THE STATE OF RANSOMWARE IN MANUFACTURING AND PRODUCTION 2025

Findings from an independent survey of 332 IT and cybersecurity leaders in the manufacturing and production sector across 17 countries whose organizations were hit by ransomware in the last year.

A Sophos Whitepaper. October 2025

Introduction

Welcome to the fifth edition of the annual Sophos State of Ransomware in Manufacturing and Production report, which reveals the reality of ransomware for manufacturing and production organizations in 2025.

This year's report unveils how manufacturing and production organization's experiences of ransomware have evolved over the past year. It also shines light onto previously unexplored areas, including the operational factors that left manufacturing and production organizations exposed to attacks and the human impact of incidents on IT/cybersecurity teams.

Based on the real-world frontline experiences of 332 IT and cybersecurity leaders from the manufacturing and production sector, whose organizations were hit by ransomware in the last year, the report provides unique insights into:

- Why 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 332 manufacturing and production respondents the report is based on span 17 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 manufacturing and production organizations fall victim to ransomware

- Manufacturing and production victims identified **exploited vulnerabilities** as the most common technical root cause of attack, used in 32% of incidents. This was followed by **malicious emails** used in 23% of attacks. **Credential-based** attacks ranked third, used in one in five incidents (20%) — the lowest level recorded in three years.

- Multiple operational factors contribute to manufacturing and production organizations falling victim to ransomware, with the most common being **a lack of expertise**, named by 42.5% of victims. It is followed in very close succession by both **unknown security gaps** and **a lack of protection**, which were contributing factors in 41.6% and 41% of attacks respectively.

What happens to the data

- The **data encryption** rate in the manufacturing and production sector is at its lowest level in five years, with 40% of attacks now resulting in data encryption, down from a 74% peak in 2024.

- 39% of manufacturing and production organization that had data encrypted also experienced **data exfiltration** — the second highest rate reported by any sector in this year's survey.

- 91% of manufacturing and production organizations that had data encrypted recovered it — the lowest rate reported in this year's survey.

- The use of **backups** by manufacturing and production organizations to restore encrypted data remained consistent year over year, used, once again, in 58% of incidents.

- 51% of manufacturing and production organizations **paid the ransom** to get their data back — a decrease on the 62% reported in 2024.

Ransoms: Demands and payments

- The average (median) **ransom demand** made to manufacturing and production organizations has fallen 20% over the last year, coming in at $1.2 million in 2025 compared to $1.5 million in 2024. The primary factor behind this decline is a 23% decrease in the percentage of ransom demands between $1M and $5M, down from 44% of demands in 2024 to 34% in 2025.

- The average (median) **ransom paid** by manufacturing and production organizations has also dropped, coming in at $1 million in 2025 compared to $1.2 million in 2024. The decline is largely driven by a 29% decrease in the percentage of ransom payments between $500K and $5 million. However, it is important to note that there has been a small increase in extreme payments of $5 million or more.

- The **proportion of the ransom demand paid** by manufacturing and production organizations increased to 86% in 2025 from 70% in 2024.

- Looking closely at **demands vs. payments**, 37% of manufacturing and production organizations said their payment matched the initial demand. Close to half (49%) paid less than the initial ask, while 13% paid more.

Business impact of ransomware

- The average **cost for manufacturing and production organizations to recover f**rom a ransomware attack dropped by 24% over the last year, coming in at $1.3 million, down from $1.7 million in 2024.

- Looking at the **speed of recovery,** manufacturing and production organizations are recovering faster, with 58% recovered within a week in 2025, up from 44% in 2024.

Human impact of ransomware

Every manufacturing and production organization that had data encrypted reported that there were **direct repercussions** for the IT/cybersecurity team:

- 47% of manufacturing and production respondents cited **increased anxiety or stress** about future attacks as an impact on their IT/cybersecurity team.
- 45% reported a change of **team priorities/focus.**
- 44% of IT/cybersecurity teams reported **increased pressure** from senior leaders, while 30% reported in**creased recognition**.
- 41% of manufacturing and production respondents cited an **increased workload** and **changes to team/ organizational structure** as impacts on their IT/cybersecurity team.
- 40% of respondents cited **feelings of guilt** that the attack was not stopped as a repercussion of the incident.
- In over a quarter of cases (27%), the team's **leadership was replaced** because of the attack.
- A fifth (20%) of teams experienced **staff absence** due to **stress/mental health** issues related to the attack.

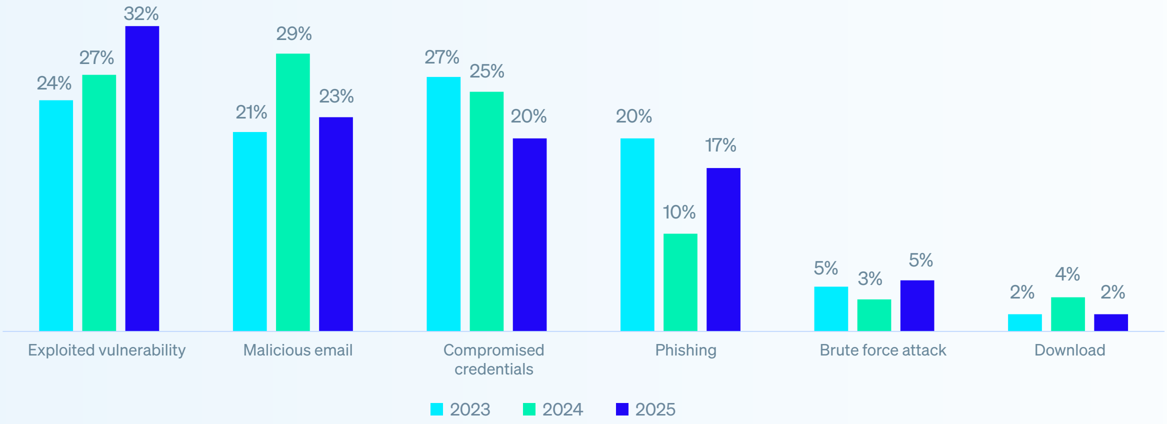
In manufacturing and production, reports of these impacts were worryingly higher than the cross-sector average across nearly all areas.

Why organizations fall victim to ransomware

Technical root cause of attacks in manufacturing and production

Exploited vulnerabilities are the leading root cause of ransomware attacks on manufacturing and production organizations, responsible for 32% of incidents. **Malicious emails** ranked second, with their share declining from 29% in 2024 to 23% in 2025. **Credential-based attacks** continue to pose a significant risk, though reports dropped — from 25% in 2024 to 20% in 2025.

Chart 1: Technical root cause of ransomware attacks in manufacturing and production 2023 - 2025

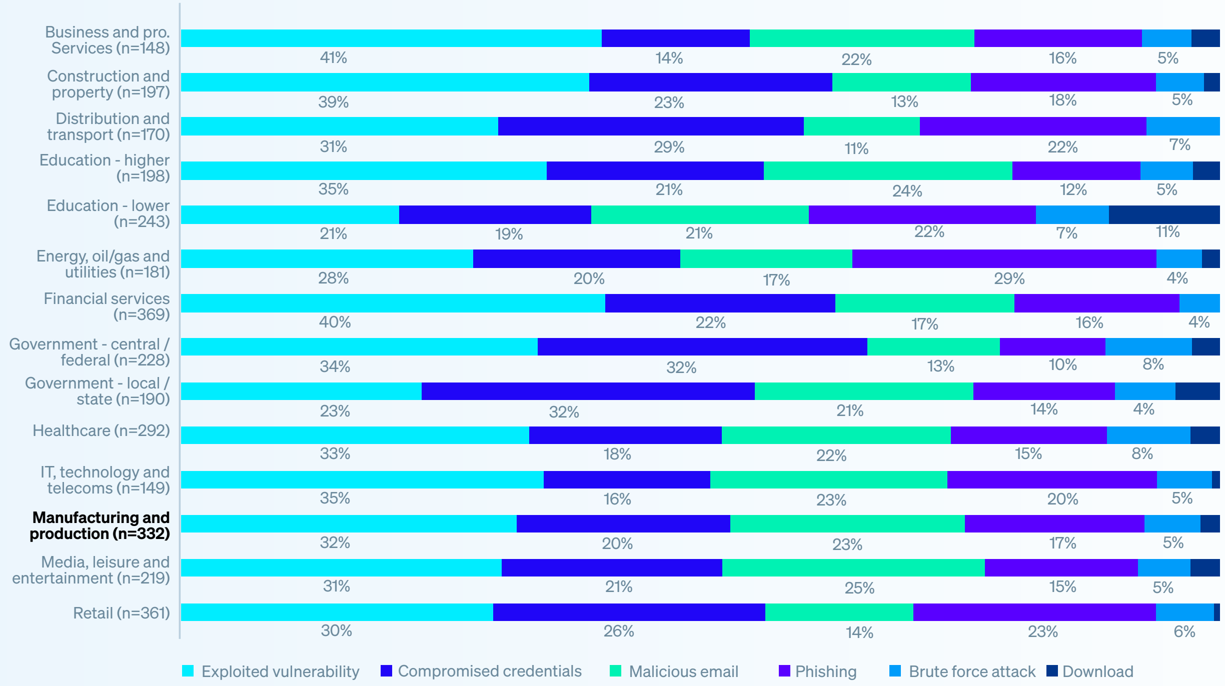


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=331 (2025), 375 (2024), 204 (2023).

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

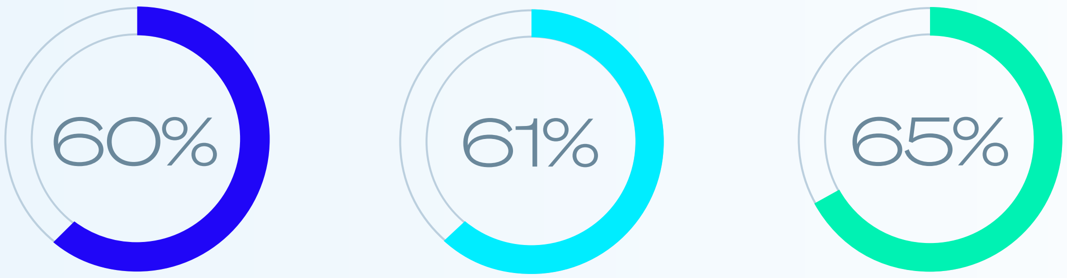


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. Base numbers in chart.

Organizational root cause of incidents in manufacturing and production

This year's report explores for the first time the organizational factors that left manufacturing and production organizations exposed to attacks. The findings reveal that victims in the manufacturing and production sector are typically facing multiple organizational challenges, with respondents citing three 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, manufacturing and production organizations are slightly more likely to cite a security gap (known and unknown) as the primary factor.



LACK OF/POOR QUALITY PROTECTION
Lack of protection or poor-quality protection solutions that could not stop the attack

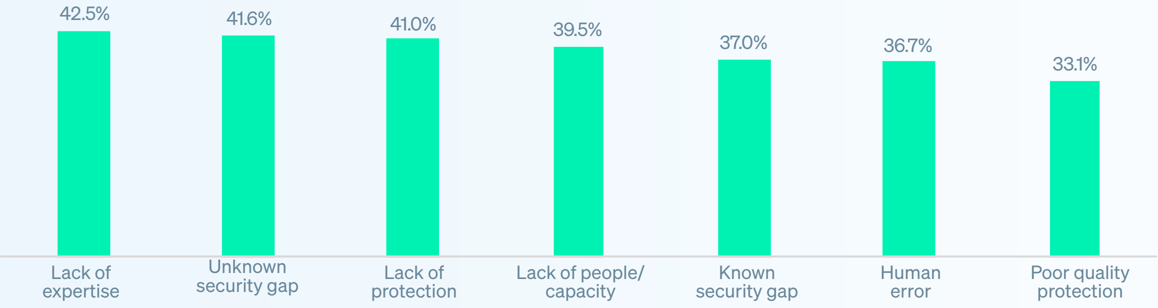
LACK OF PEOPLE/SKILLS
Lack of human expertise (skills or capacity) to detect and stop the attack in time

SECURITY GAP (KNOWN/UNKNOWN)
Had a known or unknown weakness in their defenses

Why do you think your organization fell victim to the ransomware attack? n=332. Consolidated responses.

A lack of expertise (i.e., insufficient skills or knowledge available to detect and stop the attack in time) is the most common individual reason given, named by 42.5% of manufacturing and production respondents. This is closely followed by **unknown security gaps** (i.e., weaknesses in defenses that respondents were unaware of), which contributed to 41.6% of attacks. In third place was a **lack of protection** (i.e., not having the necessary cybersecurity products and services in place), which contributed to 41% of attacks.

Chart 3: Operational root cause of ransomware attacks on manufacturing and production organizations



Why do you think your organization fell victim to the ransomware attack? n=332.

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 in place	We had weakness(es) in our defenses that 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 service, incl. insurance (44%) * Local/state government (40%)	Central/federal government (45%) IT, technology, telecoms (42%) Construction and property (41%) *	Media, leisure, & entertainment (44%) Distribution & transport (41%)

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

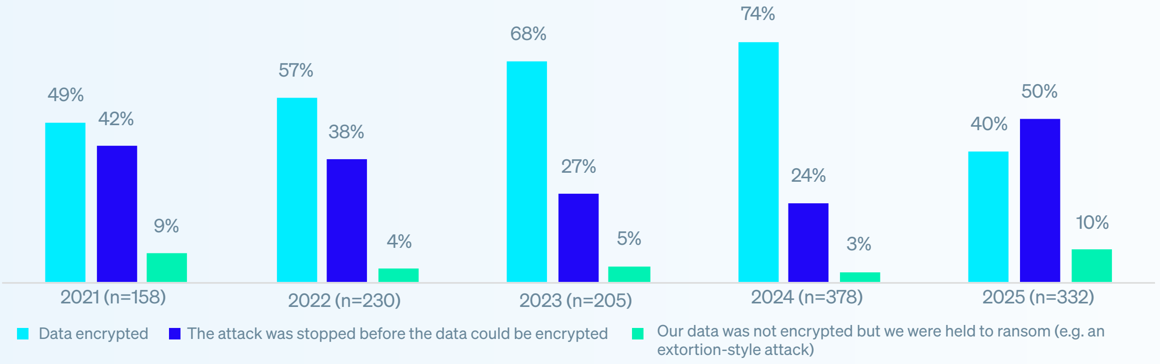
What happens to the data

Data encryption in manufacturing and production

Encouragingly, data encryption in manufacturing and production is at its lowest reported rate in the five years of our study, with only 40% of attacks resulting in data being encrypted, the third lowest percentage recorded in this year's survey and nearly half the 74% reported in 2024.

Meanwhile, the percentage of ransomware attacks that were stopped before data encryption has more than doubled over the last year, climbing from 24% in 2024 to 50% in 2025. This suggests that manufacturing and production organizations are becoming more effective at halting attacks before they cause serious damage.

Chart 5: Data encryption rate in ransomware attacks on manufacturing and production 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

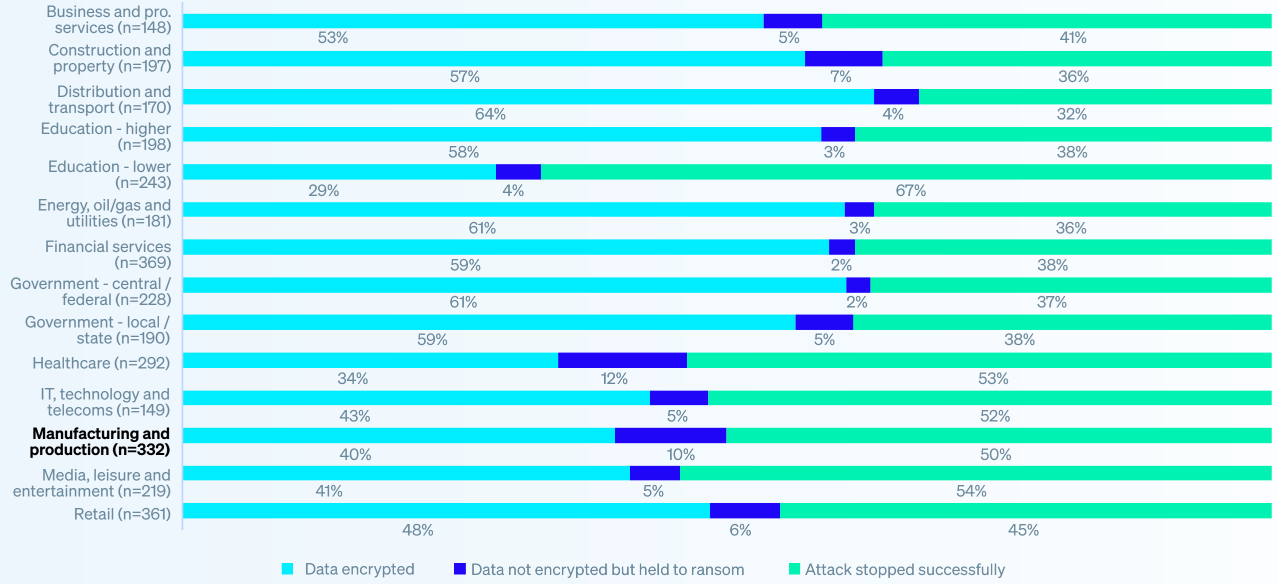
Organizations within the **distribution and transport** sector are most likely to have data encrypted (64%), indicating that organizations in this sector are less able to detect and stop the attack before encryption and/or are less able to block and roll back malicious encryption. In contrast, **lower 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 manufacturing and production sector, 15% of all ransomware victims and 39% of those that had data encrypted experienced data theft — the second highest rate reported in this year's survey. Breaking down the data by industry 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.

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 manufacturing and production organizations that did not have data encrypted but were held to ransom anyway (extortion) surged to 10% of attacks in 2025 from just 3% in 2024, the second highest rate reported in this year's survey. This is likely due to the high value of intellectual property, complex supply chains, and the operational impact of downtime in manufacturing environments.

In contrast, both **financial service** providers and **central/federal government** organizations reported experiencing the fewest of these attacks, at just 2%.

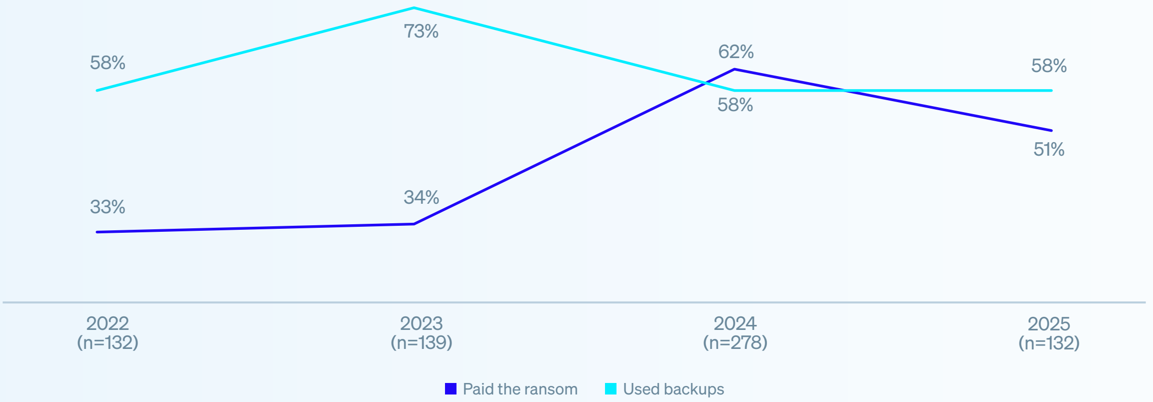
Overall, **lower education** providers are most able to successfully prevent the repercussions of a ransomware attack, (i.e., to stop data being encrypted, to prevent data exfiltration, and to avoid being subject to extortion). This suggests that lower education providers are proving surprisingly effective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

Recovery of encrypted data in manufacturing and production

91% of manufacturing and production organizations that had data encrypted were able to recover it, the lowest rate reported in this year's survey.

In 2025, just over half (51%) of manufacturing and production organizations **paid the ransom** — down from 62% in 2024. Meanwhile, **backup use** has remained consistent year over year at 58%. Collectively, these findings point to stronger resistance to demands and confidence in backup resilience.

Chart 7: Recovery of encrypted data in manufacturing and production 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

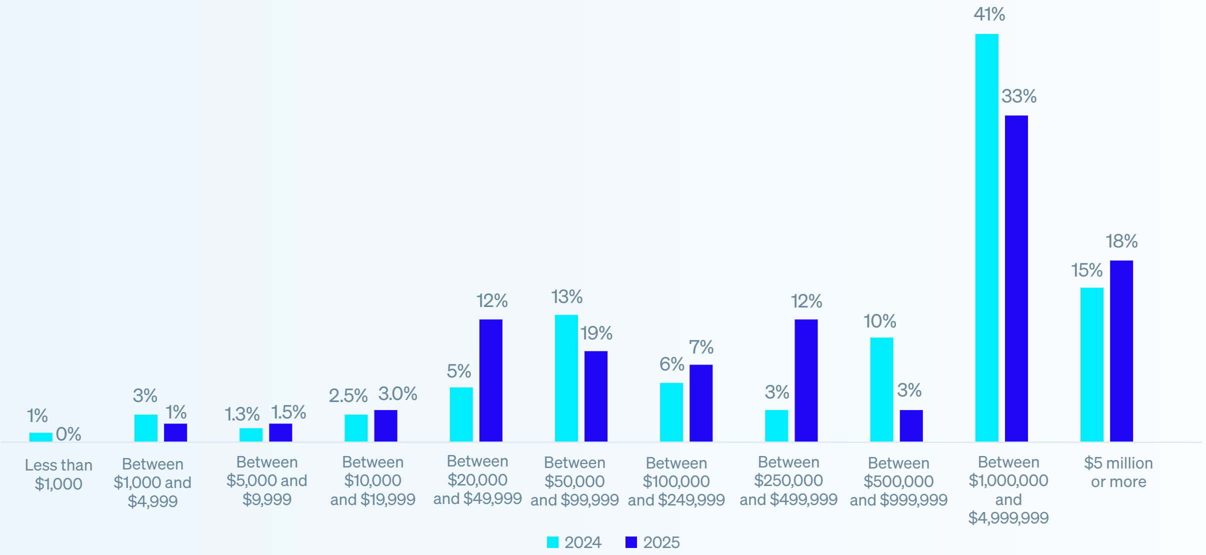
Manufacturing and production ransom demands

The average (median) ransom demand for manufacturing and production organizations dropped 20% over the last year, coming in at $1.2 million in 2025, down from $1.5 million in 2024. The decrease in ransom demands targeting manufacturing and production organizations is largely driven by a 23% decrease in demands between $1 million and $5 million. However, it's important to note that there was a small increase in extreme demands of $5 million or more — accounting for a fifth (20%) of demands — up from 15% in 2024.

Manufacturing and production ransom payments

Following this trend, the average (median) ransom paid by manufacturing and production organizations also saw a decline from $1.2 million in 2024 to $1 million in 2025. This is largely due to a 29% decrease in payments between $500K and $5 million. However, as observed in ransom demand trends, extreme payments of $5 million or more saw a small increase — accounting for 18% of payments in 2025 — up from 15% last year.

Chart 8: Ransom payments in manufacturing and production | Distribution banding

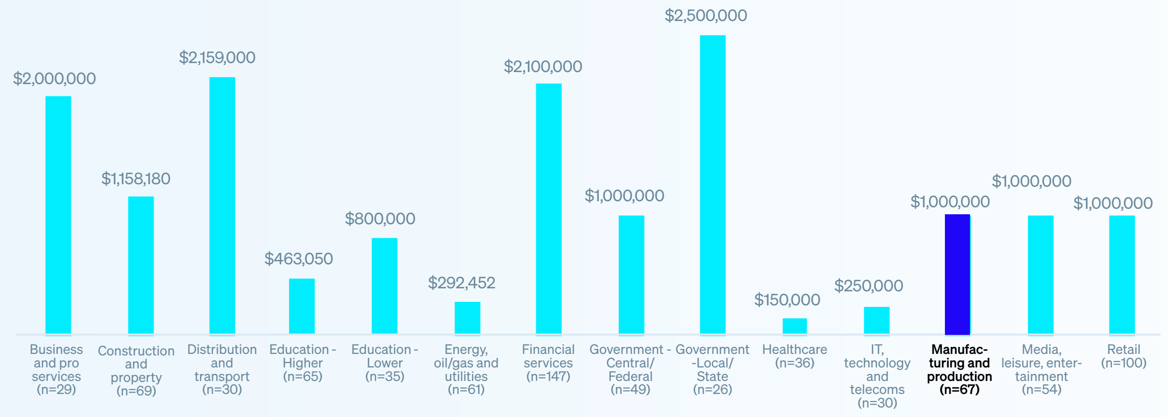


How much was the ransom payment that was paid to the attackers? n=67 (2025), 157 (2024)

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.

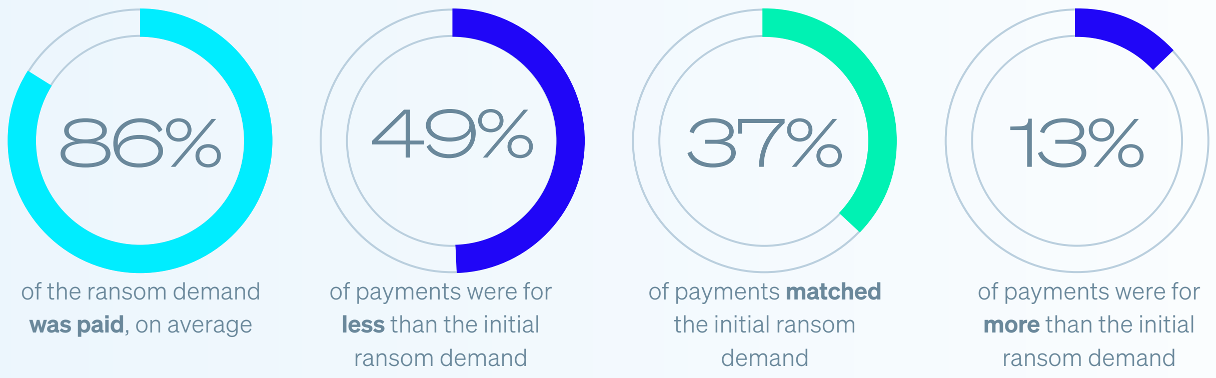
Chart 9: Ransom payments by industry



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.

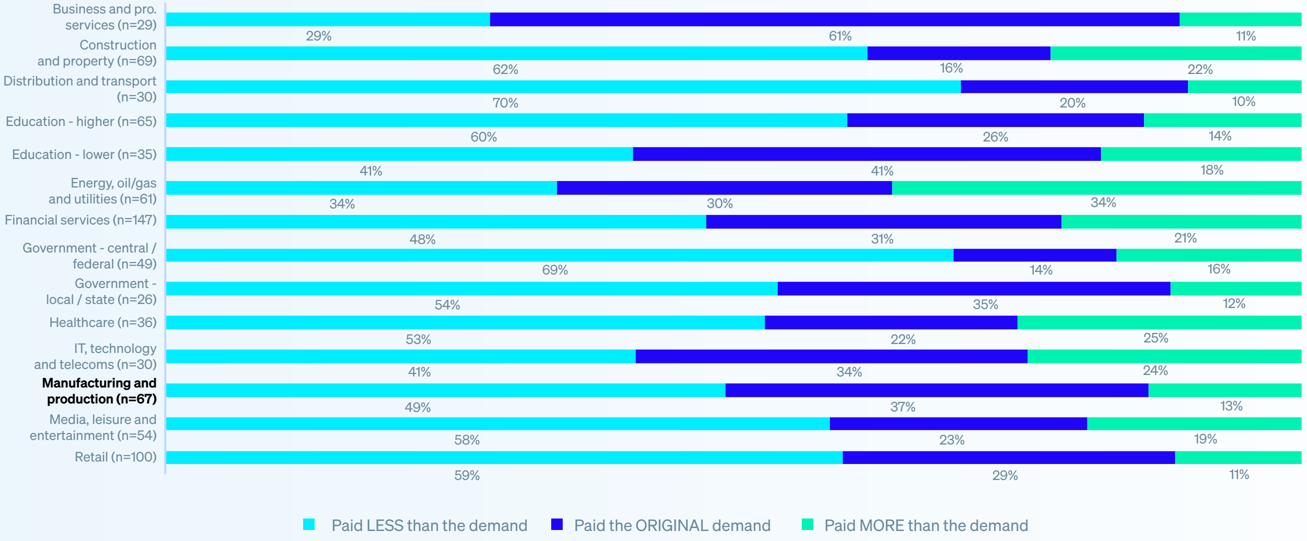
How actual payments made by manufacturing and production organizations stack up with the initial demand

67 manufacturing and production organizations that paid the ransom shared both the initial demand and their actual payment, revealing that they paid, on average, 86% of the initial ransom demand — a notable increase on the 70% recorded in 2024. Overall, just under half (49%) paid less than the initial ask,13% paid more, and 37% matched the initial demand.



Splitting the data by industry, we see that, encouragingly, in most sectors, paying less than the original ransom demand is the most common outcome. Organizations in the **distribution and transport** sector were 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.

Business consequences of ransomware

Recovery costs in manufacturing and production organizations

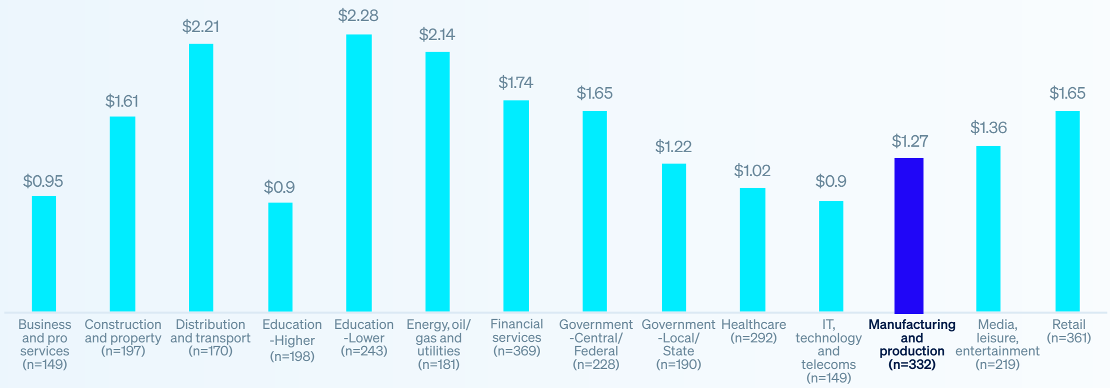
The average recovery cost for manufacturing and production organizations, excluding any ransom payments, has dropped nearly a quarter (24%) over the past year to $1.3 million — below the $1.5 million global average. However, it is $200K higher than the sum reported in 2023.

2023	2024	2025
$1.1M	$1.7M	$1.3M

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=332 (2025), 378(2024), 205 (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 industry

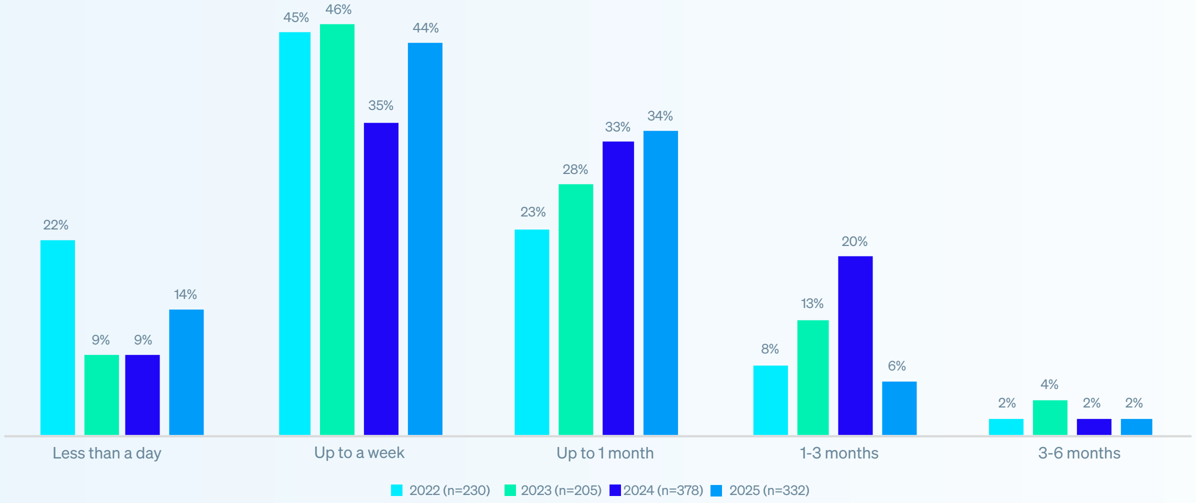


What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.) excluding any ransom payments made? Base numbers in the chart.

Recovery time in manufacturing and production

The data reveals that, in 2025, manufacturing and production organizations are getting faster at recovering from attacks. 58% recovered within a week, up from 44% reported in 2024. At the same time, the proportion taking one to three months to recover fell sharply to 6%, down from 20% in 2024. Overall, 98% of manufacturing and production victims fully recovered within three months, underscoring growing resilience and recovery capabilities across the sector.

Chart 12: Recovery time for manufacturing and production 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, manufacturing and production organizations that had data encrypted typically were slower to recover than those that were able to stop the encryption: 3% 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 and cybersecurity teams in manufacturing and production organizations, with all respondents reporting an impact. Worryingly, reports of these impacts in this sector were higher than the cross-sector average across all but two areas.

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

Cross-sector average	Manufacturing and production	
41%	47%	Increased **anxiety or stress** about future attacks
38%	45%	Change of **team priorities / focus**
40%	44%	Increased **pressure** from senior leaders
38%	41%	Ongoing **increase in workload**
37%	41%	Changes to team/ organizational **structure**
34%	40%	Feelings of **guilt** that the attack was not stopped
31%	30%	Increased **recognition** from senior leaders
25%	27%	Our team's leadership was **replaced**
31%	20%	Staff absence due to **stress / mental health** issues

What repercussions has the ransomware attack had on the people in your IT/cybersecurity team, if any? n=132.

Recommendations

Although manufacturing and production 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.

© Copyright 2025. 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.

2025-10-23 WP (NP)

SOPHOS