

REPORT

The State of Ransomware in Retail 2026

Findings from an independent survey of 217 IT and cybersecurity leaders in the retail sector across 17 countries whose organizations were hit by ransomware in the last year.

SOPHOS

Introduction

Welcome to the sixth edition of the annual Sophos State of Ransomware in Retail report, which reveals the reality of ransomware for retail organizations in 2026.

This year's report shines new light on previously unexplored areas, including where attacks start in the environment, the defensive role of multi-factor authentication (MFA) and firewalls, and the connection between identity attacks and ransomware.

Drawing on the real-world experiences of 217 IT and cybersecurity leaders in retail organizations hit by ransomware in the past year, this report offers unique insights into:

- Attack and defense methods
- Data encryption and recovery
- Ransom demands and payments
- Business and human impact

Note: The 217 retail sector respondents are part of a broader cohort of 2,158 respondents across 15 industry sectors.

Throughout this report, "cross-sector average" refers to combined answers from respondents across all sectors surveyed. Percentages are rounded to the nearest whole number after summary combinations.

About the survey

This report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. The survey asked questions about the organizational experiences of ransomware attacks and identity-based intrusions, tracking ransom payment rates, recovery costs, recovery times, and many other metrics year-over-year. Answers were gathered from January to March of 2026 and are based on respondents' experiences from the previous 12 months.

Participants came from 17 countries and 15 economic sectors, across both public and private sectors, and a bell-curve sampling of company sizes between 100 and 5,000 employees that has remained proportionally consistent over the survey's six-year history. All financial data points are in U.S. dollars.

Key findings

- **Retail saw exploited vulnerabilities initiate ransomware attacks at a higher rate than any other sector.**
  - 26% of attacks on retail organizations began with an exploited vulnerability, the highest share of any sector.
  - Among attacks that began with an exploited vulnerability, compromised credentials, or a brute-force attack, retail had the largest proportion that started on a user's device (44%).
  - Identity-based vectors (e.g., malicious email, phishing, compromised credentials, and brute-force attacks) initiated 69% of attacks against retail, the lowest rate of any sector.
  - Among attacks that retail firewalls identified before the ransomware was deployed, 60% still ended with data encrypted, versus 50% across all sectors.
- **Data encryption climbed after two straight years of decline.**
  - 62% of attacks on retail succeeded in encrypting data, up from 48% in 2025.
  - 19% of attacks encrypted data and also stole it, up from 14% in 2025.
- **Retail was the least likely sector to pay the ransom to get its data back.**
  - 32% of retail organizations with encrypted data paid the ransom and got data back, the lowest rate of any sector, and down from 58% in 2025.
  - 71% restored encrypted data from backups, up from 62% in 2025.
- **Ransom demands against retail were generally low with a group of very high outliers.**
  - The median ransom demand for retail was $225,000, the second lowest of any sector.
  - The average (mean) demand was $4.32 million, the highest of any sector.
- **When retail paid the ransom, they paid less than any other sector.**
  - The median ransom payment in retail was $57,500, the lowest of any sector.*
  - The mean ransom payment in retail was $684,361, also the lowest of any sector.*
  - 63% of retail organizations that paid a ransom paid less than the initial demand, the second-highest rate.*
  - The median ransom payment in retail was 76% of the original demand, the second-deepest reduction of any sector.*
- **Retail had its fastest recovery times in the past five years.**
  - The mean recovery time for retail was 2.54 weeks, down from 3.16 weeks in 2025.
  - 56% recovered within a week, the highest share in five years of retail data.
- **Retail IT and security teams reported the lightest human toll in the study.**
  - 22% of retail teams saw changes to team or organizational structure after the attack, the lowest share of any sector.
  - 10% saw their team's leadership replaced, also the lowest of any sector.

**Sectors with fewer than 30 respondents that paid the ransom were excluded from comparisons.*

Attack and defense methods

Root causes of attacks

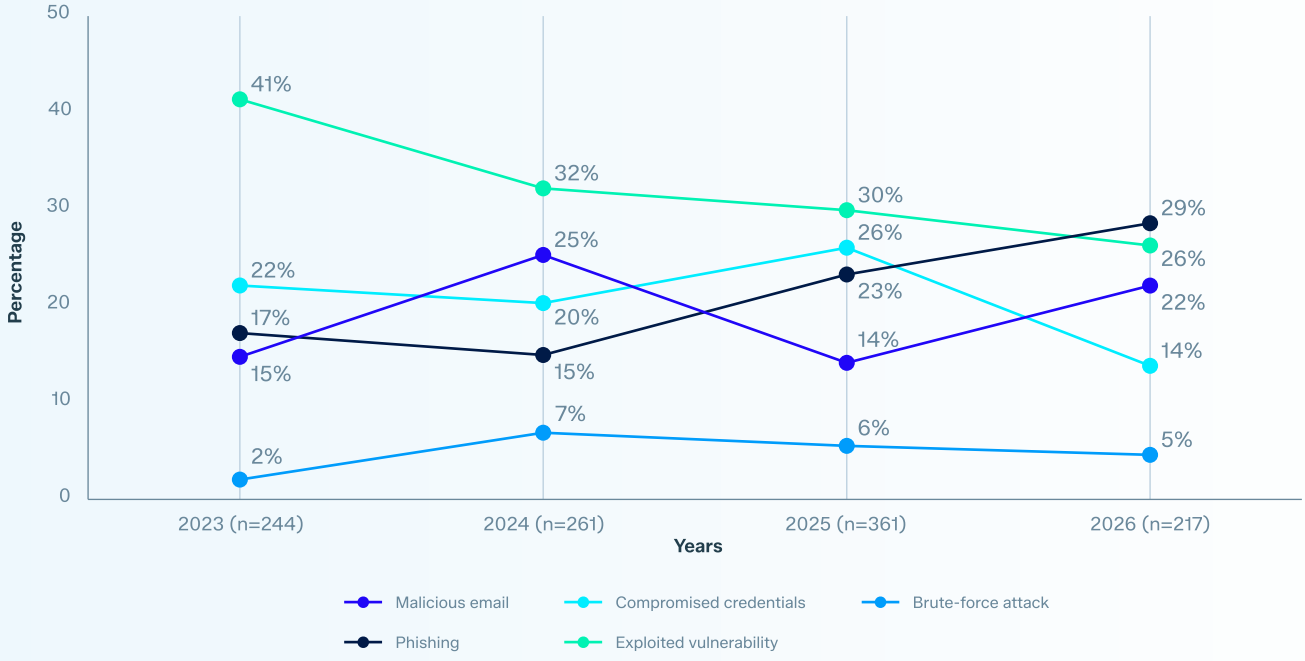
In a year where reports of exploited vulnerabilities are down considerably across sectors, retail ransomware victims saw only a slight reduction in this root cause. However, exploited vulnerabilities are no longer the top technical root cause in retail.

The top technical root cause in retail is now phishing at 29%, up from 23% in 2025. Exploited vulnerabilities were the second most common at 26%, with malicious email in third at 22%. On the other end, retail had the lowest rate of compromised credentials among all sectors, well below the 23% cross-sector rate.

26%

The percentage of retail attacks that began with an exploited vulnerability, the highest of any sector surveyed.

Technical root cause over time: Retail

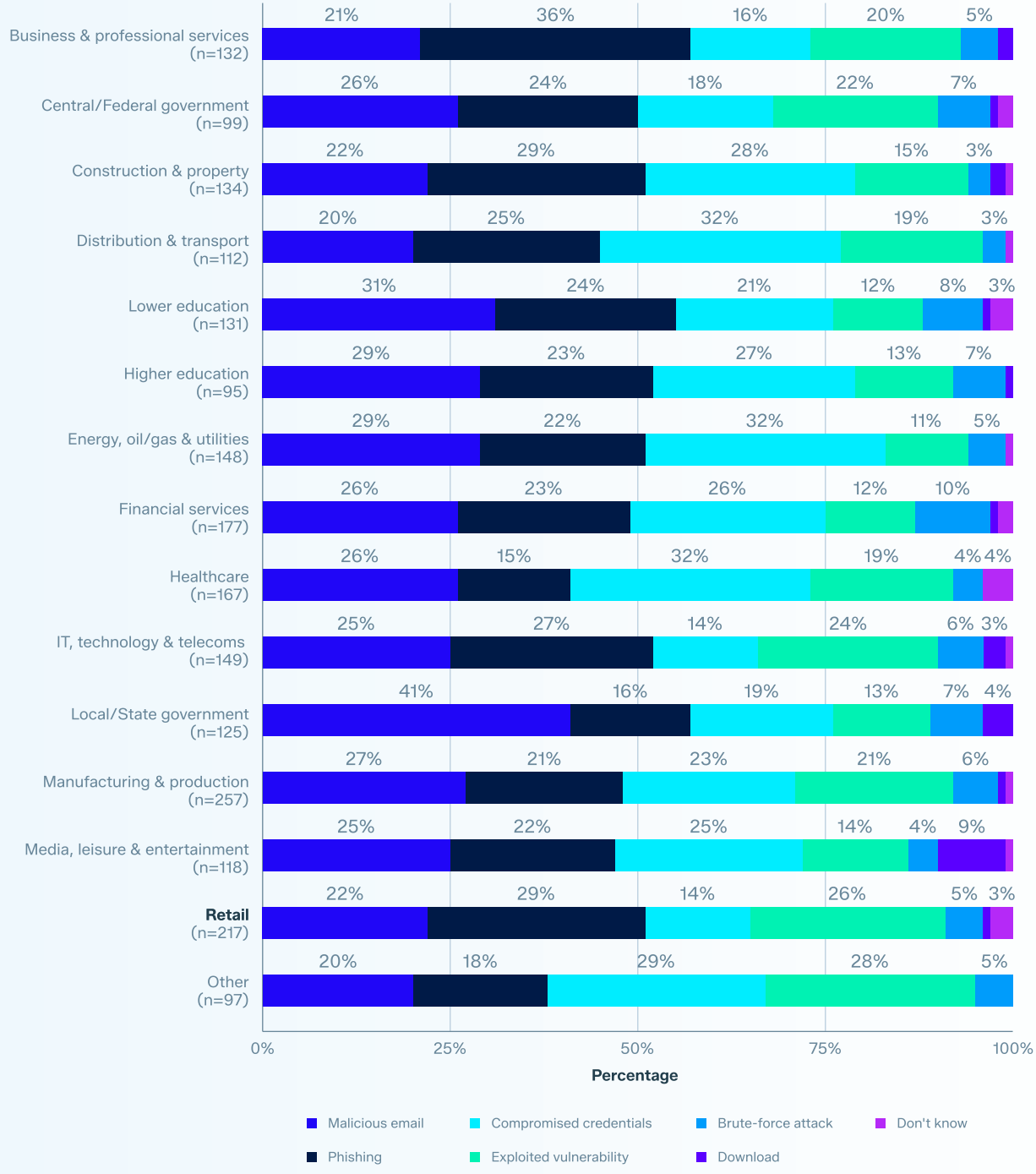


Do you know the root cause of the ransomware attack your organization experienced in the last year? "Downloads" and "Don't know" answers excluded from chart for visual clarity. Percentages may not equal 100%. Base numbers in chart.

Since it didn't see a large drop like other sectors, **retail is now the most likely sector in the survey to be breached through an exploited vulnerability (26%, versus 18% across all sectors)**. Retail continues to follow broader industry trends: both retail and the cross-sector average have seen the rate of exploited vulnerabilities fall for three consecutive years.

Taken together, identity-based vectors (e.g., malicious email, phishing, compromised credentials, and brute-force attacks) accounted for 69% of attacks on retail, the lowest share of any sector and well below the 79% cross-sector average. That total held steady from 2025 (69%), with the mix shifting from stolen credentials toward phishing and malicious email. It's notable, however, that while this rate was the lowest of any sector, it still exceeded half of all ransomware attacks.

Technical root cause by industry (2026)



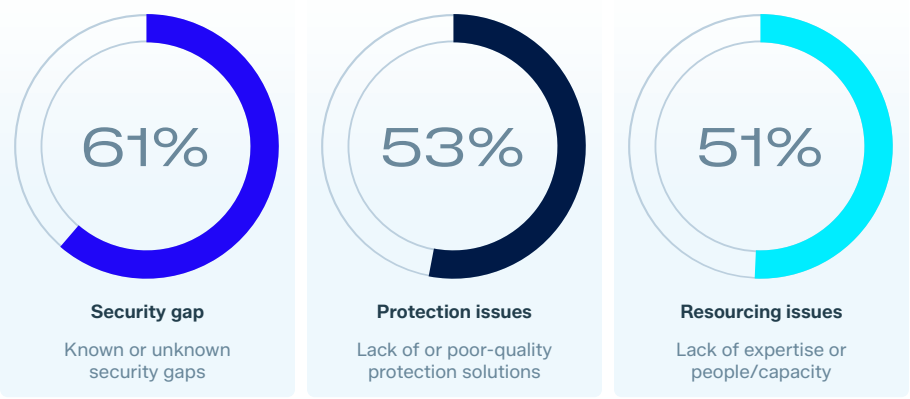
Do you know the root cause of the ransomware attack your organization experienced in the last year? Percentages in this chart rounded using the largest remainder method and may differ from percentages in the report text. Base numbers in chart.

Sophos experts expect exploits to climb again as organizations struggle to keep up with patches for vulnerabilities found by frontier AI, which means retailers have more than one strong argument for why they need to focus more resources on mitigating this attack vector.

What made organizations vulnerable

Retail organizations cited a mix of challenges with protection, resourcing, and security gaps. Across the three consolidated categories, security gaps led at 61%, followed by protection issues (53%) and resourcing issues (51%).

Operational root causes: Retail



Why do you think your organization fell victim to the ransomware attack? n=217. Consolidated responses.

The most common operational root cause for retail was known security gaps: **38% attributed their breach to a known security gap that the organization had not closed**. That rate was in line with other sectors, and it was the only operational root cause that retail cited more often than the cross-sector average.

Operational root causes: Retail vs. all sectors

Operational root cause	Retail (n=217)	All sectors (n=2,158)
Known security gap	38%	36%
Unknown security gap	34%	36%
Lack of protection	33%	36%
Lack of people/capacity	32%	35%
Lack of expertise	31%	35%
Human error	28%	35%
Poor quality protection	26%	33%

Why do you think your organization fell victim to the ransomware attack? Multiple responses permitted. Base numbers in chart.

Overall, retail victims mentioned fewer operational root causes per attack. On average, retail victims cited 2.23 operational root causes per attack (versus 2.47 across all sectors), the second fewest of any sector and down from 2.86 in 2025.

38%

The percentage of retail victims who cited a known security gap (a weakness they were aware of but had not addressed), the sector's most common operational root cause.

The table below shows sectors placed in the column of the operational root cause they cited most.

Top operational root cause of ransomware attacks by sector



Why do you think your organization fell victim to the ransomware attack? Multiple responses permitted. Sectors tied across multiple causes are marked with an asterisk (*). n=2,158.

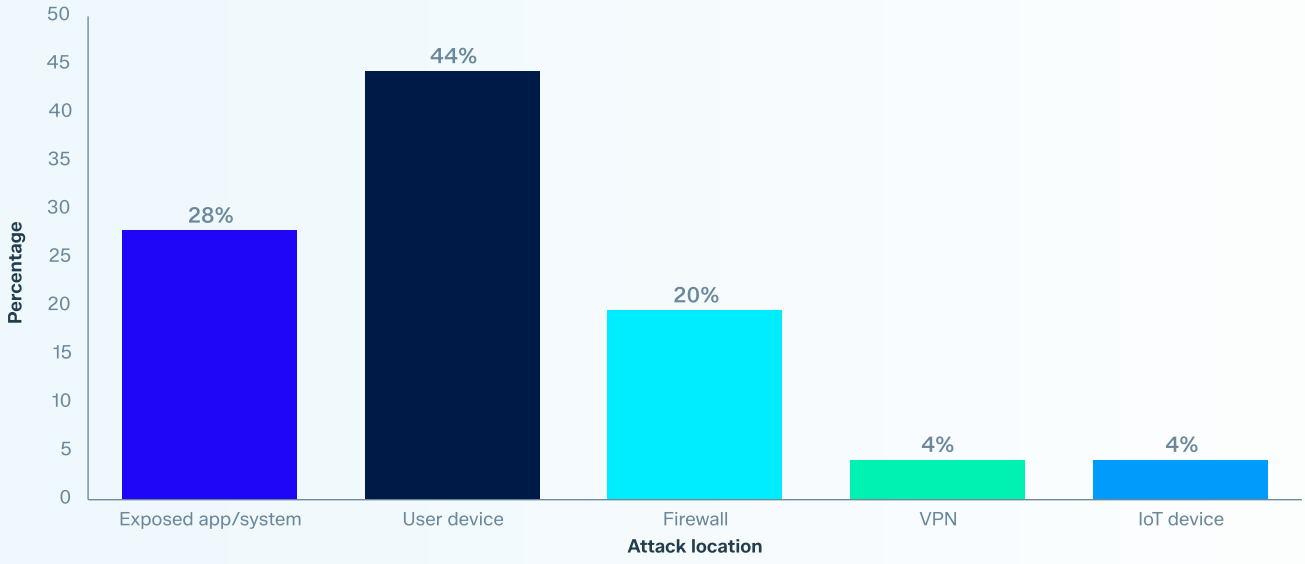
NEW RESEARCH

Where attacks start

New research this year dives into where in the environment attacks began, specifically among incidents that started with an exploited vulnerability, compromised credentials, or a brute-force attack.

For retail, user devices were the most common entry point (44%), followed by exposed applications and systems (28%), and firewalls (20%). **Retail had the highest share of attacks starting on user devices of any sector, well above the 30% cross-sector rate.**

Where ransomware attacks start: Retail



You said the root cause was an exploited vulnerability, compromised credentials, or a brute-force attack. Where did this happen in your environment? n=97.

28% of retail attacks started in exposed applications and systems, noticeably below the 38% cross-sector rate. VPNs were also a less common starting point in retail (4%, versus 8% across all sectors).

One possible factor is the shape of the retail workforce: staff laptops and desktops spread across many stores and sites may widen the endpoint attack surface.

NEW RESEARCH

The role of multi-factor authentication (MFA)

We also examined the MFA methods in place at the time of the attack among retail organizations whose attack began with compromised credentials. Almost all victims had some form of MFA enabled (97%) in credential-based attacks.

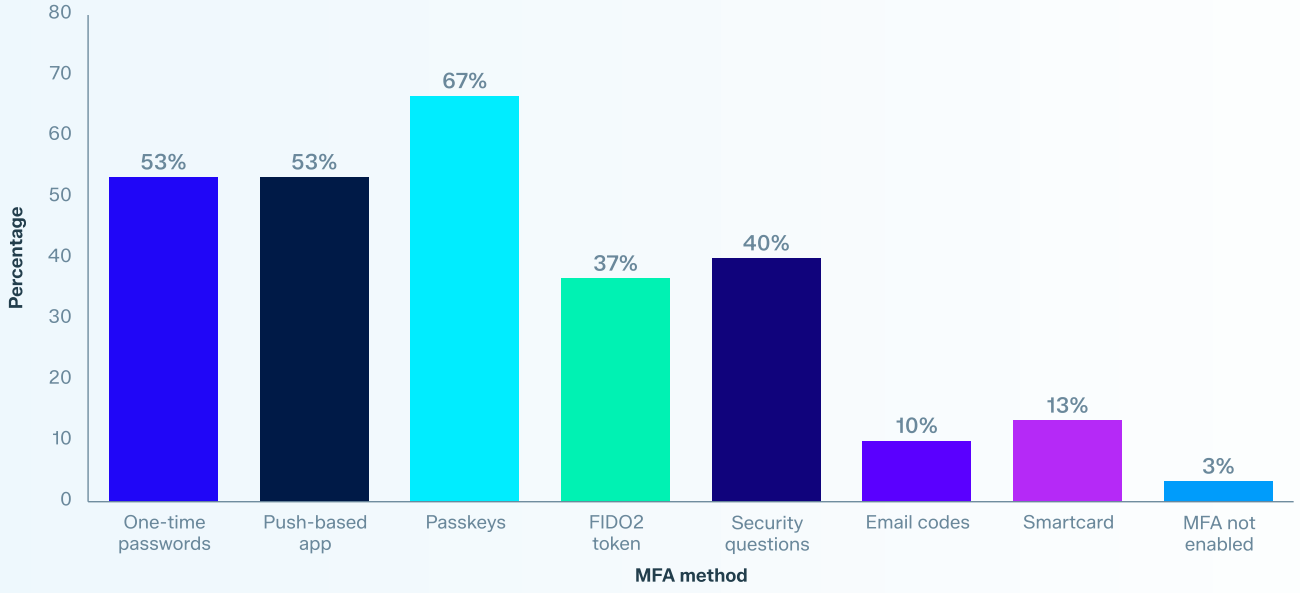
However, among retail organizations asked about MFA, **more than half still had data encrypted despite MFA enablement**. This suggests that either MFA was not comprehensively deployed across all critical systems, attackers found ways to bypass MFA protections, or the attack vectors did not rely solely on credential compromise.

Passkeys (67%) were the most frequently deployed method for the sector, followed by one-time passwords and push-based applications (53% each). Compared with the cross-sector average, retail organizations' usage of passkeys (67% versus 51% cross-sector) and security questions (40% versus 28% cross-sector) ran well above, and their usage of email codes (10% versus 25% cross-sector) ran well below.

59%

organizations with compromised credentials that still had data encrypted despite MFA enablement.

The role of MFA: Retail



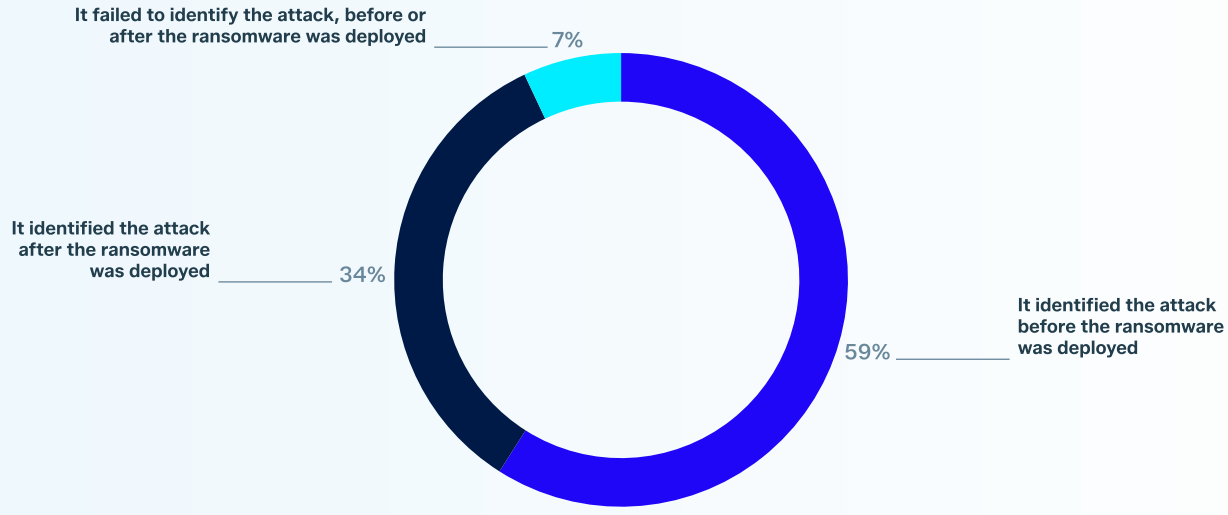
What type of multi-factor authentication was enabled at the time of the attack, if any? Multiple responses permitted. Base: the attack occurred due to compromised credentials. n=30.

NEW RESEARCH

The role of firewalls

59% of retail organizations said their firewall identified the attack before the ransomware was deployed, 34% said it identified the attack afterward, and 7% said it did not identify the attack at all. That split is in line with the cross-sector pattern.

The role of firewalls: Retail



What role did your firewall play in identifying the attack? n=217.

Among those early-detection cases, retail victims still had their data encrypted 60% of the time, well above the 50% cross-sector rate. Retail firewalls caught attacks early at about the same rate as other sectors, yet encryption followed more often.

Firewalls are doing a good job of collecting data to identify attacks, but attacks still aren't being stopped at the same rate they're being identified. It is likely that firewalls often log the data needed to detect and stop an attack, but they may not be connecting deeply enough with other systems to recognize the threat and respond in time.

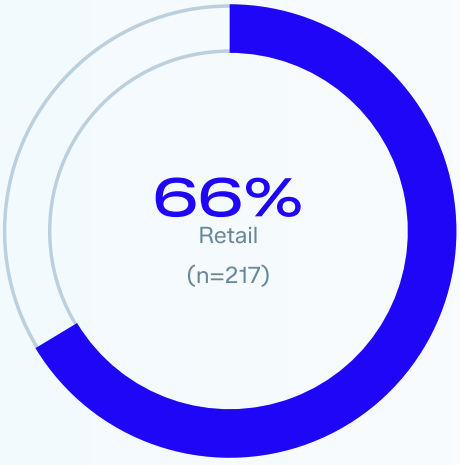
NEW RESEARCH

The identity-ransomware connection

One of the survey's clearest findings is the direct link between identity attacks and ransomware. Across all sectors, two-thirds of ransomware victims (67%) confirmed the incident was the same event as their most significant identity attack. Retail was in line with that figure at 66%.

That overlap stands out against retail's root-cause data. Retail had the lowest share of attacks that began with an identity-based vector, yet two in three retail victims still tied their ransomware incident to their most significant identity attack. One possible explanation is that identity compromise often plays a role later in an attack, after initial entry through a vulnerability or a user device.

Ransomware attack was also their most significant identity-related attack



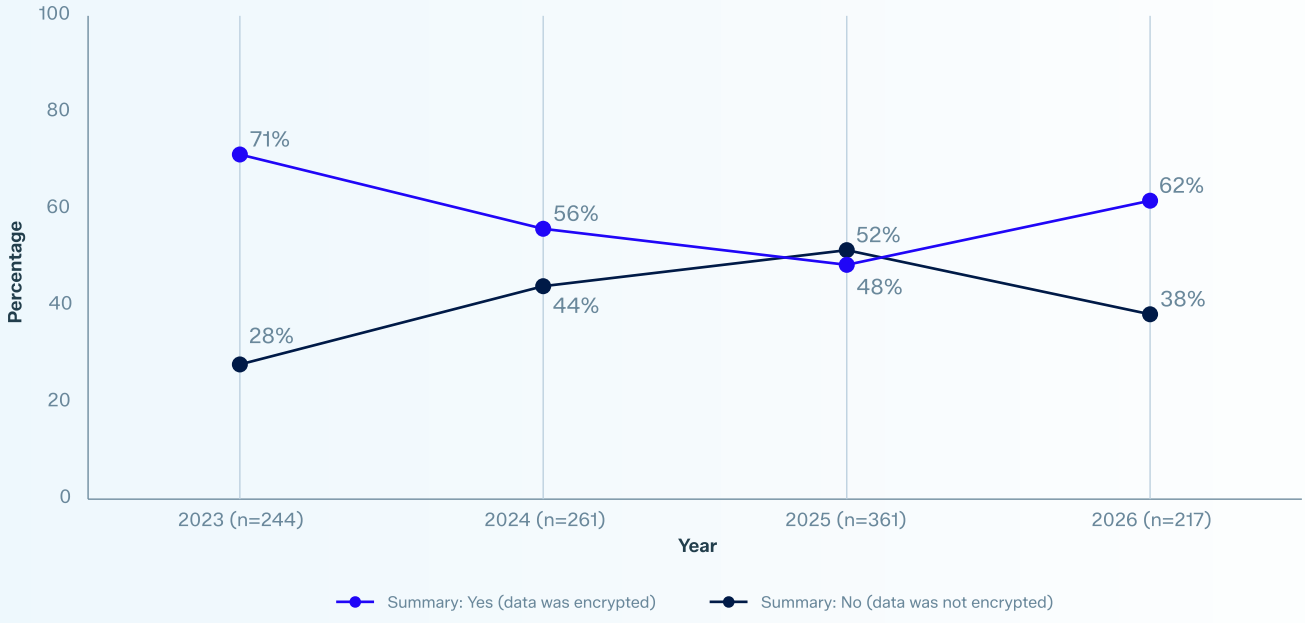
Was that ransomware incident the same event as your most significant identity-related attack? Base: organizations hit by ransomware. n=217.

Data encryption and recovery

Data encryption rate

Retail's encryption rate rose this year after two straight years of decline. 62% of attacks succeeded in encrypting data, up from 48% in 2025 and noticeably above the 56% cross-sector average. The retail encryption rate had fallen from 71% in 2023 to 56% in 2024 before reaching 48% in 2025.

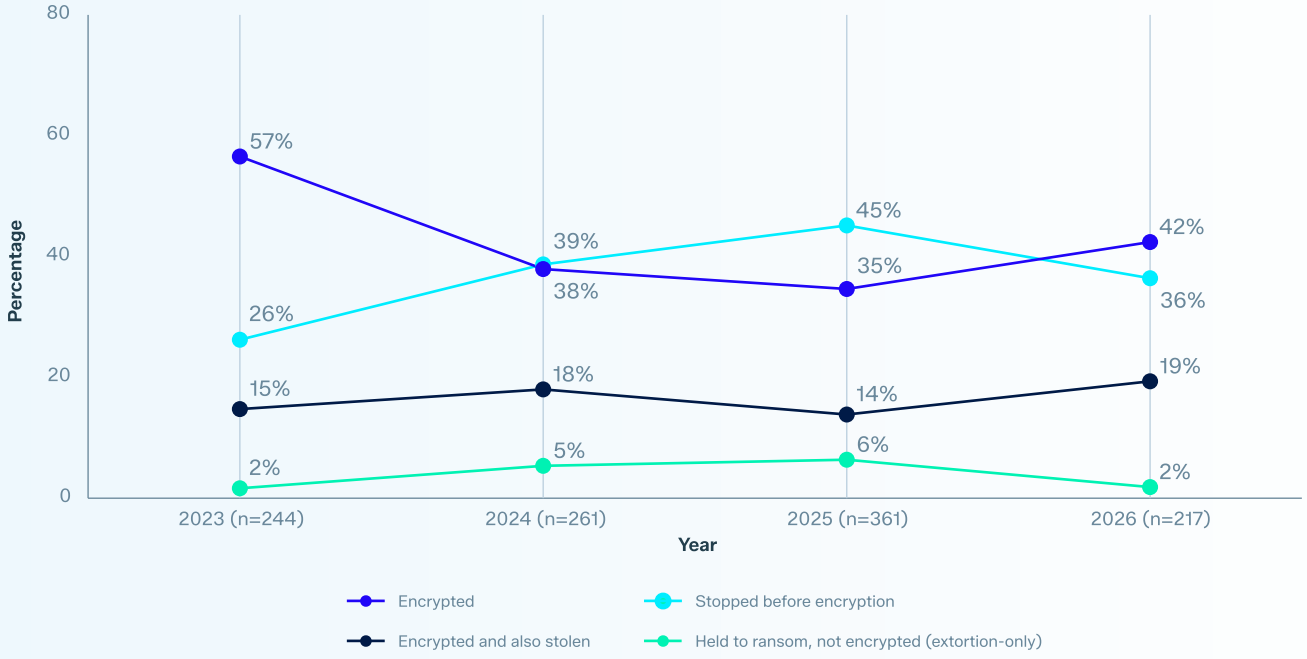
Data encryption summary (Yes/No) over time: Retail



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Summarized Yes / No answers. "Don't know" answers excluded from chart for visual clarity. Percentages may not equal 100%. Base numbers in chart.

The survey asks respondents if their data was just encrypted or encrypted and stolen in the same attack. **The proportion of attacks where data was encrypted and stolen (sometimes referred to as a "double extortion attack") rose to 19% of all retail attacks, up from 14% in 2025**. That's slightly above the 16% cross-sector rate for double extortion attacks.

Data encryption rate over time: Retail



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? "Don't know" answers excluded from chart for visual clarity. Percentages may not equal 100%. Base numbers in chart.

In double extortion attacks, the stolen data gives attackers a second point of leverage, which may weigh heavily on retailers that hold large volumes of customer payment and personal data.

Extortion-only attacks (where data is held to ransom without encryption) fell to 2%, down from 6% in 2025.

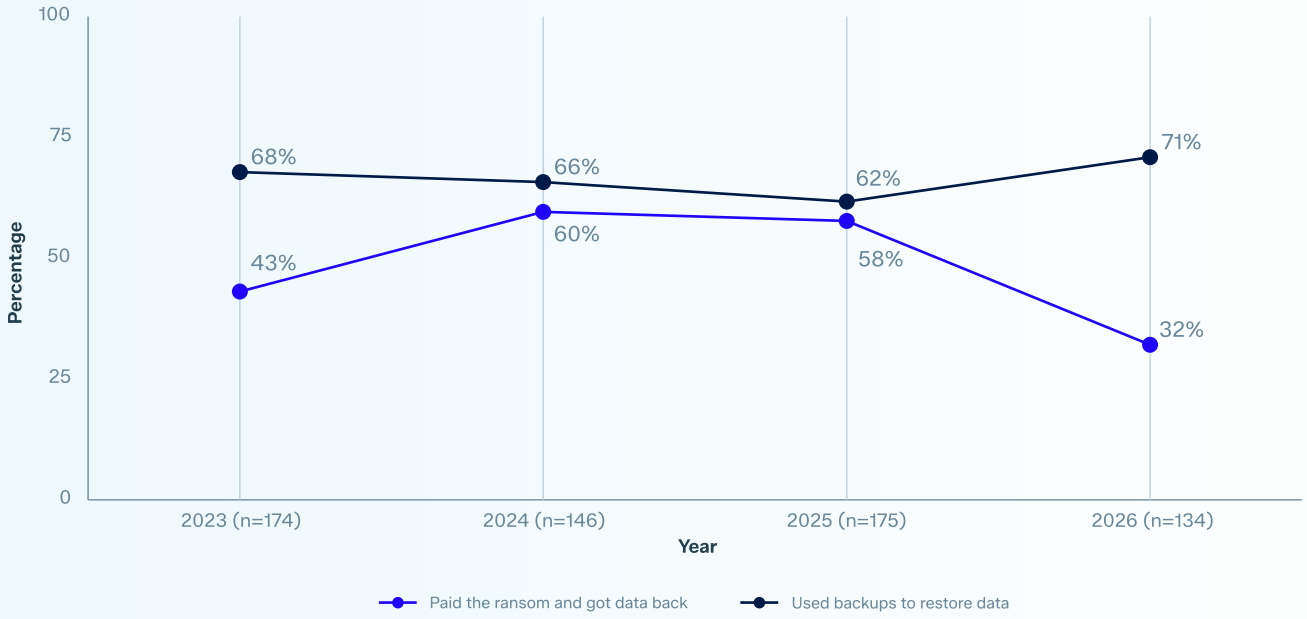
How organizations recovered encrypted data

Retail moved sharply away from paying ransoms in 2026. **Just 32% of retail organizations with encrypted data paid the ransom and got data back, the lowest rate of any sector** and well below the 48% cross-sector average. That is down from 58% in 2025 and the lowest rate in five years of retail data.

32%

The percentage of retail organizations with encrypted data that paid the ransom to get it back, the lowest rate of any sector surveyed.

Data recovery methods over time: Retail



How did your organization get the data back? Base: organizations that had data encrypted. Multiple responses permitted. Base numbers in chart.

Backups carried most of the recovery load. **71% of retail organizations restored data from backups**, up from 62% in 2025 and noticeably above the 66% cross-sector rate. Retail also relied on a single recovery route more than most sectors: 21% used more than one method to get data back, versus 33% across all sectors.

With encryption rising and payment-based recovery declining, more retail victims had their data locked this year, but far fewer paid to get it back. This may mean that the sector is recovering more on the strength of its own backups than on the attackers' cooperation.

Ransom demands and payments

Ransom demands

Retail faced a split set of ransom demands. **The median demand was $225,000, well below the $698,000 median for all sectors**. Yet the average (mean) demand was $4.32 million, the highest of any sector and well above the $3.13 million cross-sector average.

Note: Outlier ransoms of $40 million or more were removed from this data.

Median ransom demand

	2025	2026
Retail	$2.00M (n=175)	$0.23M (n=134)
All sectors	$1.32M (n=1,700)	$0.70M (n=1,214)

How much was the ransom demand from the attacker(s)? Base: organizations that had data encrypted. Base numbers in chart.

A few large ransoms drove the demand mean for retail far above the demand median. Those large ransoms correlated with organization size and revenue.

More than half of this year's retail victims came from organizations with 1,000 or fewer employees. That organizational size distribution, along with a typical pattern where attackers pitch demands tailored to the size of the target, were the key drivers of a low demand median despite a high demand mean.

Retail organizations with 100 to 1,000 employees faced a median demand of $75,000, while those with 1,001 to 5,000 employees faced a median of $1.42 million. Looking at revenue, 17 of the 23 ransom demands that were $5M or more came from organizations with $1 billion–$5 billion in revenue.

Against other sectors, retail's median demand is the second lowest.

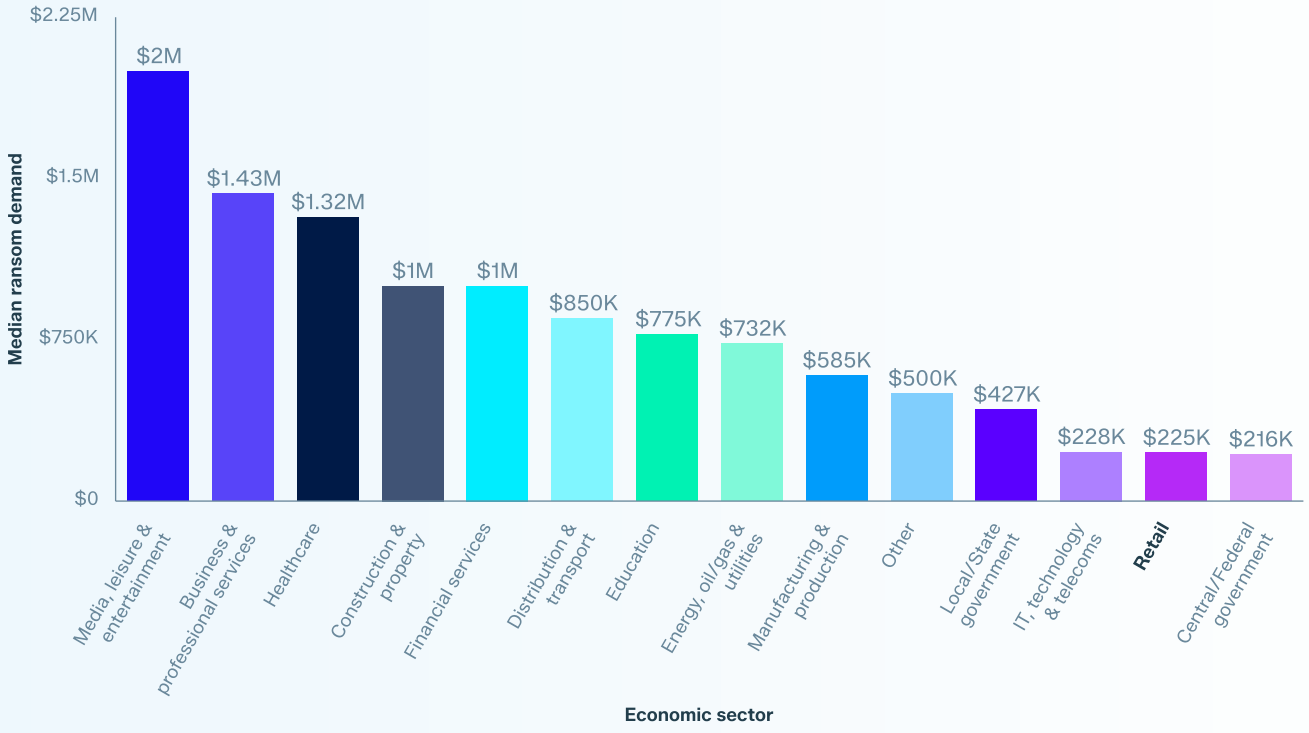
$225K

Retail's median ransom demand, among the lowest of any sector surveyed.

Average (mean) vs. Median:

The average (mean) is the total of all responses divided by the number of respondents. The median is the middle value, with half of responses above and half below. Averages can be skewed by a few unusually high or low figures, while the median shows the most typical response recorded.

Median ransom demands by sector



How much was the ransom demand from the attacker(s)? Base: organizations that had data encrypted. n=1,214.

Retail's median demand fell steeply year over year, from $2 million in 2025 to $225,000 in 2026. The mean moved in the opposite direction, rising from $3.70 million to $4.32 million. Read together, these numbers may indicate that ransom demands are getting higher for large, high-revenue retailers, while smaller retailers are growing as a proportion of ransomware victims.

Ransom payments

When retail organizations paid, they paid far less than other sectors. **The median ransom payment was $57,500, well below the $769,000 cross-sector median and the lowest of any sector**. Payments clustered low: 55% were under $100,000 (versus 27% across all sectors), the highest share of any sector.

Median ransom payment

	2025	2026
Retail	$1.00M (n=103)	$0.06M (n=43)
All sectors	$1.00M (n=847)	$0.77M (n=587)

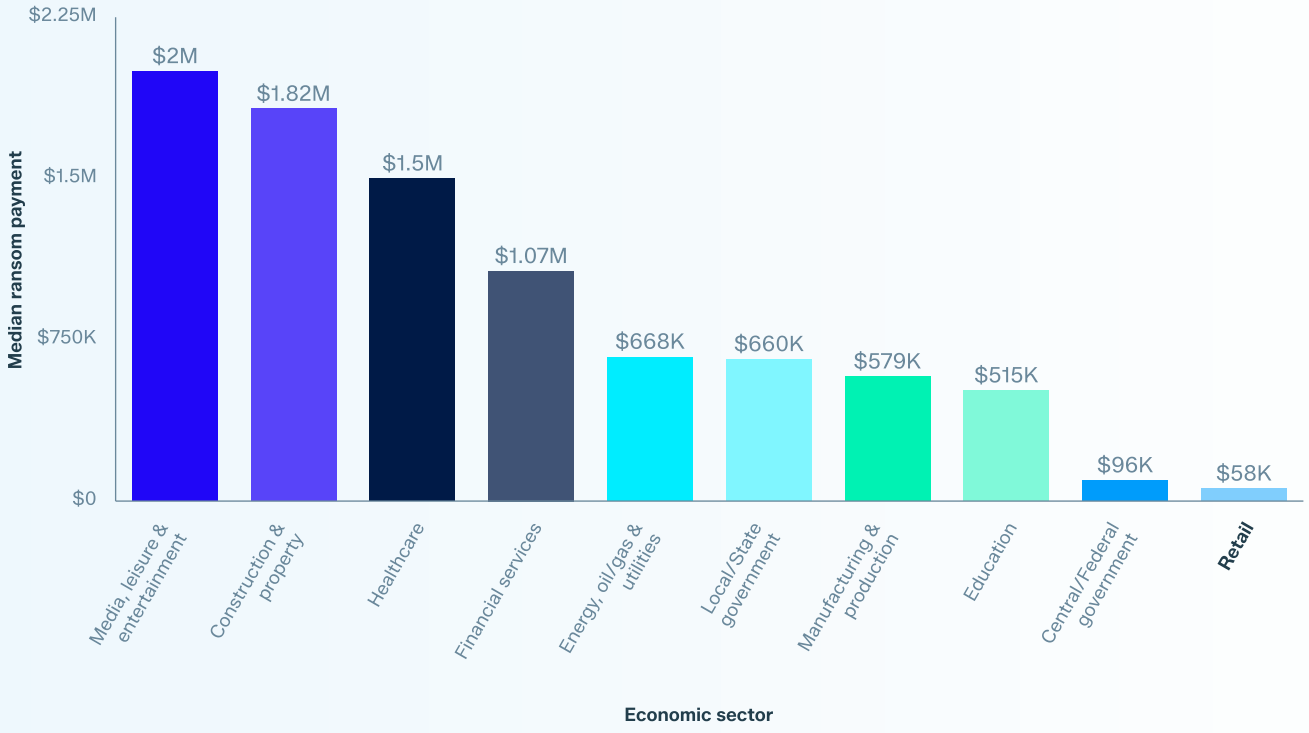
Approximately how much was the ransom payment paid to attackers? Base: organizations that paid the ransom. Base numbers in chart.

By contrast, the top end of payments was thin. 33% of retail payments were $1 million or more (versus 48% across all sectors), and just 5% were $5 million or more (versus 18% cross-sector), the lowest rate of any sector.

$57,500

Retail's median ransom payment, the lowest of any sector surveyed.

Median ransom payments by sector



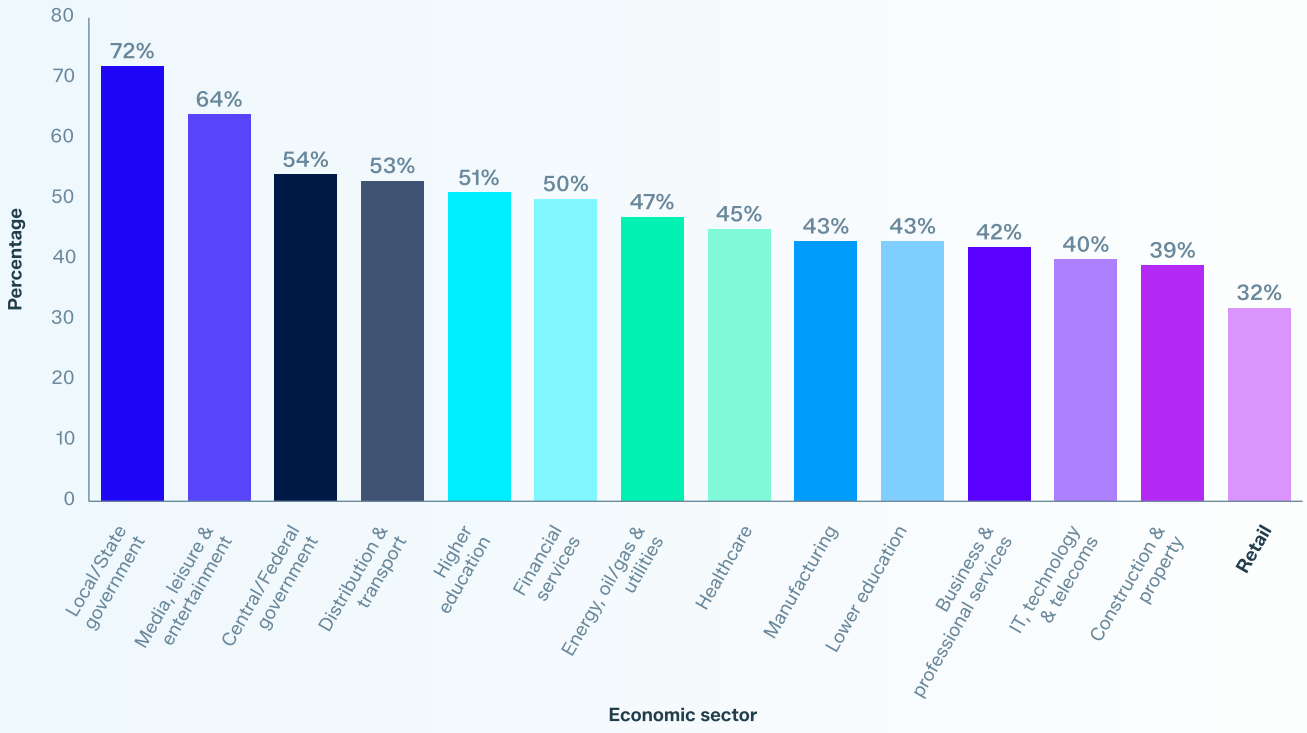
Approximately how much was the ransom payment paid to attackers? Base: organizations that paid the ransom. n=587. Excludes sectors with fewer than 30 respondents to this question.

Year-over-year, retail's median payment fell from $1.4 million in 2024 to $1 million in 2025 and $57,500 in 2026. This downward trend follows a cross-sector drop in payments from $1 million in 2025 to $769,000 in 2026.

Ransom payment rates, by sector

Just under a third of retail victims (32%) paid the ransom and got their data back, the lowest rate of any sector and significantly below the 48% cross-sector rate.

Percentage who paid the ransom and got data back, by sector



Did your organization get any data back? Answer: Yes, we paid the ransom and got data back. Base: organizations that had data encrypted. n=1,214.

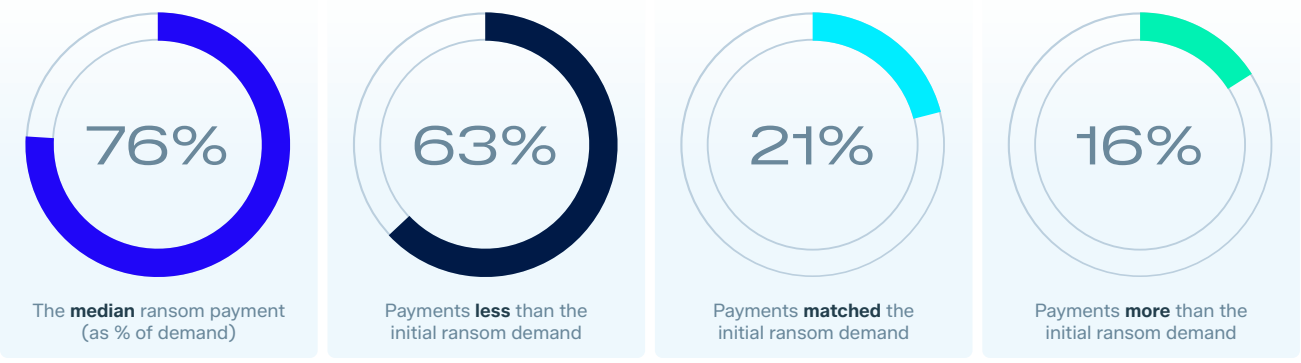
Actual payments vs. initial demands

Among retail organizations that paid their ransoms, the median payment was 76% of the original demand, the second-lowest percentage of any sector, behind only manufacturing and production (67%). In absolute ransom reduction numbers, **the retail sector negotiated attackers down by a median of $11,700, compared with a median reduction of $1,550 across all sectors**.

63% of retail organizations paid less than the initial demand, 21% paid exactly what was demanded, and 16% paid more. The 63% rate of lower payments was well above the 51% cross-sector rate and the second highest of any sector, behind manufacturing and production (75%).

The below-demand payment percentage has risen for the past two years from 53% in 2024 to 59% in 2025 and 63% in 2026. In line with that trend, the median payment as a share of the demand fell over the past two years from 90% to 86% to 76%.

Actual payment vs. initial demand: Retail



How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? Base: organizations that shared both ransom demand and payment. n=38.

Business and human impact

Ransomware recovery costs

The average (mean) cost for retail organizations to rectify a ransomware attack, excluding any ransom paid, was $1.76 million, slightly above the $1.70 million cross-sector average.

The median cost was $375,000, the same as the cross-sector median. The higher mean reflects a heavier top tier: 6% of retail recoveries cost $10 million or more, versus 2% across all sectors.

Average (mean) recovery cost

	2025	2026
Retail	$1.65M (n=361)	$1.76M (n=217)
All sectors	$1.53M (n=3,400)	$1.70M (n=2,158)

What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack? Base numbers in chart.

Year-over-year, the mean rose from $1.65 million in 2025 to $1.76 million in 2026, in step with the cross-sector average, which rose from $1.53 million to $1.70 million.

$1.76M

Retail's average (mean) cost to recover from a ransomware attack, excluding any ransom paid.

Recovery time

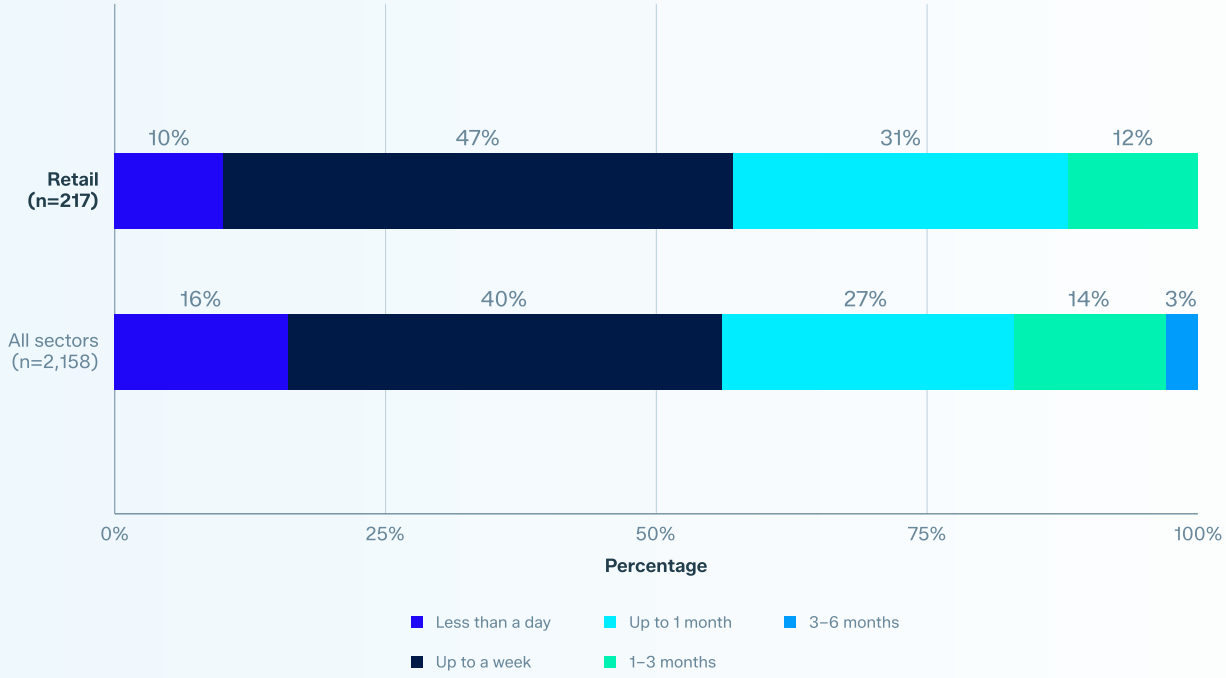
Retail recovered faster than the average sector with **a mean time to fully recover of 2.54 weeks, below the 2.80-week cross-sector average**, placing retail in the middle of the sector rankings.

56% of retail organizations recovered within a week, in line with 55% across all sectors and the highest share in five years of retail data. 12% took a month or more to fully recover.

2.54 weeks

The average time retail organizations took to fully recover from a ransomware attack, the fastest in five years of retail data.

How long it took to recover from ransomware



How long did it take your organization to fully recover from the ransomware attack? Percentages in this chart rounded using the largest remainder method and may differ from percentages in the report text. Base numbers in chart.

Year-over-year, retail recovery time improved by more than half a week, from 3.16 weeks in 2025 to 2.54 weeks in 2026.

Human impact

The human toll on retail IT/cybersecurity teams after a ransomware attack was lighter than in any other sector. Nearly every team still felt some effect, but retail teams reported fewer repercussions than the cross-sector average. Retail respondents selected an average of 2.46 repercussions from their ransomware attacks, versus 2.93 average selections across all sectors.

22% saw changes to team or organizational structure, the lowest share of any sector and well below the 32% cross-sector rate. Other pressures in retail ran below the cross-sector average too: 23% reported an ongoing increase in workload (versus 31%), and 24% reported staff absence due to stress or mental health issues (versus 29%). However, anxiety about future attacks was in line with other sectors at 41%.

22%

The proportion of retail IT/cybersecurity teams that saw changes to team or organizational structure after an attack, the lowest of any sector.

Human impact of ransomware

Repercussion	Retail (n=134)	All sectors (n=1,214)
Increased anxiety or stress about future attacks	41%	41%
Increased pressure from senior leaders	37%	40%
Increased recognition from senior leaders	32%	36%
Feelings of guilt that the attack was not stopped	30%	31%
Change of team priorities/focus	27%	32%
Staff absence due to stress/ mental health issues	24%	29%
Ongoing increase in workload	23%	31%
Changes to team/ organizational structure	22%	32%
Team's leadership was replaced	10%	21%

What repercussions has the ransomware attack had on the people in your IT/cybersecurity team? Base: organizations that had data encrypted. Base numbers in chart.

Leadership turnover was also the lowest of any sector, with 10% of retail teams seeing their leadership replaced after the attack, compared with 21% across all sectors and down from 26% in 2025.

Most of these measures fell sharply from 2025, when 43% of retail teams reported an ongoing increase in workload and 41% saw changes to team or organizational structure.

Recommendations

Strengthen identity security as a ransomware defense. Retail had the lowest share of attacks that began with an identity-based approach (69%), yet that still covers roughly seven in ten attacks, and two-thirds of retail victims (66%) said their ransomware incident and most significant identity attack were the same event. That's why retail and every other sector should prioritize identity threat detection and response (ITDR), enforce multi-factor authentication across all access points, and regularly audit both human and non-human identity credentials.

Enable MFA comprehensively, specifically phishing-resistant MFA. The survey showed that 97% of retail organizations with compromised credentials had enabled MFA in some capacity at the time of their attack, yet more than half still had data encrypted. MFA alone is not enough to stop attacks, and it needs to be comprehensively enabled rather than left on for the SaaS apps that force it and off for VPN logins, firewall admin consoles, and legacy apps.

Strengthen endpoint protection against AI-discovered exploits. Retail was the sector most likely to be breached through an exploited vulnerability (26%), and 44% of attacks that began with brute force, a vulnerability, or stolen credentials started on a user's device. Sophos experts expect exploits to climb again. Having strong endpoint defenses that automatically block exploit-based attacks is essential.

Bring in specialist support or MDR. Retail's operational weaknesses are concentrated in security gaps, but the resourcing burden is still an issue for roughly half of organizations. 51% cited a resourcing issue: a lack of expertise or people and capacity. Dealing with AI-augmented threats will put even more strain on these areas as security teams try to stay current with fast-changing AI technology. Unless you can confidently staff a security operations team in-house, look to an external specialist to fill the gap, either a 24/7 MDR vendor or a managed services provider. Vendors that resolve more incidents end-to-end with AI and automation act as a force multiplier that helps close skills and capacity gaps.

Invest in backup and recovery infrastructure. Backups were the dominant recovery route for retail (71%), alongside the lowest ransom payment rate of any sector. They should be tested regularly, stored offline or in immutable formats, and integrated into a documented incident response plan that can be executed under pressure.

Maintain exposure management programs. Known security gaps were retail's most common operational root cause (38%), and exploited vulnerabilities started a larger share of retail attacks than in any other sector, so closing the loop between awareness and remediation is the highest-value move here. Retailers should maintain aggressive patching cadences and focus on mitigations including segmentation, zero trust network access, and MFA/ continuous authentication deployments.

Reduce exposure via the firewall and leverage firewall telemetry to detect attacks early. Firewalls identified most attacks, but early detection did not reliably prevent encryption: 59% of retail firewalls identified the attack before the ransomware was deployed, yet among those early-detection cases, victims still had their data encrypted 60% of the time. Ensure your firewall receives rapid, ideally automated, updates and minimize internet-facing services like admin access and user portals. Connect firewalls to XDR and MDR so firewall telemetry helps detect ransomware attacks before payloads deploy. A cybersecurity defense system, where controls share signal, is the answer.

Recommended actions at a glance:

- Segmentation to slow attackers down
- ZTNA to replace legacy VPNs and contain app exploits
- Identity threat detection and response (ITDR) to harden identity infrastructure
- Phishing-resistant MFA as the destination rather than the starting line
- Disciplined patching of internet-facing devices
- 24/7 detection and response

Conclusion

The State of Ransomware in Retail 2026 report reveals a threat landscape in transition.

There are signs of progress: retail was the least likely sector to pay the ransom to recover data (32%), backup-based recovery rose to 71%, and recovery times were the fastest in five years of retail data. When retail organizations did pay, their median payment was the lowest of any sector.

At the same time, the challenges that remain are significant. More than six in ten ransomware attacks against retail now succeed in encrypting data, up from under half in 2025. Double extortion is climbing, and **retail faced the highest average ransom demand of any sector**.

Retail led all other sectors in attacks that began with an exploited vulnerability, and user devices were the most common place that ransomware attacks started. But identity still matters: even with the lowest identity-based share of any sector, roughly seven in ten retail attacks began with an identity-based approach.

Retailers also need to prepare for the defining cybersecurity challenge of the next decade: AI-augmented threats. The data already hints at why: 61% of retail organizations cited a security gap as an operational root cause and known security gaps were the sector's most common operational root cause at 38%. Both known and unknown gaps become more consequential as AI accelerates the speed and scale of attacks, with adversaries using AI to find weaknesses faster and orchestrate attacks on multiple control points at machine speed.

There's a deeper signal in this year's root-cause data, too. The perceived root-cause mix is equalizing; across all sectors, no single vector dominates. Retail shows the same pattern, with phishing, exploited vulnerabilities, and malicious email each accounting for between 22% and 29% of attacks. That makes focusing defenses too narrowly on any one entry method risky, because attackers are succeeding through multiple vectors.

The pattern across this year's findings, especially the high rate of encryption after early firewall detection and the limited effect of MFA enablement on outcomes, points in a consistent direction: when defenses operate in isolation, you're not protected. Closing the gap on AI-era attacks will depend less on adding more tools and more on connecting the ones already in place, so context, detection, and response can move at the speed the threats now demand.

The retail organizations that will fare best against ransomware in the years ahead are those that sustain executive attention on this issue while adopting integrated, AI-driven defensive systems, investing in technology and processes as well as in the people who defend against these threats every day.

SOPHOS

To learn more about ransomware and how Sophos can help you defend your organization, visit our website.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

© Copyright 2026. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2026-11-05 EN (DD)