SOPHOS
Cybersecurity evolved.

The State of Ransomware in Healthcare 2021

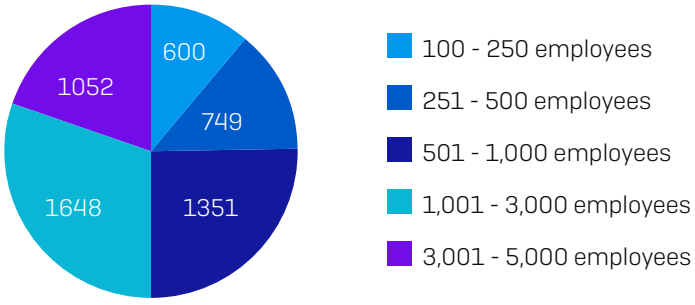
This report shares the latest findings as well as new insights into the state of ransomware in the healthcare sector. It explores the prevalence of ransomware in healthcare, its impact on victims, the cost to remediate ransomware attacks, and the proportion of data victims were able to recover after they paid the ransom. The survey also reveals how healthcare stacks up with other sectors, as well as future expectations and readiness of healthcare organizations in face of these attacks.

A Sophos Whitepaper. May 2021

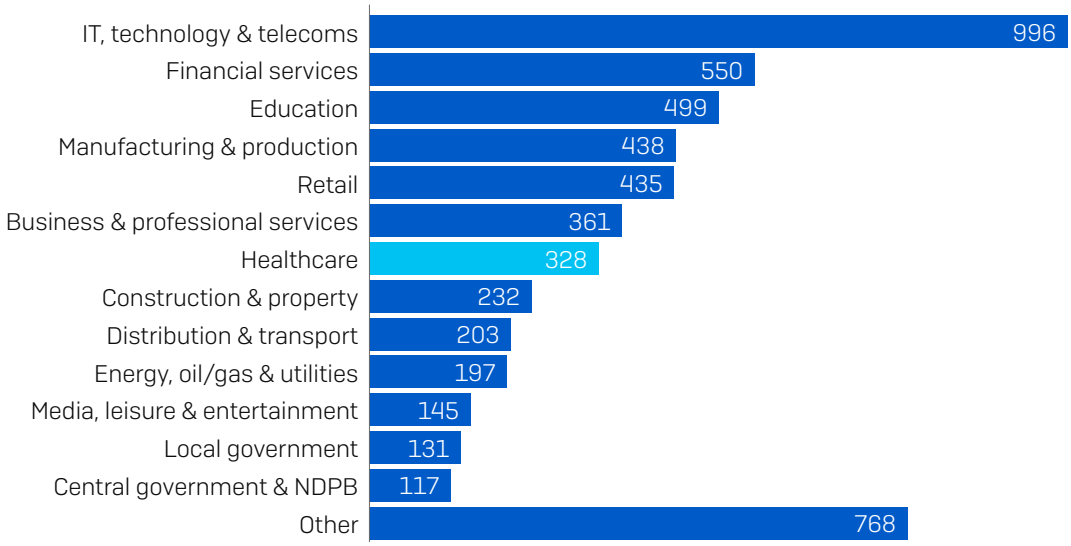
About the survey

Sophos commissioned independent research house Vanson Bourne to survey 5,400 IT decision makers across 30 countries. Respondents came from a wide range of sectors, including **328 respondents from healthcare**. The survey was conducted in January and February 2021.

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



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



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. The 328 healthcare IT decision makers came from all geographic regions surveyed: the Americas, Europe, the Middle East, Africa, and Asia Pacific.

Region	# Respondents
Americas	66
Europe	127
Middle East and Africa	37
Asia Pacific	98

328 IT Decision Makers in Healthcare

Key findings

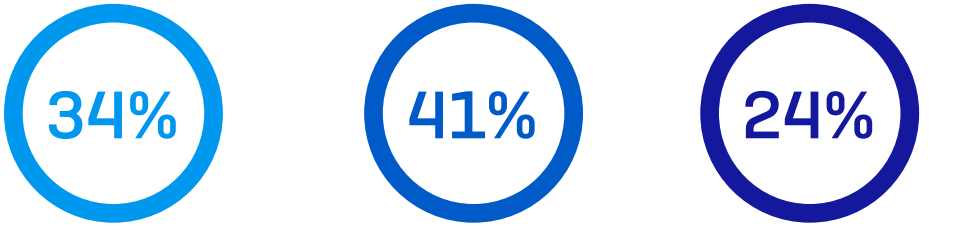
- **34%** of healthcare organizations **were hit by ransomware in the last year.**
- **65%** that were hit by ransomware in the last year said the **cybercriminals succeeded in encrypting their data** in the most significant attack.
- **44%** of those whose data was encrypted **used backups to restore data.**
- **34%** of those whose data was encrypted **paid the ransom to get their data back** in the most significant ransomware attack.
- However, on average, only **69% of the encrypted data was restored** after the ransom was paid*.
- **89%** of healthcare organizations have a **malware incident recovery plan**.
- The **average bill for rectifying a ransomware attack**, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. was **US$1.27 million**. While this is a huge sum, it's also **the lowest among all sectors surveyed**.

**Indicative number – low response base*

The prevalence of ransomware in healthcare

Majority of organizations not hit by ransomware expect an attack in the future

Of the 328 healthcare respondents that were surveyed, 34% were hit by ransomware in the last year, defined as multiple computers being impacted by a ransomware attack, but not necessarily encrypted. Among the organizations not hit last year, 41% said they expected to be hit by ransomware in the future, while 24% were confident that they are safe from future attacks. We'll dive deeper into the reasons behind expecting to be hit in the future as well as what gives others confidence in the face of future attacks later in the report.

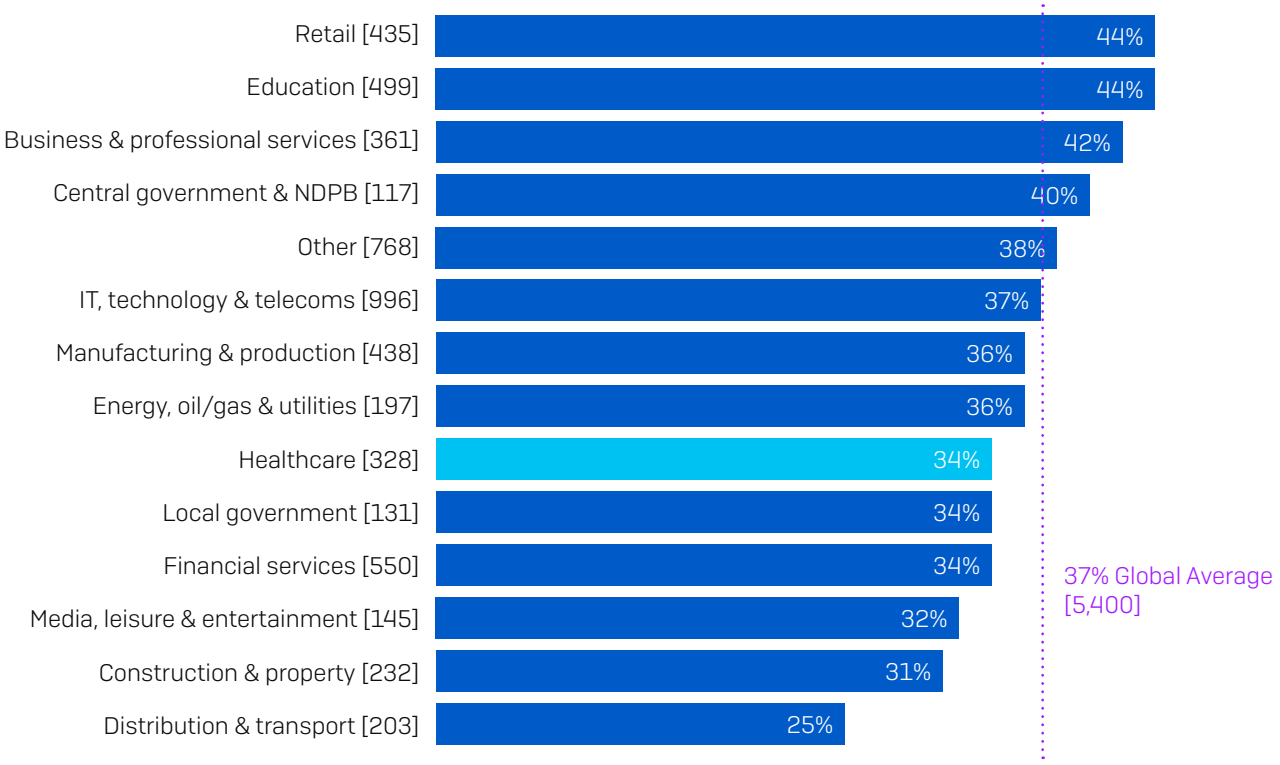


In the last year, has your organization been hit by ransomware? [328 healthcare respondents]

Healthcare surprises with below average levels of attack

With just a little over a third of healthcare organizations reporting being hit by ransomware, healthcare actually fared slightly better than the global average across all sectors, which came in at 37%. **Retail** and **education** sectors experienced the highest number of ransomware attacks with 44% of respondents reporting being hit.

% respondents hit by ransomware in the last year



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

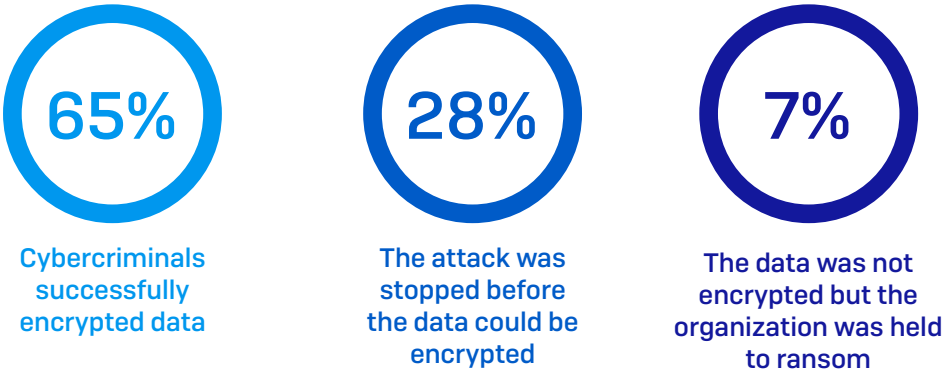
With **healthcare** often making headlines for ransomware attacks, it's perhaps a welcome surprise that this sector experiences below average numbers of attacks. Their over-representation in the news reports is likely due to healthcare organizations' obligations to make public an attack, where many commercial organizations are able to keep the bad news private.

Globally across all sectors, the percentage of organizations hit by ransomware in the last year has dropped considerably from last year, when 51% admitted being hit. While the drop is welcome news, it's likely due in part to evolving attacker behaviors observed by SophosLabs and the Sophos Managed Threat Response. 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.

The impact of ransomware

Attackers succeed in encrypting healthcare data

We asked the respondents whose organizations had been hit by ransomware whether the cybercriminals succeeded in encrypting data. Almost two-thirds of the respondents, 65%, said yes. 28% of respondents said that they were able to stop the attack before the data was encrypted.

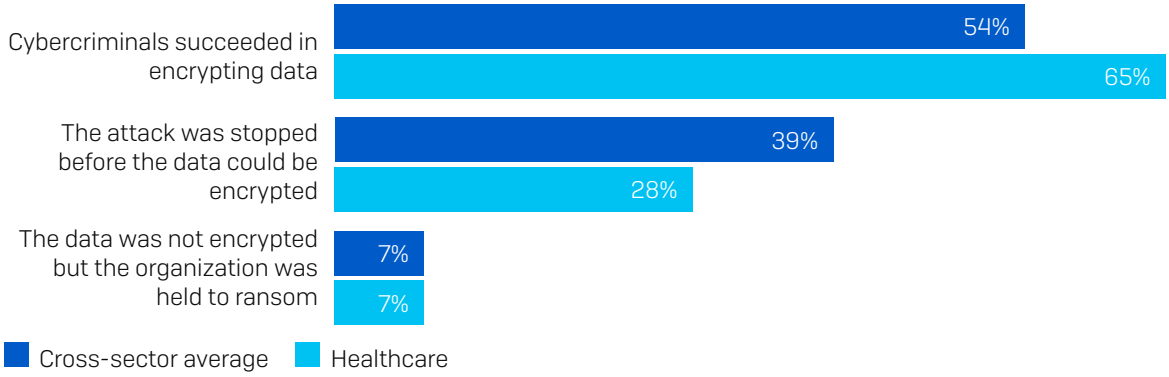


Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? [113 healthcare organizations that have been hit by ransomware in the last year]

Another 7% said the data was not encrypted but the organization was still held to ransom. This is because some attackers are turning to extortion-style attacks; 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 is needed. Adversaries often leverage the punitive fines for data breaches in their demands in a further effort to make victims pay up.

Healthcare is less able to stop ransomware than other sectors

When compared with other sectors globally, attackers have a much higher success rate in encrypting healthcare data (65%) than the global average (54%). Healthcare organizations also fall behind the global average in their success rate at stopping attacks before the data could be encrypted: 28% vs. 39%.



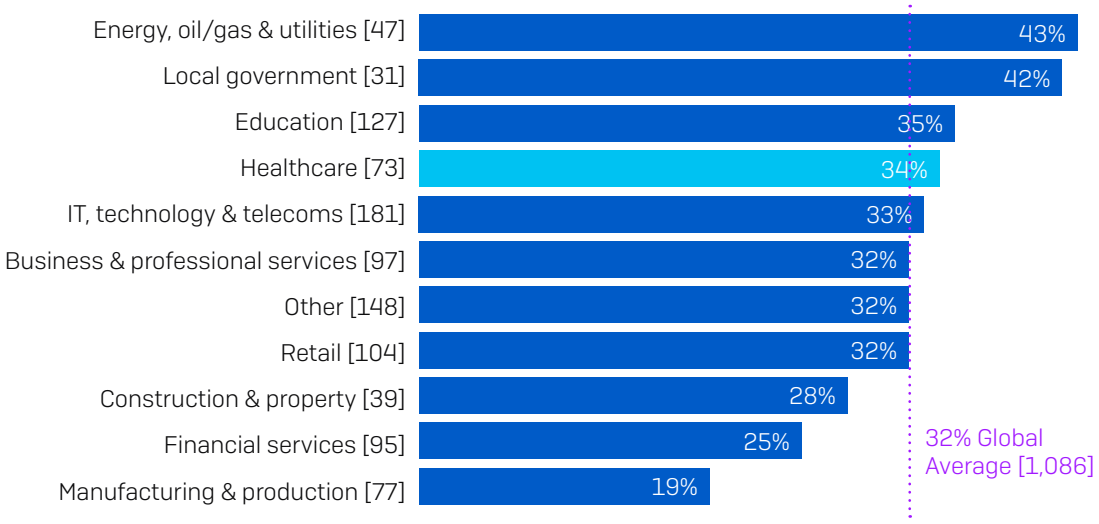
Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? [2006 cross-sector; 113 healthcare organizations that have been hit by ransomware in the last year]

This is likely because of the financial and resource challenges that healthcare IT faces. These teams are commonly understaffed, and they were particularly stretched last year due to the pandemic. At the same time, many healthcare organizations don't want to divert funds to cybersecurity when those funds could be used to buy medical resources that more directly relate to patient care. Another possible factor contributing to the higher impact of ransomware on healthcare is legacy equipment that is difficult to update or patch, providing easy entry points for attackers.

Healthcare is more likely to pay ransom...

Healthcare is one of the sectors most likely to pay the ransom, with 34% of respondents whose data was encrypted admitting to paying the ransom compared with a cross-sector average of 32%. This may be due to the pressures on healthcare teams to ensure continuity of services.

% that paid the ransom to get their data back



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

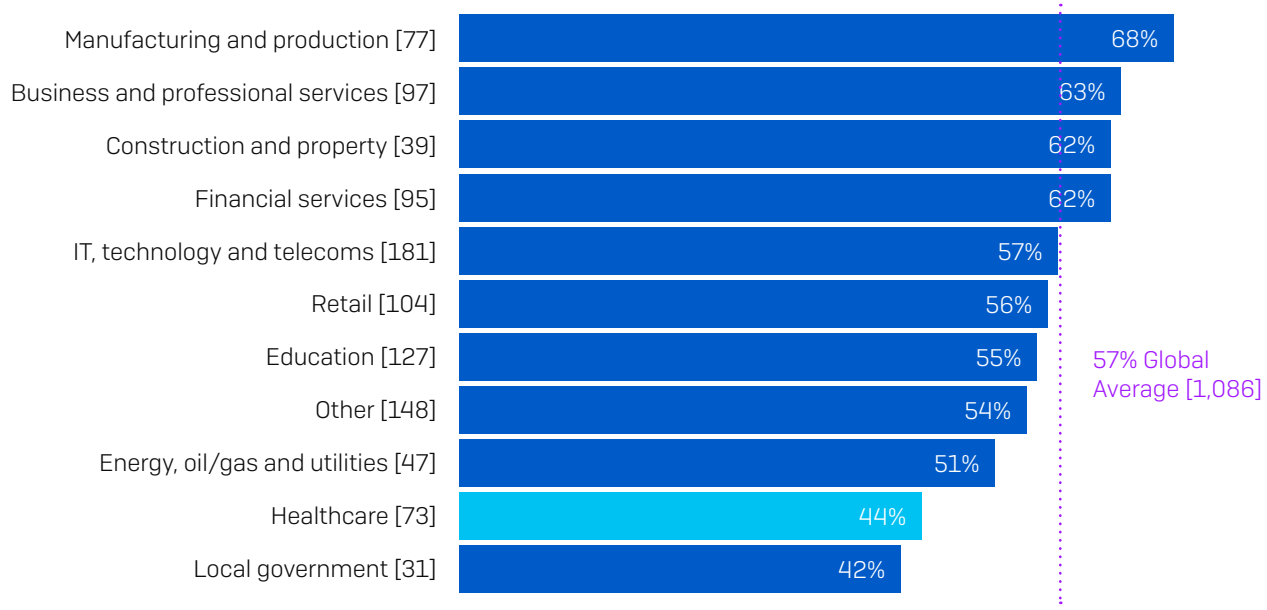
Across sectors, **energy, oil/gas, and utilities** is most likely to pay the ransom, with 43% submitting to the ransom demand. This sector typically has a lot of legacy infrastructure that cannot easily be updated, so victims may feel compelled to pay the ransom to enable continuation of services.

Local government reports the second-highest level of ransom payments (42%). This is also 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.

... And less likely to back up data

Healthcare's high rate of ransom payment may also be due to the inability of organizations in this sector to restore their data from backups. Globally, 57% of organizations whose data was encrypted were able to restore their data from backups. This drops, however, to just 44% in healthcare – the second lowest rate of all industries surveyed.

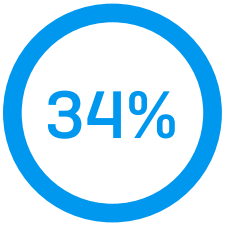
% that used backups to restore data



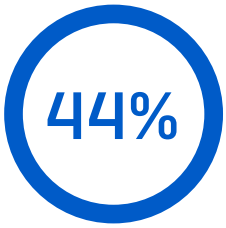
Did your organization get the data back in the most significant ransomware attack?
Yes, we used backups to restore the data [base numbers in chart] organizations where the cybercriminals succeeded in encrypting their data in the most significant ransomware attack, omitting some answer options, split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

93% of healthcare organizations got their data back

Among the healthcare respondents whose data was encrypted by cybercriminals after a ransomware attack, 93% got their data back, which is in line with the cross-sector global average of 96%. Of this cohort, just over a third (34%) paid the ransom to get the data back, while 44% restored the data using backups, and 15% used other means to get their data back.



Paid ransom to get the data back



Used backups to restore their data

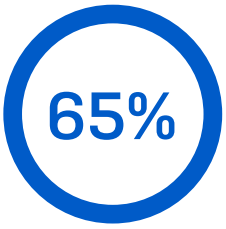
Used other means to get their data back

Did your organization get the data back in the most significant ransomware attack? [73] Healthcare organizations responded.

Paying the ransom doesn't pay

What attackers omit 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 their data, leaving over a third inaccessible.

Percentage of data restored after paying the ransom



CROSS-SECTOR AVERAGE

Percentage of data restored after paying the ransom

HEALTHCARE AVERAGE

Average amount of data organizations got back in the most significant ransomware attack [344/25] organizations that paid the ransom to get their data back

The base number of respondents in healthcare was 25, so the data here is not robust. However, anecdotally, healthcare respondents reported getting back on average 69% of their data – a little better than the global average but still leaving a considerable proportion of the data inaccessible.

Across all respondents from all sectors, 29% got back 50% or less of their data, and only 8% got all their data back.

The cost of ransomware

Revealed: The ransom payments

Of the 357 respondents across sectors who reported that their organization paid the ransom, 282 also shared the exact amount paid, including 23 in healthcare. Again, the healthcare base number is somewhat low, so the findings here should be considered indicative only.

$ 170,404

Average global ransom payment

$ 131,304

Average healthcare ransom payment

How much was the ransom payment your organization paid in the most significant ransomware attack? [282/23] organizations that paid the ransom to get their data back

Globally across all sectors, the average ransom payment was US$170,404. However, in healthcare the average ransom payment was almost US$40,000 lower – US$131,304.

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

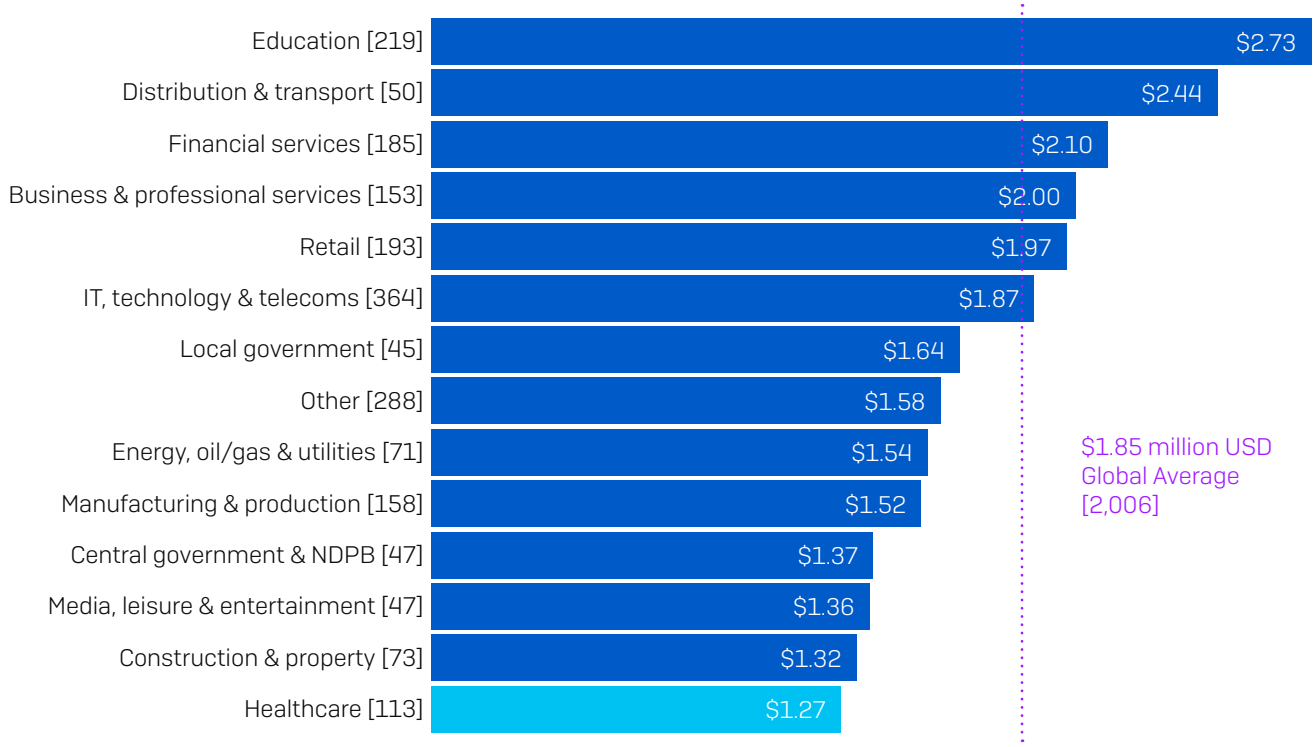
1. **Organization size.** Our respondents are from smaller and mid-sized organizations between 100 and 5,000 users who, in general, have fewer financial resources than larger organizations. Ransomware actors adjust their ransom demand to reflect their victim's ability to pay, typically accepting lower 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 1,001 to 5,000 employee organizations is US$225,588.

2. **The nature of the attack.** There are many ransomware actors, and many types of ransomware attacks, 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.** As we saw at the start, this survey covers 30 countries across the globe, with varying levels of GDP. 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. Conversely, in India, the average ransom payment was US$76,619, less than half the global number (base: 86 respondents).

Healthcare has the lowest ransomware recovery cost

When we look at the average approximate cost to organizations to recover from ransomware attacks and rectify the impact of their most recent such attack (considering downtime, hours lost, device cost, network cost, lost opportunity, ransom paid, and so on), healthcare reported the lowest overall remediation cost at US$1.27 million. In comparison, the cross-sector average is US$1.85 million.



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 sector, Millions of US$

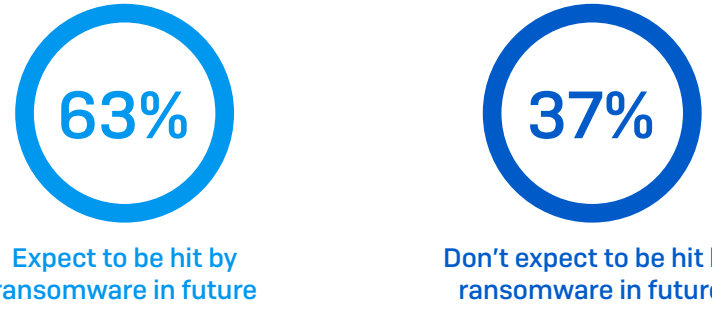
There are several likely factors behind the lower healthcare costs:

1. Healthcare organizations often have lower budgets than many other sectors, limiting the amount that is available to be spent on remediation.
2. In many parts of the world healthcare is a public service. People have little choice but to use certain healthcare facilities even if they have experienced a ransomware attack, so there is little or no reputational or opportunity costs involved. This is contrary to what happens in most other sectors when they are under attack.

The future

Healthcare's expectations on the future attacks

Almost two-thirds of healthcare respondents (63%) who reported that they hadn't been hit by ransomware in the last year expect to be hit by ransomware in the future. Conversely, 37% don't anticipate an attack.

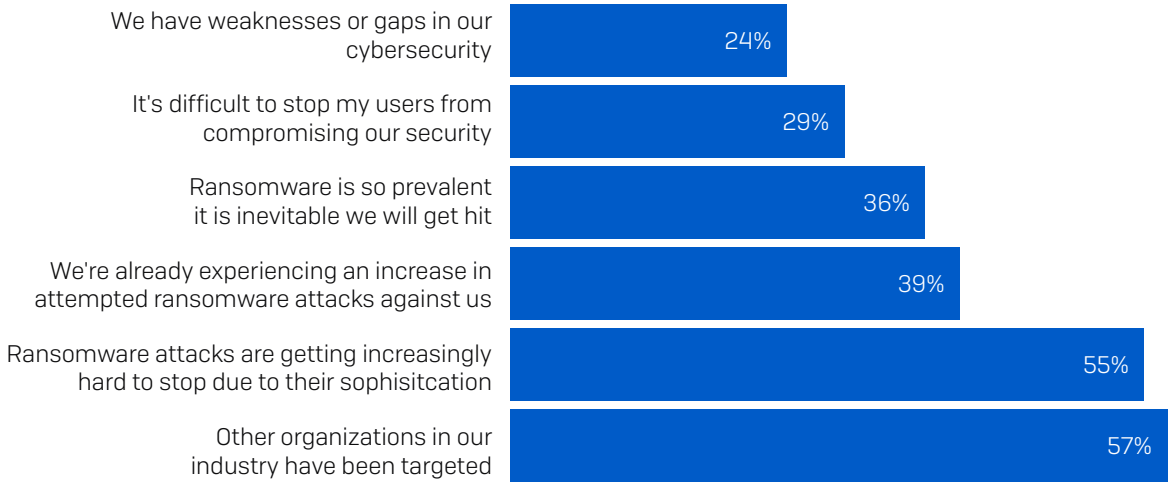


[214] Healthcare respondents who answered "No" to the question "In the last year, has your organization been hit by ransomware?"

Within this group, we see considerable variation in their attitude towards, and confidence in dealing with ransomware.

Why healthcare expects to be hit

Among the 63% of healthcare organizations that weren't hit by ransomware but expect to be in the future, the most common reason (57%) is that other organizations in the healthcare sector have been targeted. In addition, 55% of respondents said that ransomware attacks are getting increasingly hard to stop due to their sophistication. 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 successfully block any potential ransomware attack last year.



Why do you expect your organization to be hit by ransomware in the future? [135 healthcare organizations that haven't been hit by ransomware but expect to be in the future, omitting some answer options]

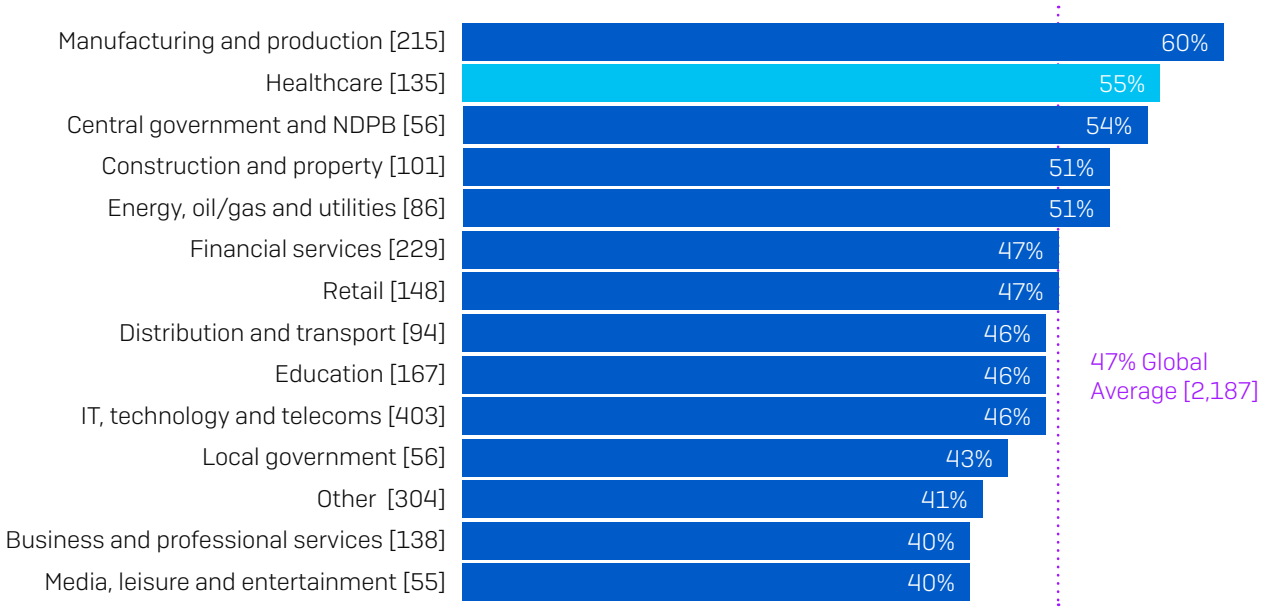
29% of respondents see users compromising security as a major factor behind why they will likely be hit by ransomware in the future. It is encouraging to see that, in the face of sophisticated attackers, most IT teams are not taking the easy option of blaming their users.

Similarly, 24% of respondents admit to having weaknesses or gaps in their cybersecurity. While it's clearly not a good thing to have security holes, recognizing that these issues exist is an important first step to enhancing your defenses.

High awareness of ransomware sophistication in healthcare

Respondents from healthcare showed themselves to be one of the sectors most alert (55%) to the growing sophistication of ransomware, versus the global average of 47%.

% of respondents attributing rise in attacks to increased sophistication



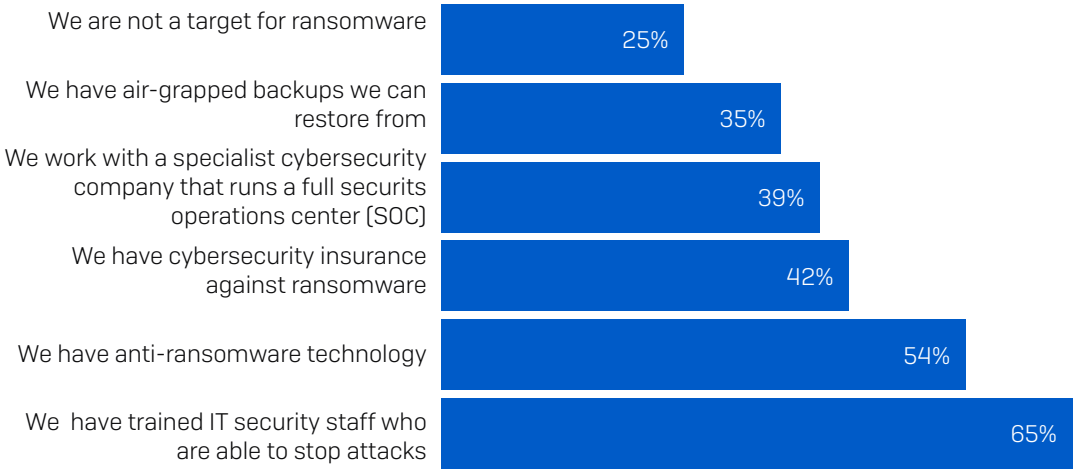
Why do you expect your organization to be hit by ransomware in the future? [2,187] organizations that cited ransomware attacks getting increasingly hard to stop due to their sophistication as a reason for their expectation to be hit in the future

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 – and healthcare has borne the brunt of many successful attacks.

Trained IT staff give ransomware confidence

79 healthcare respondents whose organizations were not hit by ransomware last year said they don't expect to be hit in the future. The number one reason for this confidence in the face of ransomware is having trained IT staff who are able to stop attacks, followed closely by their confidence in their anti-ransomware technology. It was encouraging to note that over half of the survey respondents have deployed anti-ransomware technology.

Why respondents do not expect to be hit by ransomware in the future



Why do you not expect your organization to be hit by ransomware in the future? [79] Healthcare organizations that haven't been hit by ransomware 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 telltale signs that ransomware attackers have you in their sights. We strongly recommend all organizations build up their human expertise in the face of the ongoing ransomware threat.

39% of healthcare respondents that haven't been hit by ransomware and don't expect to be hit by ransomware work with a specialist cybersecurity company that runs a full security operations center (SOC). This represents a major shift in cybersecurity delivery for mid-sized organizations. Only a few years ago SOCs were exclusive to the largest of organizations; however, the data shows they are now mainstream.

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

- 47% of respondents that don't expect to be hit are putting their faith in approaches that don't offer any protection from ransomware.
  - 35% 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 from being attacked.
  - 42% of respondents claimed that having cybersecurity insurance protects them from being hit by ransomware. Again, it can help deal with the aftermath of the attack, but doesn't prevent and attack in the first place.

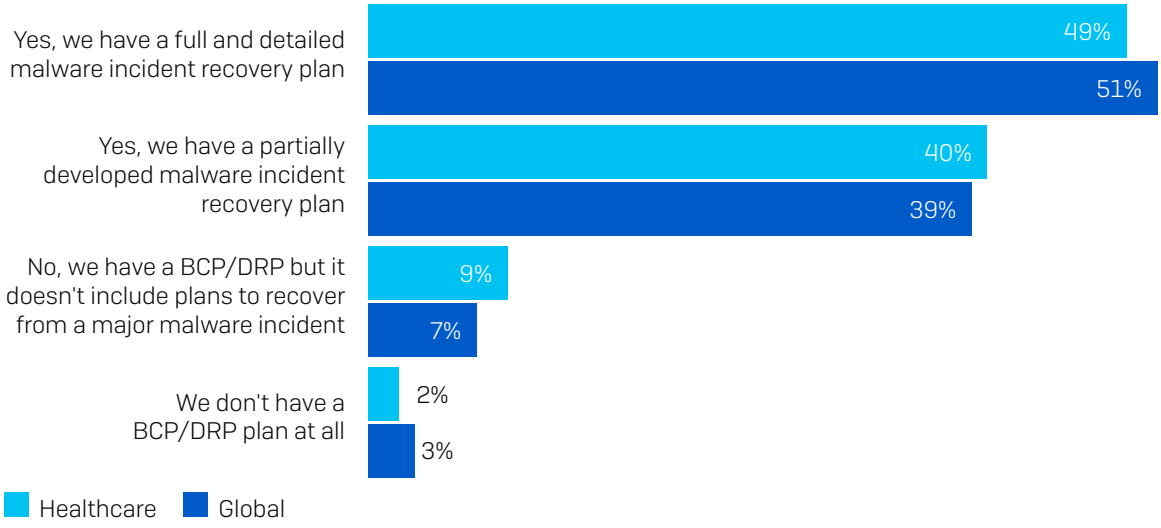
N.B. Some respondents selected both options, with 47 selecting at least one of these two options.

- 25% of respondents don't believe they are a target for ransomware. Sadly, this is not true. No organization is safe.

Most healthcare organizations have a malware incident recovery plan

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

It's therefore encouraging to discover that 89% of healthcare organizations have a malware incident recovery plan, with just under half (49%) having a full and detailed plan and 40% having a partially developed plan. These statistics are very much aligned with the cross-sector average numbers.



Does your organization's Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP) include plans to recover from a major malware incident? [5,400 Global /328 Healthcare respondents]

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 number one 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.

A simple memory aid for backups is "3-2-1." You should have at least **three** different copies (the one you are using now plus two or more spares), using at least **two** different backup systems (in case one should let you down), and with at least **one** copy stored offline and preferably offsite (where the crooks can't tamper with it during an attack).

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 telltale 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 to enlist 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.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2021-05-05 (SB-NP)

SOPHOS