SOPHOS
Cybersecurity evolved.

The State of Ransomware in Retail 2021

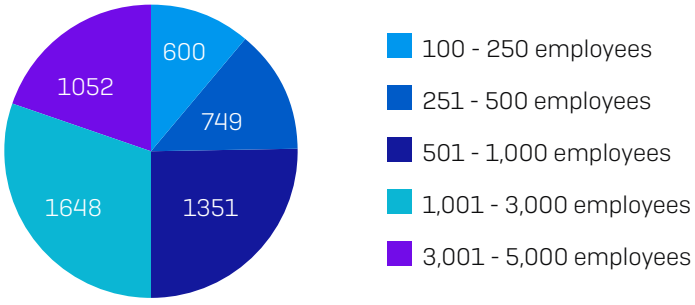
Based on an independent survey of 435 IT decision makers, this report shares new insights into the current state of ransomware in the retail sector. It provides a deep dive into the prevalence of ransomware in retail, the impact of those attacks, the cost of ransomware remediation, and the proportion of data that retail organizations could recover after an attack. The survey also reveals how retail stacks up with other sectors, as well as the future expectations and readiness of retail organizations in the face of these attacks.

A Sophos Whitepaper. August 2021

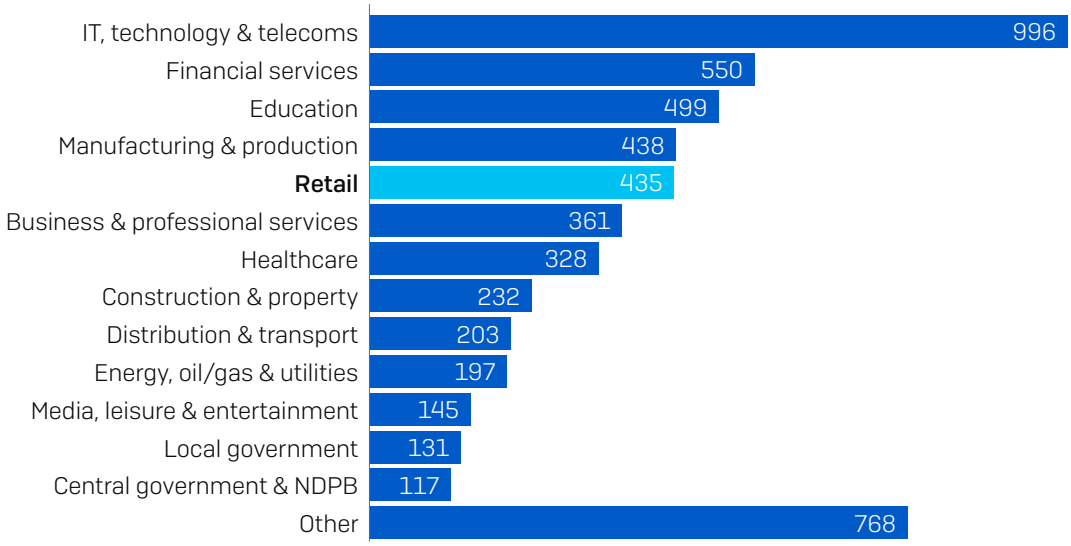
About the survey

Sophos commissioned a global survey of 5,400 IT managers across 30 countries by the independent research house Vanson Bourne. Respondents came from a wide range of sectors, including 435 respondents from retail 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 435 retail IT decision makers came from all geographic regions surveyed: the Americas, Europe, the Middle East, Africa, and Asia Pacific.

Region	# Respondents
Americas	146
Europe	147
Middle East and Africa	55
Asia Pacific	87

435 IT decision makers in retail

Key findings in Retail

- **44%** of retail organizations **were hit by ransomware in the last year**
- **54%** of organizations hit by ransomware said the **cybercriminals succeeded in encrypting their data** in the most significant attack
- **32%** of those whose data was encrypted **paid the ransom to get their data back** in the most significant ransomware attack
- The **average ransom payment** was **US$147,811**
- However, **those who paid the ransom got back just 67% of their data** on average, leaving almost a third of the data inaccessible
- The **average bill for rectifying a ransomware attack in the retail sector**, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, and more, was **US$1.97 million**
- **56%** of those whose data was encrypted **used backups to restore data**
- **91%** of retail organizations have a **malware incident recovery plan**

Retail, together with education, was the sector most hit by ransomware in 2020. Cybercriminals were quick to exploit opportunities presented by the pandemic, which in the retail sector was primarily the rapid growth in online shopping. Some retail organizations started trading online for the first time, while others saw a huge increase in their web traffic and the percentage of transactions that happened online.

Enabling and managing this change introduced new challenges for IT teams while also consuming significant capacity: nearly three quarters (72%) of respondents said their cybersecurity workload increased over 2020. The good news is that, in light of this increase in workload, 77% of IT teams in retail said their ability to develop cybersecurity knowledge and skills increased over the course of 2020, *the highest among all industries*.

The growth in online retail also exacerbated existing security challenges facing the retail sector, including the extensive use of legacy systems that are harder to maintain and update, and frequent mergers and acquisitions that require IT teams to integrate disparate systems. Add to this the need to protect a wide range of valuable information, including customers' personal and financial data, and the challenge of securing complex, distributed environments, and it is easy to see why retail is an attractive target for cybercriminals.

In the face of these challenges, almost a third (32%) of retail organizations whose data was encrypted paid the ransom to get their data back, which is in line with the cross-sector average. However, those who did pay only got back, on average, 67% of their data, leaving almost a third inaccessible, and just 9% got all their encrypted data back. While this is slightly higher than the global average (65%/8%), it's clear that paying the ransom doesn't really pay off.

While the average ransom paid by retail organizations (US$147,811) is considerably below the cross-sector average (US$170,404), the overall average ransomware recovery cost comes in higher than the global average (US$1.97 million vs. US$1.85 million). This is likely due to high costs of notifying individuals whose data has been breached, as well as the considerable impact of reputational damage in this sector – it's generally much easier to switch to a different retailer than to a different school or hospital.

Retail organizations should prioritize strengthening their defenses against ransomware. Investing in modern infrastructure, together with cybersecurity technology and skills, will considerably reduce both the overall cost and impact of ransomware.

The prevalence of ransomware in retail

Retail's experience with ransomware last year

Of the 435 retail sector respondents that were surveyed, 44% were hit by ransomware in the last year, defined as *multiple computers being impacted by a ransomware attack, but not necessarily encrypted*.

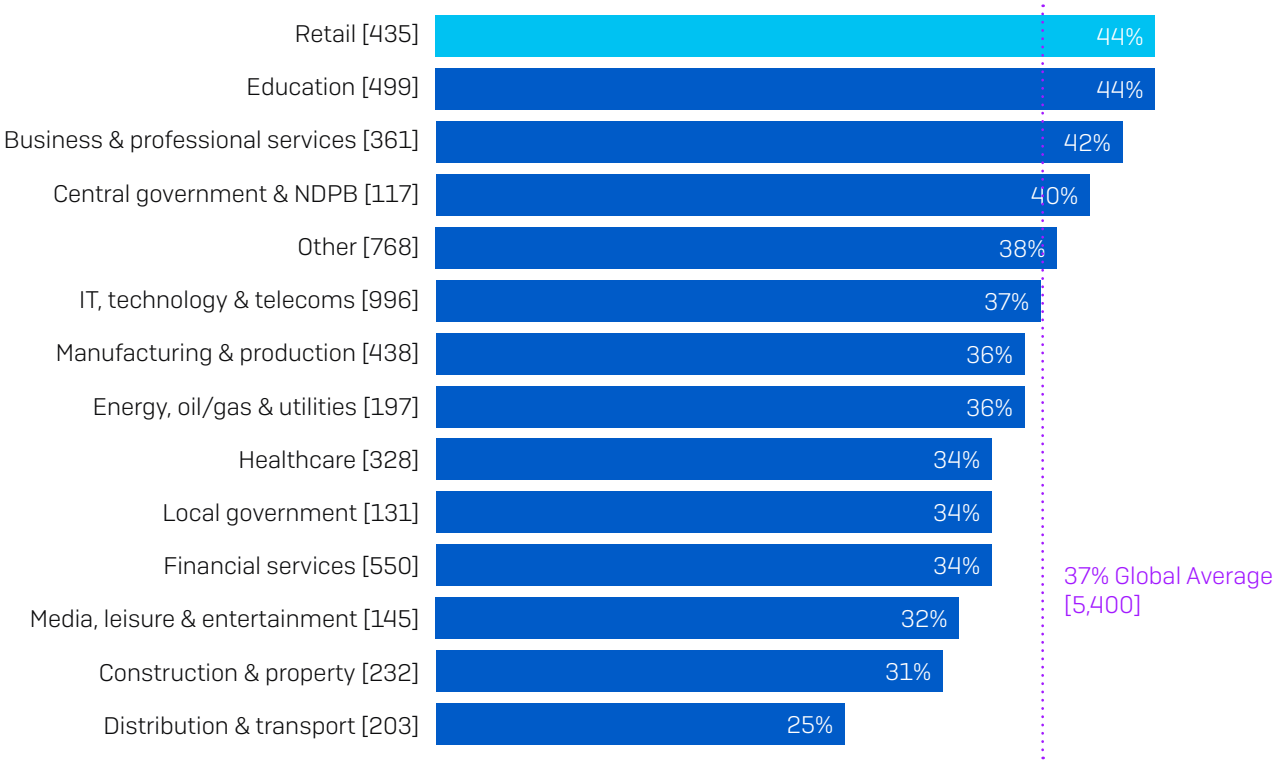
In the last year, has your organization been hit by ransomware? [435 retail respondents]

Among the organizations not hit last year, 34% said they expected to be hit by ransomware in the future, while 21% were confident that they are safe from future attacks. We'll dive deeper into the reasons behind the expectation to be hit in the future, as well as what gives others confidence in the face of future attacks, later in the report.

Retail saw the highest level of ransomware attack

Looking at the prevalence of ransomware across all the sectors surveyed, retail, along with education, experienced the highest level of ransomware attacks: 44% of respondents in these sectors reported being hit compared to the global average of 37%.

% respondents hit by ransomware in the last year



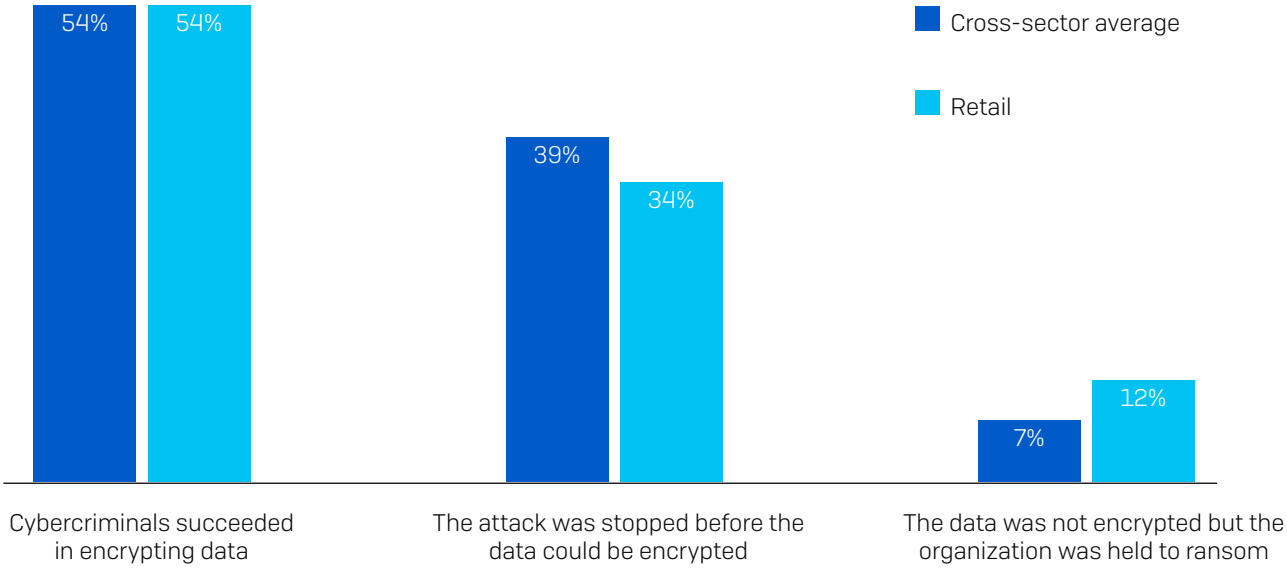
In the last year, has your organization been hit by ransomware? Yes [base numbers in chart] omitting some answer options, split by sector

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 team. 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

Ability of retail to stop data encryption

We asked those organizations that were hit with ransomware whether the cybercriminals succeeded in encrypting their data. 54% of retail respondents said their data was encrypted, which is the same as the global average.



Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? [2006 cross-sector; 193 retail establishments that have been hit by ransomware in the last year]

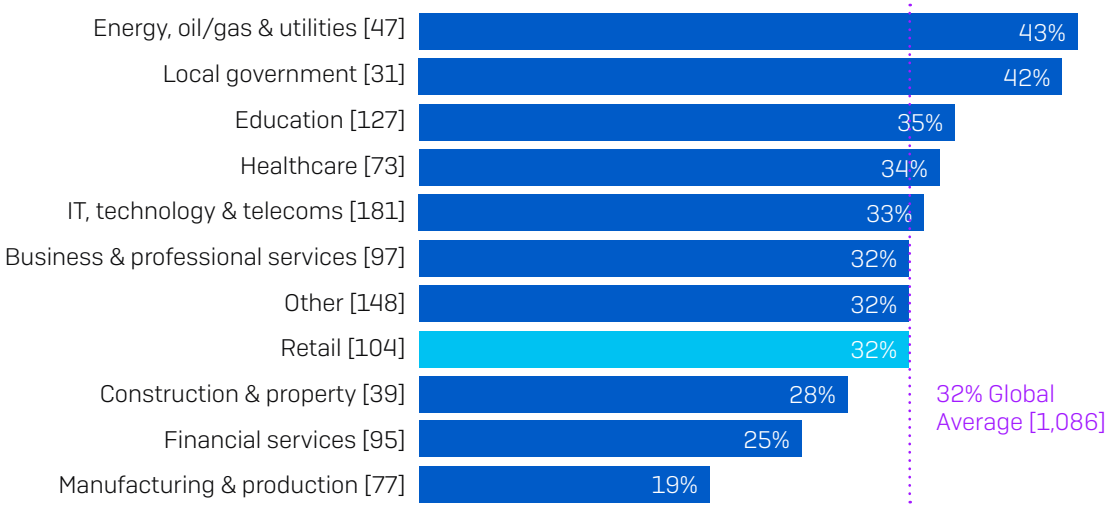
Retail organizations are less successful at stopping encryption than the global average: 34% vs. 39%. This sector also saw the second highest number of attacks across all industries (12% vs 7% of global average) where the data was not encrypted but they were held to ransom based on the threat of exposing the data.

SophosLabs has seen an increase in extortion-style attacks over the last year where, instead of encrypting files, adversaries steal data and threaten to publish it unless the ransom demand is paid. This requires less effort on the part of the attackers as 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.

Propensity to pay the ransom

Retail organizations (32%) are on par with the global industry average (32%) when it comes to propensity to pay the ransom to get their data back. This is encouraging to note given that retail sector is, along with education, the most hit by ransomware.

% 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

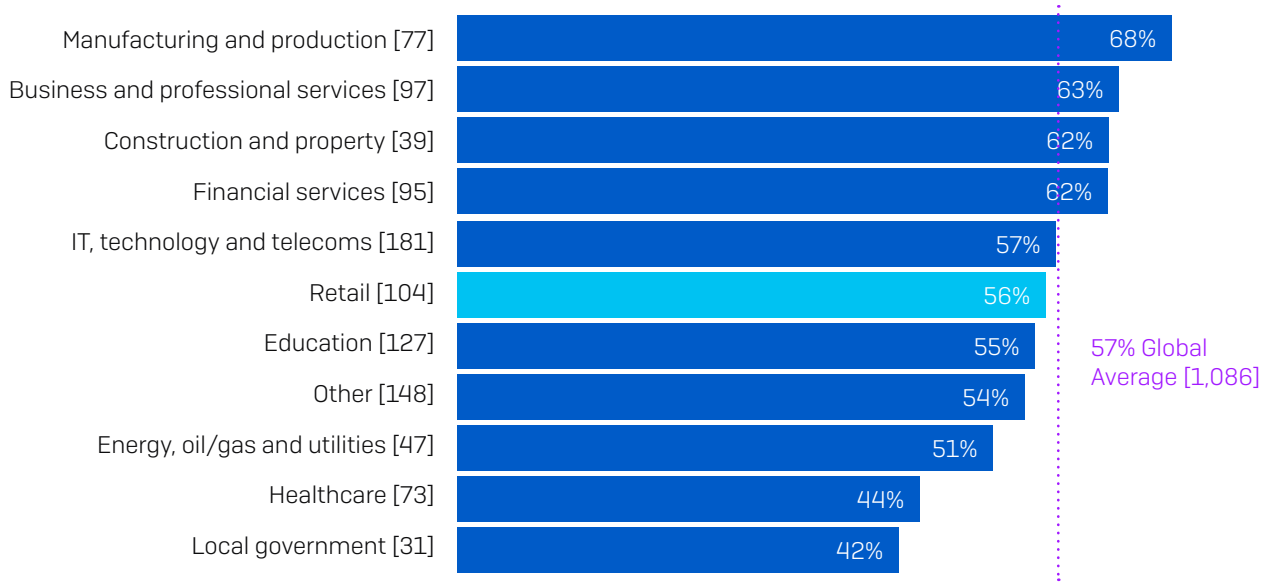
Across sectors, the **energy, oil/gas, and utilities sector** is most likely to pay the ransom, with 43% submitting to the ransom demand. This sector typically has a lot of legacy infrastructure that cannot easily be updated, so victims may feel compelled to pay the ransom to enable continuation of services.

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.

Ability to restore data using backups

There is a correlation between ability to restore data from backups and propensity to pay the ransom, with those organizations most able to use backups also least likely to pay up.

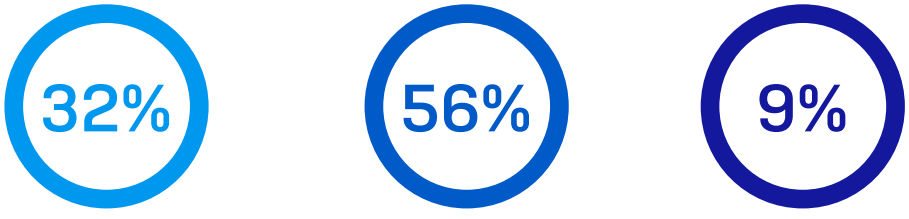
% that used backups to restore encrypted data



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

In the previous chart we saw that retail's likeliness to pay the ransom was in line with the global average. Similarly, 56% of retail organizations were able to restore their data from backups – a notch lower than the global average of 57%.

97% got encrypted data back



Did your organization get the data back in the most significant ransomware attack? [104] retail organizations responded.

The good news for retail organizations is that 97% of those whose data was encrypted got it back. As we've seen, 32% paid the ransom, 56% used backups, and 9% used other means to get their data back.

Paying the ransom only gets you some of your data

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

Percentage of data restored after paying the ransom **RETAIL AVERAGE**

Average amount of data organizations got back in the most significant ransomware attack. [344/33] organizations that paid the ransom to get their data back

The bad news, however, is that retail organizations that paid the ransom rarely got *all* their data back. On average, those that paid out got back just 67% of their data, leaving almost a third inaccessible. This is slightly better than the global average (65%) but still leaves a considerable proportion of the data inaccessible.

Got ALL their data back

Got half or less of their data back

Average amount of data Retail organizations got back in the most significant ransomware attack. [33] organizations that paid the ransom to get their data back

In fact, just 9% of retail organizations that paid the ransom got back all their data, and 24% got back **half or less** of their data. Clearly paying up doesn't pay off.

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, including 36 in the retail sector.

$ 170,404

Average GLOBAL ransom payment

$ 147,811

Average RETAIL ransom payment

How much was the ransom payment your organization paid in the most significant ransomware attack? [282/36] organizations that paid the ransom to get their data back

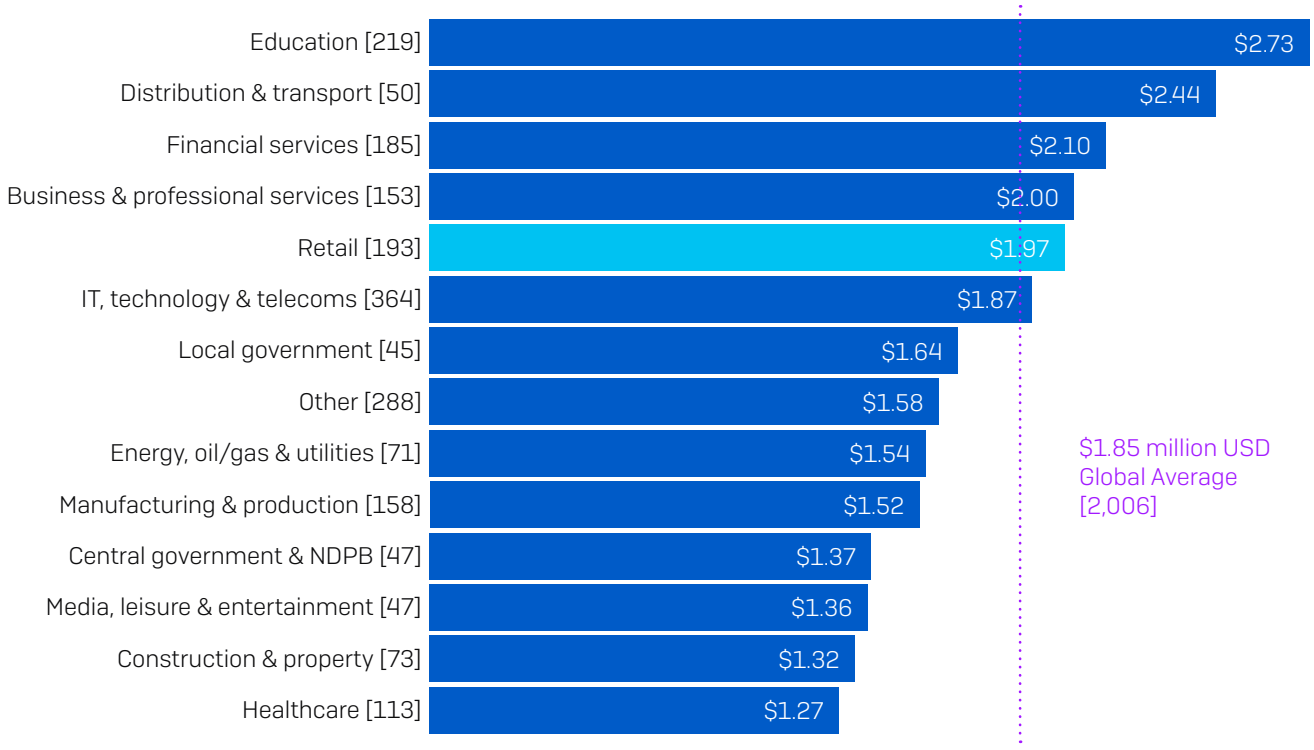
Globally across all sectors, the average ransom payment was US$170,404. However, in retail, the average ransom payment was almost US$23,000 lower, coming in at US$147,811.

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 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).

Ransomware recovery cost in retail

The ransom is just a small part of the overall cost of recovering from a ransomware attack. Victims face a wide range of additional expenses including the cost to rebuild and secure their IT systems, PR, and forensic analysis.



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 survey revealed that the retail sector experiences an average remediation cost of US$1.97 million (considering downtime, hours lost, device cost, network cost, lost opportunity, ransom paid, and so on), which is above the global average (US$1.85 million).

There are several likely factors behind this. Firstly, due to the nature of their business, retail organizations typically hold a lot of sensitive data, including their customers' personal as well as financial information. As a result, they are disproportionately affected by the high costs of dealing with a data breach, which include notifying affected individuals and putting in place credit monitoring services. Secondly, retail is far more impacted by reputational damage than many other sectors – it's generally much easier to switch to a different retailer than to a different school or hospital. Another factor contributing to high recovery costs in this sector is the need to often rebuild legacy systems from the ground up in the wake of an attack.

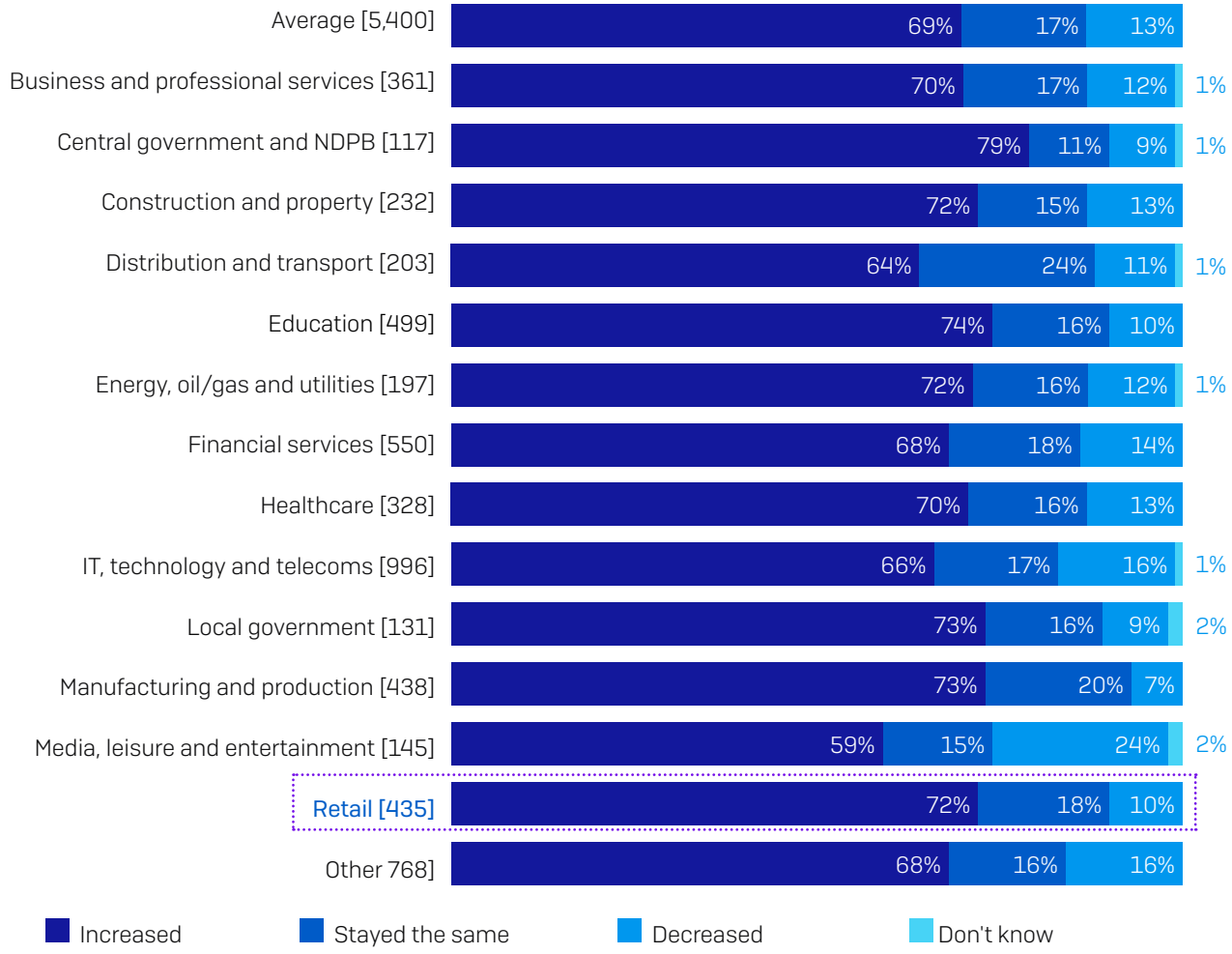
Ransomware is just a part of the cybersecurity challenge

Ransomware is a major cybersecurity issue for retail 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.

How cybersecurity workload changed over the course of 2020



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

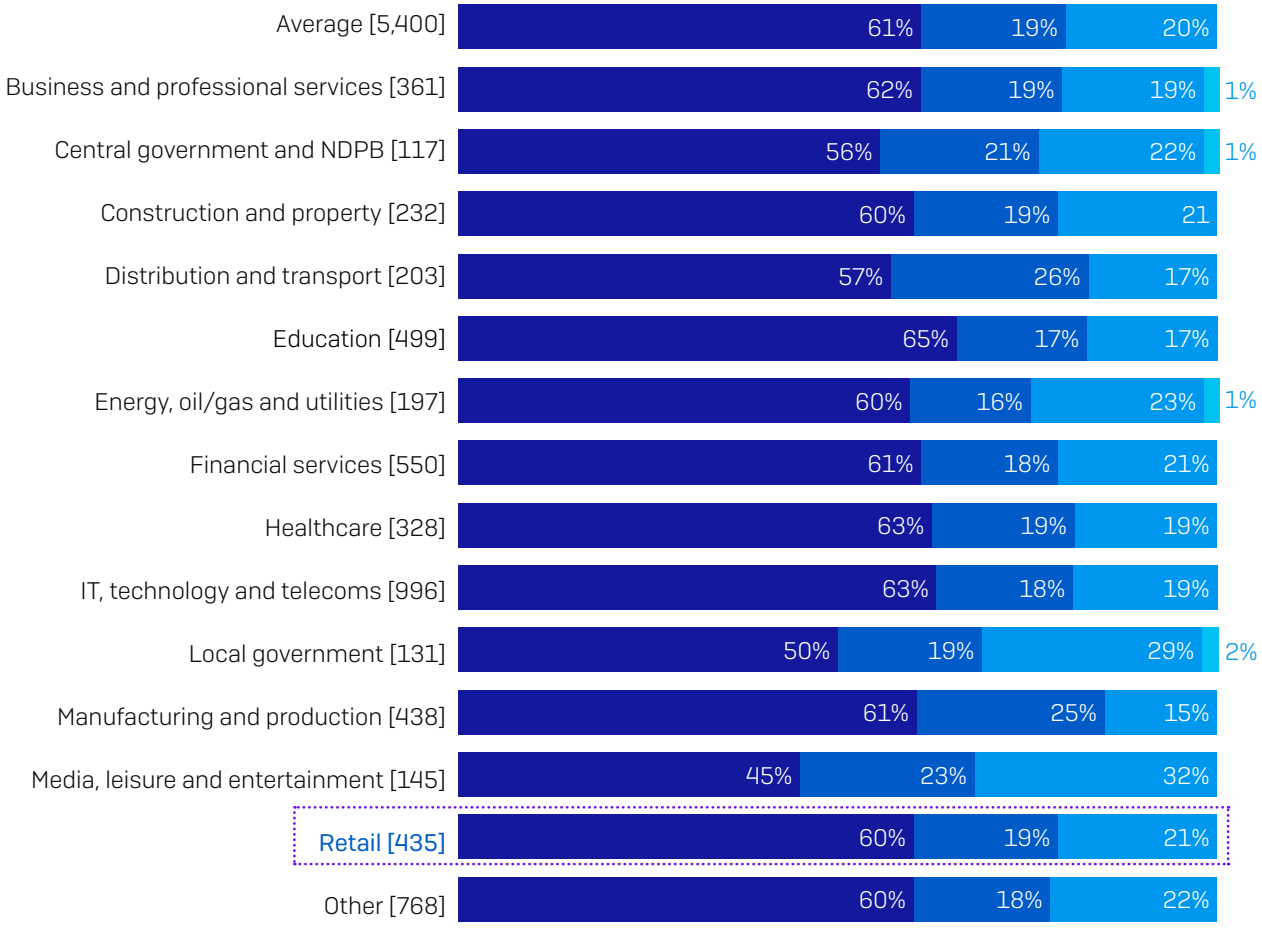
IT teams in the retail sector were impacted by the pandemic, with 72% experiencing an increase in cybersecurity workload over the course of 2020. While the majority of respondents in all sectors reported an increase, central government saw the most increase in growth in workload.

The switch to online shopping was likely a major factor behind the increased workload with IT teams needing to secure new online platforms as well as the increased traffic to their online sites. The heavy focus on securing online platforms would have likely reduced IT teams' capacity to monitor for and respond to ransomware threats.

Increased workload slowed response times

One of the consequences of the increase in cybersecurity workload over 2020 was a slowdown in response time to IT cases.

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



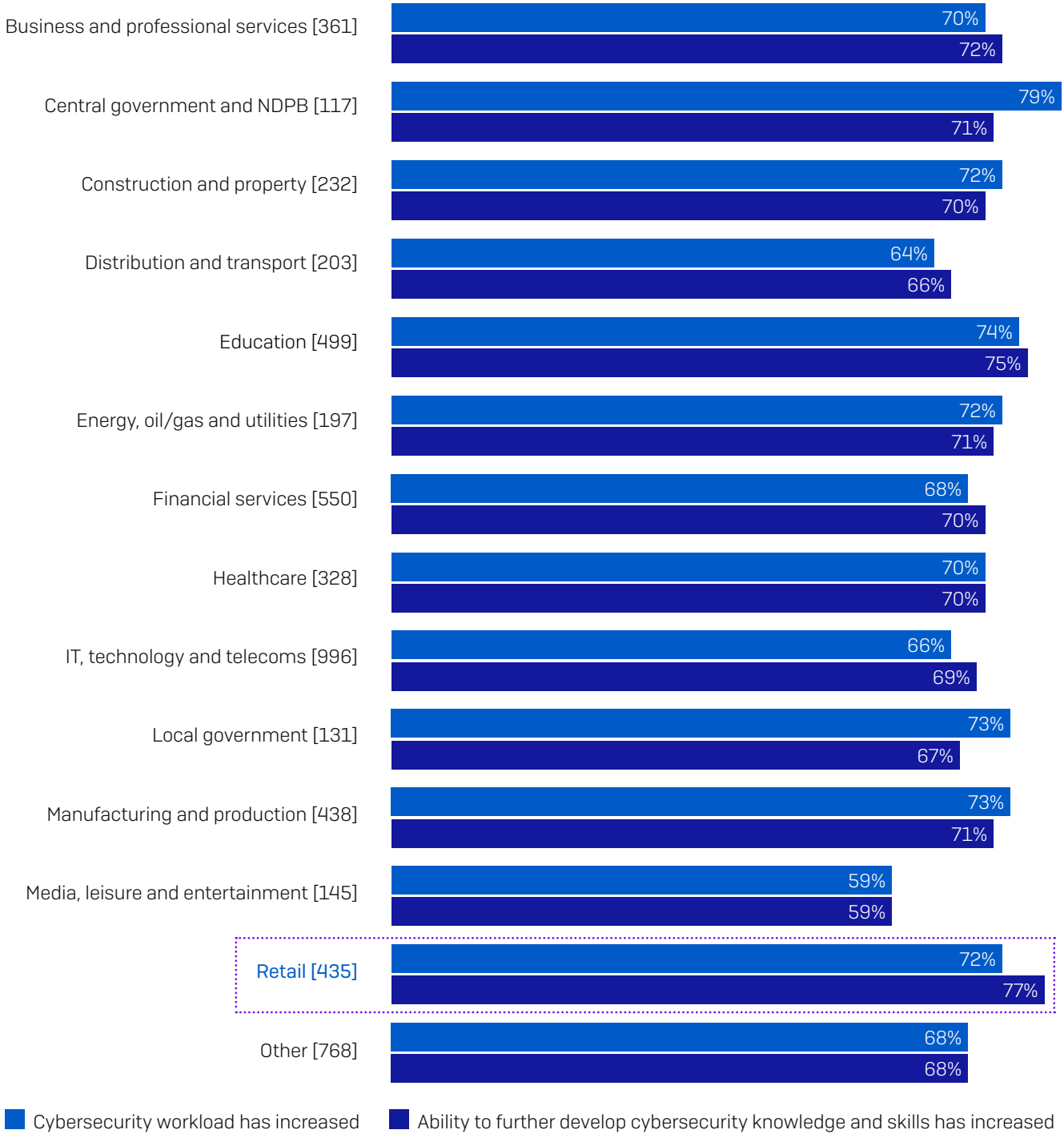
Over the course of 2020, our response time to IT cases has decreased/increased/stayed the same. [base sizes in chart], split by sector. N.B. Due to rounding, some totals are greater than 100%

The retail sector was significantly affected, with 60% respondents reporting that response time increased over last year. When an adversary is in your environment, it's imperative to stop them as early as possible. The longer they are allowed to explore your network and access your data, the greater the financial and operational impact of the attack. The slowdown in response time is therefore a cause for alarm.

Increased workload increased knowledge and skills

Every cloud has a silver lining, and there is also a clear correlation between increase in cybersecurity workload and increased ability to develop cybersecurity knowledge and skills.

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



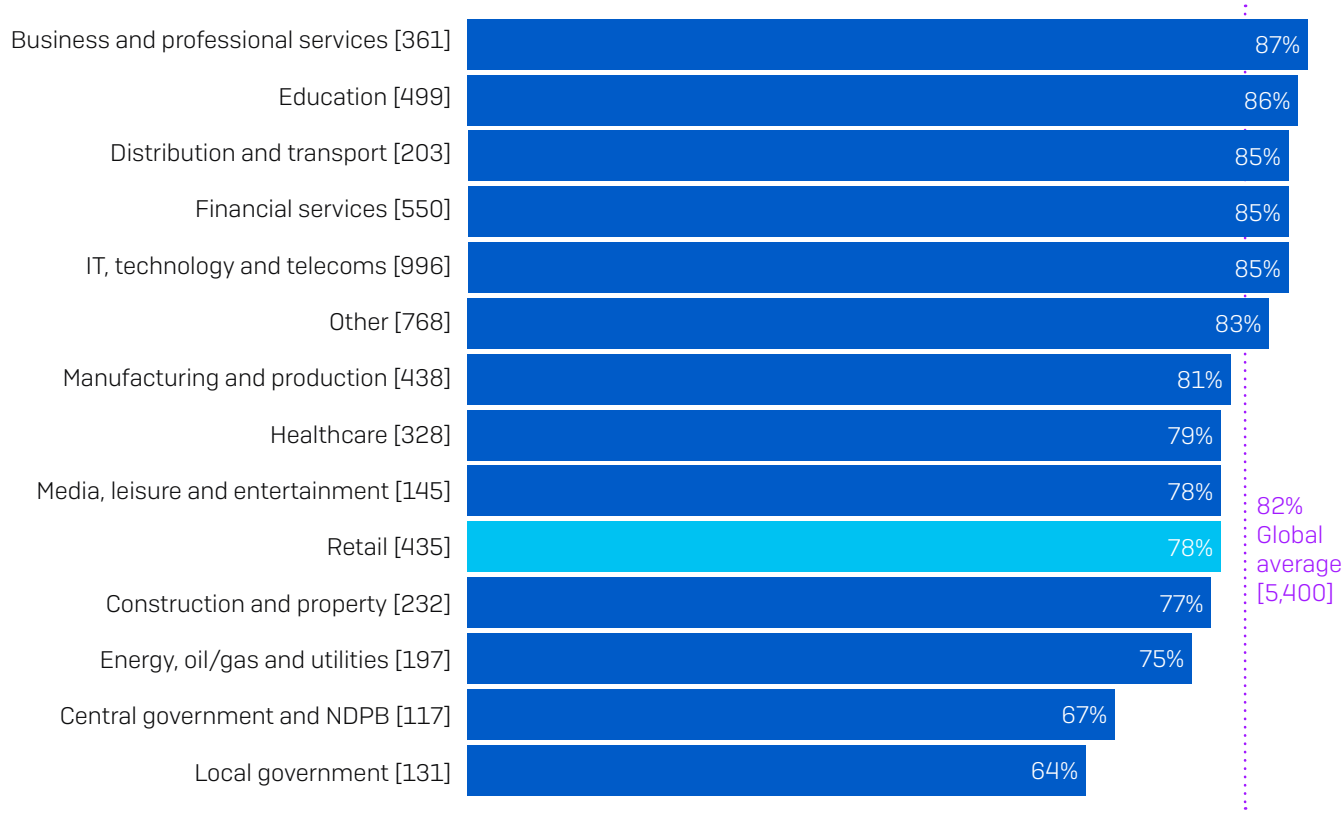
Over the course of 2020, our cybersecurity workload/our ability to further develop our cybersecurity knowledge and skills has increased [base sizes in chart], split by sector

77% of IT teams in retail said their ability to develop cybersecurity knowledge and skills increased over the course of 2020, the highest of all industries. While increased workload adds pressure, it also provides more opportunities to learn new things. It's also likely that the unique circumstances of the pandemic also required IT teams to deliver outputs that they had never been asked for before.

Readiness to take on future challenges

Even though the IT teams in retail reported to have the highest ability to develop cybersecurity knowledge and skills over 2020, this confidence was not reflected proportionally when asked if they had the tools and knowledge needed to investigate suspicious activities in their organization.

Have the tools and knowledge to investigate suspicious activity

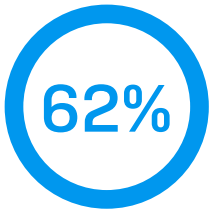


If I detect suspicious activities in my organization, I have the tools and knowledge I need to investigate fully: Strongly agree, Agree. Omitting some answer options [base sizes in chart], split by sector

Only 78% of retail respondents said they have the tools and knowledge needed – lower than the global average (82%). This is a cause for worry given the high level of ransomware attacks experienced by the retail sector and the increased cybersecurity workload. Having the right tools and knowledge is key to being able to investigate and address cyberthreats.

The future

Retail's expectations of the future attacks



Expect to be hit by ransomware in future

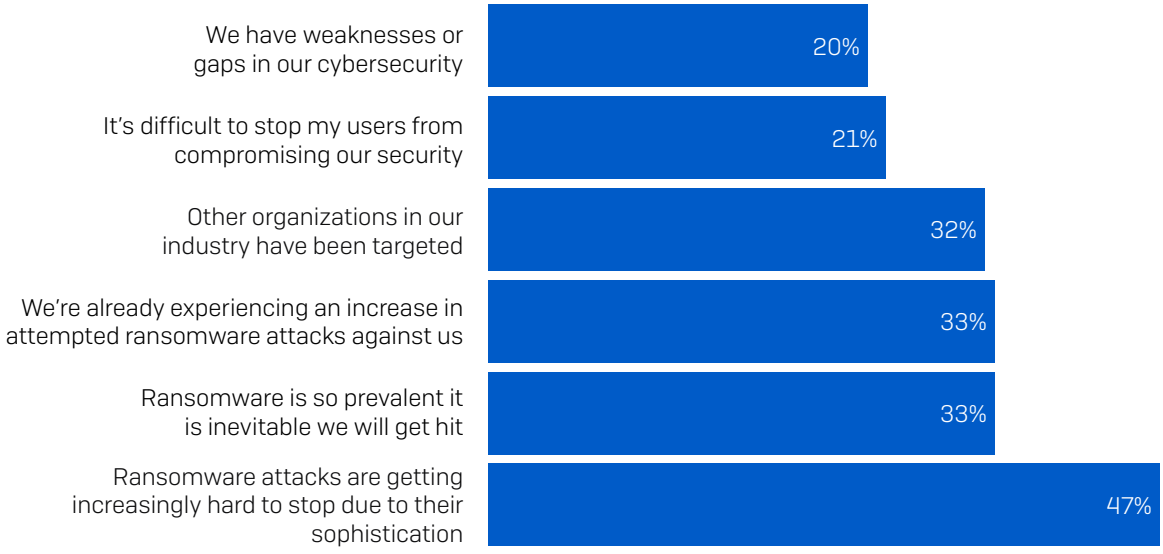
Don't expect to be hit by ransomware in future

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

We saw at the start that 55% of respondents in the retail sector were not hit by ransomware last year. Of them, almost two-thirds (62%) expect to be hit by ransomware in the future. Conversely, 38% don't anticipate an attack.

Why the retail sector expects to be hit

Among the retail organizations that weren't hit by ransomware but expect to be in the future, the most common reason (47%) is 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.



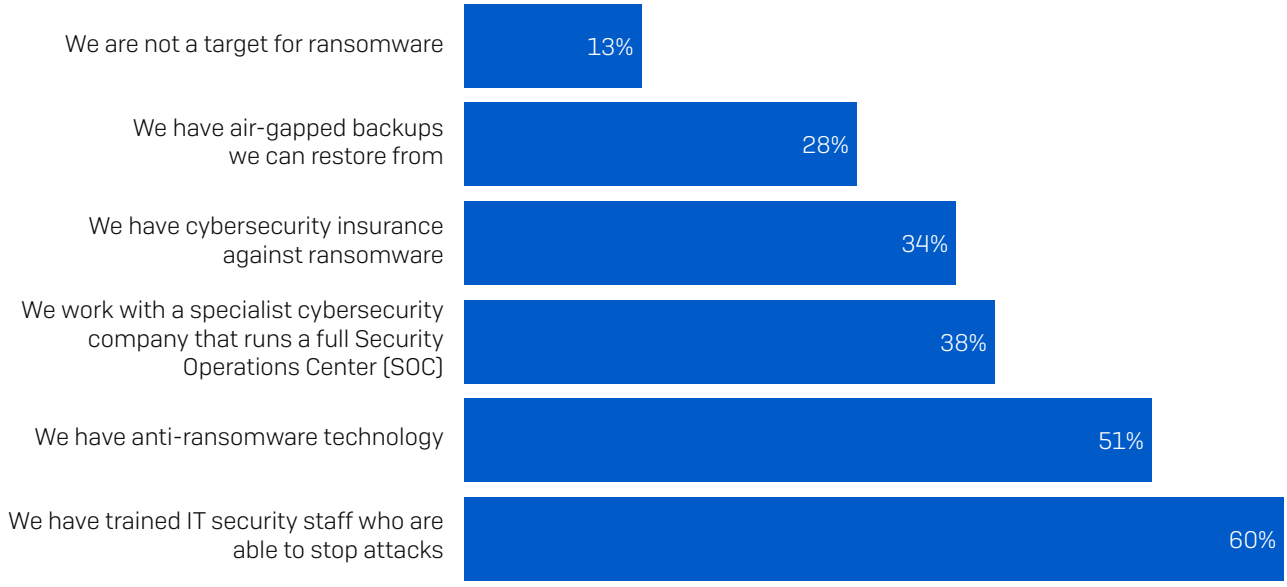
Why do you expect your organization to be hit by ransomware in the future? [148 retail organizations that haven't been hit by ransomware in the last year but expect to be in the future, omitting some answer options]

33% of respondents said that ransomware was too prevalent for them to not be hit by it, while 21% 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, 20% of retail 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.

Why retail doesn't expect to be hit by ransomware

92 retail respondents said their organization was not hit by ransomware in the last year and they don't expect to be hit in the future.



Why do you not expect your organization to be hit by ransomware in the future? [92] retail establishments that haven't been hit by ransomware in the last year and do not expect to be in the future, omitting some answer options

The #1 reason for this confidence is having trained IT staff who are able to stop attacks (60%), followed by the use of anti-ransomware technology (51%). 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.

38% of retail respondents who don't expect to be hit by ransomware work with a specialist cybersecurity company that runs a full Security Operations Center (SOC). It is encouraging to see that organizations are outsourcing cybersecurity expertise when needed, extending their protection.

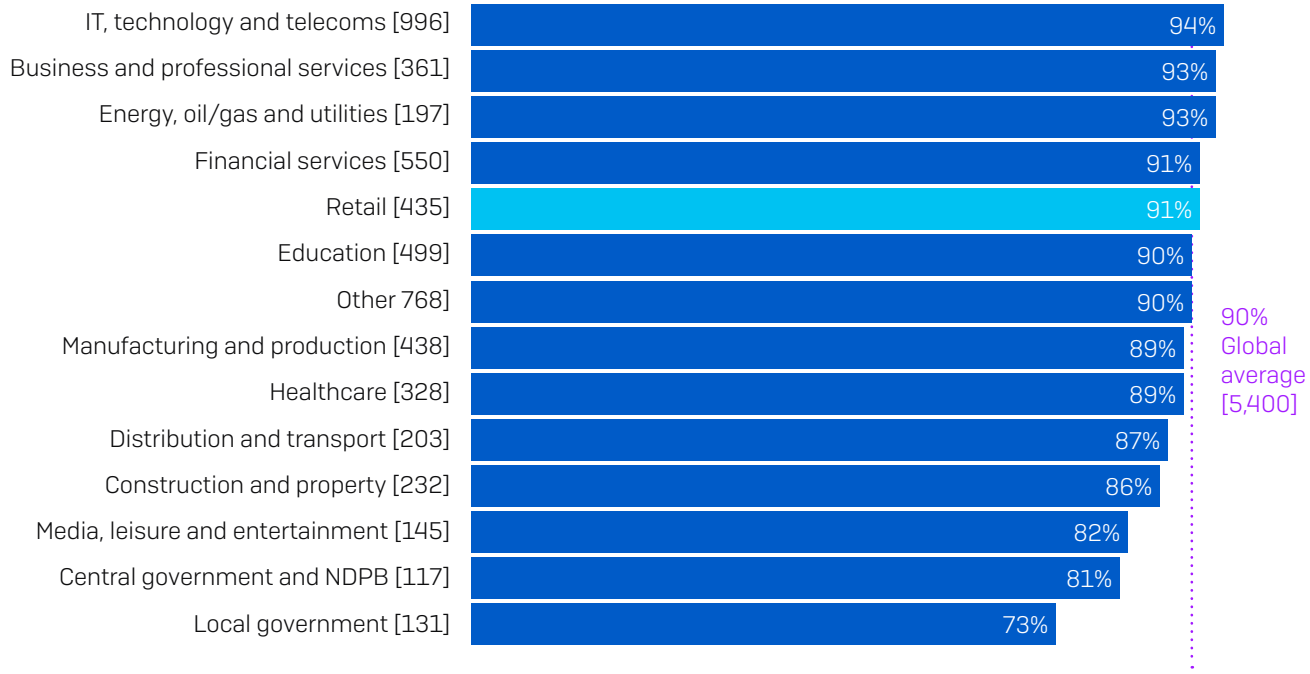
It's not all good news. Some results are cause for concern:

- 50% of retail respondents that don't expect to be hit are putting their faith in approaches that don't offer any protection from ransomware.
  - 34% cited cybersecurity insurance against ransomware. Insurance helps cover the cost of dealing with an attack, but doesn't stop the attack itself.
  - 28% cited 'air-gapped backups; while backups are valuable tools for restoring data post attack, they don't stop you getting hit.
    N.B. Some respondents selected both the above options, with 50% selecting at least one of these two options.
- 13% believe that they are not a target of ransomware. Sadly, this is not true. No organization is safe.

Retail organizations are well prepared

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.

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

It's therefore encouraging to discover that 91% of retail organizations have a malware incident recovery plan, with just under half (49%) having a full and detailed plan and 41% having a partially developed plan. These statistics are aligned with the cross-sector average numbers (90%).

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**. The 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 when 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 it's 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, which 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.

2021-07-26 (SB-MP)

SOPHOS