SOPHOS

THE STATE OF RANSOMWARE IN RETAIL 2025

Findings from an independent survey of 361 IT and cybersecurity leaders in the retail sector across 16 countries whose organizations were hit by ransomware in the last year.

A Sophos Whitepaper. Aug 2025

Introduction

Welcome to the fifth edition of the annual Sophos State of Ransomware in Retail report, which reveals the reality of ransomware for retail organizations in 2025.

This year's report unveils how retailers' experiences of ransomware – both causes and consequences – have evolved over the last year. It also shines new light onto previously unexplored areas, including the operational factors that left retail organizations exposed to attacks and the human impact of incidents on retail IT/cybersecurity teams.

Based on the real-world frontline experiences of 361 IT and cybersecurity leaders from the retail sector, across 16 countries whose organizations were hit by ransomware in the last year, the report provides unique insights into:

- Why retail organizations fall victim to ransomware
- What happens to the data
- Ransom demands and payments
- Business impact of ransomware
- Human impact of ransomware

A note on reporting dates

To enable easy comparison of data across our annual surveys, we name the report for the year in which the survey was conducted: in this case, 2025. We are mindful that respondents are sharing their experiences over the previous year, so many of the attacks referenced occurred in 2024.

About the survey

The report is based on the findings from an independent, vendor-agnostic survey into organizational experiences of ransomware that was commissioned by Sophos and conducted by a third-party specialist between January and March 2025. All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

The 361 retail respondents in the report span 16 countries, ensuring that the survey results reflect a broad and diverse range of experiences. The report includes comparisons with the findings from our previous reports, enabling year-over-year juxtaposition. All financial data points are in U.S. dollars.

Key findings

Why organizations fall victim to ransomware

- For the third year running, retail victims identified **exploited vulnerabilities** as the most common technical root cause of attack, used in 30% of incidents.
- Multiple operational factors contribute to retail organizations falling victim to ransomware, with the most common being **a security gap the organization was not aware of,** named by 46% of victims. It is followed in very close succession by a **lack of expertise,** which was a contributing factor in 45% of attacks (the highest rate recorded of any sector surveyed). In third place was **a lack of protection,** which contributed to 44% of attacks.

What happens to the data

- The **data encryption** rate in the retail sector is at its lowest level in five years, with 48% of attacks now resulting in data encryption, down from a 71% peak in 2023.
- 29% of retail organizations that had data encrypted also experienced **data exfiltration.**
- 98% of retail organizations that had data encrypted were able to recover it.
- The use of **backups** by retailers to restore encrypted data is at the lowest rate in four years, used in 62% of incidents.
- 58% of retail victims **paid the ransom** to get their data back. While this represents a slight drop from last year's 60%, it is the second highest ransom payment rate in five years.

Ransoms: Demands and payments

- The average (median) **ransom demand** made to retail organizations has doubled over the last year, coming in at $2M in 2025 compared to $1 million in 2024. The primary factor behind this significant escalation is a 59% increase in the percentage of ransom payments of $5M or more, up from 17% of payments in 2024 to 27% in 2025.
- Despite this, the average (median) **ransom payment** has risen just 5% in the last year to $1M in 2025, up from $950K in 2024. This suggests that retail organizations may be becoming more resistant to inflated ransom demands.
- The **proportion of the ransom demand paid** by retailers dropped to 81% in 2025 from 85% in 2024.
- Looking closely at **demands vs. payments,** only 29% of retailers said their payment matched the initial demand. 59% paid less than the initial ask, while 11% paid more.

Business impact of ransomware

- The average **cost for retail organizations to recover** from a ransomware attack dropped by 40% over the last year, coming in at $1.65 million, down from $2.73 million in 2024.
- Looking at **speed of recovery,** retail organizations are recovering faster, with 51% recovered within a week in 2025, up from 46% in 2024.

Human impact of ransomware

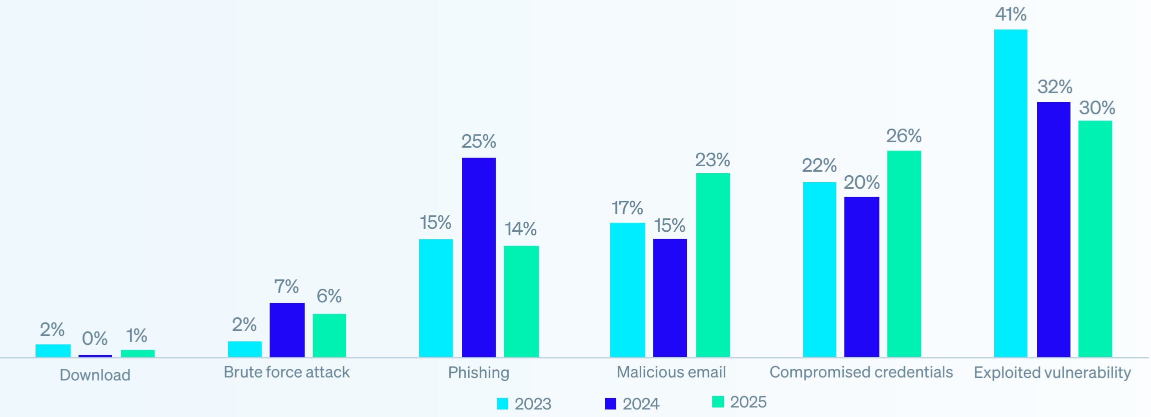
- Every retail organization that had data encrypted reported that there were **direct repercussions** for the IT/cybersecurity team:
  - Close to half (47%) of retail IT/cybersecurity teams reported **increased pressure** from senior leaders, while 30% reported **increased recognition**.
  - 43% of retail respondents cited both increased anxiety or stress about future attacks and an **ongoing increase** in workload as impacts on their IT/cybersecurity team.
  - 41% reported changes to the **team/organizational structure** as a consequence of the incident.
  - 37% of teams experienced **staff absence** due to **stress/mental health** issues related to the attack.
  - One third (34%) said the team experienced **feelings of guilt** that the attack was not stopped in time.
  - In one quarter of cases (26%), the team's **leadership was replaced** because of the attack.

Why organizations fall victim to ransomware

Technical root cause of attacks

For the third year running, retail victims identified exploited vulnerabilities as the most common root cause of ransomware incidents, used to penetrate organizations in 30% of attacks. Compromised credentials remain the second most common perceived attack vector, with the percentage of attacks that used this approach increasing from 20% in 2024 to 26% in 2025. Email remains a major attack vector, with 23% of retailers reporting phishing as the root cause (a significant jump from the 15% reported in 2024) and a further 14% citing malicious email.

Chart 1: Technical root cause of ransomware attacks in retail 2023 - 2025

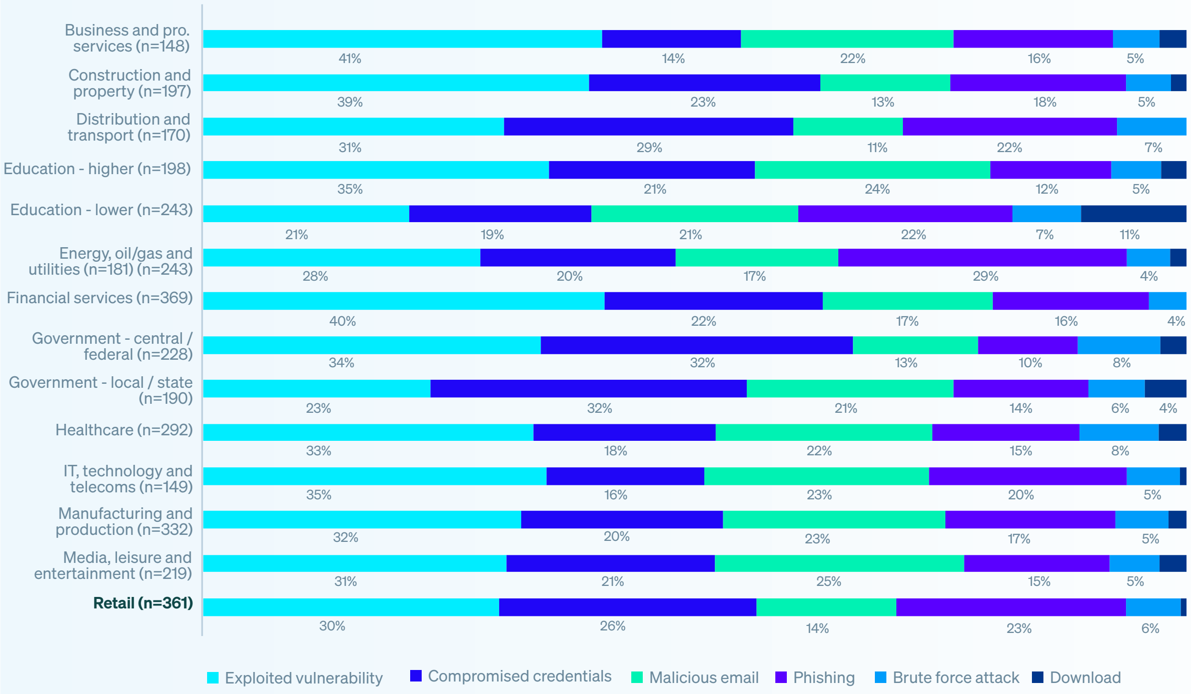


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=359 (2025), 261 (2024), 243 (2023).

The research reveals that while root causes vary by industry, exploited vulnerabilities are a major vector for most sectors. Notable exceptions:

- **Phishing** was the most common root cause cited by both **lower education** (22%) and **energy, oil/gas and utilities** (29%) providers.
- **Compromised credentials** were the most perceived attack vector for **local/state government** organizations – accounting for nearly a third of incidents (32%).

Chart 2: Technical root cause of ransomware attacks split by industry

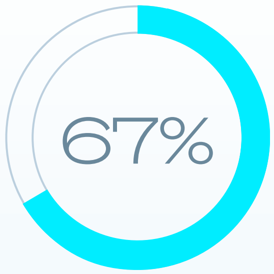


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. Base numbers in chart.

Organizational root cause of incidents in retail

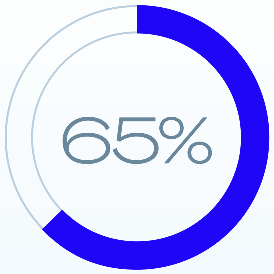
This year's report explores for the first time the organizational factors that left retail organizations exposed to attacks. The findings reveal that victims in the retail sector are typically facing multiple organizational challenges, with respondents citing 2.9 factors, on average, that contributed to them falling victim to the ransomware attack.

Overall, the organizational root causes are fairly evenly split across protection issues, resourcing challenges, and security gaps. However, retail organizations are slightly more likely to cite a security gap (known and unknown) as the primary factor.



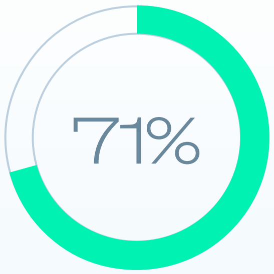
Protection challenges

Lack of protection or poor-quality protection solutions that could not stop the attack



Resourcing issues

Lack of human expertise (skills or capacity) to detect and stop the attack in time



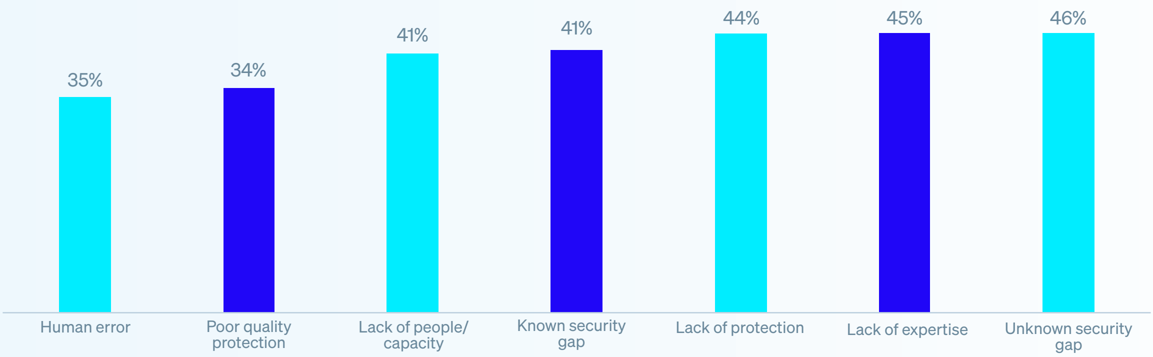
Security gap

Had a known or unknown weakness in their defenses

Why do you think your organization fell victim to the ransomware attack? n=361. Consolidated responses.

Unknown security gaps (i.e., weaknesses in defenses the organization was unaware of) are the most common individual reason given, named by 46% of retail respondents. This is closely followed by a **lack of expertise** (i.e., insufficient skills or knowledge to stop the attack in time), which contributed to 45% of attacks, the highest rate reported by any sector for this particular organizational root cause. In third place was lack of protection (i.e., not having the necessary cybersecurity products and services in place), which contributed to 44% of attacks.

Chart 3: Operational root cause of ransomware attacks on retail organizations



Why do you think your organization fell victim to the ransomware attack? n=361.

Organizational root cause by sector

The most common organizational root cause also varies by sector, reflecting the differing challenges businesses face. It's worth noting that no sector reported human error as the most common reason they fell victim to the ransomware attack.

Chart 4: Top operational root cause of ransomware attacks by sector

LACK OF **EXPERTISE**	UNKNOWN **SECURITY GAP**	LACK OF **PEOPLE/CAPACITY**	LACK OF **PROTECTION**	KNOWN **SECURITY GAP**	POOR **QUALITY PROTECTION**
We did not have the skills or knowledge available to detect and stop the attack in time	We had a weakness in our defenses that we were not aware of	We did not have sufficient cybersecurity experts monitoring our systems at the time of the attack	We did not have the necessary cybersecurity products and services	We had weakness(es) in our defenses we were aware of but had not addressed	Our cybersecurity products and services were not able to stop the attack
Energy, oil/gas and utilities (43%) Lower education (K-12) (42%)* Manufacturing and production (42%) Construction and property (41%)*	Higher education (18 years+) (49%) Business & professional services (46%) **Retail (46%)** Financial service, incl. insurance (44%)*	Lower education (K-12) (42%)* Healthcare (42%)	Financial services, incl. insurance (44%)* Local/state government (40%)	Central/federal government (45%) IT, technology, telecoms (42%) Construction and property (41%)*	Media, leisure, & entertainment (41%) Distribution & transport (41%)

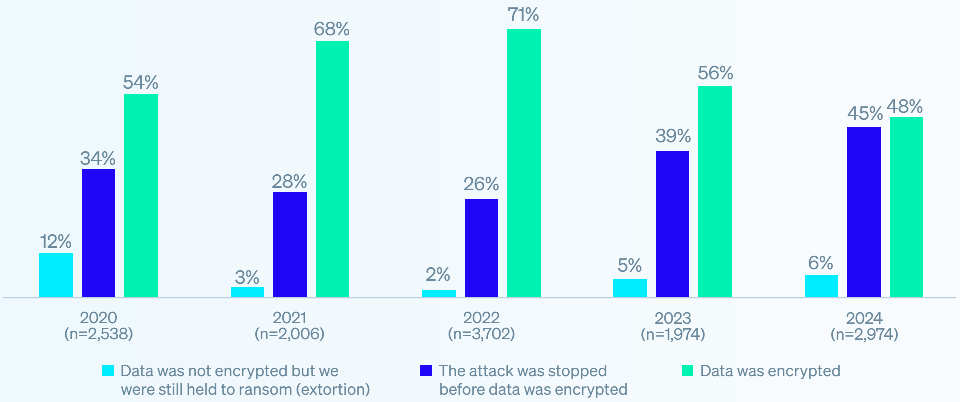
Why do you think your organization fell victim to the ransomware attack? n=3,400. Split by industry.

What happens to the data

Data encryption in retail

Encouragingly, data encryption in retail organizations is at its lowest reported rate in the five years of our study, with just under half (48%) of attacks resulting in data being encrypted. There has been a marked drop in the percentage of attacks that resulted in data encryption over the last two years, down from 71% in our 2023 survey, suggesting that retailers are more capable of stopping attacks before data gets encrypted.

Chart 5: Data encryption rate in ransomware attacks on retail organizations 2021 - 2025



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base numbers in chart.

Data encryption rate by industry

Organizations within the **distribution and transport** sector are most likely to have data encrypted (64%), indicating that organizations in this sector are less able to detect and stop the attack before encryption and/or are less able to block and roll back malicious encryption. In contrast, **lower education** providers reported the lowest data encryption rate, at just 29% — well below the 50% cross-sector average.

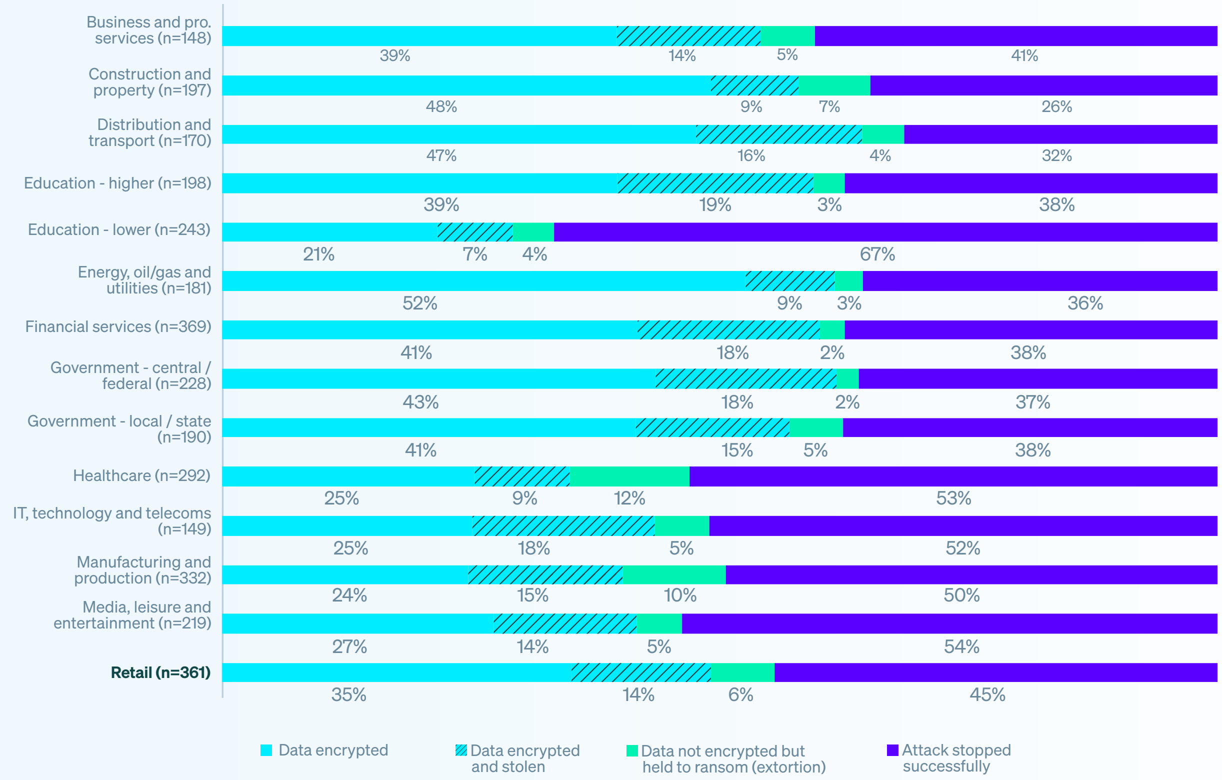
Data theft

Adversaries don't only encrypt data — they also steal it. Within the retail sector, 14% of all ransomware victims and 29% of those that had data encrypted experienced data theft. Breaking down the data by i ndustry we see that:

- At the higher end, 42% of organizations in the **IT, technology, and telecoms** sector that experienced data encryption also had data stolen.
- By contrast, only 15% of organizations in both the construction and property and **energy, oil/gas, and utilities** sectors faced data theft alongside encryption.

While it is possible that smaller organizations are more able to prevent the data theft than larger ones, this variance is probably due to attackers being more likely to attempt to exfiltrate data in larger organizations and/or smaller companies being less able to identify that data has been stolen.

Chart 6: Data encryption and theft by industry



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base numbers in chart.

Extortion-style attacks

As shown in chart 5, the percentage of retail organizations that did not have data encrypted but were held to ransom anyway (extortion) is at its highest rate in three years, having tripled to 6% of attacks in 2025 from just 2% in 2023.

Breaking down the data by industry, we see that **healthcare providers** faced the most extortion-style attacks (12%). This is likely due to the high sensitivity of medical data (patient records, etc.) In contrast, both **financial service** providers and **central/federal government** organizations reported experiencing the fewest of these attacks at just 2%.

Overall, **lower education** providers are most able to successfully prevent the repercussions of a ransomware attack, (i.e., to stop data being encrypted, to prevent data exfiltration, and to avoid being subject to extortion). This suggests that lower education providers are proving surprisingly effective at early detection and intervention — even with limited budgets.

Recovery of encrypted data in retail

98% of retail organizations that had data encrypted were able to recover it.

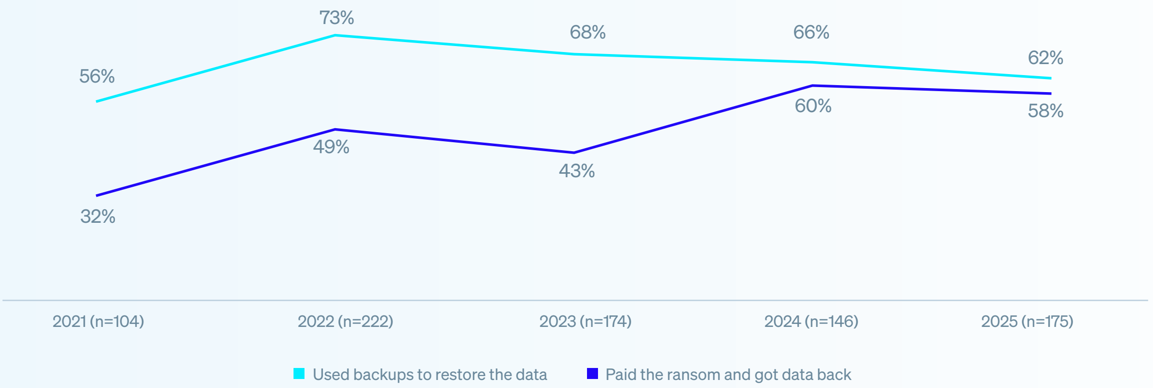
62% of retail organizations restored their data **using backups** - the lowest rate in four years, yet still one of the top three sectors for backup usage.

58% within the sector **paid the ransom and got their data back**. While this represents a small reduction from last year's 60%, it remains the second highest rate of ransom payments made by retailers in the last five years.

The narrowing gap between retailers paying the ransom to recover data and using backups to restore data suggests an increasing reliance on multiple/alternative recovery methods.

Evidencing this, we found that 39% of retail organizations that had data encrypted said they **used more than one method to restore their data**. No other sector reported a higher percentage.

Chart 7: Recovery of encrypted data in retail 2021 - 2025



Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data. Base numbers in chart.

Ransoms

Retail ransom demands

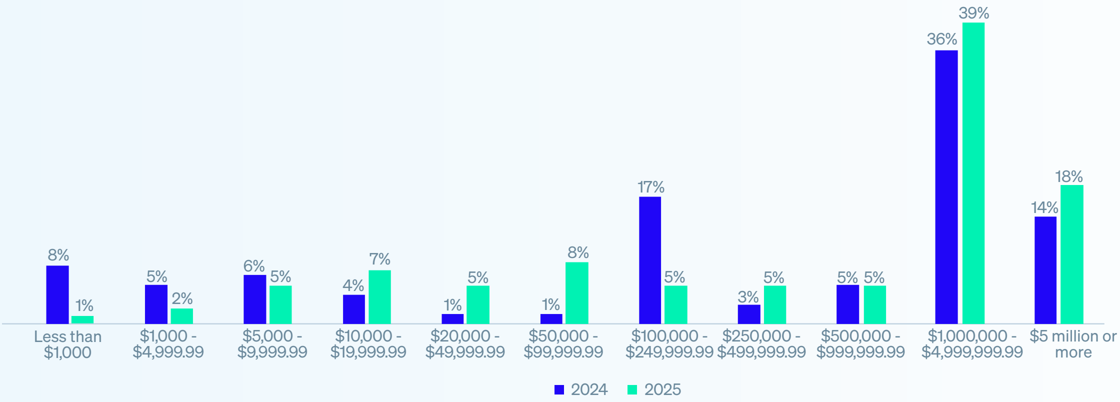
The average (median) ransom demand for retail organizations doubled over the last year, coming in at $2 million in 2025, up from $1 million in 2024. The increase in ransom demands targeting retailers is largely driven by a 59% increase in demands of $5 million or more over the last year. In addition, 63% of all ransom demands made to retailers exceeded $1 million, a sharp rise from the 50% reported in 2024.

In contrast, the cross-sector average has dropped by a third (34%) to $1.32 million in 2025 from $2 million in 2024.

Retail ransom payments

Despite a sharp increase in the ransom demanded, the average (median) ransom paid by retail organizations rose just 5%, suggesting that businesses in this sector may be becoming more resistant to inflated ransom demands. However, while the median ransom paid by retailers has increased modestly, the distribution shows a trend toward higher ransom payments overall, with a clear decline in smaller payouts and an increase in organizations paying over $1 million.

Chart 8: Ransom payments in retail | Distribution banding

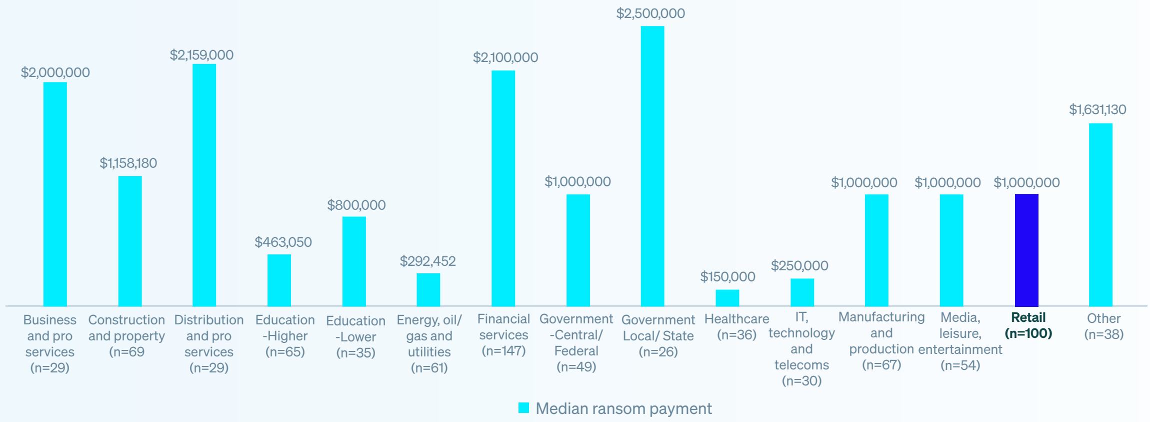


How much was the ransom payment that was paid to the attackers? n=100 (2025), 78 (2024)

Ransom payments by industry

Ransom payments varied considerably by industry, with **state and local government** organizations paying the highest average amount to attackers at $2.5 million. This may be due to critical service pressures, limited cyber resilience, and attackers exploiting their urgency to recover quickly. In contrast, **healthcare** providers paid the lowest at just $150,000.

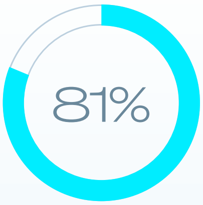
Chart 9 : Ransom payments by industry



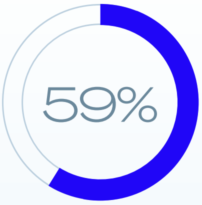
How much was the ransom payment that was paid to the attackers? Base numbers in chart. Note: Business and pro services and Government – Local/State have low base numbers, so findings should be considered indicative only.

How actual payments made by retailers stack up with the initial demand

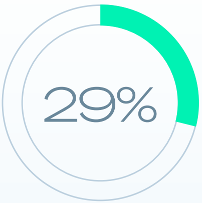
100 retail organizations that paid the ransom shared both the initial demand and their actual payment, revealing that they paid, on average, 81% of the initial ransom demand – a welcome drop from the 85% recorded in 2024. Overall, 59% paid less than the initial ask (notably above the cross-sector average of 53%), 11% paid more, and 29% matched the initial demand.



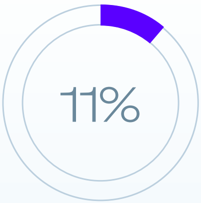
of the ransom demand **was paid**, on average



of payments were for **less** than the initial ransom demand



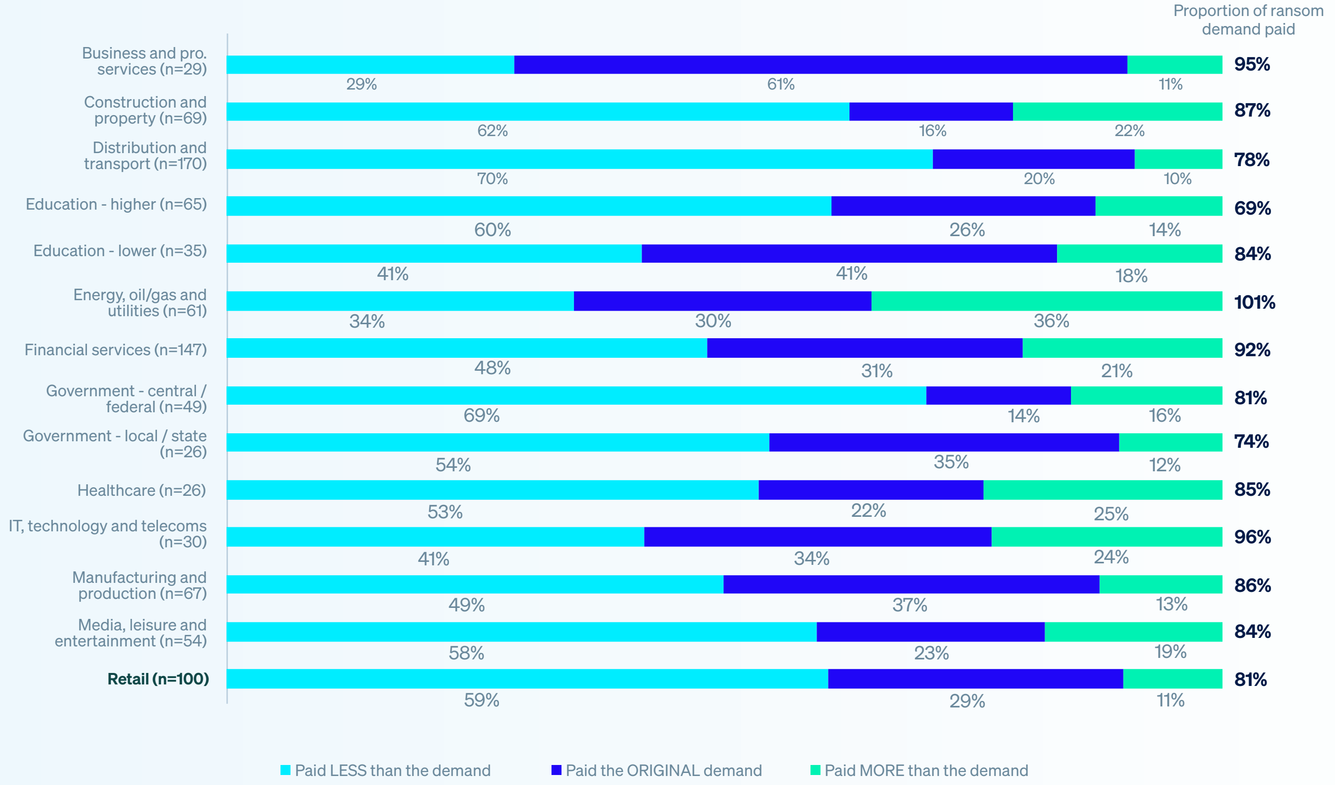
of payments **matched** the initial ransom demand



of payments were for **more** than the initial ransom demand

Splitting the data by industry, we see that, encouragingly, in the majority of sectors, paying less than the original ransom demand is the most common outcome. Organizations in the **distribution and transport** sector were by far the most likely to pay less than the original ransom demand (70%), suggesting a strong resistance to ransom demands. In contrast, **energy, oil/gas and utilities** providers were the most likely to pay more than what was initially demanded (36%), while **business and professional services** were most likely to match the initial ransom demand (61%).

Chart 10: How organizations respond to demands by industry



How much was the ransom payment that was paid to the attackers? Note: Business and pro services and Government – Local/State have low base numbers, so findings should be considered indicative only. Base numbers in chart.

Why most ransom payments made by retail organizations differ from the amount initially demanded

This year, for the first time, we have explored why some retail organizations pay more than the initial demand and others pay less, shining new light on an important area when dealing with a ransomware attack.

11 retail organizations* that **paid more** than the initial demand revealed that:

- 45%: The attackers realized we are a high-value target.
- 45%: The attackers got frustrated and increased the price.
- 45%: Our backups failed or were malfunctioning.
- 36%: The attackers believed we could afford to pay more.
- 18%: We did not pay quickly enough, so the price went up.

Retail organizations typically cited two factors behind the decision to pay more, revealing the multiple challenges that victims face when trying to recover their data.

*Please note: Due to a very low base number, findings are indicative only.

60 retail organizations that **paid less** than the initial demand explained how they were able to lower their payment:

- 60%: The attackers reduced their demand due to external pressures (e.g., from the media or law enforcement).
- 47%: The attackers reduced their demand to encourage us to pay.
- 43%: A third party negotiated a lower amount with the attackers.
- 42%: We paid the ransom quickly, so we got a discount.
- 35%: We negotiated a lower amount with the attackers.

This cohort also reported, on average, 2 factors behind their lower ransom payment, further emphasizing the complex, multi-faceted situation that ransomware victims face.

Business consequences of ransomware

Recovery costs in retail

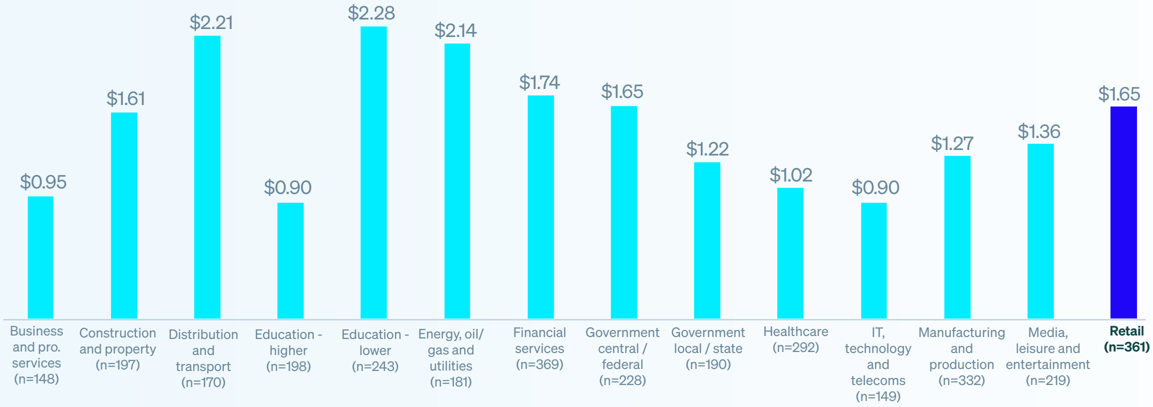
The average (mean) cost for retail organizations to recover from a ransomware attack (excluding any ransom payment) has fallen to its lowest point in three years, dropping by 40% over the past year to $1.65 million, down from $2.73 million in 2024. It is also $200,000 lower than the sum reported in 2023.

2023	2024	2025
$1.85 million	$2.73 million	$1.65 million

What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.) excluding any ransom payments made? n=361 (2025), 261 (2024), 244 (2023).

When looking at an industry split, recovery varies considerably. **Lower education** providers reported the highest average cost to rectify incidents at $2.28 million. In contrast, both **higher education** providers and organizations within the **IT, technology and telecoms sector** equally reported the lowest cost at $0.90 million.

Chart 11: Ransomware recovery cost split by company size

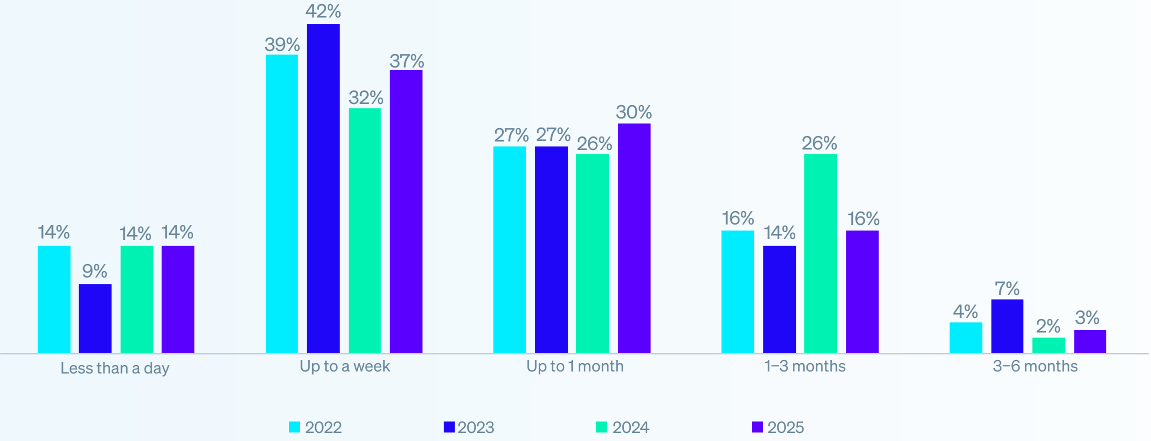


What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.) excluding any ransom payments made? Base numbers in the chart.

Recovery time

The data reveals that, in 2025, retail organizations showed signs of faster recovery following ransomware attacks. Over half (51%) recovered within a week, up from 46% in 2024. At the same time, the proportion taking one to three months to recover fell sharply to 16%, down from 26% in 2024. Overall, 96% of retail victims fully recovered within three months, underscoring growing resilience and recovery capabilities across the sector.

Chart 12: Recovery time for retail organizations from ransomware attacks 2022 - 2025



How long did it take your organization to fully recover from the ransomware attack? Base numbers in chart.

Somewhat unsurprisingly, retail organizations that had data encrypted typically were slower to recover than those that were able to stop the encryption: 6% that had data encrypted were fully recovered in a day, compared to 22% of those where the adversaries were unsuccessful in encrypting the data.

Human consequences of ransomware

The survey makes clear that having data encrypted in a ransomware attack has significant repercussions for IT/cybersecurity teams in the retail sector, with all respondents saying their team has been impacted in some way.

Chart 13: The consequences on IT/cybersecurity teams of having data encrypted

Cross-sector average	Retail organizations	
40%	47%	Increased **pressure** from senior leaders
41%	43%	Increased **anxiety or stress** about future attacks
38%	43%	Ongoing increase in **workload**
37%	41%	Changes to **team/organizational structure**
31%	37%	Staff absence due to **stress/mental health** issues
38%	35%	Change of **team priorities/focus**
34%	34%	Feelings of **guilt** that the attack was not stopped
31%	30%	Increased **recognition** from senior leaders
25%	26%	Our team's **leadership** was replaced

What repercussions has the ransomware attack had on the people in your IT/cybersecurity team, if any? n=175.

Recommendations

Although retail organizations have experienced several changes in their encounters with ransomware over the last year, it remains a significant threat. As adversaries continue to iterate and evolve their attacks, it’s essential that defenders and their cyber defenses keep pace with ransomware and other threats. Leverage the insights in this report to fortify your defenses, sharpen your threat response, and limit ransomware's impact on your business and people. Focus on these four key areas to stay ahead of attacks:

- **Prevention**. The most successful defense against ransomware is one where the attack never happens because adversaries couldn't breach your organization. Take steps to eliminate the technical and operational root causes highlighted in this report.
- **Protection**. Strong foundational security is a must. Endpoints (including servers) are the primary destination for ransomware actors, so ensure that they are well defended, including dedicated anti-ransomware protection to stop and roll back malicious encryption.
- **Detection and response**. The sooner you stop an attack, the better your outcomes. Around-the-clock threat detection and response is now an essential layer of defense. If you lack the resources or skills to deliver this in-house, look to work with a trusted managed detection and response (MDR) provider.
- **Planning and preparation**. Having an incident response plan that you are well-versed in deploying will greatly improve your outcomes if the worst happens and you experience a major attack. Be sure to make quality backups and regularly practice restoring data from them to accelerate recovery if you do get hit.

To explore how Sophos can help you optimize your ransomware defenses, speak to an advisor or visit www.sophos.com

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.

2025-08-19 WP (MP)