August 2025

Market report

The Ransomware Insights Report 2025

Examining the experience and impact of ransomware on organizations worldwide

Barracuda®
Your business, secured.

Contents

Introduction

Ransomware is a widespread and evolving threat, powered by ransomware-as-a-service kits that enable ever more cybercriminals to launch attacks. Ransomware incidents can damage brand reputations and cripple day-to-day operations, causing disruption, loss of data, customer trust and more. Every organization is a potential target.

This report explores the experience and impact of successful ransomware attacks on organizations around the world in the last 12 months. It draws on the findings of an international survey of 2,000 IT and security decision-makers undertaken by Barracuda and Vanson Bourne.

The findings can be grouped into three overarching themes, namely:

- **Ransomware victims are more likely to have fragmented security**, with too many disconnected security tools and insufficient cover in key security areas.
- **Ransomware attacks are multidimensional.** They are no longer just about data encryption, but now involve data theft and exposure, the installation of additional malicious payloads, and more.
- **The impact crater of a successful ransomware attack is expanding**, including the loss of new business opportunities, and payment pressure tactics that extend to employees, partners, customers, and the authorities.

We hope this report will help organizations of all sizes and industries to understand the threat and impact of ransomware in 2025 and to identify and address areas where they could potentially be at risk.

Methodology

Barracuda commissioned independent market research company Vanson Bourne to conduct a global survey of 2,000 senior security decision-makers in IT and business roles in organizations with between 50 and 2,000 employees from a broad range of industries in the U.S., UK, France, DACH (Germany, Austria, Switzerland), Benelux (Belgium, the Netherlands, Luxembourg), the Nordics (Denmark, Finland, Norway, Sweden), Australia, India, and Japan. The fieldwork was conducted in April and May 2025.

Key findings

57%

of organizations experienced a successful ransomware attack in the last 12 months

71%

of organizations that had experienced an email breach were also hit with ransomware

32%

paid a ransom to recover their data — 41% of them did not get all their data back

65%

of ransomware victims were able to restore data from backups

24%

of ransomware victims had data encrypted — while 27% had data stolen, and 29% said the attackers installed additional payloads

25%

of ransomware victims lost existing customers — the same proportion lost new business opportunities

Ransomware affects more than half of organizations

Overall, 57% of the organizations surveyed had experienced a successful ransomware attack in the last 12 months.

One in three victims (31%) were affected twice or more.

The prevalence of multiple successful attacks suggests that security gaps are not fully investigated and addressed after each incident. Throughout this report we look at the difference between organizations affected once and those affected multiple times to see what can be learned from the data and how organizations can use this to boost their security posture.

The most affected industry sectors in our survey included healthcare (with 67% of organizations affected), local government (65%) and retail (61%). According to the data, the manufacturing industry was the least impacted, with just under half (46%) of respondents reporting a successful hit.

Size does not appear to be a factor when it comes to ransomware, with the results remaining consistent across all the company size ranges surveyed, from 50 to 2,000 employees.

71% of organizations that had experienced an email breach were also hit with ransomware — highlighting the link between the two types of attacks.

Ransomware victims have a different profile for security tools and priorities

Security sprawl and the risk of ransomware

The survey shows that excess security tools — known as security sprawl — accompanied by a lack of integration can increase risk and create gaps in protection by making it harder for organizations to detect and mitigate active threats, including ransomware.

The data shows that the proportion of organizations affected by security sprawl/lack of integration increases in line with their experience of ransomware.

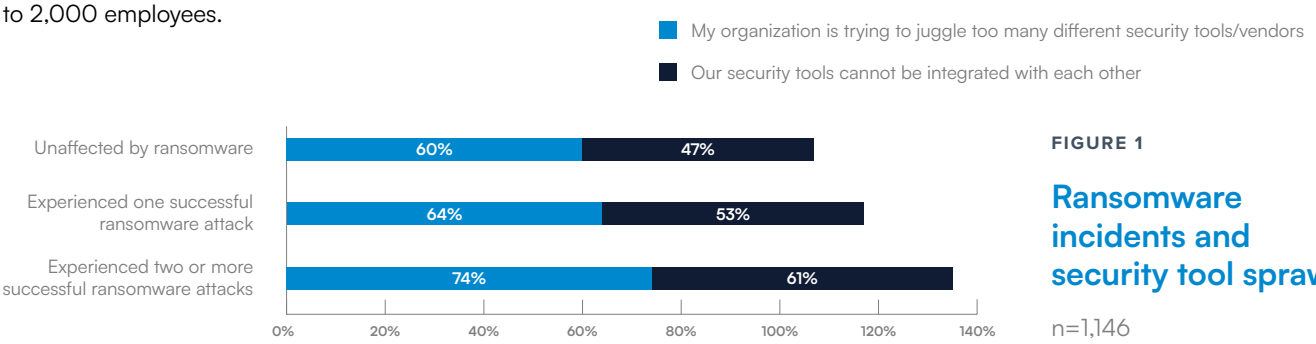


FIGURE 1

Ransomware incidents and security tool sprawl

n=1,146

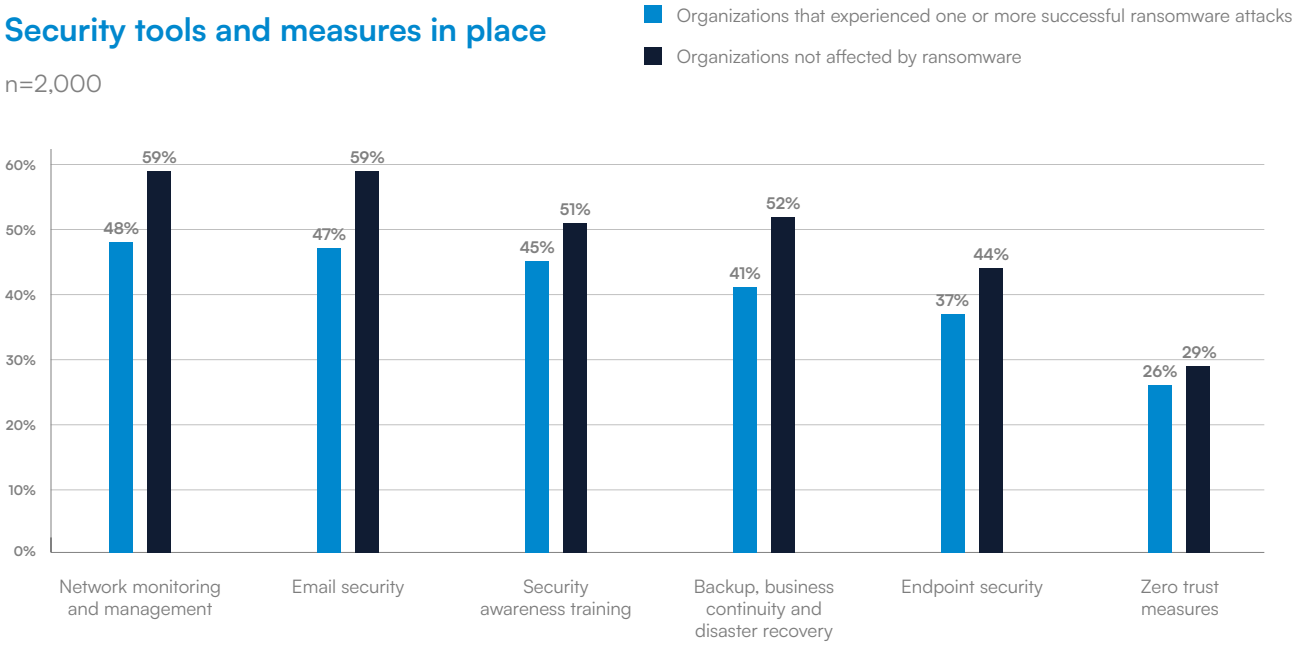
The different types of security tools and measures

According to respondents, the most widely deployed security measures are email security (implemented by 52%), network security (52%) and security awareness training (48%). Organizations that reported a successful ransomware incident are less likely to have implemented any of these.

FIGURE 2

Security tools and measures in place

n=2,000



For example:

- 47% of ransomware victims had implemented an email security solution — compared to 59% of non-victims
- 48% of ransomware victims had network management and monitoring in place — compared to 59% of non-victims
- 45% of ransomware victims had security awareness training in place — compared to 51% of non-victims
- 37% had implemented endpoint security — compared to 44% of non-victims

These findings suggest that ransomware victims may be under-investing in security areas that could help to reduce their risk exposure.

For example, email, network and endpoint security, together with security awareness training, provide a robust defense against email-borne phishing and social engineering attacks designed to steal credentials and allow attackers to breach networks, compromise devices and move laterally — all techniques that are characteristic of a ransomware attack.

Ransomware gangs have a one in three chance of getting paid

32% of ransomware victims paid a ransom to recover or restore data.

The results show a correlation between an organization's propensity to pay a ransom and the number of times they are affected by ransomware.

Organizations that only experienced one successful ransomware attack were slightly less likely to pay the ransom, with 29% doing so, while among those affected twice or more, 37% paid the ransom to get their data back.

These figures have changed little since the last survey two years ago. In 2023, the findings showed that 31% of those affected once, and 38% of those affected twice or more, paid a ransom to recover data.

One possible explanation for a link between multiple hits and ransomware payments is that once it is shown that an organization is willing to pay, other attackers will target the same victim, or the same attacker may return more than once.

The good news is that the majority (65%) of those affected by ransomware were able to restore their data using backups.

As a stark reminder that paying the ransom doesn't pay: 41% of those who paid (13% overall) didn't get all or even any of their data back.

Data encryption is now just one part of a ransomware attack

Aside from the financial burden of paying a ransom, the research shows that the commercial, operational and even emotional impact of a successful ransomware attack is considerable.

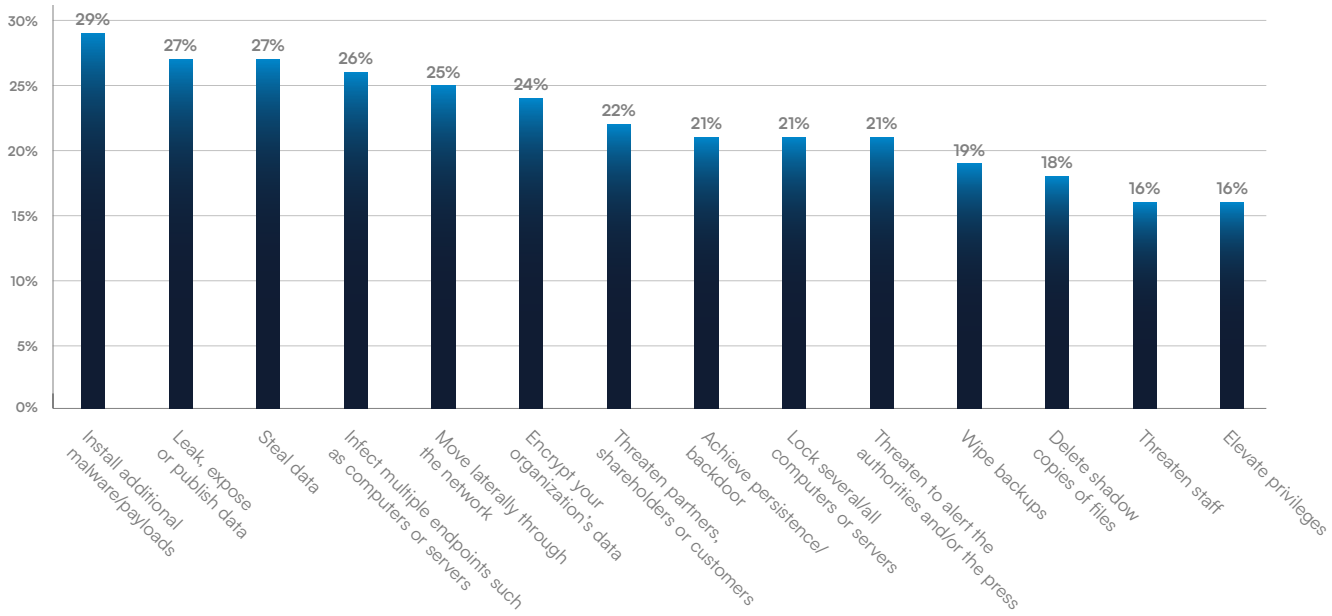
In most ransomware incidents, the data encryption and the locking of systems and computers is generally the endgame. This is the most visible part of the attack and therefore the most likely to reveal the presence of intruders to the security team and result in the containment and removal of the threat.

The research findings underscore the breadth of activity that takes place under the radar before the ransomware is executed, either to enable the attack or to potentially pave the way for other activity.

FIGURE 3

Activities undertaken by ransomware gangs during most significant incident

n=1,146



Around a quarter of the ransomware incidents experienced by respondents involved the encryption of data (24%), locking endpoints (21%) and data theft (27%).

Attacks also feature lateral movement across the network (25%), the infection of multiple endpoints such as computers or servers (26%), the installation of additional malicious payloads (29%), privilege elevation (16%), and embedding backdoors and other persistence mechanisms (21%).

Further, to make it harder for victims to restore their data without paying, around one in five attackers accessed and wiped backups and deleted shadow copies of files (both experienced by 19% of victims).

The findings also show that once the ransomware has been executed and the payment demand submitted, the attackers start to exert pressure on the victim through psychological tactics. These include threatening partners, shareholders or customers (experienced by 22%), threatening to alert the press or the authorities (21%) and even threatening staff (16%).

In 27% of successful ransomware incidents, the attackers went on to leak, expose or publish the stolen data.

Ransomware victims lose customers and new business opportunities

Once the dust has settled on the actual attack, victims are left facing operational and commercial repercussions.

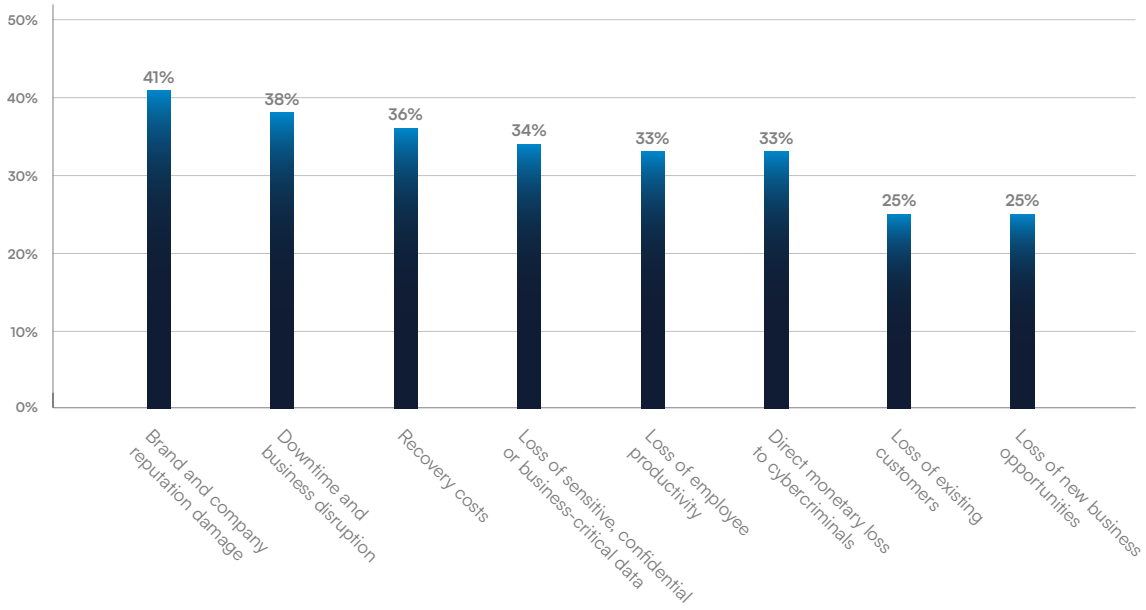
The top impact cited by ransomware victims was damage to their brand and reputation (affecting 41%). This is followed by downtime (38%) and recovery costs (36%). A third (34%) admitted losing sensitive data.

One in four ransomware victims faced the longer-term business impact of losing existing customers and new business opportunities (both 25%).

FIGURE 4

The impact of the most significant ransomware attack in the last 12 months

n=1,146



Conclusion

To be ransomware-resilient, organizations need integrated and multilayered security that protects their ever-expanding attack surface from cyberthreats.

The following practical steps can help:

- **Ensure data is backed up regularly and securely** and kept offline. Run tests to ensure you can effectively restore data.
- **Implement multifactor authentication and enforce the principle of least privilege** to limit access to corporate assets and applications. This prevents attackers from targeting high-value data and systems even with stolen credentials.
- **Keep software updated** with the latest security patches to close security gaps.
- **Provide regular cybersecurity awareness training** for employees, focusing on the latest phishing and ransomware tactics.
- **Segment the network**, isolating critical systems to prevent lateral movement by attackers.
- **Check all configurations**, including in the cloud. Misconfigurations are a key contributor to security breaches.
- **Install a robust email security solution.** Email remains a primary entry point for ransomware, and advanced, AI-powered protection can detect malicious payloads and recognize advanced social engineering tactics designed to bypass security.
- **Secure web applications** such as file-sharing services, web forms and e-commerce sites. Applications are often targeted through the user interface or an API interface.
- **Have — and regularly rehearse — an incident response plan.**
- **Consider collaborating with external experts,** including managed service providers and security vendors, for additional support. These partners can support you in implementing advanced integrated security platforms and solutions to detect, block and respond to active threats 24/7, containing and neutralizing incidents before they can cause serious damage.

About Barracuda

Barracuda is a leading global cybersecurity company providing complete protection against complex threats for all sized businesses. Our AI-powered platform secures email, data, applications, and networks with innovative solutions, managed XDR and a centralized dashboard to maximize protection and strengthen cyber resilience. Trusted by hundreds of thousands of IT professionals and managed service providers worldwide, Barracuda delivers powerful defenses that are easy to buy, deploy and use.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research in the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision-makers across technical and business functions in all business sectors and all major markets. For more information, visit vansonbourne.com.