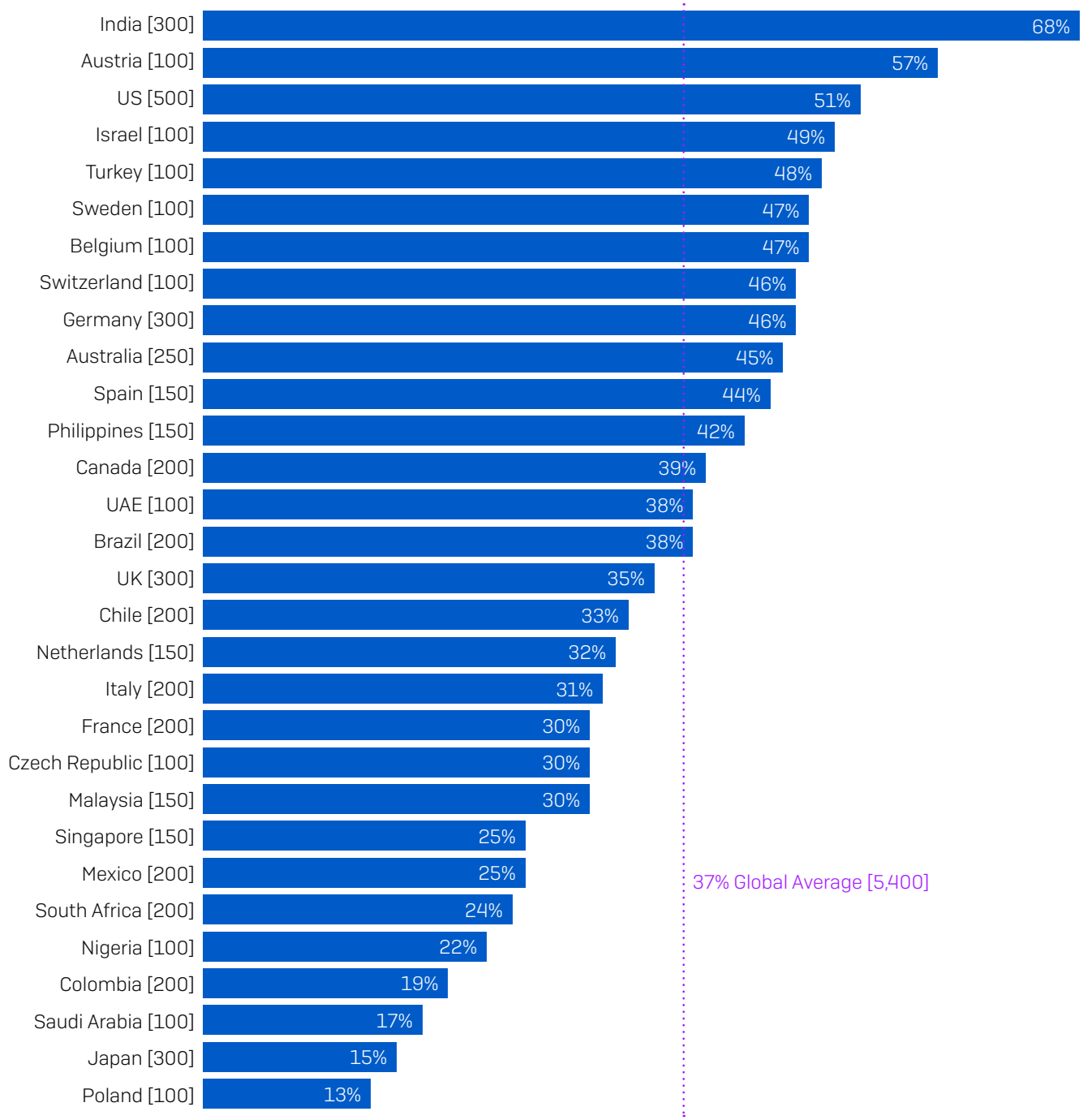


In the last year, has your organization been hit by ransomware? Yes [5,400] omitting some answer options, split by size of organization

This year the gap between the smaller and larger organizations has also widened from seven percentage points in 2020 to nine percentage points. The increased attacker focus on larger organizations is perhaps not surprising: bigger companies are likely to have more money, and therefore be a more lucrative target. That said, one in three smaller organizations were hit by ransomware in the last year, confirming that they remain very much on the radar of the attackers. There are no winners here.

Attack levels vary across the globe

Analyzing the data based on the country the respondent was located in reveals some interesting results.



In the last year, has your organization been hit by ransomware? Yes [base numbers in chart] omitting some answer options, split by country

India has the dubious honor of topping the list with 68% of respondents reporting that they were hit by ransomware last year. While the ransomware actors that make the headlines are often based out of China, North Korea, Russia, and other former Eastern Bloc countries, SophosLabs sees high levels of domestic ransomware in India, i.e., Indian adversaries attacking Indian companies.

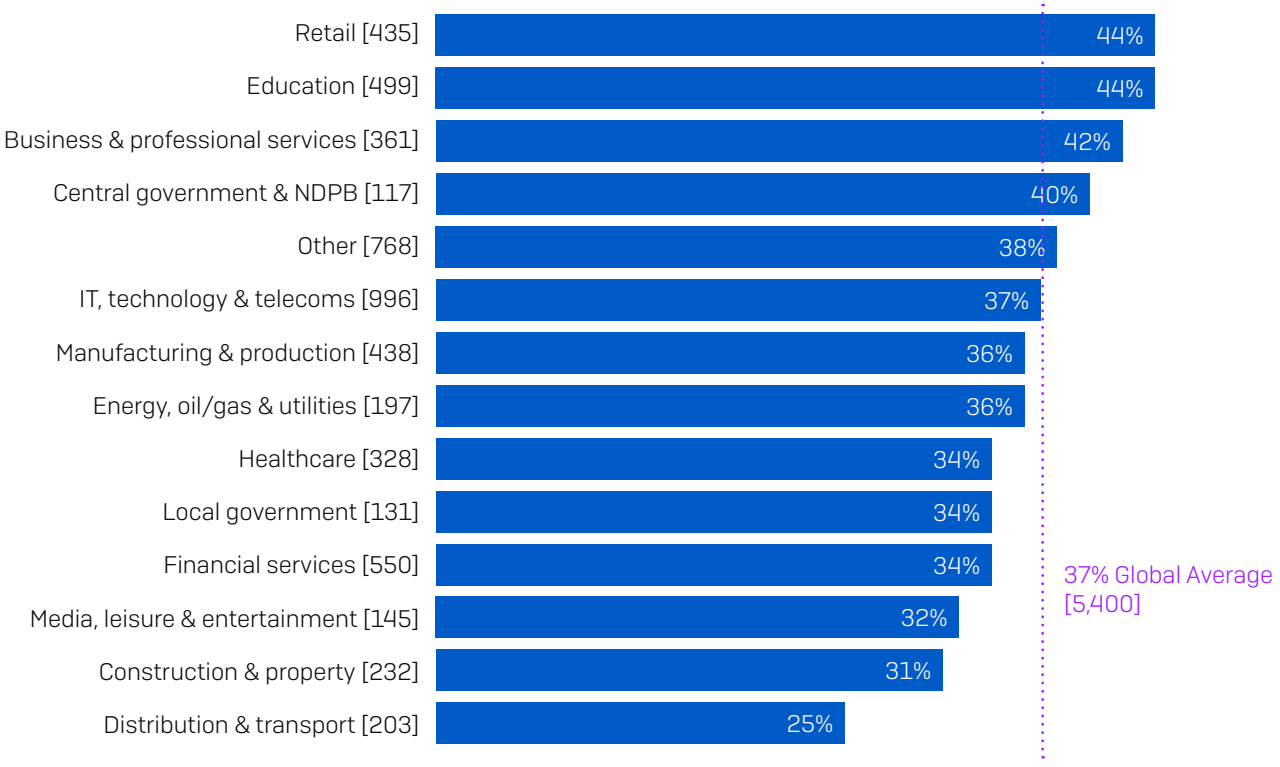
The **U.S.** is a very popular target with cybercriminals due to the perceived potential to demand high ransom payments and just over half – 51% – of US respondents report being hit last year.

Poland, Colombia, Nigeria, South Africa, and **Mexico** report some of the lowest levels of attack, which is likely a result of lower GDP and therefore lower ransom potential for the attackers.

Japan stands out as a developed economy with very low levels of ransomware – just 15% of respondents reported being hit by ransomware last year. Japan traditionally reports very low ransomware levels in our annual surveys. It may be that Japanese organizations have invested heavily in anti-ransomware defenses, or that the unique nature of the Japanese language makes it a more challenging target for adversaries.

Retail and education suffer the most ransomware attacks

Looking at the level of attacks by sector, we see considerable variation in the propensity to be hit by ransomware across different industries.



In the last year, has your organization been hit by ransomware? Yes [base numbers in chart] omitting some answer options, split by sector

Retail and **education** experienced the highest level of attacks, with 44% of respondents in these sectors reporting being hit.

Healthcare, which often hits the headlines for ransomware attacks, actually reported slightly below average levels of attacks, with 34% of respondents saying their organization was hit. The sector's over-representation in news reports is likely due to regulatory obligations that require healthcare organizations to reveal an attack, while many commercial organizations can keep them private.

The impact of ransomware

Encryption is down. Extortion is up.

We asked the organizations hit by ransomware whether the criminals succeeded in encrypting the data. 54% said yes. 39% were able to stop the attack before their data could be encrypted, while 7% said that their data was not encrypted but they were held to ransom anyway.

When we compare these numbers with the findings from our 2020 survey a very interesting story appears.

2020	2021	
73%	54%	Cybercriminals succeeded in encrypting data
24%	39%	Attack stopped before the data could be encrypted
3%	7%	Data not encrypted but victim still held to ransom

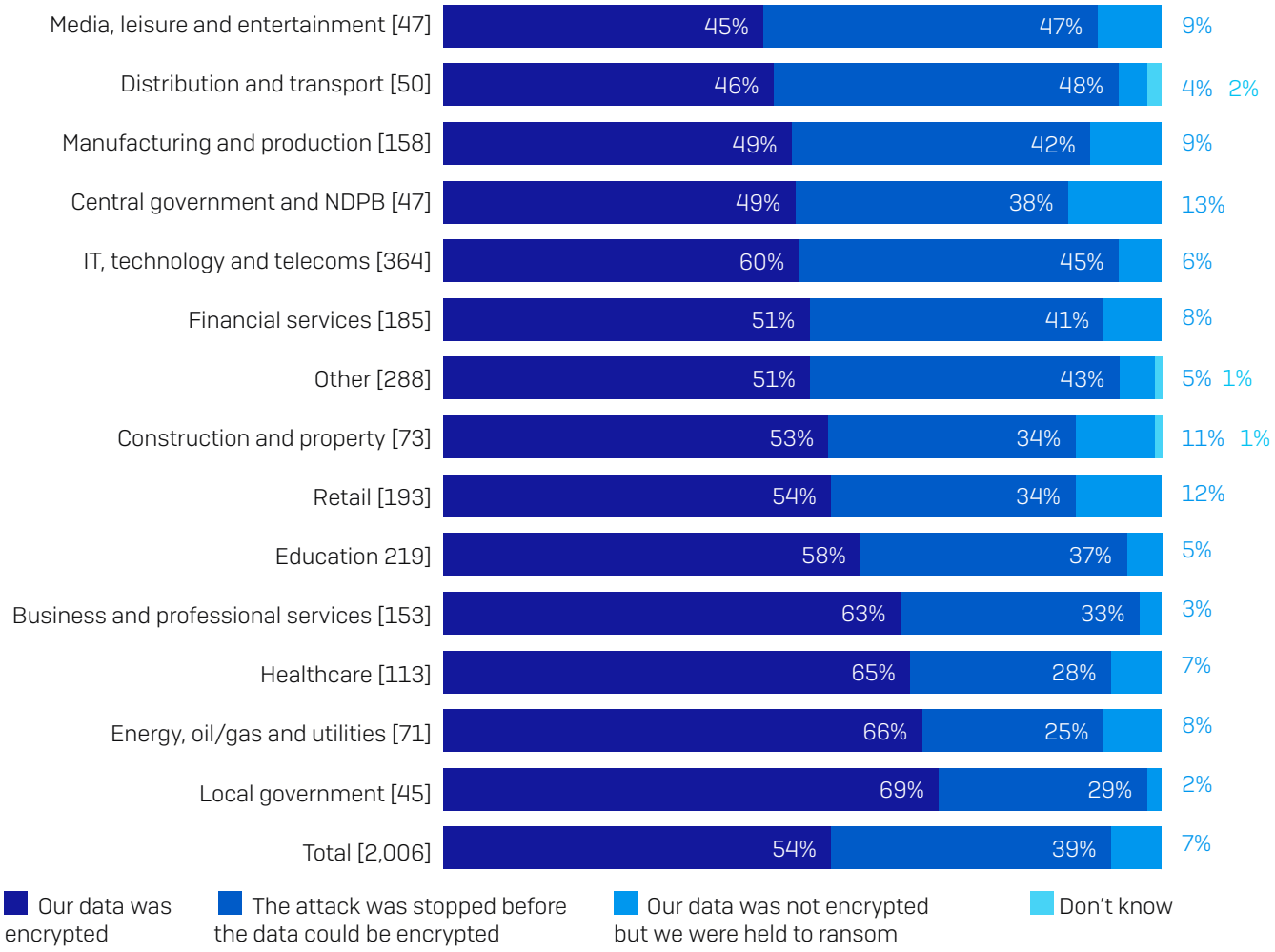
Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? [2021=2,006, 2020=2,538] organizations that had been hit by ransomware in the last year

Firstly, over the last year there has been a large drop in the percentage of attacks where the criminals succeed in encrypting data, down from 73% to 54%, with many more organizations now able to stop the attack before the data could be encrypted. This indicates that the adoption of anti-ransomware technology is paying off.

However, we also see that the percentage of attacks where data was not encrypted but the victim was still held to ransom has more than doubled. Some attackers are moving to extortion-style attacks where instead of encrypting files they steal and then threaten to publish data unless the ransom demand is paid. This requires less effort on their part – no encryption or decryption needed. Adversaries often leverage the punitive fines for data breaches in their demands in a further effort to make victims pay up.

Ability to stop encryption varies greatly by sector

When it comes to stopping the encryption of files, some sectors are far more successful than others.



Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? [base numbers in chart] organizations that have been hit by ransomware in the last year

Distribution and transport is the sector most able to stop attackers encrypting files (48%), closely followed by **media, leisure, and entertainment** (47%).

Conversely, **local government** is the sector where organizations are most likely to have their data encrypted in a ransomware attack (69%). This is probably due to the double whammy of:

- Weaker defenses: In general, local government organizations struggle with lower IT budgets and stretched/limited IT staff.
- Increased attacker focus: Due to their size and access to public funds, government organizations are often considered lucrative targets, and therefore the focus for more sophisticated attacks. Plus – as we'll see later – local government is also the sector with the second highest propensity to pay the ransom.

Central government and non-departmental public bodies (NDPB) is the sector most likely to experience extortion (13%).

Healthcare, as we've seen, experiences a below-average number of attacks. However, attackers succeed in encrypting files in almost two-thirds (65%) of incidents, which is considerably above average.

More victims are paying the ransom

We asked the organizations whose data had been encrypted (1,086) whether they got their data back and, if so, how.

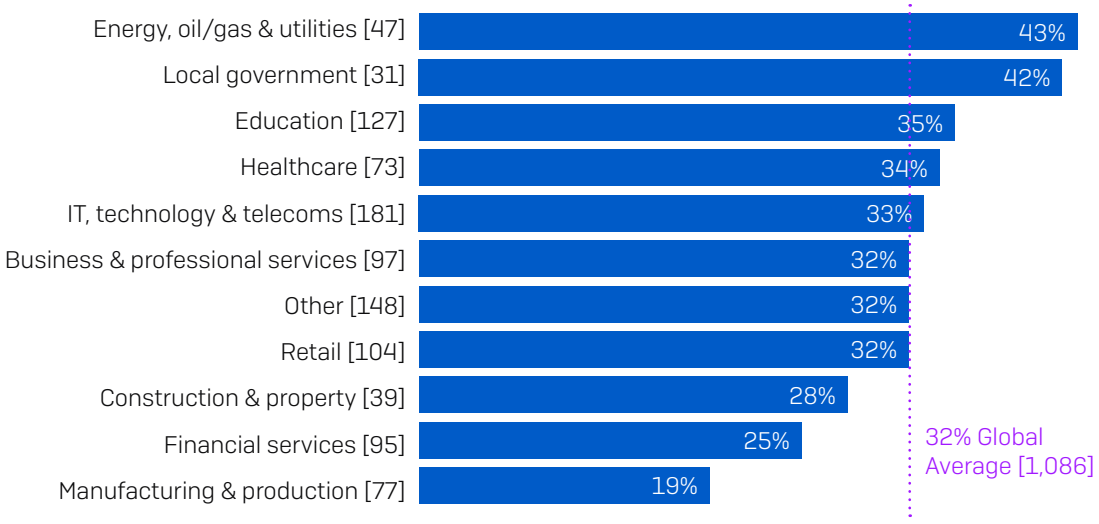
2020	2021	
26%	32%	Paid ransom to get data back
56%	57%	Used backups to get data back
12%	8%	Used other means to get data back
94%	96%	Total that got data back

Note: Due to rounding, some totals do not correspond with the sum of separate figures
Did your organization get the data back in the most significant ransomware attack?
[2021=1,086, 2020=1849] organizations whose data had been encrypted

As you can see in the chart above, 32% paid the ransom to get their data back, an increase on 26% in last year's survey. 57% were able to use backups to restore their data, which is in line with last year's finding. Overall, almost everyone (96%) got some of their data back.

Propensity to pay varies by sector

There is considerable difference in the payment of ransoms across sectors.



Did your organization get the data back in the most significant ransomware attack? Yes, we paid the ransom [base numbers in chart] organizations where the cybercriminals succeeded in encrypting their data in the most significant ransomware attack, omitting some answer options, split by sector

Energy, oil/gas, and utilities is the sector most likely to pay the ransom, with 43% of respondents from those organizations submitting to the ransom demand. This sector typically has a lot of legacy infrastructure that cannot easily be updated, so victims may feel compelled to pay the ransom to enable continuation of services.

Local government reports the second highest level of ransom payments (42%). Interestingly, this follows the earlier finding that local government is the sector most likely to have its data encrypted. It may well be that the propensity of local government organizations to pay up is driving attackers to focus their more complex and effective attacks on this audience.

There appears to be a link between an organization's ability to restore data from backups and their likelihood of paying the ransom. **Manufacturing and production** is the sector least likely to pay the ransom and also the sector most able to restore data from backups (68%). Similarly, **construction and property**, as well as **financial services**, have both below-average levels of ransom payment and above average ability to restore their data from backups.

Central government and NDPB has been excluded from this chart as the base is too low to be statistically significant. Anecdotally, of the 23 organizations in this sector whose data was encrypted, 61% reported that they were able to restore data from backups and only 26% paid the ransom. This indicative finding may help explain why this sector is a particular focus for extortion-style attacks.

Paying the ransom only gets you some of your data

65%

Of data restored after paying the ransom

Average amount of data organizations got back in the most significant ransomware attack [344] organizations that paid the ransom to get their data back

What attackers omit to say when issuing ransom demands is that even if you pay, your chances of getting all your data back are slim. On average, organizations that paid the ransom got back just 65% of the encrypted files, leaving over one-third of their data inaccessible. 29% of respondents reported that 50% or less of their files were restored, and only 8% got all their data back.

The cost of ransomware

Ransom payments vary greatly

Of the 357 respondents who reported that their organization paid the ransom, 282 also shared the exact amount paid. Across this cohort, the **average payment was US$170,404**. However, the spectrum of ransom payments was very wide. The most common payment was US$10,000 (paid by 20 respondents), with the highest payment a massive US$3.2 million (paid by two respondents).

These numbers vary greatly from the eight-figure dollar payments that dominate the headlines for multiple reasons.

1. **Organization size.** Our respondents are from smaller and mid-sized organizations between 100 and 5,000 users who, in general, have fewer financial resources than larger companies. Ransomware actors adjust their ransom demand in line with their victim's ability to pay, typically accepting lower payments from smaller companies. The data backs this up, with the average ransom payment for 100-1,000 employee organizations coming in at US$107,694, while the average ransom paid by 1,000 to 5,000 employee organizations was US$225,588.
2. **Attack nature.** There are many ransomware actors and many types of ransomware attack, ranging from highly skilled attackers who use sophisticated tactics, techniques and procedures (TTPs) focused on individual targets, to lower skilled operators who use 'off the shelf' ransomware and a general 'spray and pray' approach. Attackers who invest heavily in a targeted attack will be looking for high ransom payments in return for their effort, while operators behind generic attacks often accept lower return on investment (ROI).
3. **Location.** Attackers target their highest ransom demands on developed Western economies, motivated by their perceived ability to pay larger sums. The two highest ransom payments were both reported by respondents in Italy. Furthermore, the average ransom payment across the U.S., Canada, the U.K., Germany and Australia was US$214,096, which is 26% higher than the global average (base: 101 respondents). Conversely, in India, the average ransom payment was US$76,619, less than half the global number (base: 86 respondents).

Ransomware remediation cost has more than doubled since last year

Paying the ransom is just part of the cost of remediating an attack. While both the number of ransomware attacks and the percentage of attacks where adversaries succeed in encrypting data has declined since last year, the overall cost of remediating a ransomware attack has increased.

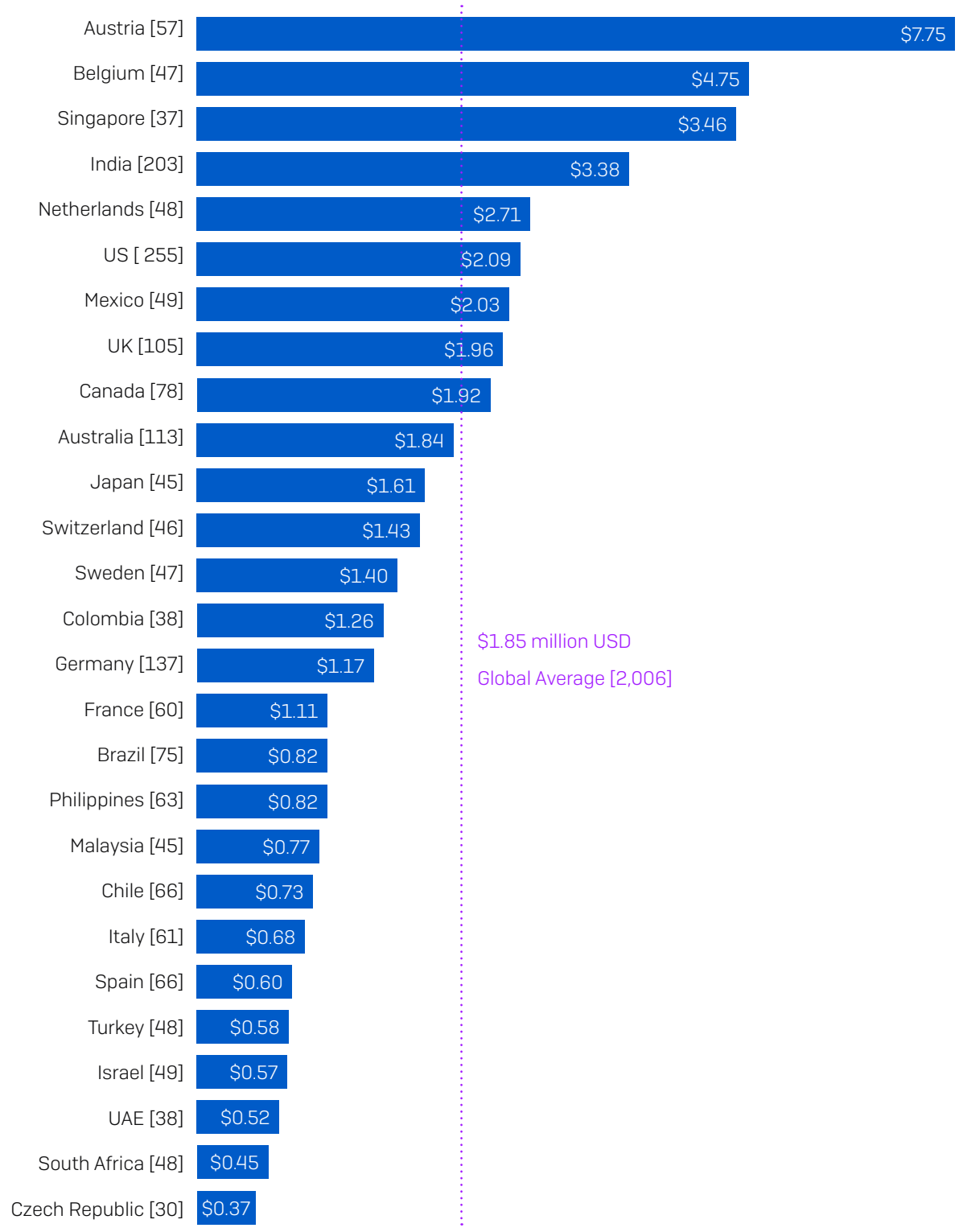
Respondents reported that the average cost to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) was US$1.85 million, more than double the US$761,106 cost reported last year.

Average approximate cost to organizations to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) [2021=2,006, 2020=2,538] respondents whose organization had been hit by ransomware in the last year, split by year

In the last year, Sophos ransomware experts have seen a considerable increase in advanced ransomware attacks that combine automation with hands-on human hacking. These complex attacks require more complex recovery processes, and this may be a key factor behind the overall increase in ransomware recovery costs.

Remediation costs vary based on your location

Looking at the ransomware remediation costs at a country level, we see considerable variations.



Average approximate cost to organizations to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) [base numbers in chart] respondents whose organization had been hit by ransomware in the last year,split by country, millions of USD

Austria stands out as the country with the highest ransomware remediation cost. There were a number of high-profile cyberattacks on Austrian organizations last year, with Austria's foreign ministry reportedly targeted by a state actor, and the Netwalker ransomware group claiming on Twitter to have stolen data from the Austrian city of Weiz. It's worth noting that if we exclude Austria from the data, the average remediation cost only drops to US$1.68 million, still more than double last year's figure.

In general, higher salary countries – Belgium, Singapore, the Netherlands, the U.S. – report among the highest overall costs, while lower salary countries – Czech Republic, South Africa – report the lowest overall costs. This reflects the considerable manual effort required to remediate an attack. Indeed, the total cost to remediate a ransomware attack is 10X the average ransom payment.

Israel is among the countries with the lowest overall ransomware remediation costs despite being a developed economy. For geopolitical reasons, Israel is a major target for cyberattacks (not just ransomware), resulting in very high levels of cyber defenses, preparedness, and remediation expertise across the country. These combine to lower the financial impact of an attack.

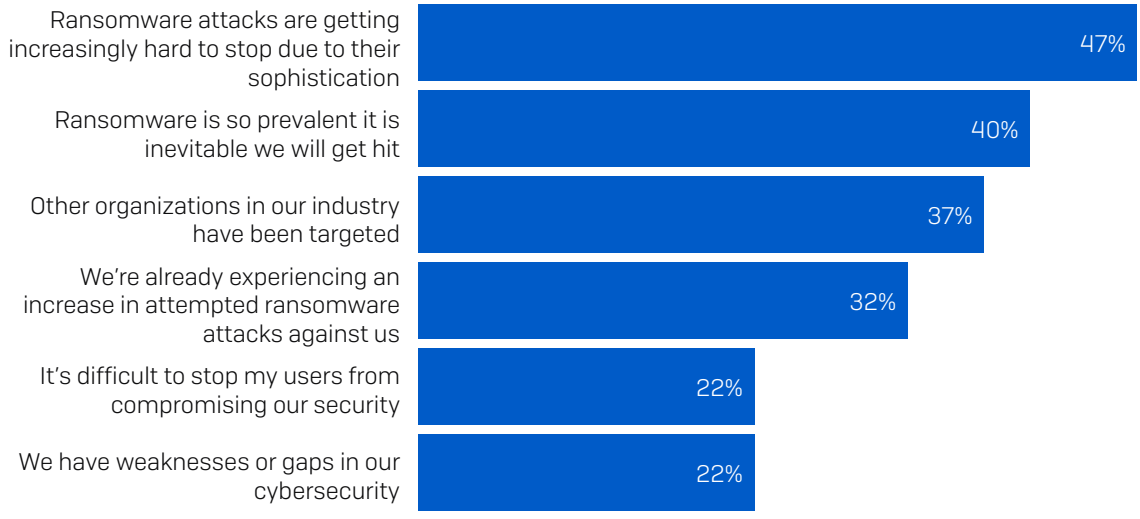
The future

Expectations of ransomware attacks vary

62% of survey respondents (3,353) reported that their organization hadn't been hit by ransomware in the last year. Within this group, we see considerable variation in their attitude towards and confidence in dealing with ransomware. 65% expect to be hit by ransomware in the future, while 35% don't anticipate an attack.

Why organizations expect to be hit by ransomware

Among the 2,187 respondents from organizations that weren't hit by ransomware in the last year but expect to be in the future, the most common reason they expect to suffer an attack is that "ransomware attacks are getting increasingly hard to stop due to their sophistication," cited by 47% of respondents in this group.



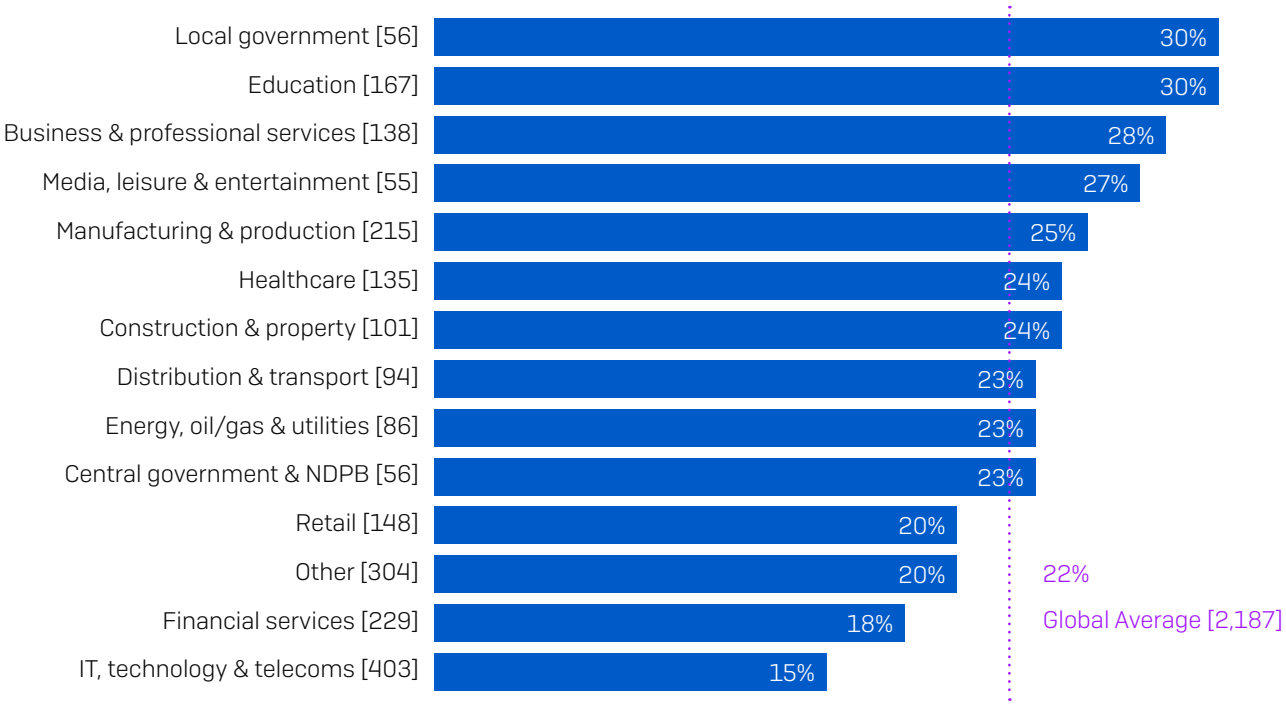
Why do you expect your organization to be hit by ransomware in the future? [2,187] organizations that weren't hit by ransomware last year but expect to be in the future, omitting some answer options

While this is a high number, the fact that these organizations are alert to ransomware becoming ever more advanced is a good thing, and may well be a contributing factor to them being able to block any potential ransomware attack last year.

22% of respondents see users compromising security as a major factor when it comes to being hit by ransomware in the future. It is encouraging to see that, in the face of sophisticated attackers, most IT teams are not taking the easy option of blaming their users.

Similarly, 22% of respondents admit to having weaknesses or gaps in their cybersecurity. While it's clearly not a good idea to have security holes, recognizing these issues is an important first step to enhancing your defenses.

Diving deeper into this point, we see that the local government and education sectors are most likely to admit to security weaknesses (30% each).



Why do you expect your organization to be hit by ransomware in the future? We have weaknesses or gaps in our cybersecurity [base numbers in chart] organizations that weren't hit by ransomware last year but expect to be in the future, omitting some answer options, split by sector

While the respondents to this question weren't themselves hit by ransomware last year, it is likely that they have been influenced by the broader ransomware experiences in their sectors:

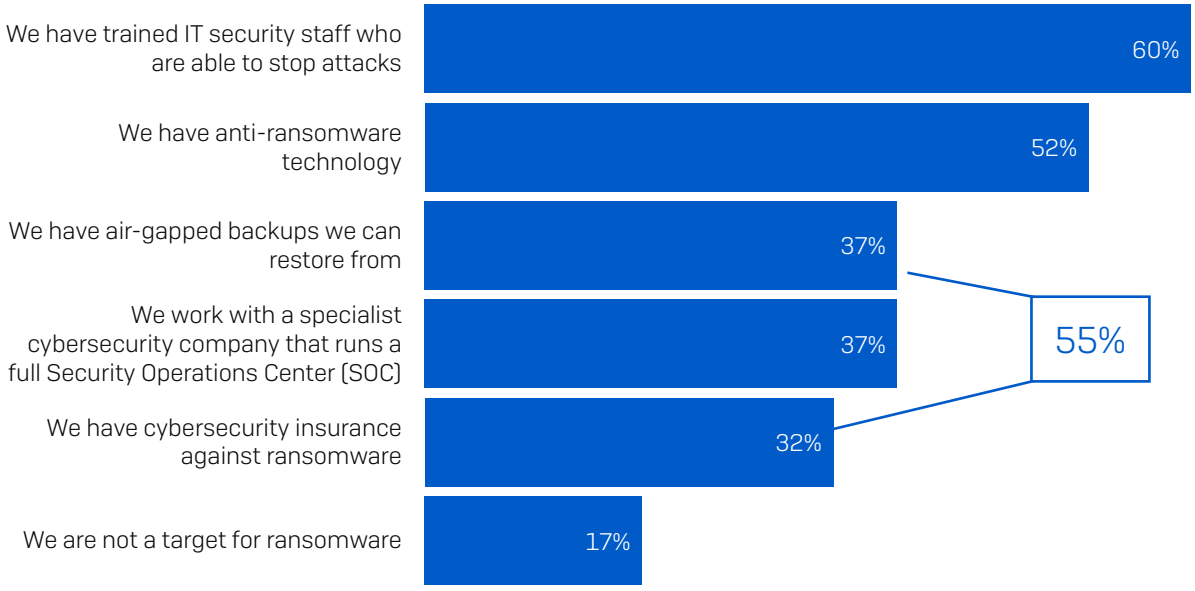
- **Local government** is the sector where attackers are most likely to succeed in encrypting the victim's data
- **Education** (jointly with retail) is the sector that reported the highest percentage of organizations hit by ransomware last year

In addition, both sectors typically struggle with funding for both technology and IT resources, which also leads to security holes.

Conversely **IT, telecoms, and technology** (15%) and **financial services** (18%) have the lowest percentage of respondents admitting to security gaps. These are sectors that are generally quick to adopt new technology and have larger budgets, so have more opportunities to address areas of weakness.

Trained IT staff give ransomware confidence

1,166 respondents said they weren't hit by ransomware last year, and don't expect to be hit in the future. The #1 reason for this confidence in the face of ransomware is having trained IT staff who are able to stop attacks.



Why do you not expect your organization to be hit by ransomware in the future? [1,166] organizations that weren't hit by ransomware in the last year and do not expect to be in the future, omitting some answer options

While advanced and automated technologies are essential elements of an effective anti-ransomware defense, stopping hands-on attackers also requires human monitoring and intervention by skilled professionals. Whether in-house staff or outsourced pros, human experts are uniquely able to identify some of the tell-tale signs that ransomware attackers have you in their sights.

37% of respondents who don't expect to be hit by ransomware work with a specialist cybersecurity company that runs a full security operations center (SOC). Only a few years ago SOCs were the exclusive preserve of the largest companies, so this represents a major shift in cybersecurity delivery for mid-sized organizations.

It's not all good news. Some results are cause for concern:

- 55% of respondents that don't expect to be hit are putting their faith in approaches that don't offer any protection from ransomware:
  - 37% of respondents cited 'air-gapped backups' as a reason why they don't expect to be hit. Backups, as we have seen, are valuable tools for restoring data post attack, but they don't stop you getting hit.

- 32% of respondents claimed that having cybersecurity insurance protects them from being hit by ransomware. Again, insurance can help deal with the aftermath of the attack, but doesn't prevent it in the first place.

N.B. Some respondents selected both options, with 55% selecting at least one of these two options.

- Furthermore, 17% of respondents don't believe they are a target for ransomware. Sadly, this is not true. No organization is safe.

Malware incident recovery plans are standard

Responding to a critical cyberattack or incident can be incredibly stressful. While nothing can fully alleviate the stress of dealing with an attack, having an effective incident response plan in place is a sure-fire way to minimize the impact.

It's therefore encouraging to discover that 90% of respondents report their organization has a malware incident recovery plan, with just over half (51%) having a full and detailed plan and 39% having a partially developed plan.

There are many parallels between recovering from malware and recovering from a natural disaster; in both scenarios you need to be able to start again from scratch. The Philippines, a country that suffers frequent flooding and earthquakes, is the most prepared for a malware incident with 83% of respondents having a full and detailed malware incident recovery plans.

Government organizations are least prepared to respond to a malware attack

Most sectors are well prepared to recover from a malware incident. However, government organizations emerged as the least prepared: only 73% of **local government** and 81% of **central government and NDPB** have a malware recovery plan.

This is concerning as these sectors are among the most affected by ransomware; local government is the sector most likely to have its data encrypted in an attack while central government and NDPB are most likely to experience extortion.

The lack of malware recovery plan may be a contributing factor behind local government being the second most likely sector to pay the ransom demands.

Recommendations

In light of these findings, Sophos experts recommend the following best practices:

1. **Assume you will be hit.** Ransomware remains highly prevalent. No sector, country, or organization size is immune from the risk. It's better to be prepared but not hit, than the other way round.

2. **Make backups.** Backups are the #1 method organizations used to get their data back after an attack. And as we've seen, even if you pay the ransom, you rarely get all your data back, so you'll need to rely on backups either way.

3. **Deploy layered protection.** In the face of the considerable increase in extortion-based attacks, it is more important than ever to keep the adversaries out of your environment in the first place. Use layered protection to block attackers at as many points as possible across your environment.

4. **Combine human experts and anti-ransomware technology.** Key to stopping ransomware is defense in depth that combines dedicated anti-ransomware technology and human-led threat hunting. Technology gives you the scale and automation you need, while human experts are best able to detect the tell-tale tactics, techniques, and procedures that indicate that a skilled attacker is attempting to get into your environment. If you don't have the skills in house, look at enlisting the support of a specialist cybersecurity company – SOCs are now realistic options for organizations of all sizes.

5. **Don't pay the ransom.** We know this is easy to say, but far less easy to do when your organization has ground to a halt due to a ransomware attack. Independent of any ethical considerations, paying the ransom is an ineffective way to get your data back. If you do decide to pay, be sure to include in your cost/benefit analysis the expectation that the adversaries will restore, on average, only two-thirds of your files.

6. **Have a malware recovery plan.** The best way to stop a cyberattack from turning into a full breach is to prepare in advance. Organizations that fall victim to an attack often realize they could have avoided a lot of cost, pain, and disruption if they had an incident response plan in place.

Further resources

The Sophos Incident Response Guide helps organizations define the framework for your cybersecurity incident response plan and explores the 10 main steps your plan should include.

Defenders may also like to review Four Key Tips from Incident Response Experts, which highlights the biggest lessons everyone should learn when it comes to responding to cybersecurity incidents.

Both resources are based on the real-world experience of the Sophos Managed Threat Response and Sophos Rapid Response teams, who have collectively responded to thousands of cybersecurity incidents.

Learn more about ransomware and how Sophos can help you defend your organization.

2021-04-19 (SB-NP)

SOPHOS