SOPHOS
Cybersecurity evolved.

The State of Ransomware in Government 2021

A national emergency

This report shares new insights into the current state of ransomware in both **central government and non-departmental public bodies (NDPB)** as well as **local government** organizations based on an independent survey of IT professionals. It provides a deep dive into the prevalence of ransomware in government, the impact of ransomware, the cost of remediating attacks, and the proportion of data that government organizations were able to recover after they paid the ransom.

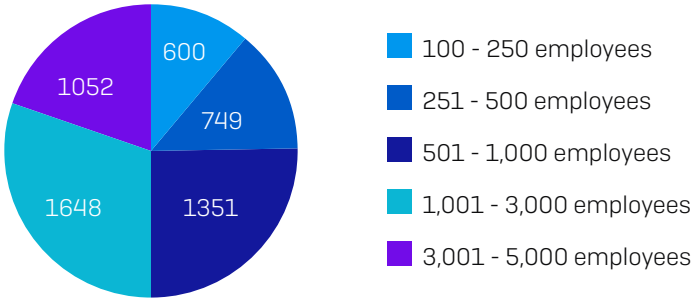
The survey also reveals how the experiences of central and local government organizations compare with those of other sectors, as well as the future expectations and readiness of government organizations in face of these attacks.

A Sophos Whitepaper. June 2021

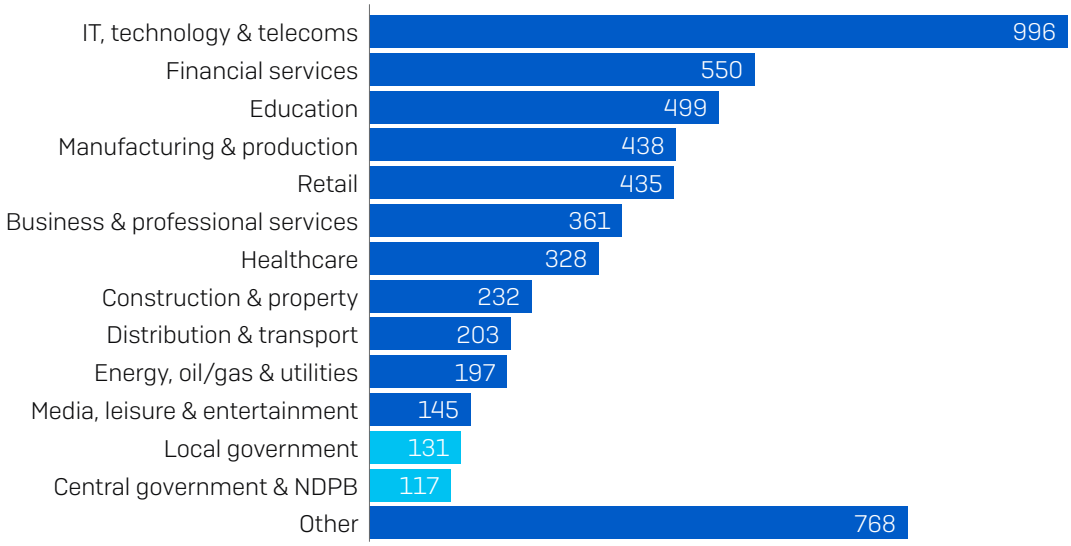
About the survey

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 117 respondents from central government and NDPB and 131 respondents from the local government sector. 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 117 IT decision makers in central government and NDPB and 131 in local government came from all geographic regions surveyed: the Americas, Europe, the Middle East, Africa and Asia Pacific.

Region	# Respondents Central Government	# Respondents Local Government
Americas	29	39
Europe	52	57
Middle East and Africa	16	18
Asia Pacific	20	17
TOTAL	**117**	**131**

117 IT decision makers in central government & NDPB; 131 in local government

Key findings in central government and NDPB

- **40%** of central government and NDPB organizations **were hit by ransomware in the last year**
- **49%** of organizations hit by ransomware said the **cybercriminals succeeding in encrypting their data** in the most significant attack
- **13%** of those hit by ransomware in the last year said their data was not encrypted, but they **were held to ransom** anyway; these extortion-style attacks are the **highest among all sectors**
- **61%** of those whose data was encrypted **used backups to restore data**
- **81%** of central government and NDPB organizations have a **malware incident recovery plan – the second lowest of all sectors** surveyed
- The **average bill for rectifying a ransomware attack**, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, and more, was **US$1.37 million**

Key findings in local government

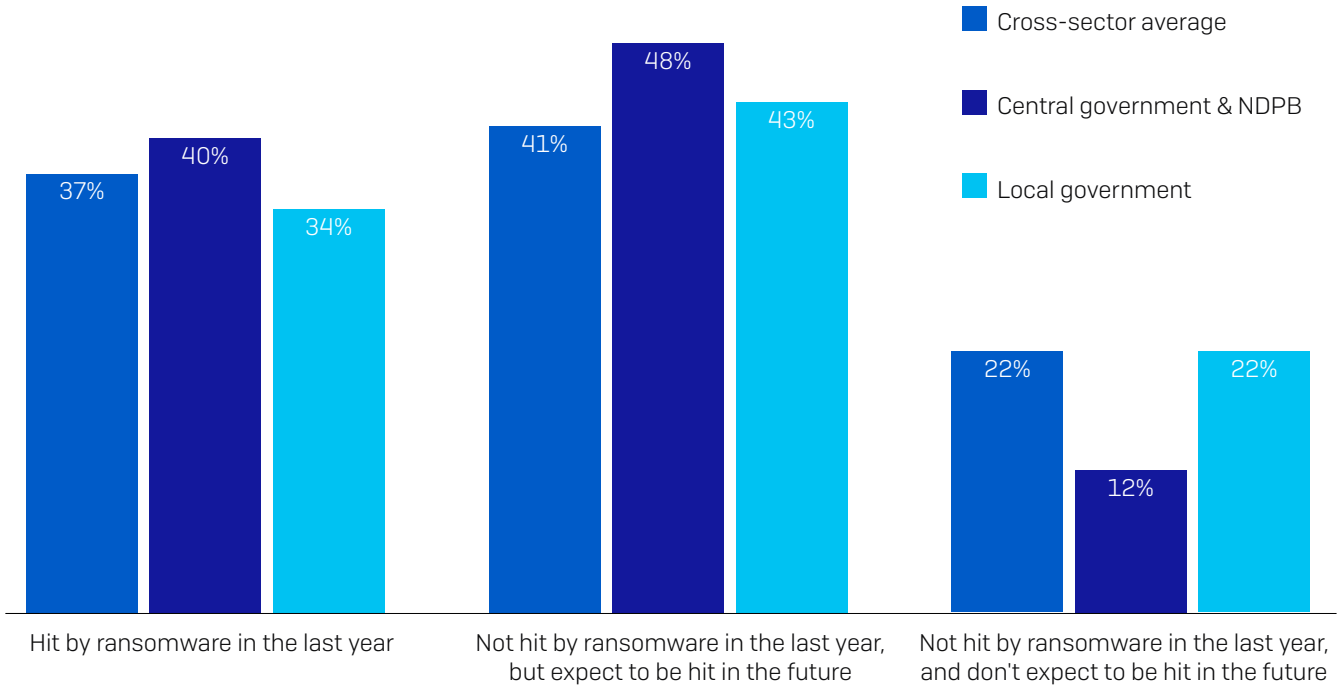
- **34%** of local government organizations **were hit by ransomware in the last year,** which is a little lower than the central government figure
- **69%** of organizations hit by ransomware said the **cybercriminals succeeding in encrypting their data** in the most significant attack – a full 20 percentage points higher than central government
- **42%** of those whose data was encrypted **paid the ransom** to get their data back in the most significant ransomware attack
- **42%** of those whose data was encrypted **used backups to restore data**
- **73%** of local government organizations have a **malware incident recovery plan** – the **lowest of all sectors** surveyed
- The **average bill for rectifying a ransomware attack**, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, and more, was **US$1.64 million**

The prevalence of ransomware in government

Central government is a more frequent target than the local government

When government respondents were asked if their organization was hit by ransomware in the last year, defined as multiple computers being impacted by a ransomware attack, but not necessarily encrypted, 40% in central government and 34% in local government said yes compared to the cross-sector average of 37%.

% respondents hit by ransomware in the last year



In the last year, has your organization been hit by ransomware? [Cross sector: 5400; Central government: 117; Local government:131]

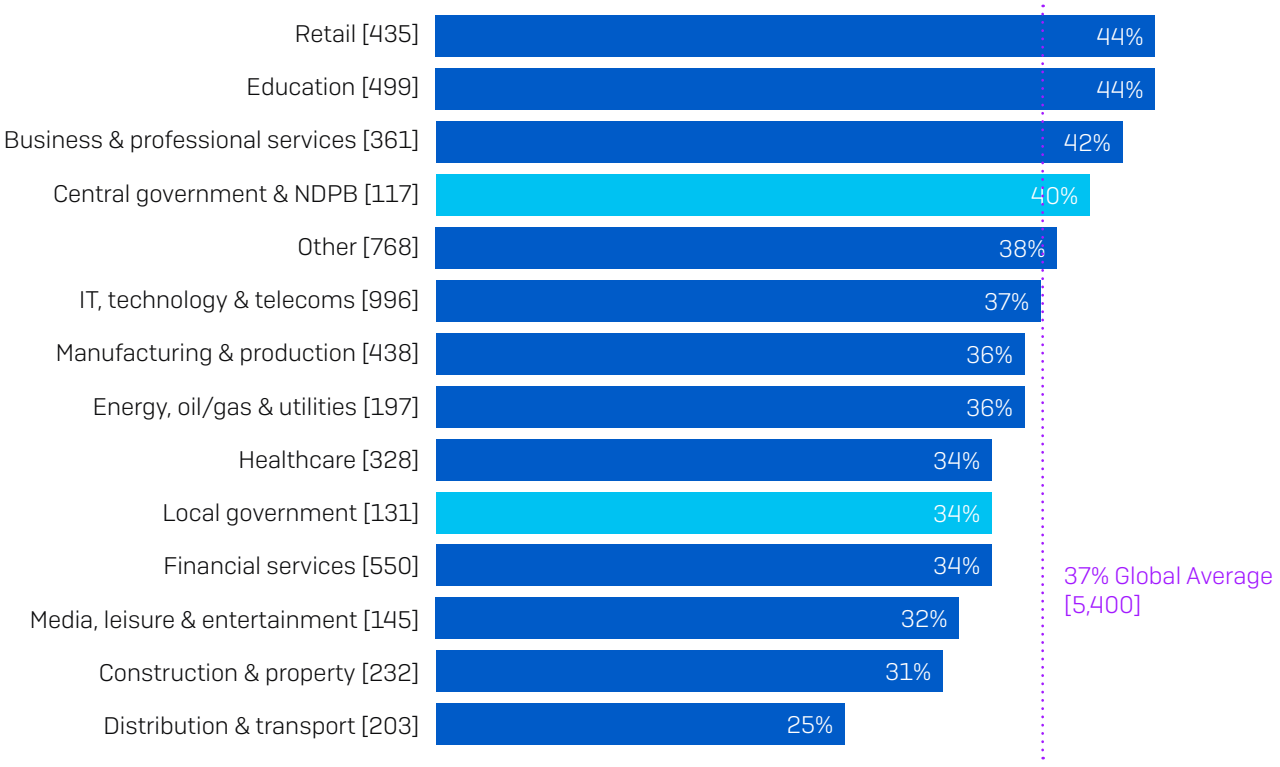
At the same time, 48% in central government and 43% in local government organizations said they were not hit last year, but they expect to be hit in the future. This is higher than the cross-sector average of 41% in both cases, indicating that awareness of the risk of ransomware runs high in government organizations.

When it comes to the percentage of respondents who weren't hit and don't expect to be hit in the future, local government is in line with the cross-sector average at 22%, but central government is far less confident with just 12% of respondents choosing this option. 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.

Government's ransomware experience compared to other sectors

Across all the sectors surveyed, the **retail** and **education** sectors experienced the highest level of ransomware attacks with 44% of respondents in these sectors reporting being hit, while **distribution and transport** were least likely to experience attacks.

% 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

Overall, the percentage of organizations reporting being hit by ransomware has dropped considerably from last year when 51% of survey respondents 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. Many attackers have moved from larger scale, generic, automated attacks to more targeted attacks that include human operated, hands-on-keyboard hacking. As a result, while the overall number of attacks is lower, our experience shows that the potential for damage from these targeted attacks is much higher.

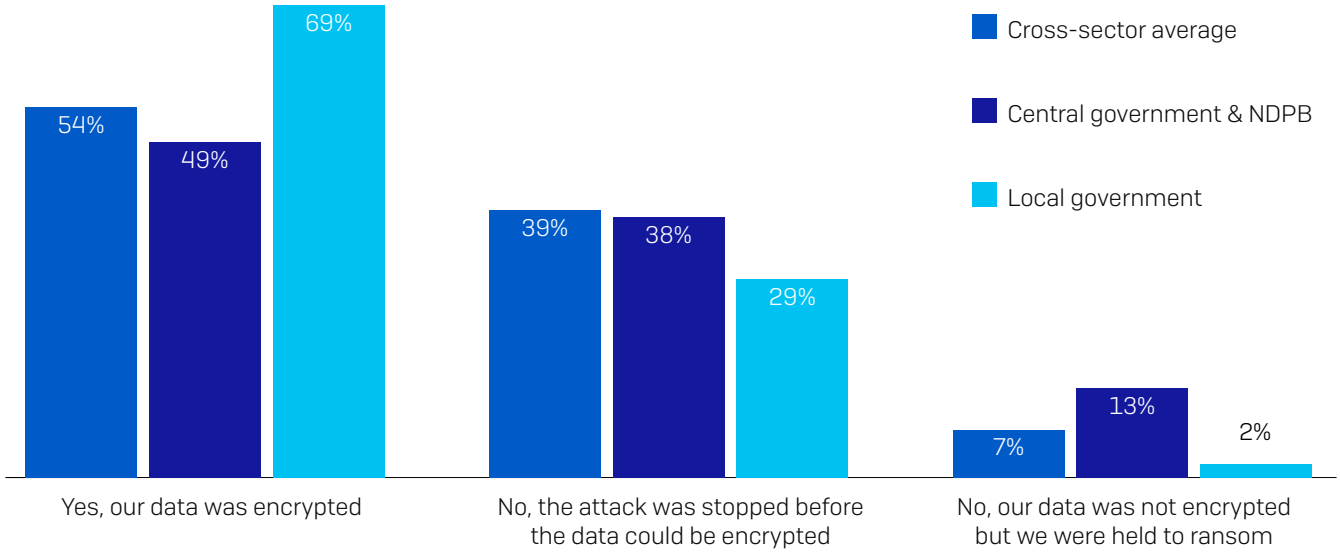
The impact of ransomware

Attackers succeed in encrypting government data

We asked the respondents whose organizations had been hit by ransomware whether the cybercriminals succeeded in encrypting data.

Local government organizations were far less successful at stopping the attacks than many other sectors, with 69% saying their data was encrypted, compared with a global average of 54%. Conversely, **central government and NDPB** organizations had an above-average ability to stop attacks, with just under half (49%) of attacks resulting in data being encrypted.

The ability of government organizations to stop ransomware



Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? [2006 cross-sector; 47 central government & NDPB; 45 local government respondents]

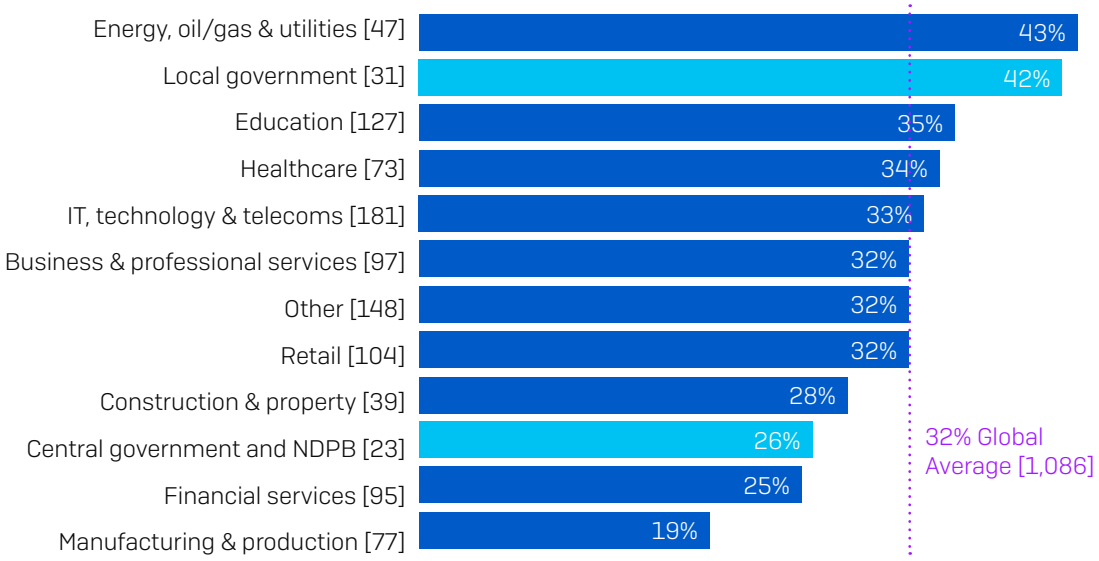
The high encryption rate in **local government** may be due, in part, to the financial and resourcing challenges that IT teams in this sector face. Budgets are constrained, teams are small, and organizations face pressure not to divert funds to cybersecurity that could be used to improve and facilitate public services.

Although, as we saw previously, **central government and NDPB** experienced an above-average level of attacks, they have one of the lowest percentage of attacks in which the data was encrypted. This is likely due in part to their investment in trained IT staff, and use of Security Operations Centers (SOCs) - more on this to come.

However, attackers are pivoting their attack techniques for this sector. The central government and NDPB sector saw the highest percentage of attacks across all industries (and almost double than the global average) where the data was not encrypted, but they were held to ransom based on the threat of exposing the data.

Big differences in propensity to pay the ransom

% 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

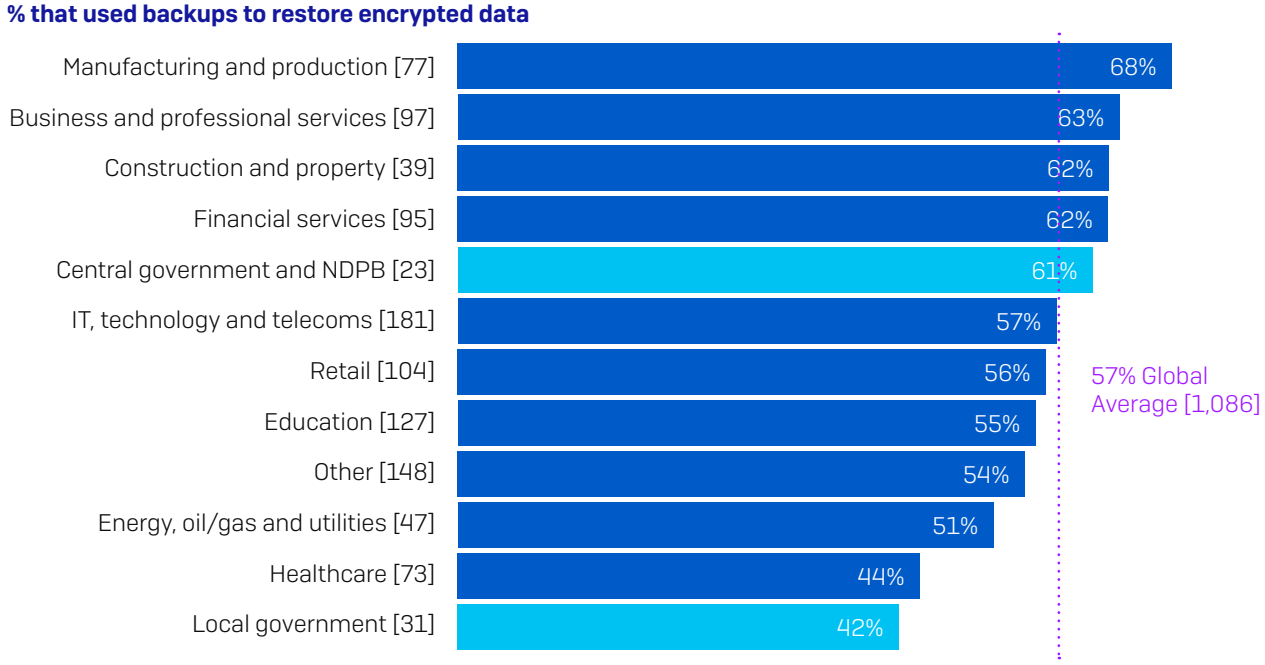
Not only do **local government** organizations experience an above average rate of data encryption – they also have the second highest level of ransom payments (42%) of all sectors. It may well be that the propensity of local government organizations to pay up is driving attackers to focus their more complex and effective attacks on this audience. In parallel, the pressures on local government teams to ensure continuity of public services may also be a driving factor behind them paying the ransom.

Conversely, **central government and NDPB** is near the bottom of the chart, with only 26% paying the ransom to get their data back – much below the cross-sector average of 32%. As we'll see shortly, this sector has other tools at its disposal to restore data. It is important to note that the central government figure is based on 23 respondents so is not statistically significant.

Across sectors, **energy, oil/gas, and utilities** is the sector 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.

Ability to restore data using backups

There is a clear correlation between an organization's propensity to pay the ransom and its ability to restore their data from backups.

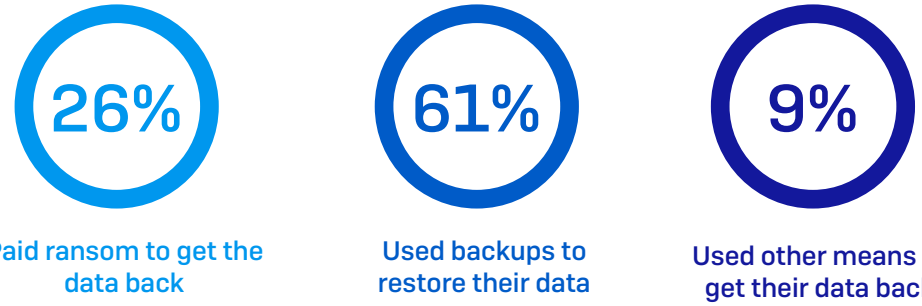


Did your organization get the data back in the most significant ransomware attack?
Yes, we used backups to restore the data [base numbers in chart] organizations where the cybercriminals succeeded in encrypting their data in the most significant ransomware attack, omitting some answer options, split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

Local government is the least able to restore data using backups compared to all other sectors. Globally, 57% of organizations whose data was encrypted were able to restore their data from backups; this drops, however, to just 42% in local government. On the other hand, over six in ten (61%) **central government and NDPB** organizations could restore data using backups, higher than the global average.

96% of central government and NDPB organizations got encrypted data back

Let's now look at the percentage of organizations who could recover their data after it was encrypted. The base number of respondents in central government & NDPB was 23, so the data captured here is not statistically significant. However, anecdotally, 96% of **central government and NDPB** organizations got data back. Of this, 61% restored data using backups, 26% paid the ransom to get data back, and 9% used other means.



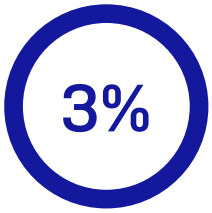
Did your organization get the data back in the most significant ransomware attack? [23] Central government & NDPB organizations responded.

87% of local government organizations got encrypted data back

87% of **local government** respondents whose data was encrypted got data back. This sector saw an equal number of respondents who paid the ransom (42%) and used backups (42%) to restore data. Only 3% used other means to get their data back.

Paid ransom to get the data back

Used backups to restore their data

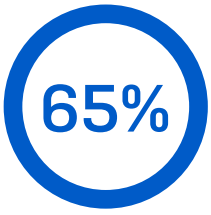


Used other means to get their data back

Did your organization get the data back in the most significant ransomware attack? [31] Local government organizations responded.

Paying the ransom doesn't pay

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 their data, leaving over one third of their data inaccessible.



Percentage of data restored after paying the ransom
CROSS-SECTOR AVERAGE

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

The base number of respondents in central as well as local government organizations was less than 30, so the data for these respondents is not statistically robust. However, anecdotally, **central government** reported getting back on average 63% of their data and **local government** reported getting back 70% of their data on average – a little better than the global average but still leaving a considerable proportion of data inaccessible. Across all sectors, 29% of organizations 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 all sectors who reported that their organization paid the ransom, 282 also shared the exact amount paid.

$ 170,404

Average global ransom payment

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

Globally across all sectors, the average ransom payment was US$170,404. The base number of **central government** respondents was too low to report here. However, anecdotally, 11 respondents in **local government** organizations paid on average US$296,136, almost US$126,000 higher than the average ransom amount.

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

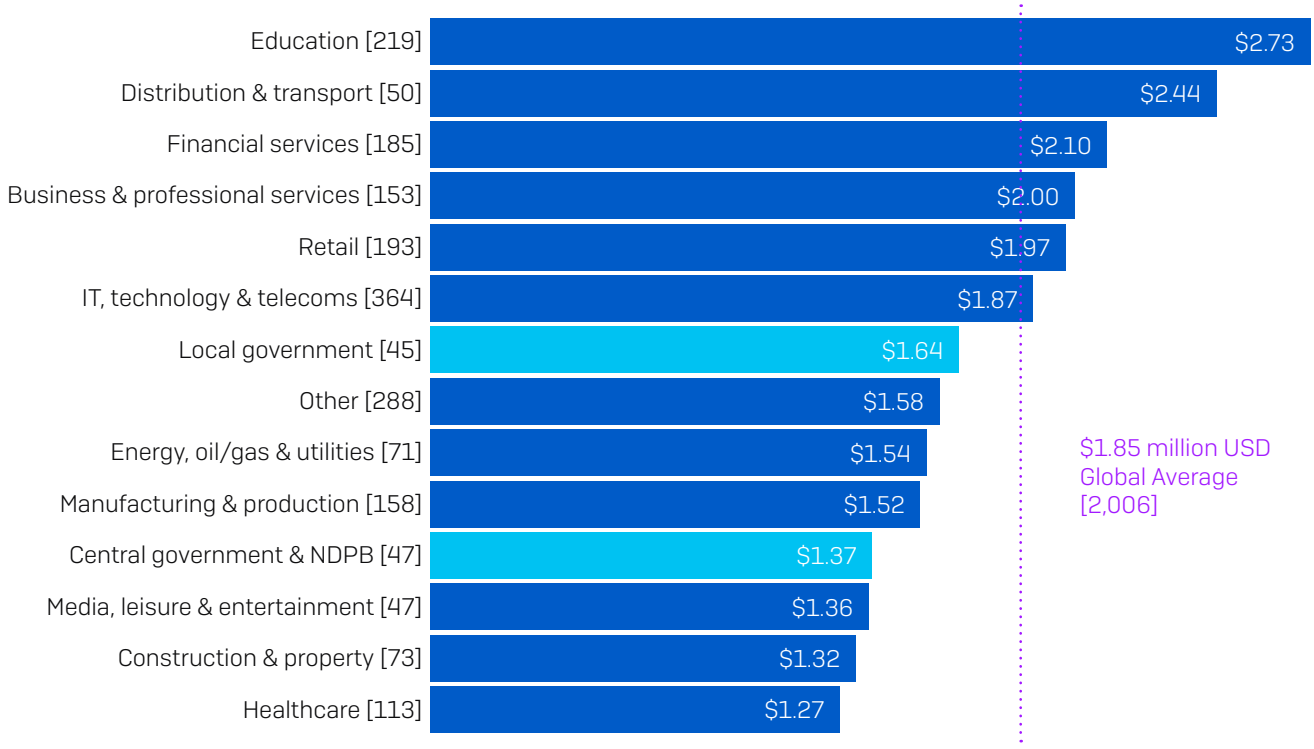
1. **Organization size.** Our respondents are from mid-sized organizations between 100 and 5,000 users who, in general, have fewer financial resources than larger companies. Ransomware actors adjust their ransom demand in line with their victim's ability to pay, typically accepting lower payments from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

The ransomware recovery costs

Moving on to the overall ransomware recovery costs, when we look at the 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, and so on) we see that **local government** has an overall remediation cost of US$1.64 million in comparison with the cross-sector average of 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$

The lower-than-global average cost is likely because local government organizations often have smaller budgets, limiting the amount of money available to be spent on remediation. Additionally, reputational and opportunity costs are generally much lower for public sector organizations than private ones.

Central government reports remediation costs (US$1.37 million) that are much lower than the global average, likely reflecting their strong ability to use backups to restore data and their lower dependence on making ransom payments.

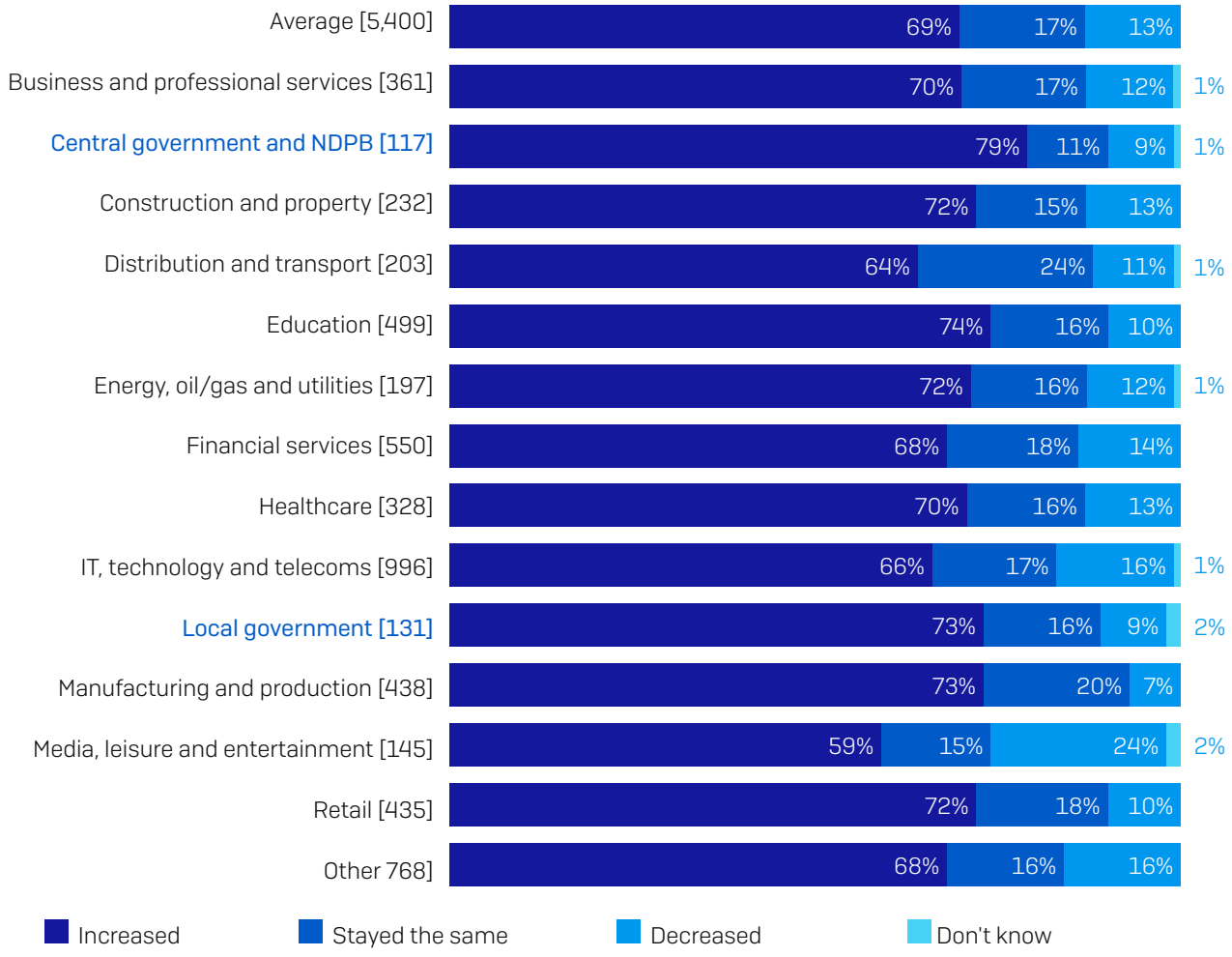
Ransomware is just a part of the cybersecurity challenge

Ransomware is a major cybersecurity issue for government organizations, but not the only one. IT teams are juggling multiple cybersecurity demands, and their challenge has been exacerbated by the pandemic.

Cybersecurity workload increased in 2020

We asked the survey respondents how their cybersecurity workload had changed over the course of 2020. **Central government and NDPB** reported the highest increase of all sectors, with almost four in five (79%) saying their workload went up. **Local government** was not far behind with 73% reporting an increase. In comparison, the cross-sector average was 69%.

How cybersecurity workload changed over the course of 2020



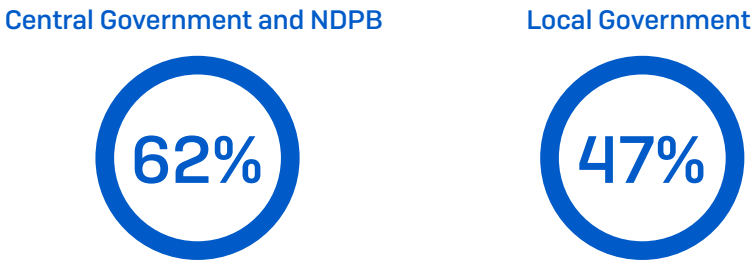
Over the course of 2020, our cybersecurity workload has decreased/increased/stayed the same [5,400]

The key role played by government organizations in responding to the pandemic is likely a major factor behind the increase in workload: IT teams were central to the continued delivery of essential services while also enabling government organizations to meet new needs of their citizens. This increased workload likely reduced IT teams' capacity to monitor for and respond to ransomware threats.

Attacks are getting harder to stop

Threats are also constantly growing more advanced. Adversaries are using myriad tactics, techniques and procedures (TTPs) in the course of an attack, often combining automation with legitimate IT tools to bypass an organization's defenses. Dealing with these evolving attacks is becoming increasingly challenging – in fact, for over half of the survey respondents (54%) cyberattacks are now too advanced for their IT team to deal with on their own.

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



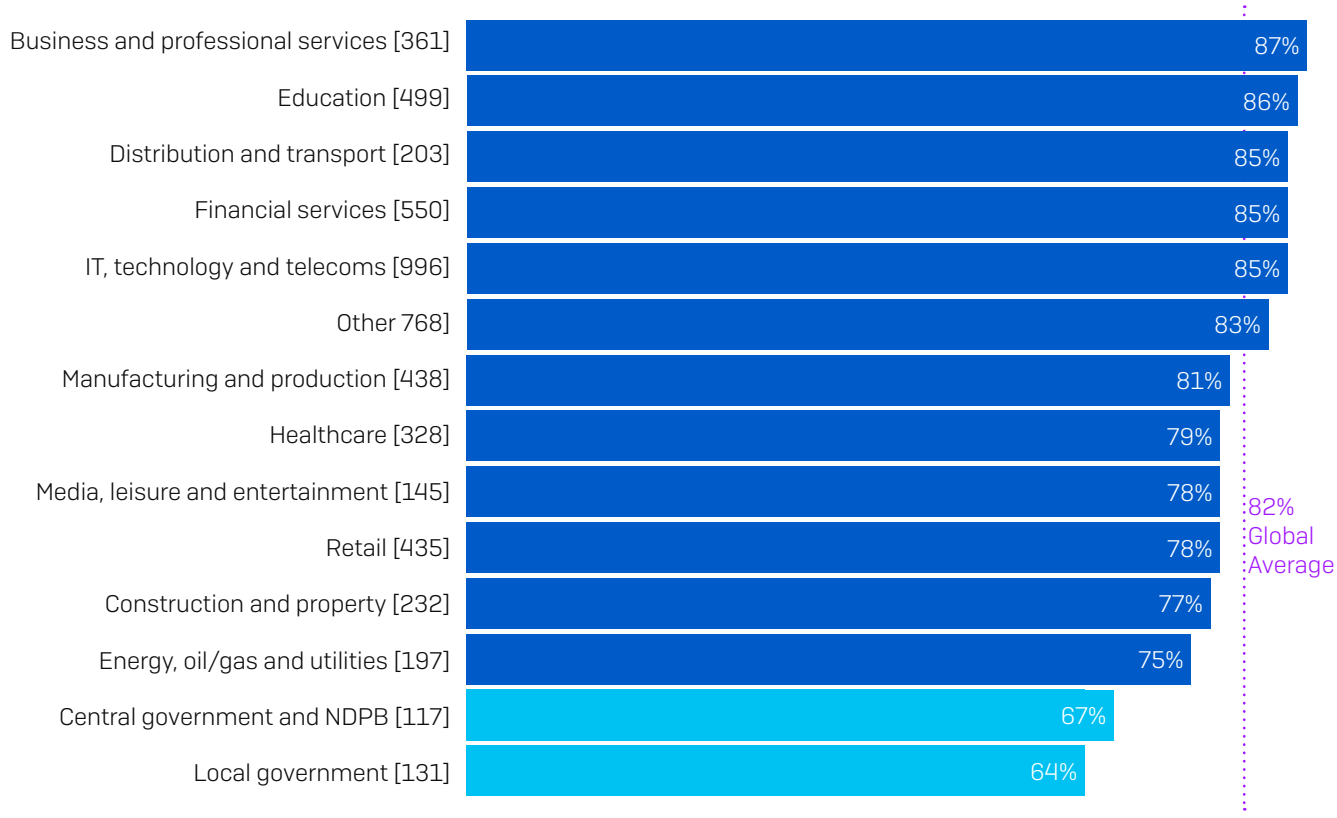
Cyberattacks are now too advanced for my organization's IT team to deal with on their own: Strongly agree, Agree. Excluding some answer options [Central government: 117; Local government: 131]

This challenge is particularly acute for **central government and NDPB**, with 62% admitting attacks are beyond their in-house skills. Conversely, **local government** reported the fewest challenges with in-house capabilities, with 47% of respondents saying the attacks are now too complex for their IT team to deal with on their own. In the case of the local government, this is surprising, given, as we have seen, this sector is the most likely to have their data encrypted in a ransomware attack.

Readiness to take on future challenges

Having the right tools and knowledge is key to being able to investigate and address cyberthreats. It's encouraging that 82% of IT decision makers say they have the tools and knowledge they need to investigate fully suspicious activities in the face of increased workload and frequency of cyberattacks. However, there are two clear outliers: **central** and **local government.**

Have the tools and knowledge to investigate suspicious activity



If I detect suspicious activities in my organization, I have the tools and knowledge I need to investigate fully: Strongly agree, Agree. Excluding some answer options [5,400]

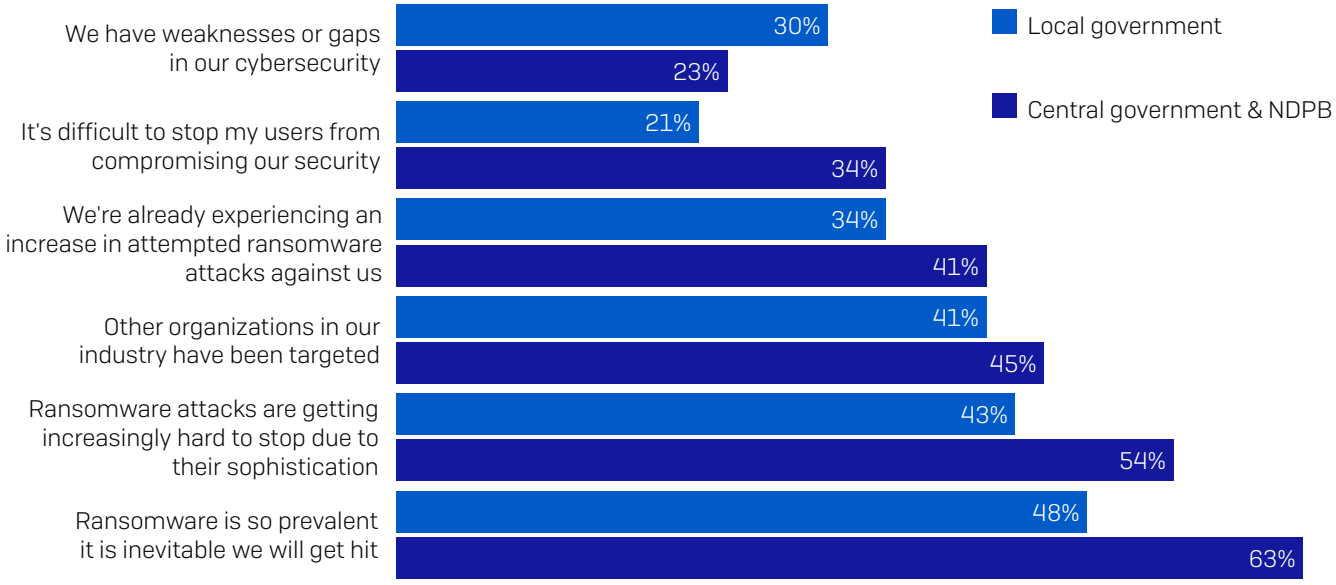
Lack of budget may play a part here, with public sector funding being and ongoing challenge in many countries. Either way, with threat actors continuing to refine their attack techniques, it's essential that IT teams in government are given the resources to catch up with other sectors.

The future

As we saw at the start of this report, almost half of the government respondents (48% in **central government** and 43% in **local government**) who reported that they hadn't been hit by ransomware in the last year expect to be hit by ransomware in the future – compared to a cross-sector average of 41%. Conversely, 12% in **central government** and 22% in **local government** don't anticipate a future ransomware attack.

Why the government sector expects to be hit

Among the government organizations that weren't hit by ransomware but expect to be in the future, the most common reason (**central government:** 63%; **local government** 48%) is that ransomware is so prevalent it is inevitable they will get hit. In addition, 54% in central government and 43% in local government said that ransomware attacks are getting increasingly hard to stop due to their sophistication.



Why do you expect your organization to be hit by ransomware in the future? [56/56] organizations that haven't been hit by ransomware in the 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 their ability to block any potential ransomware attack last year.

45% in central government and 41% in local government believe that because others in their industry have been targeted, they are likely to be hit too.

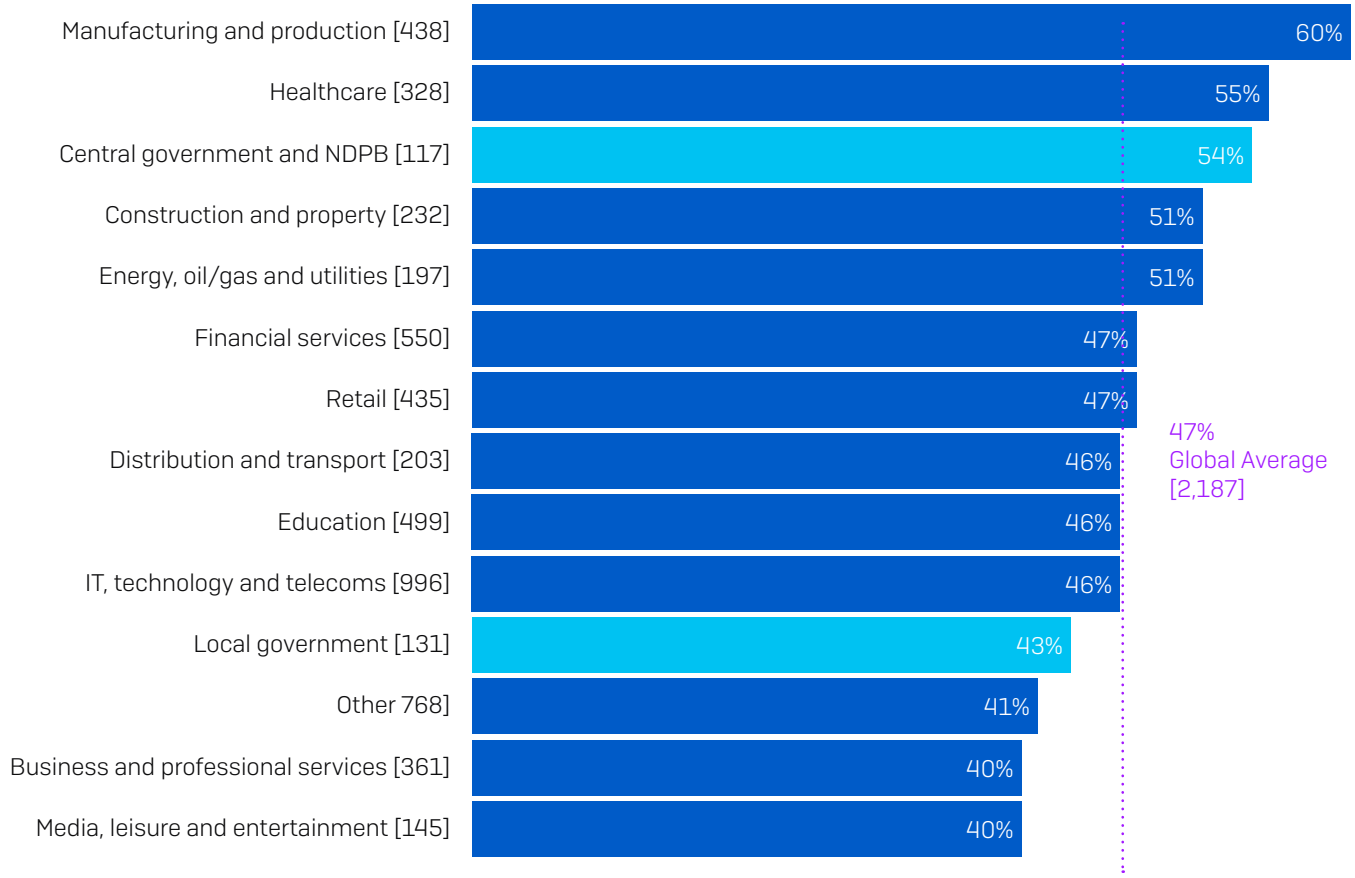
Local government (30%), along with the education sector, is the sector most likely to admit to having weaknesses or gaps in its cybersecurity. This number is 23% for central government respondents. While it's clearly not a good idea to have security holes, recognizing these issues is an important first step to enhancing your defenses.

Over a third (34%) of central government respondents blame their users for compromising security and putting them at risk of ransomware. This is much higher than the global average of 22% and the 21% of local government respondents.

Awareness of increasing sophistication of ransomware

Diving deeper, we see that **central government** is one of the sectors most alert to the growing sophistication of ransomware, with 54% of respondents citing this as a reason why they expect to to be hit in the future. Conversely, **local government** (43%) is just below the cross sector average (47%).

% 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

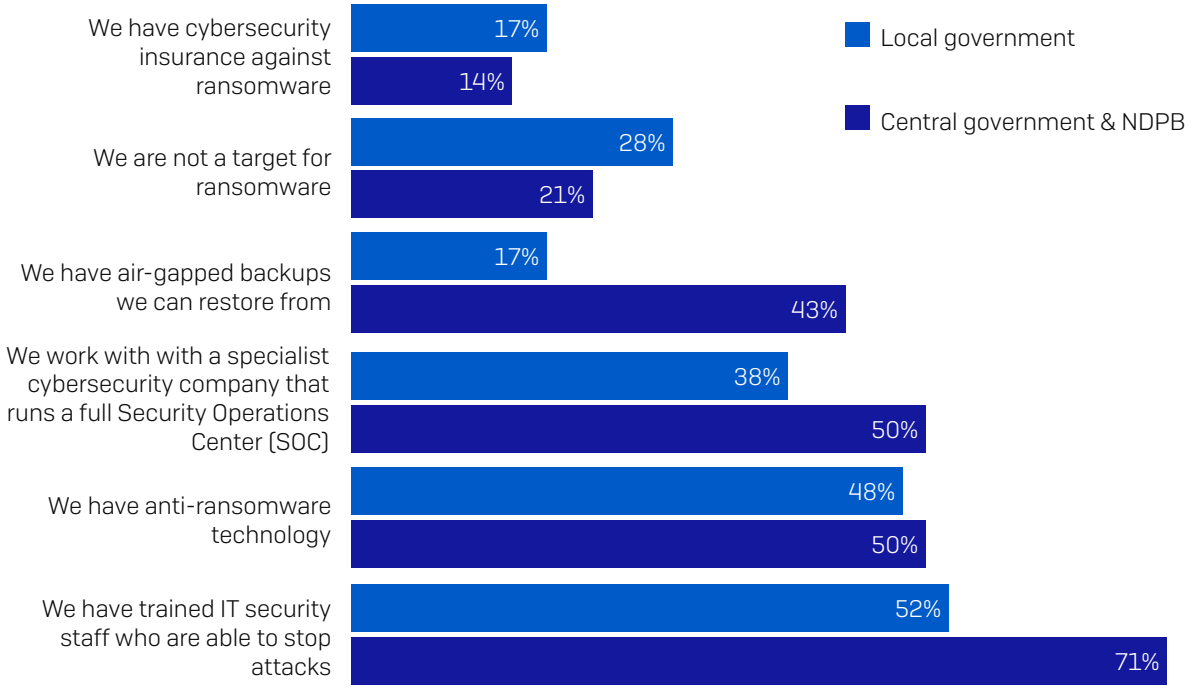
While the respondents to this question weren't themselves hit by ransomware last year, it is likely that they have been influenced by the broader ransomware experiences in their sectors – and the government sector has borne the brunt of many successful attacks.

Trained IT staff give ransomware confidence

29 local government and 14 central government respondents answered this question so the findings should be considered indicative only.

Among the government respondents that weren't hit by ransomware in the last year and don't expect to be hit in the future, the #1 reason for this confidence is having trained IT staff who are able to stop attacks, followed by the use of 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? [29 local government/14 central government] Organizations that haven't been hit by ransomware in the last year and do not expect to be in the future, omitting some answer options

A strong 71% of **central government** respondents reported to have invested in trained IT staff, along with 52% in **local government**. Half (50%) of the central government respondents and 38% of local government respondents who don't expect to be hit by ransomware work with a specialist cybersecurity company that runs a full Security Operations Center (SOC).

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. We strongly recommend all organizations build up their human expertise in the face of the ongoing ransomware threat.

It is also encouraging to note that around half of the survey respondents have deployed anti-ransomware technology.

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

- 57% of central government and 31% of local government respondents that don't expect to be hit are putting their faith in approaches that don't offer any protection from ransomware.
  - 43% of central government respondents cited air-gapped backups as a reason why they don't expect to be hit, along with 17% in local government. This is a cause for concern as while backups – as we have seen – are valuable tools for restoring data post attack, they don't stop you getting hit by ransomware.
  - 14% of central government and 17% of local government respondents said that having cybersecurity insurance protects them from being hit by ransomware. Again, this can help deal with the aftermath of the attack, but doesn't prevent it in the first place.

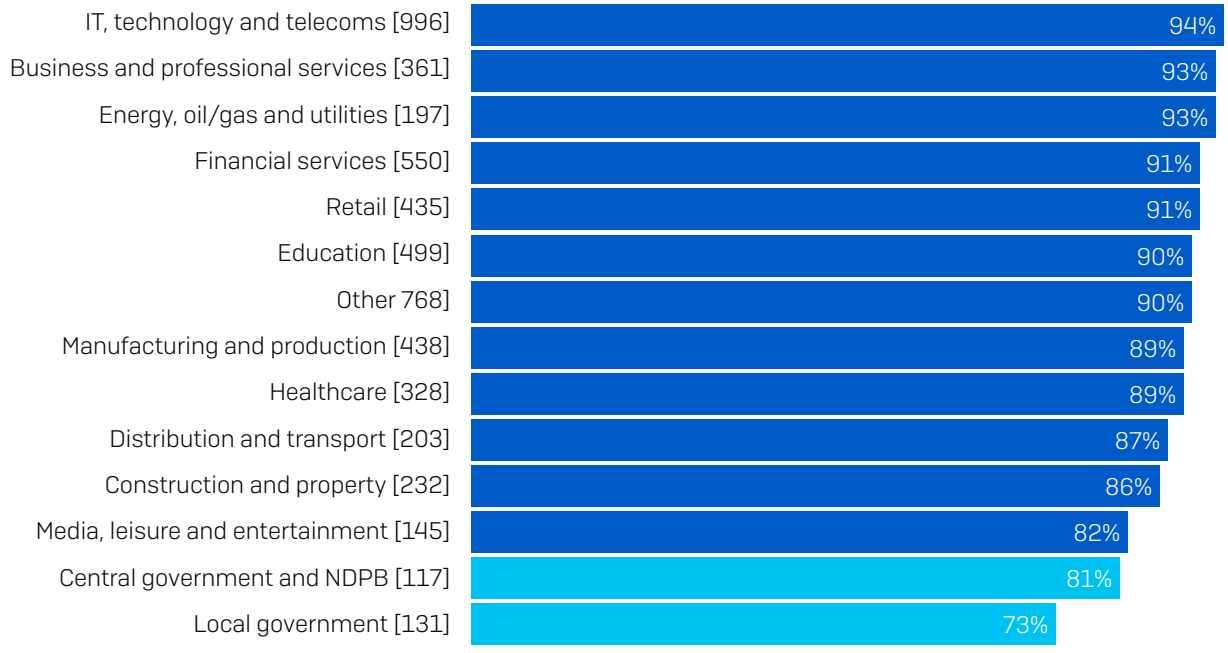
  N.B. Some respondents selected both the above options, with 57%/31% selecting at least one of these two options.
- 21% and 28% in central and local government respectively believe that they are not a target of ransomware. Sadly, this is not true. No organization is safe.

Government organizations are least prepared for a major malware incident

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.

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

Have a plan to recover from a major malware incident



Does your organization's Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP) include plans to recover from a major malware incident? Yes, we have a full and detailed malware incident recovery plan and Yes, we have a partially developed malware incident recovery plan [base numbers in chart], omitting some answer options, split by sector

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** is most likely to experience extortion. The lack of a malware recovery plan may be a contributing factor to the fact that local government is the second-most likely to pay the ransom.

Summary

Local government

The survey reveals that local government is caught up in a vicious ransomware circle, fueled by its inability to defend against ransomware. Even though this sector experienced a below average number of attacks, it has the lowest ability of all sectors to stop data encryption and to restore data using backups. As a result, local government is one of the sectors with the highest propensity to pay the ransom – further encouraging attackers to target local government organizations.

While this sector recognizes gaps in their cybersecurity, it ranks the lowest as far as implementation of a malware recovery plan is concerned. The sector needs to take urgent action to address the situation.

Central government

Central government and NDPB is more skilled in stopping ransomware than local government due to its high investment in trained IT professionals and SOCs. Even though this sector experienced above-average levels of attacks, it has one of the lowest levels of data encryption. It is also one of the sectors most able to restore data using backups.

However, in the face of central government's success in defending against ransomware, attackers are turning to extortion-style attacks where they steal data and then threaten to expose it unless a ransom is paid. This sector experienced the highest number of such attacks last year – almost double the cross-sector average.

The central government sector needs to keep up its momentum against ransomware, and also focus on preventing attackers accessing data in the first place. Creating a malware incident recovery plan should be a priority for those organizations that do not yet have one.

Recommendations

In light of the survey findings, Sophos experts recommend the following best practices for all organizations across all sectors:

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 more difficult 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.

2021-06-10 (SB-NP)

SOPHOS