illumio

The Global Cost of Ransomware Study

January 2025

Contents

PART 1

Introduction

Despite advances in cybersecurity technologies, including artificial intelligence (AI), organizations continue to find it difficult to detect and prevent ransomware attacks. 88% of organizations in this research experienced one or more ransomware attacks in the past three months to more than 12 months. According to the research, based on the hours and practitioners involved, organizations spent an average of $146,685 to contain and remediate the largest ransomware attack experienced. In 2021, the average cost was slightly higher at $168,910.

The purpose of this research is to learn the extent of the ransomware threats facing organizations and the steps being taken to mitigate the risks and their consequences. Ponemon Institute surveyed 2,547 IT and cybersecurity practitioners in the U.S. (578), U.K. (424), Germany (516), France (471), Australia (256), and Japan (302) who are responsible for addressing ransomware attacks.

In addition to the 2024 findings, the report also presents research from a ransomware study Ponemon Institute conducted in 2021 and published in 2022.[1] A comparison of the studies reveals changes in ransomware risks and the practices used to reduce the threats in the past three years. Since 2021, while the perception that their organization is a target of ransomware has declined from 68% to 54% of respondents, the consequences of a ransomware attack such as downtime, loss of significant revenue, and brand damage has increased.

Since 2021, organizations have become more vulnerable to the risks of ransomware because of AI-generated attacks and unrestricted lateral movement in cybersecurity.

AI-generated attacks refer to cyber threats that leverage AI to deceive and compromise individuals, organizations, and systems. These attacks are becoming increasingly sophisticated, imitating the language and style of legitimate emails to trick users into letting the ransomware in. Other attacks use AI to improve the ransomware's performance or automate some aspects of the attack path. 51% of respondents say their organizations are highly or extremely concerned that their organizations may experience such an attack.

Lateral movement refers to methods cyber criminals use to explore a compromised network to find vulnerabilities, escalate access privileges and reach their ultimate target. It is called lateral movement because of the way the attacker moves sideways from device to device, a hallmark of most successful ransomware attacks.

Research highlights

- An average of 25% of critical systems were affected by ransomware attacks experienced in the past 12 months. These systems were down an average of 12 hours.
- The average amount of currency demanded equated to $1.2 million (USD).
- 51% of respondents paid the ransom. However, only 13% of these respondents say all the impacted data was recovered.
- It took an average of 132 hours and 17.5 staff and third parties to contain and remediate an organization's **largest** ransomware incident. In 2021, it took an average of 190 hours and 14 staff and third parties.

[1] The Cost & Consequences of Ransomware for Small to Large-sized Enterprises. Conducted by Ponemon Institute and sponsored by CBI and Checkpoint, published in February 2022.

According to the findings, since 2021 unpatched systems have become increasingly vulnerable to being exploited by attackers moving laterally. 52% of respondents in this year's research say unpatched systems are targeted for lateral movement, an increase from 33% of respondents in 2021. Targeting cached credentials increased from 42% of respondents in 2021 to 48% of respondents in 2024.

The following findings highlight organizations' efforts to mitigate ransomware attacks.

Organizations are slow to adopt AI to combat ransomware. Although AI is considered helpful for reducing ransomware attacks by increasing overall SecOps efficiency and detecting ransomware activity within the environment, only 42% of respondents say their organizations have specifically adopted AI to help combat ransomware.

Since 2021 more organizations believe their security controls will protect them from ransomware attacks. Confidence in mitigating a variety of ransomware risks has increased significantly, especially with respect to their current security controls (32% of respondents in 2021 versus 54% of respondents in 2024). Multi-factor authentication and automated patching/updates are the top two technologies used to combat ransomware, 37% and 36% of respondents, respectively. Only 27% of respondents say their organizations use segmentation/microsegmentation.

Since 2021, more organizations are assigning responsibility for stopping ransomware attacks to one organizational function. 92% of respondents say one person or function is most responsible for addressing the threat of ransomware. The most responsible are the CISO (21% of respondents) or the CIO/CTO (21% of respondents). In 2021, 82% of respondents said one person or function was most responsible.

To prevent ransomware attacks, organizations should secure the cloud and endpoints. 49% of respondents say the cloud is most vulnerable in a ransomware attack followed by the endpoint, at 45% of respondents. Desktops/laptops continue to be the devices most often compromised by criminals.

Phishing continues to be the most common way ransomware is delivered. Phishing and Remote Desktop Protocol (RDP) compromises continue to be the primary methods used to unleash ransomware. Ransomware is typically spread through emails that contain links to malicious web pages or attachments. Infection can also occur when a user visits an infected website and malware is downloaded without the user's knowledge. RDP is one of the main protocols used for remote desktop sessions.

Insider negligence can delay an effective response to ransomware and increase the negative consequences. To improve prevention and reduce the time it takes to respond, organizations should address negligent user behavior and the lack of security awareness. Training programs should focus on how users can make better decisions about the content they receive through email, what they view or click in social media, how they access the web, and other common practices. Because no cybersecurity control can prevent every attack, containment and response strategies were equally critical.

44% of respondents say their organizations are not prepared to quickly identity and contain the ransomware attack. This indicates the importance of having incident response plans, skilled respondents, and key controls to stop an attack from spreading.

Ransomware attacks can reduce revenues due to downtime, lost customers, and brand damage. Since 2021, organizations that had to shut down to recover from the attack increased from 45% to 58% in 2024. Respondents that report a loss of significant revenue increased from 22% of respondents to 40% of respondents.

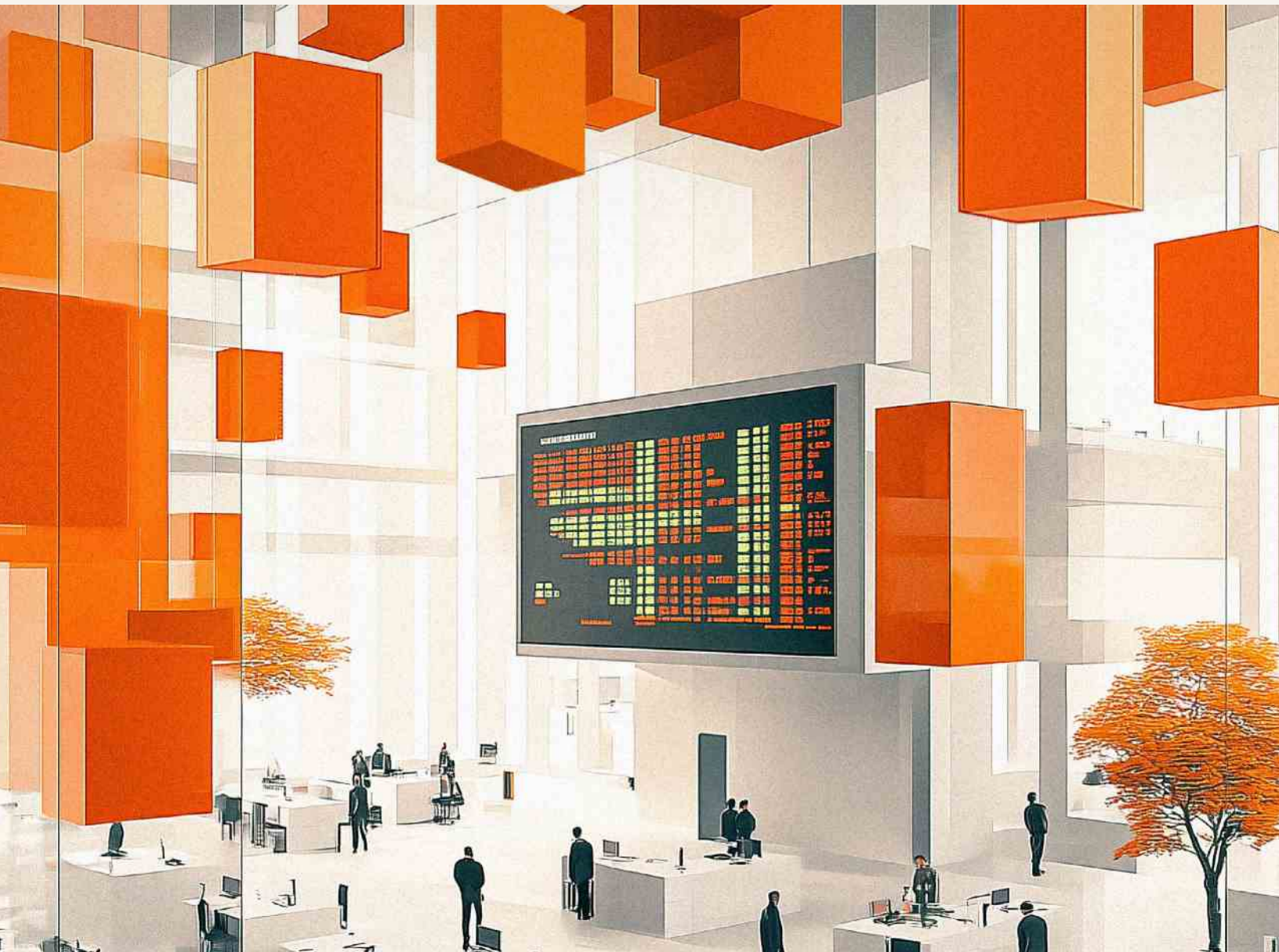
Since 2021, more organizations are reporting that brand damage was a consequence of the ransomware attack (an increase from 21% to 35% of respondents). The findings also reveal that recovering from damage to brand can cost organizations the most following a ransomware attack. In 2021, the highest cost was due to legal and regulatory actions.

PART 2

Key findings

In this section of the report, we provide an analysis of the research. Whenever possible, we present the findings from the 2021 study to show three-year trends in ransomware threats and risks. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics.

- The ransomware security gap
- Anatomy of a ransomware attack
- The response to ransomware demands
- Country differences



The ransomware security gap

Fewer organizations pay the ransom.

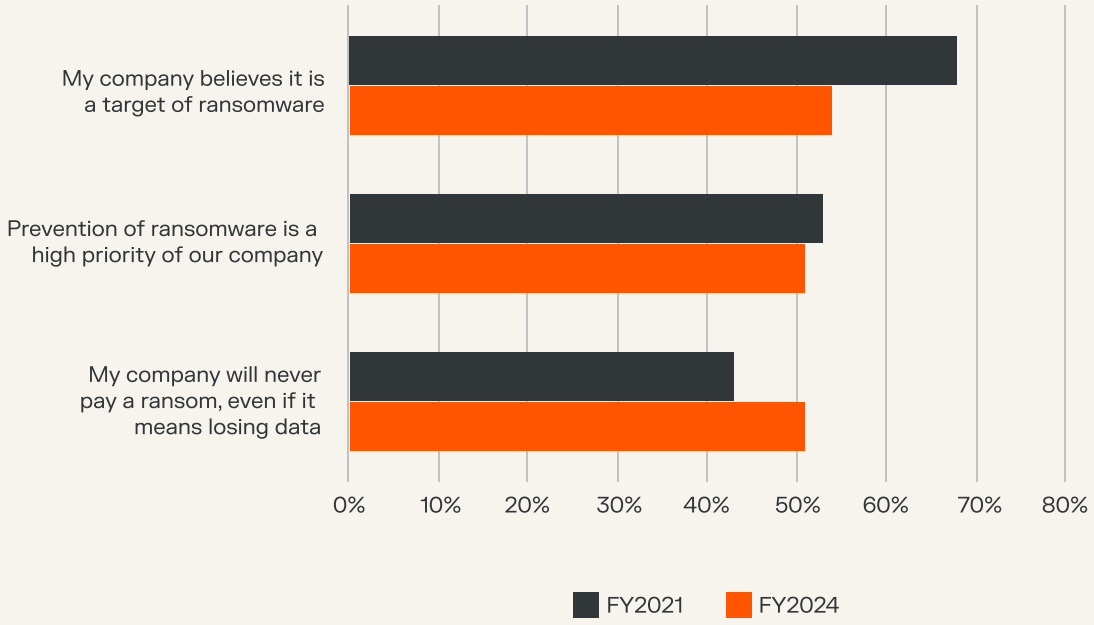
According to Figure 1, since 2021, more respondents say their organizations will never pay the ransom even if it means losing data, an increase from 43% of respondents to 51% of respondents. In an October 2, 2019 Public Service Announcement (PSA), the FBI urges victims not to pay the ransom. According to the PSA, the payment of the ransom does not guarantee that the exfiltrated data will be returned, as shown in this research. The FBI also warns that paying might embolden attackers to target other victims.

Other trends are the decline in the belief that their organizations are targeted (54% of respondents in 2024 versus 68% of respondents in 2021). A little more than half of respondents continue to say prevention of ransomware is a high priority.

51%

of respondents say their organizations will never pay ransom even if it means losing data

FIGURE 1. PERCEPTIONS ABOUT RANSOMWARE RISKS AND THREATS
Strongly agree and agree responses combined



Organizations worry about the possibility of an AI-generated ransomware attack.

Respondents were asked to rate their concerns about ransomware risks on a scale of 1 = no concern to 10 = extremely concerned.

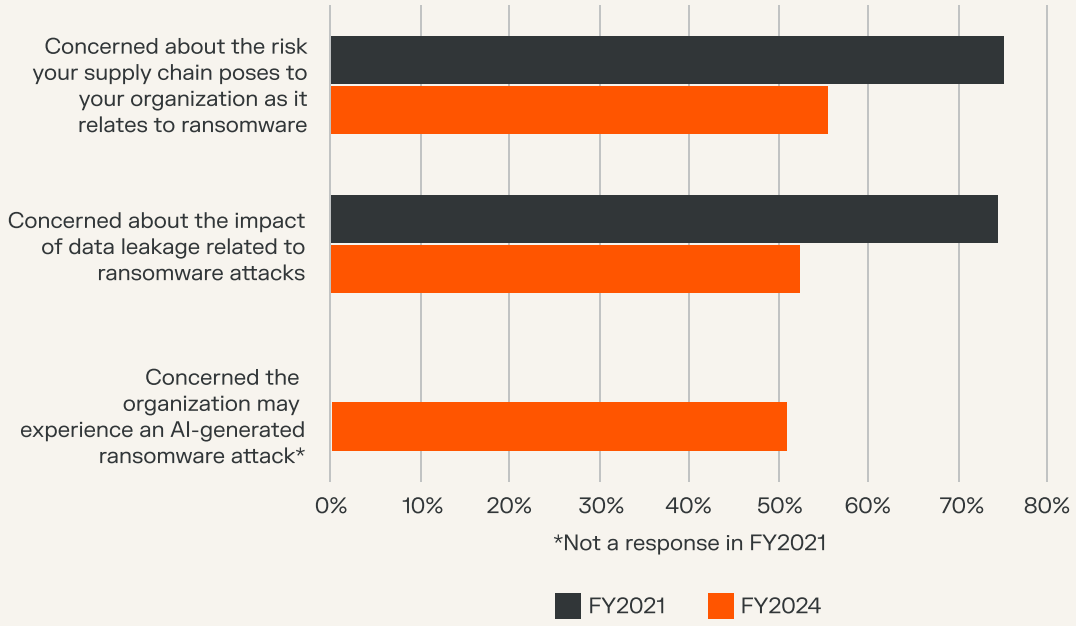
Figure 2 presents the high and extremely concerned responses (7+ on the 10-point scale). For the first time, respondents were asked if they are concerned about AI-generated attacks, and 51% say they are very or highly concerned.

As shown, fewer respondents are worried their organizations will be affected by ransomware attacks against the supply chain (75% in 2021 versus 56% in 2024) and data leakage (73% in 2021 versus 52% in 2024).

51%

of respondents are concerned their organization may experience an AI-generated attack

FIGURE 2. RANSOMWARE CONCERNS
On a scale from 1 = not concerned to 10 = extremely concerned, 7+ responses presented



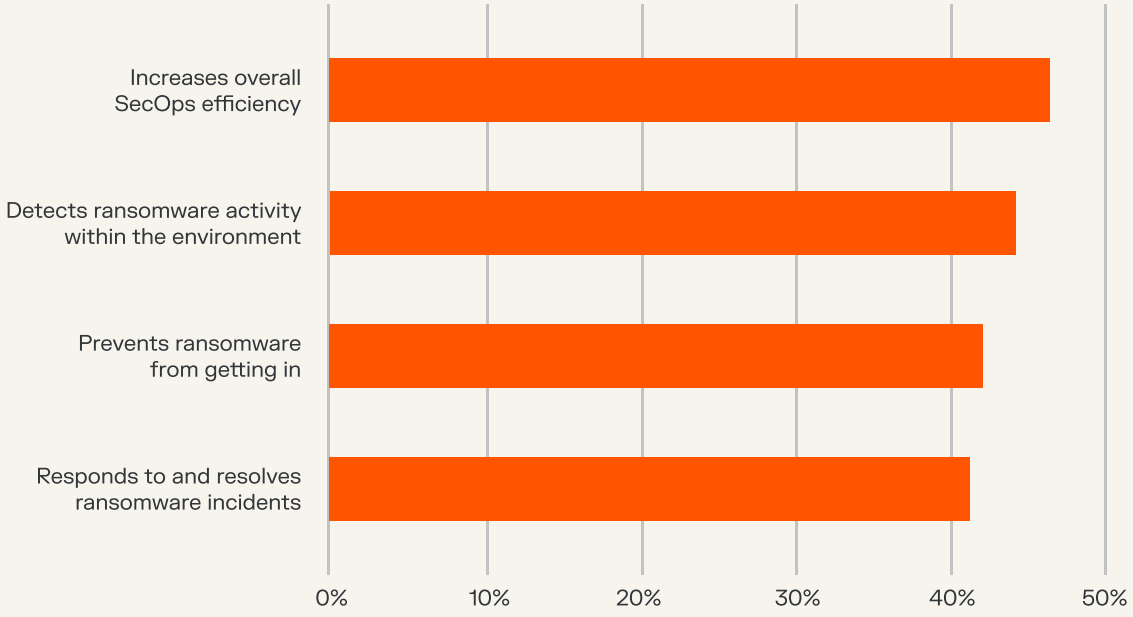
Organizations are slow to adopt AI to combat ransomware.

Only 42% of respondents say their organizations have adopted AI to help combat ransomware. Of those respondents who are using AI to reduce the risk, 46% say AI increases overall SecOps efficiency, and 44% say it detects ransomware activity within the environment.

42%

of respondents say their organizations have adopted AI to help combat ransomware

FIGURE 3. WHAT ARE THE BENEFITS OF AI IN REDUCING RANSOMWARE RISKS?
More than one response permitted



Since 2021, more organizations believe their security controls will protect them from ransomware attacks.

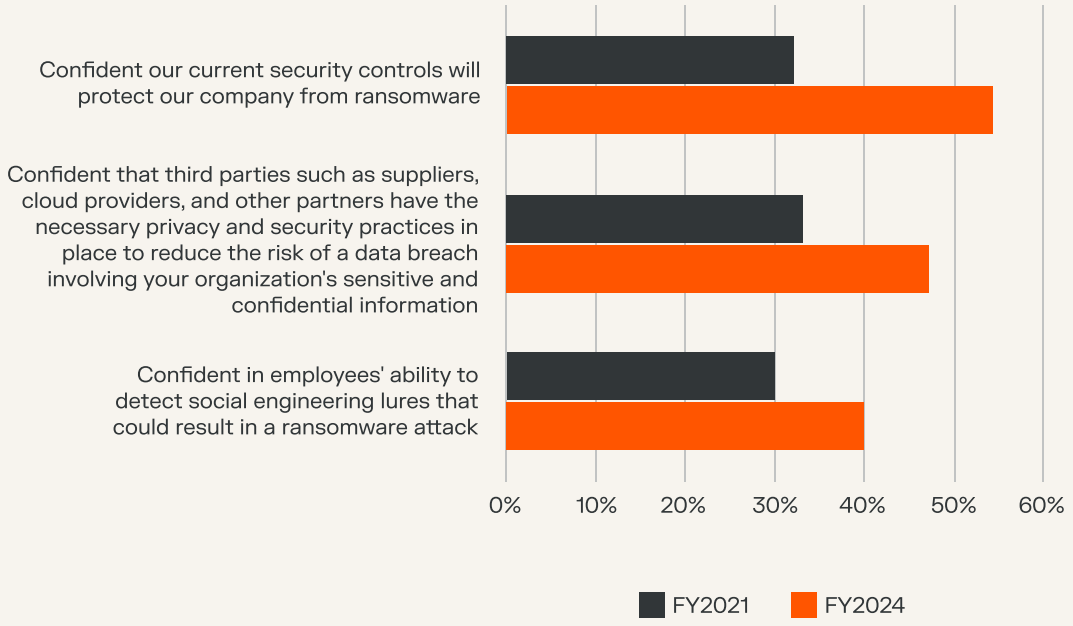
Respondents in both the 2021 and 2024 research were asked to rate their confidence in addressing ransomware attacks on a scale from 1 = not confident to 10 = highly confident.

Figure 4 presents the very and highly confident responses (7+ on the 10-point scale). As shown, confidence in mitigating a variety of ransomware risks has increased significantly, especially with respect to their current security controls (32% of respondents in 2021 versus 54% of respondents in 2024). Respondents are also more confident in third parties' privacy and security practices (33% versus 47%) and the ability of employees to detect social engineering lures (30% versus 40%).

54%

of respondents say they are confident current security controls will protect their company from ransomware

FIGURE 4. THE CONFIDENCE TO REDUCE RANSOMWARE RISKS INCREASES
On a scale from 1 = not confident to 10 = highly confident, 7+ responses presented



Multi-factor authentication and automated patching/updates are the top two technologies used to prevent ransomware attacks.

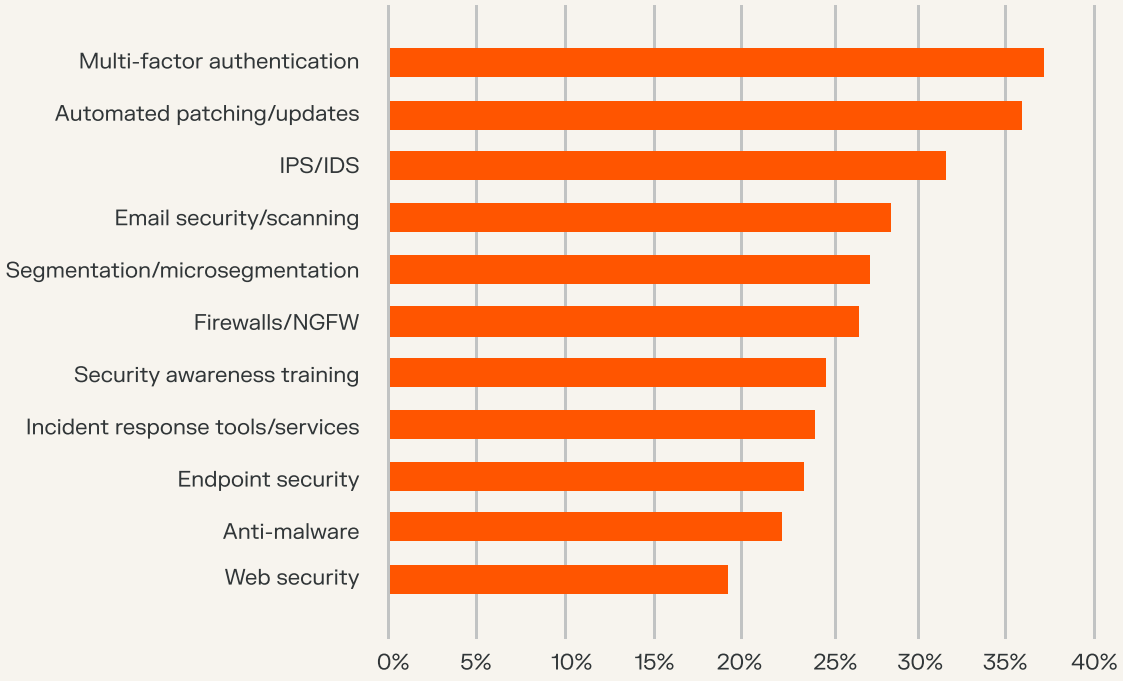
According to the findings, 54% of respondents have confidence in their security controls.

Figure 5 presents a list of cybersecurity controls that can be used to manage ransomware risks. MFA (37% of respondents) and automated patching/updates (36% of respondents) are most often used.

37%

of respondents say they use multi-factor authentication

FIGURE 5. THE CYBERSECURITY CONTROLS USED TO COMBAT RANSOMWARE
More than one response permitted



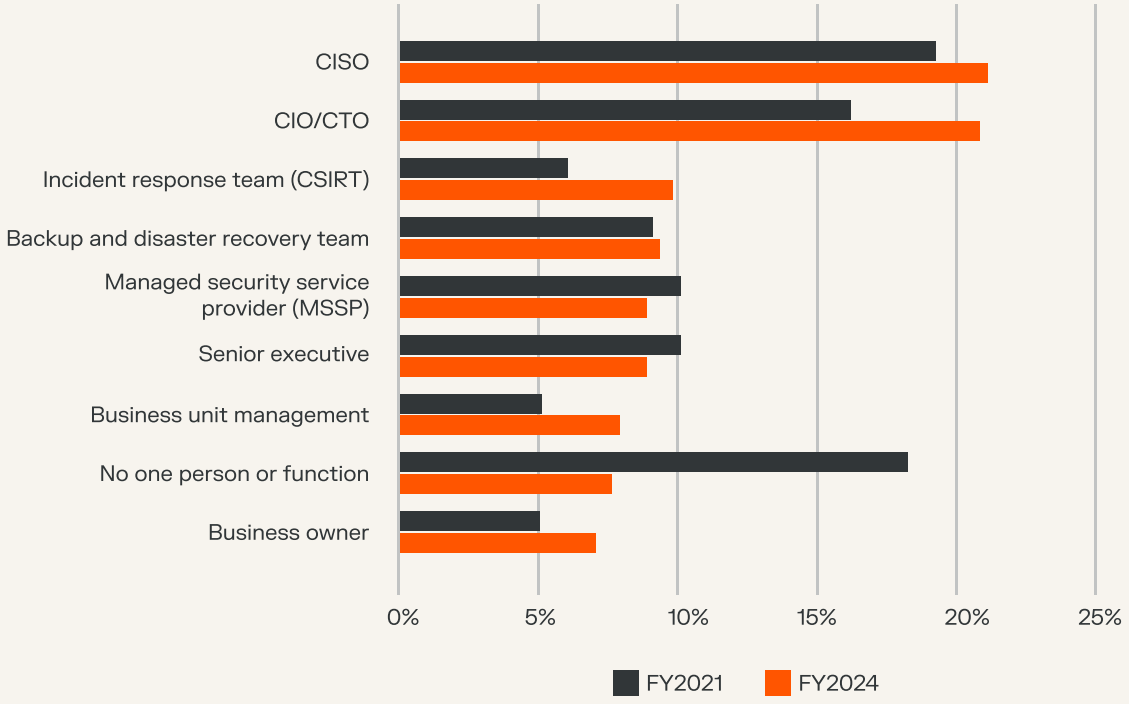
More organizations are assigning one function as responsible for addressing the threat of ransomware.

According to Figure 6, respondents who say no one person or function is mostly responsible for ransomware threats has declined from 18% to 8%. Organizations that assigned the CIO/CTO as most responsible increased from 16% to 21% of respondents. This is a positive indicator and shows the importance of centralizing accountability to prevent ransomware attacks.

21%

of respondents say that the CISO and CIO/CTO are most responsibe for addressing ransomware threats

FIGURE 6. WHO IN YOUR ORGANIZATION IS MOST RESPONSIBLE FOR ADDRESSING THE THREAT OF RANSOMWARE?
Only one choice permitted



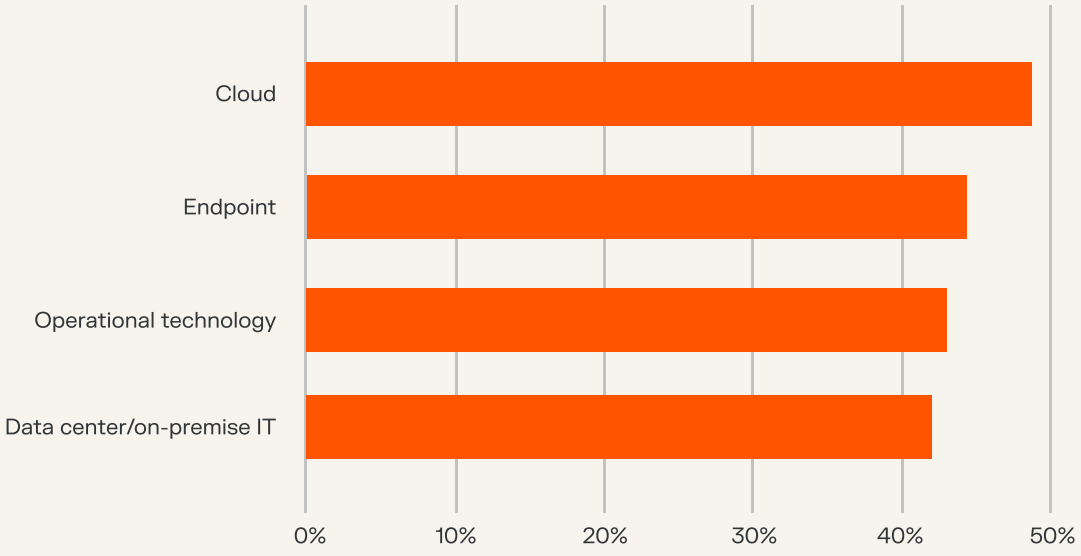
To prevent ransomware attacks, organizations should secure the cloud and endpoints.

According to Figure 7, the cloud is considered the most vulnerable according to 49% of respondents followed by endpoints (45% of respondents).

21%

of respondents say that the cloud is the most vulnerable in a ransomware attack

FIGURE 7. WHICH AREAS OF YOUR ORGANIZATION'S NETWORK ARE MOST VULNERABLE IN A RANSOMWARE ATTACK?
More than one response permitted



Breaking down the cost of a ransomware attack

The time and effort to contain and remediate a ransomware attack places a burden on staff and can keep them from completing other important IT security tasks. In 2024, the containment and remediation of an organization's largest ransomware attack took an average of 132 hours and 17.5 staff and third parties.

Based on the number of hours and staff and third parties required to deal with the attack, organizations spent an average of $146,685 on just one attack. In 2021, organizations spent an average of 190 hours and had 14 staff and third parties involved. The average cost was $168,910.

The cost of reputation and brand damage because of IT security failure replaces legal and regulatory actions as the highest cost of a ransomware attack. Respondents were asked to rate the most significant financial impact caused by their largest ransomware attack from 1 = most significant to 6 = least significant financial impact. In 2024, as shown in Table 1, the most significant financial impact is caused by reputation and brand damage because of IT security failure. According to the research, more organizations are experiencing damage to their reputation and brand in the aftermath of a ransomware attack.

In 2021, the most significant impact was caused by legal and regulatory actions. The least impactful expense in 2024 was the cost of users' idle time and lost productivity because of IT security failures. In 2021, the least cost was due to revenues or income lost because of IT security failures.

	2024 Ranking	2021 Ranking
Cost associated with legal and regulatory actions	2.21	1.65
Cost of users' idle time and lost productivity because of IT security failure	4.42	2.25
Cost resulting from the organization's response to information misuse or theft	2.92	2.36
Cost of technical support, including forensics and investigative operations	3.86	3.34
Cost associated with reputation and brand damage because of IT security failure	2.18	3.89
Revenues or income lost because of IT security failure	2.59	4.58

TABLE 1. SIX COST CATEGORIES FOR A RANSOMWARE ATTACK
Ranked 1 = most significant financial impact and 6 = least significant financial impact

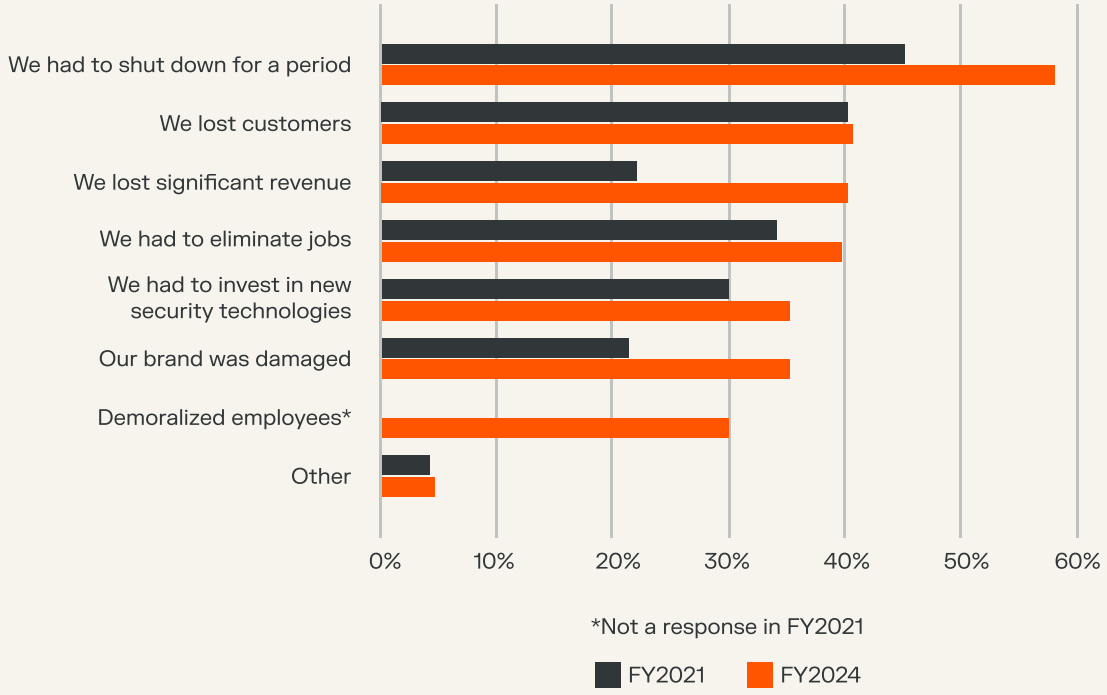
Ransomware attacks can decrease revenues.

Figure 8 presents trends in how ransomware attacks affected organizations. The most significant changes since 2021 are the increase in organizations having to shut down for a period from 45% of respondents to 58% of respondents, the loss of significant revenue, often an outcome of shutdowns, rose from 22% of respondents in 2021 to 40% of respondents this year. The damage to brand from 21% of respondents to 35% of respondents. 30% of respondents this year say employees were demoralized.

58%

of respondents say that they had to shut down for a period of time due to a ransomware attack

FIGURE 8. WHAT WERE THE CONSEQUENCES OF THE RANSOMWARE ATTACK?
More than one response permitted



Phishing continues to be the most common way ransomware is delivered.

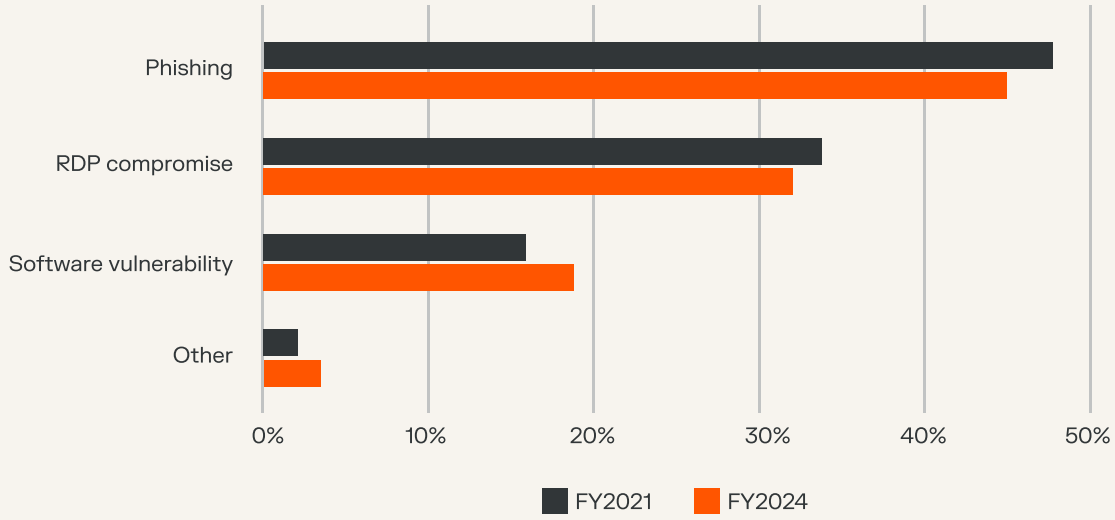
As shown in Figure 9, phishing and Remote Desktop Protocol (RDP) compromises continue to be the primary methods used to unleash ransomware.

Ransomware is typically spread through emails that contain links to malicious web pages or attachments. Infection can also occur when a user visits an infected website and malware is downloaded without the user's knowledge. RDP, typically used to provide remote access to organizations' systems, is both an initial attack vector and also the protocol most commonly used by attackers to move laterally between systems within a target environment.

58%

of respondents say that phishing was a primary method used to unleash ransomware

FIGURE 9. HOW WAS THE RANSOMWARE UNLEASHED?



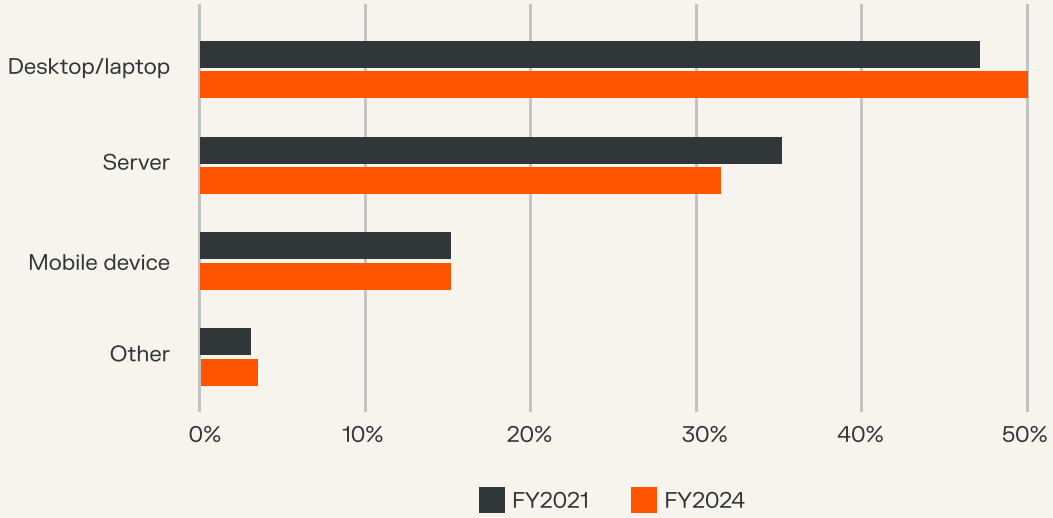
Desktop/laptops continue to be the most common devices compromised by criminals.

As shown in Figure 10, the devices most vulnerable to compromises are desktops/laptops (50% of respondents). As discussed above, RDP is often used by ransomware to spread from system to system.

50%

of respondents say that desktop/laptops were most vulnerable to compromises

FIGURE 10. WHAT TYPE OF DEVICES WERE COMPROMISED?



Cybercriminals are increasingly targeting systems with unpatched vulnerabilities to cause great damage to an organization's operations and critical business assets.

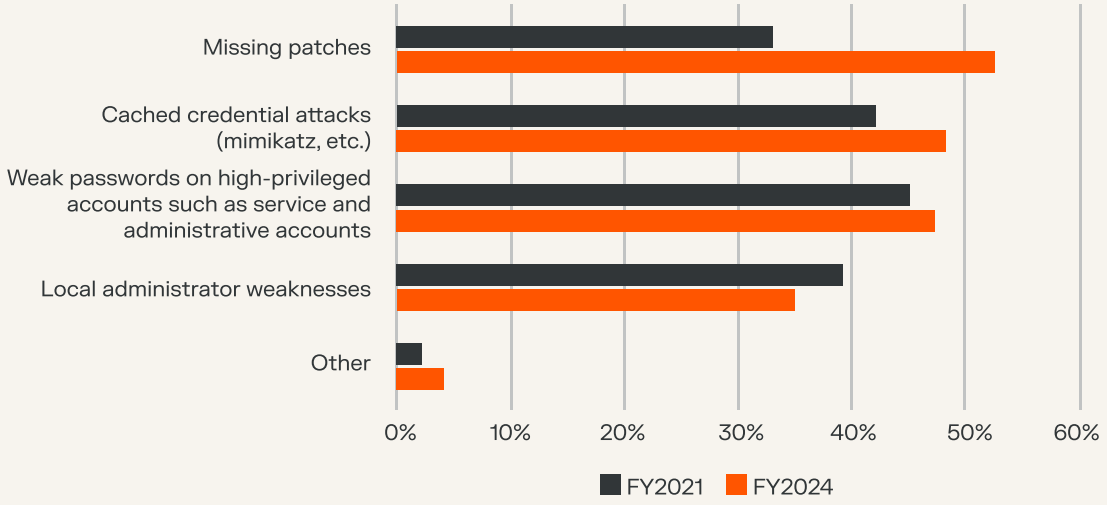
Lateral movement refers to methods cyber criminals use to explore an infected network to find vulnerabilities, escalate access privileges, and reach their ultimate target. It is called lateral movement because of the way the hacker moves sideways from device to device and so forth.

According to Figure 11, 52% of respondents in this year's research say systems with unpatched vulnerabilities are targeted followed by cached credential attacks (48% of respondents) and weak passwords on high-privilege accounts such as service and administrative accounts (47% of respondents).

52%

of respondents say that systems with unpatched vulnerabilities are targeted for lateral movement and privilege escalation

FIGURE 11. WHICH TECHNIQUES WERE USED FOR LATERAL MOVEMENT AND PRIVILEGE ESCALATION?
More than one response permitted



Insider negligence can delay an effective response to ransomware and increase the negative consequences.

Figure 12 lists why organizations face challenges when responding to a ransomware attack. Number one is insider negligence which makes it difficult to respond to ransomware attacks, according to 50% of respondents.

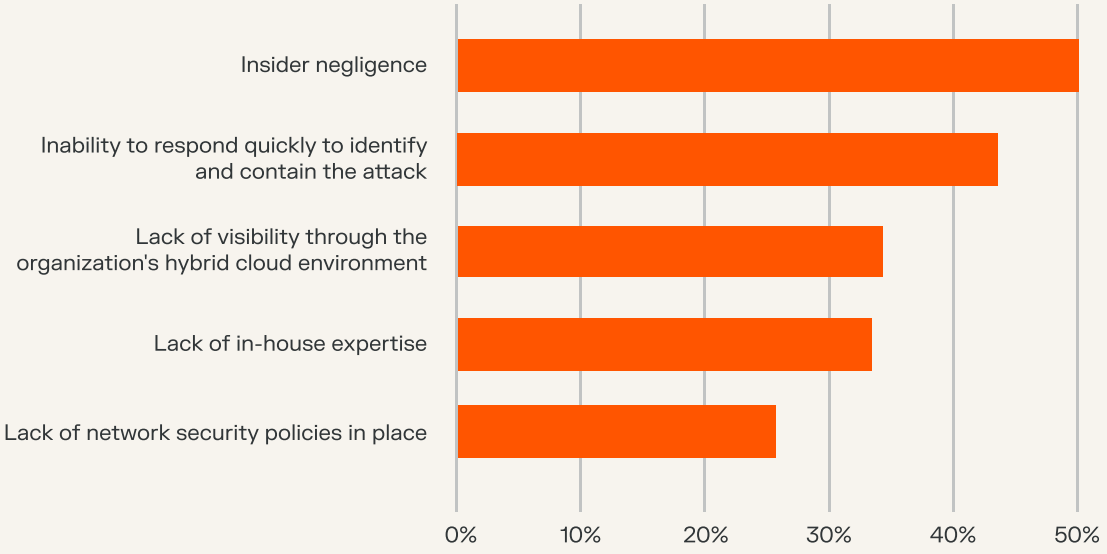
To improve prevention and reduce the time it takes to respond, organizations should address negligent user behavior and the lack of security awareness. Training programs should focus on how users can make better decisions about the content they receive through email, what they view or click in social media, how they access the web, and other common practices.

44% of respondents say their organizations are not prepared to quickly identity and contain the ransomware attack, which indicates the importance of having incident response teams, plans, and technologies to respond to and contain ransomware attacks.

50%

of respondents say that insider negligence made it more difficult to respond to ransomware attacks

FIGURE 12. WHICH FACTORS MADE IT MORE DIFFICULT TO RESPOND TO THE RANSOMWARE ATTACK?
More than one response permitted



The response to ransomware demands

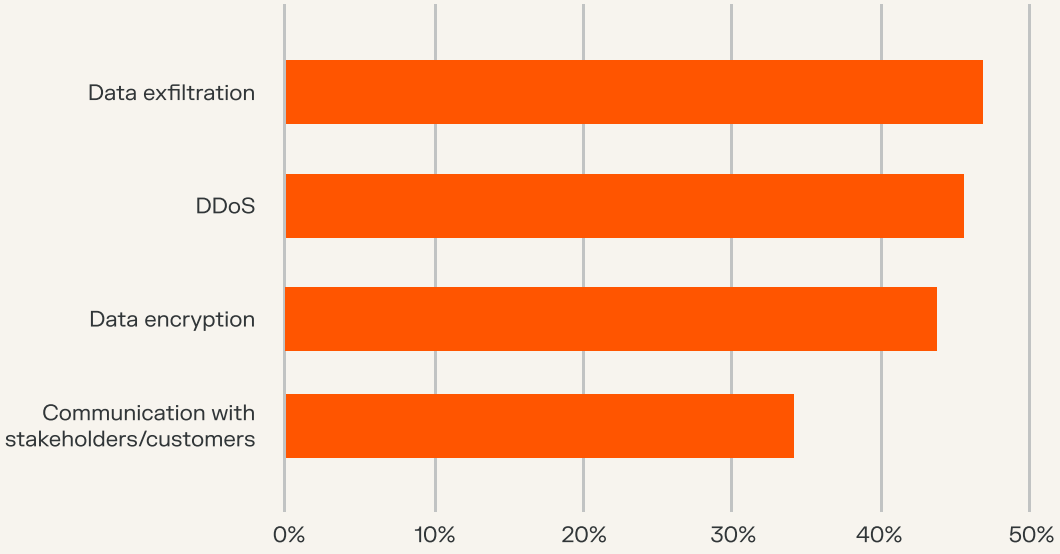
Criminals are most likely to threaten the theft of data when demanding a ransom.

As shown in Figure 13, 47% of respondents say data exfiltration and 45% of respondents say distributed denial of service (DDoS) are the primary tactics used to exert pressure.

47%

of respondents say that attackers used data exfiltration to exert pressure when demanding a ransom

FIGURE 13. WHICH EXTORTION TACTIC DID THE ATTACKERS USE TO EXERT PRESSURE?
More than one response permitted



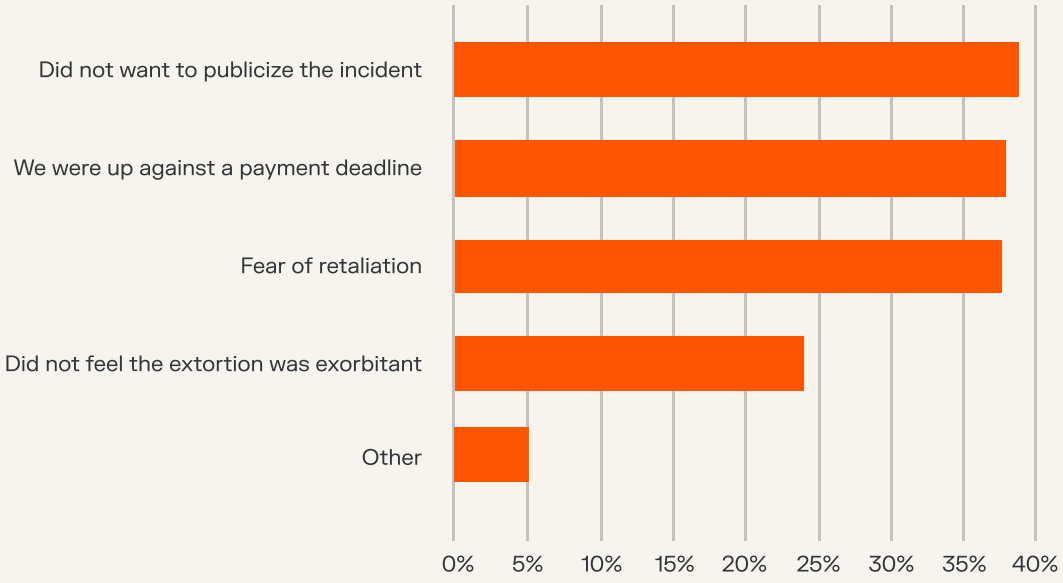
Only a small percentage of organizations represented in this research report the ransomware incident to law enforcement.

Only 28% of respondents say their organizations informed law enforcement about the incident. A primary concern is receiving unwanted publicity (39% of respondents). According to the research, the costliest consequence of ransomware is dealing with reputation and brand diminishment which may result from unwanted publicity. Respondents also cite the need to pay (38%) and fear of retaliation (38%).

28%

of respondents say their organizations informed law enforcement about the ransomware incident

FIGURE 14. WHY DID YOU *NOT* REPORT THE RANSOMWARE INCIDENT TO LAW ENFORCEMENT? (2024)
More than one response permitted



An effective backup strategy can motivate organizations to not pay the ransom.

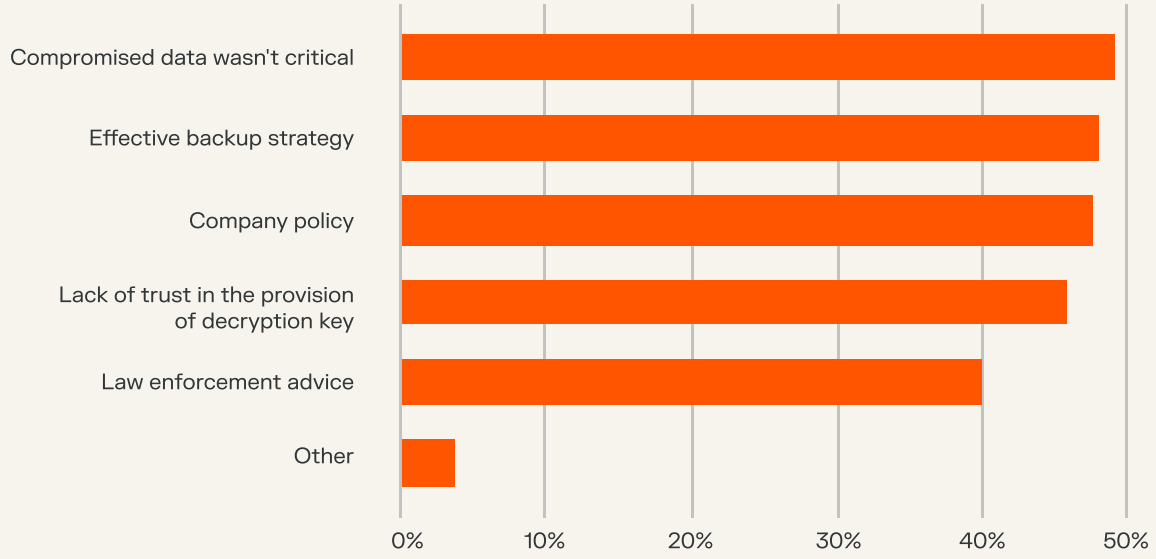
49% of respondents did not pay the ransom. According to the research, many organizations are not willing to pay the ransom even if it means losing data.

As shown in Figure 15, the top two reasons for not paying the ransom are compromised data wasn't critical (49% of respondents) and there was an effective backup strategy (48% of respondents).

49%

of respondents say their organization did not pay the ransom because the compromised data wasn't critical

FIGURE 15. IF YOUR ORGANIZATION DID NOT PAY THE RANSOM, WHY NOT?
More than one response permitted



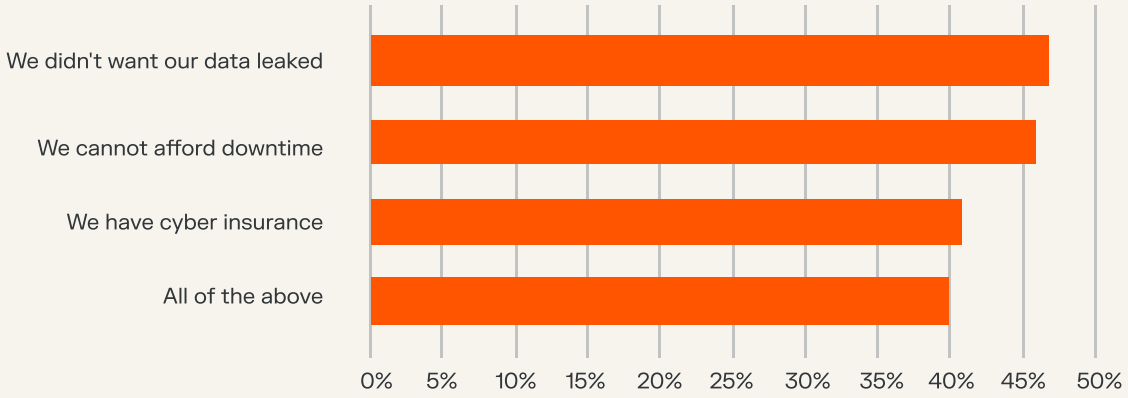
Concerns about data exfiltration and downtime are the primary reasons organizations paid the ransom.

51% of respondents say their organizations paid the ransom. As shown in Figure 16, organizations did not want their data leaked and they could not afford the downtime.

47%

of respondents say their organization paid the ransom because they didn't want their data leaked and could not afford downtime

FIGURE 16. IF YOUR ORGANIZATION PAID THE RANSOM, WHY?
More than one response permitted



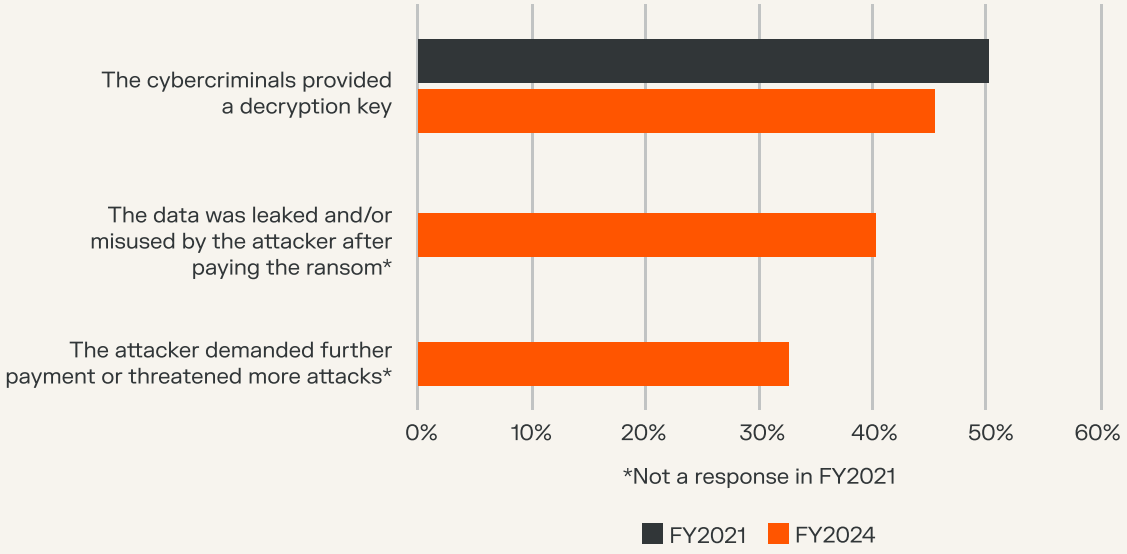
Paying the ransom does not prevent the negative consequences of such an attack.

According to the research, only 13% of respondents say that, following the payment of the ransom, all impacted data was recovered. As shown in Figure 17, 40% of respondents say that despite paying the ransom the data was still leaked or misused, and 32% of respondents say the attacker demanded further payment or threatened more attacks.

40%

of respondents say despite paying the ransom, the data was still leaked or misused

FIGURE 17. THE CONSEQUENCES OF PAYING THE RANSOM
Yes responses presented



PART 3

Country differences

In this section, interesting differences among the countries represented in this research are shown. Ponemon Institute surveyed 2,547 IT and cybersecurity practitioners in the U.S. (578), U.K. (424), Germany (516), France (471), Australia (256), and Japan (302) who are responsible for addressing ransomware attacks.

AI-generated attacks can be used by cybercriminals to launch ransomware attacks.

These cyber threats leverage AI and natural language processing to deceive and compromise individuals, organizations, and systems. Respondents were asked to rate their concern about a possible AI-generated attack on a scale from 1 = not concerned to 10 = extremely concerned. Figure 18 shows the very or extremely concerned responses.

Respondents in Germany and France are most concerned (56% and 55% of respondents, respectively). Respondents with less concern are in the U.K. and Australia (both 46% of respondents).

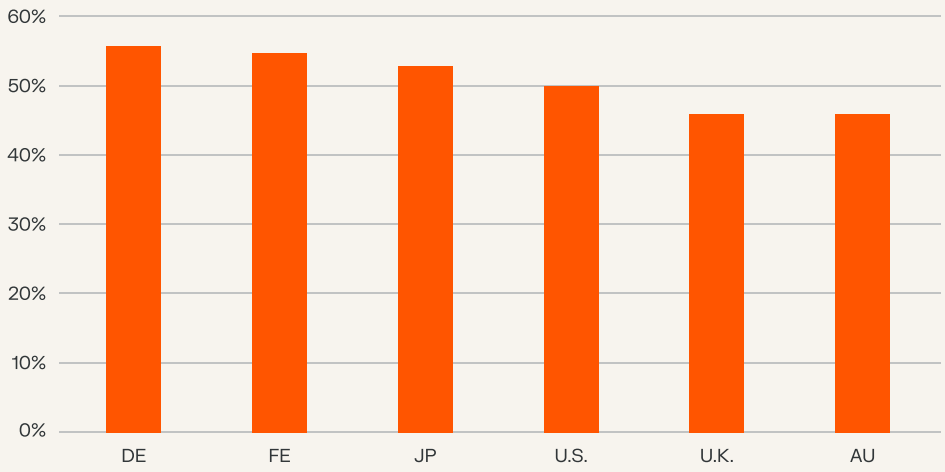


FIGURE 18. HOW CONCERNED IS YOUR ORGANIZATION THAT IT MAY EXPERIENCE AN AI-GENERATED RANSOMWARE ATTACK? 7+ responses
On a scale from 1 = not concerned to 10 = extremely concerned, 7+ responses presented

Adoption of AI as a technology to prevent ransomware varies among countries.

According to Figure 19, 52% of respondents in the U.S. and 47% of respondents in Japan say their organizations have adopted AI. In contrast, France and Australia are slow to adopt AI (36% and 35% of respondents, respectively).

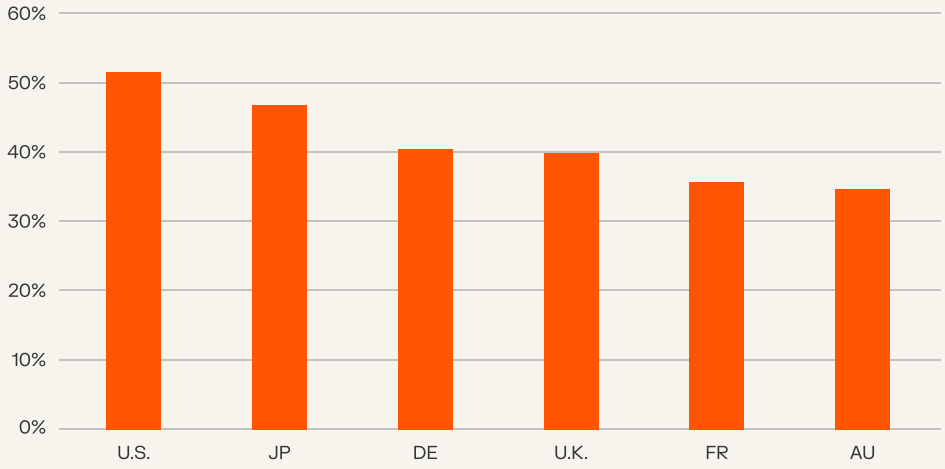


FIGURE 19. HAS YOUR ORGANIZATION ADOPTED AI TO HELP COMBAT RANSOMWARE?
Yes responses presented

With the exception of respondents in Germany and France, most countries are very concerned about data leakage due to a ransomware attack.

Respondents were asked to rate the concern about data leakage on a scale from 1 = not concerned to 10 = extremely concerned. Figure 20 presents the very and extremely concerned responses. The most concerned about data leakage following a ransomware attack are respondents in the U.S. (59%), Australia (54%), and the U.K. (53%).

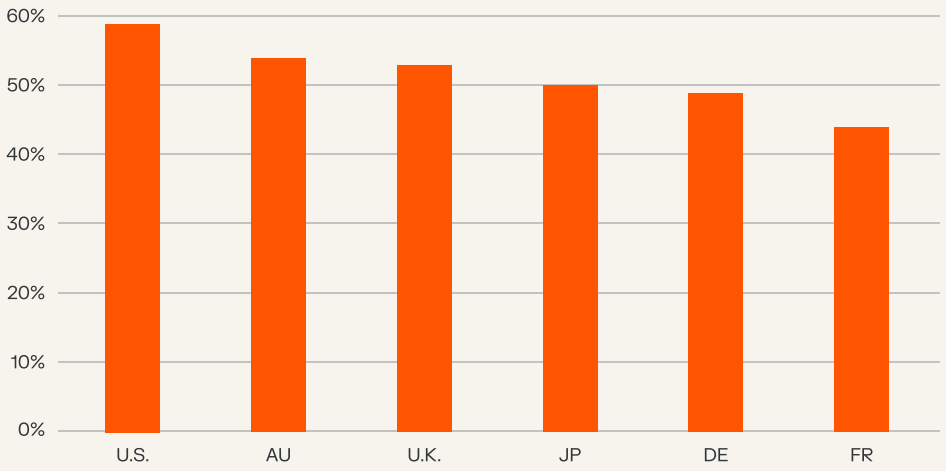


FIGURE 20. HOW CONCERNED IS YOUR ORGANIZATION ABOUT THE IMPACT OF DATA LEAKAGE RELATED TO RANSOMWARE ATTACKS? 7+ responses
On a scale from 1 = not concerned to 10 = extremely concerned, 7+ responses presented

Respondents in Germany and Japan (63% and 56%, respectively) say they have been very or highly effective in reducing the risk of a ransomware attacks.

Respondents were asked to rate their effectiveness in reducing ransomware risks on a scale from 1 = not effective to 10 = highly effective. Figure 21 presents the highly effective responses. Least effective, according to 49% and 48% of respondents, are Australia and the U.K.

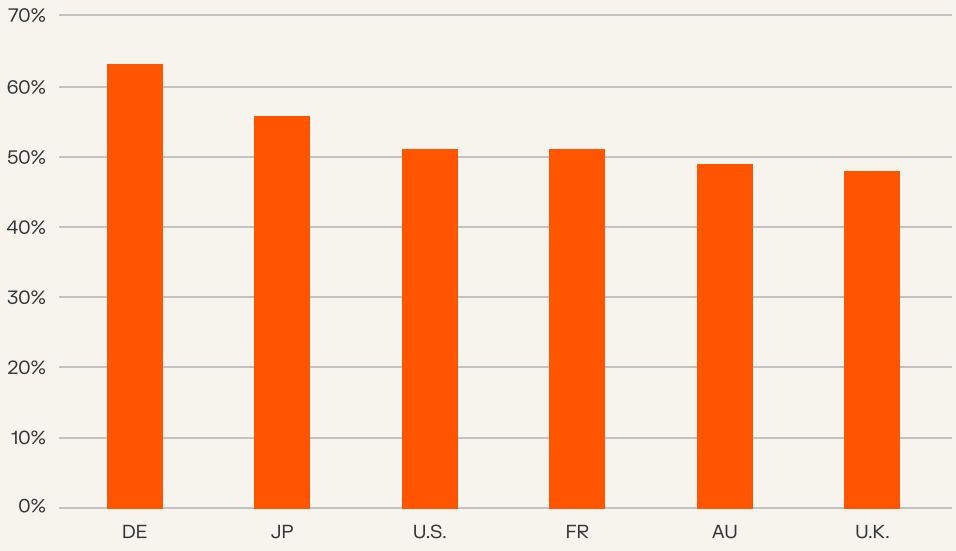


FIGURE 21. HOW EFFECTIVE WERE YOUR ORGANIZATION'S RANSOMWARE-PROTECTION MEASURES IN MITIGATING THE RISK OF A RANSOMWARE ATTACK? 7+ responses
On a scale from 1 = not effective to 10 = highly effective, 7+ responses presented

Countries differ significantly in the confidence that current security controls will stop ransomware.

As shown in Figure 22, the US and Germany (60% and 59% of respondents) are most confident in their controls. The U.K. (48% of respondents) and Japan (45% of respondents) are less confident.

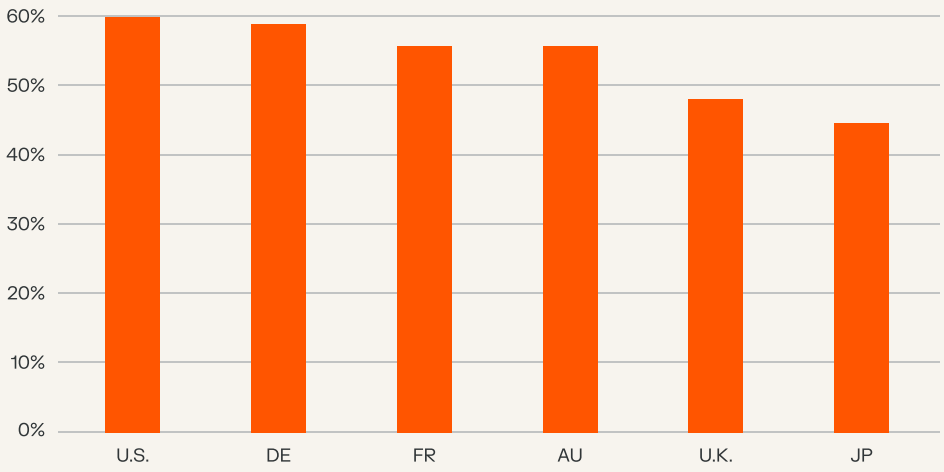


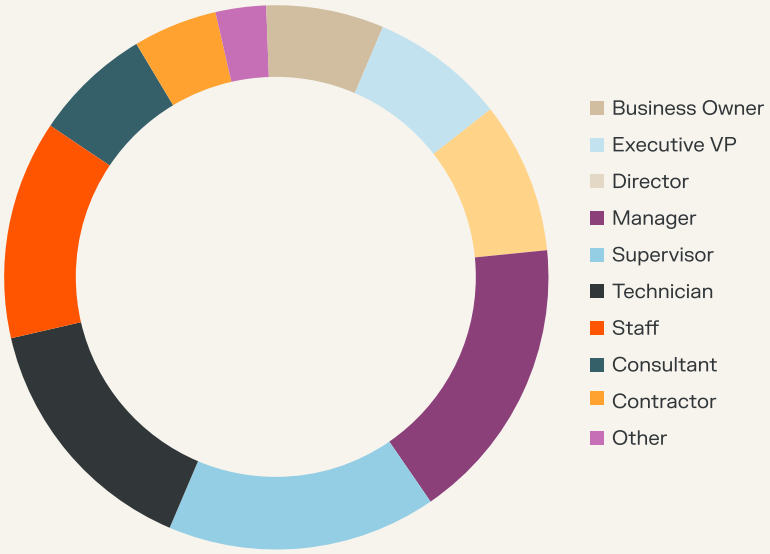
FIGURE 22. IS YOUR ORGANIZATION CONFIDENT THAT ITS CURRENT SECURITY CONTROLS WILL PROTECT IT FROM RANSOMWARE?
Strongly agree and agree responses combined

PART 4

Methodology

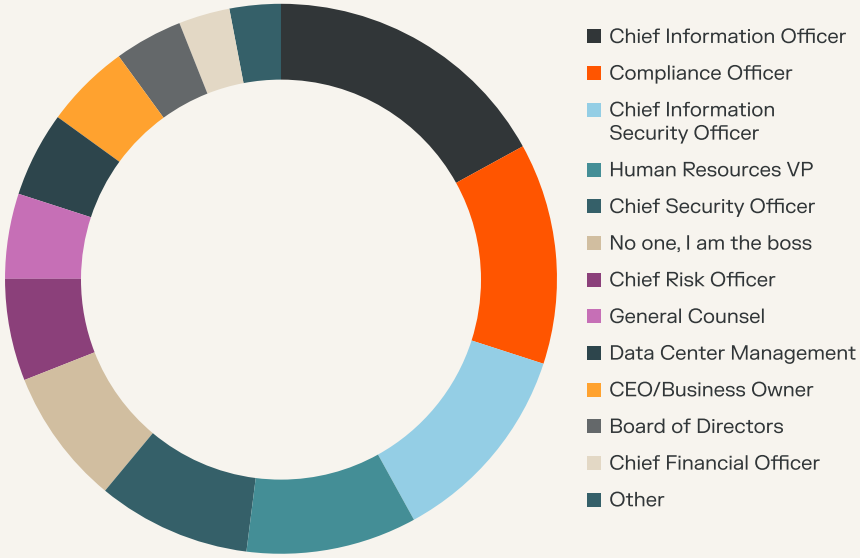
A sampling frame of 2,547 IT and cybersecurity practitioners in the U.S. (578), U.K. (424), Germany (516), France (471), Australia (256), and Japan (302) who are responsible for addressing ransomware attacks were selected as participants to this survey.

Pie chart 1 reports the respondent's organizational level within participating organizations. 57% of respondents are at or above the supervisory levels. The largest category at 17% of respondents is manager.



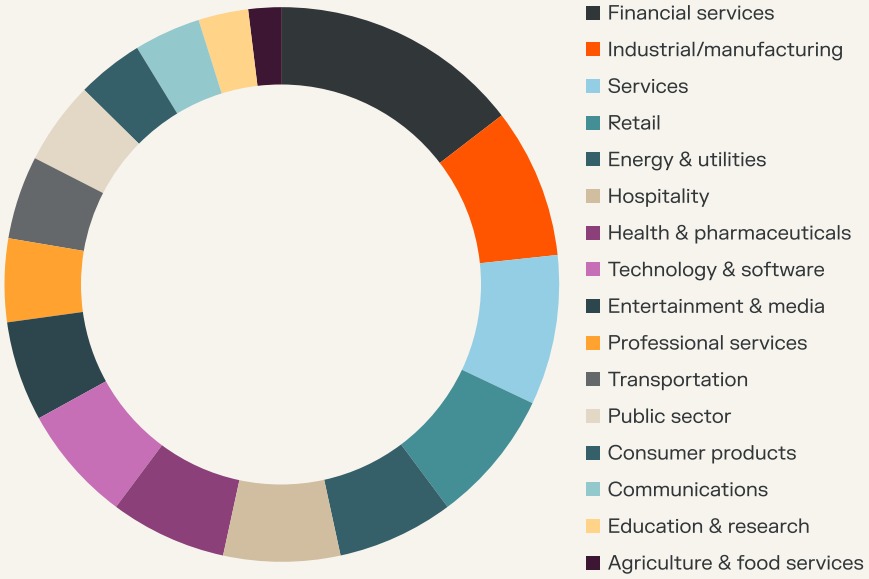
PIE CHART 1. CURRENT POSITION WITHIN THE ORGANIZATION

As shown in Pie chart 2, 17% of respondents report to the chief information officer, 13% of respondents report to the compliance officer, 12% of respondents report to the chief information security officer, and 10% of respondents report to the human resource VP.



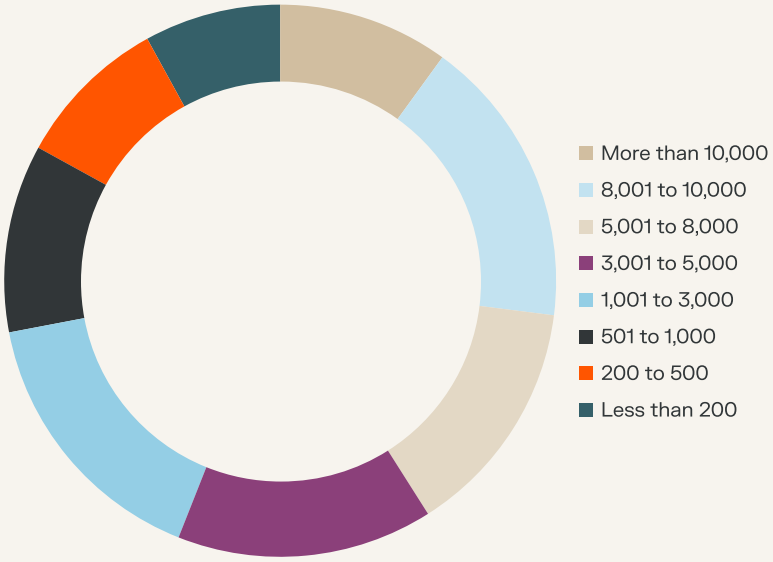
PIE CHART 2. DIRECT REPORTING CHANNEL

Pie chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (15% of respondents) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments, and credit cards. This is followed by industrial/manufacturing (9% of respondents), services (9% of respondents), retail (8% of respondents), and energy and utilities, hospitality, health and pharmaceuticals, technology, and software (each at 7% of respondents).



PIE CHART 3. PRIMARY INDUSTRY CLASSIFICATION

As shown in Pie chart 4, more than half (56%) of respondents are from organizations with a headcount of more than 3,000 employees



PIE CHART 4. WORLDWIDE HEADCOUNT

PART 5

Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT and cybersecurity practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

APPENDIX

Detailed survey results

The following tables provide the frequency or percentage frequency of responses to survey questions. All survey responses were captured in October 2024.

	Sample Size 2,547
S1. Does your role include responsibility for addressing ransomware attacks?	**Global**
Yes, full responsibility	27%
Yes, some responsibility	36%
Yes, minimum responsibility	37%
No responsibility (Stop)	0%
Total	100%

Q1a. My company believes it is a target of ransomware.	**Global**
Strongly agree	29%
Agree	25%
Unsure	20%
Disagree	15%
Strongly disagree	12%
Total	100%

Q1b. My company will never pay a ransom, even if it means losing data.	**Global**
Strongly agree	24%
Agree	27%
Unsure	20%
Disagree	16%
Strongly disagree	13%
Total	100%

Q1c. Prevention of ransomware is a high priority for our company.	Global
Strongly agree	26%
Agree	25%
Unsure	16%
Disagree	18%
Strongly disagree	14%
Total	100%

Q1d. We are confident our current security controls will protect our company from ransomware.	Global
Strongly agree	28%
Agree	26%
Unsure	19%
Disagree	16%
Strongly disagree	11%
Total	100%

Q2a. Does your organization rely on the expertise of an MSSP or other service provider to assist in mitigating the risk of a ransomware attack?	Global
Yes	28%
No (please skip to Q4)	72%
Total	100%

Q2b. Using the following 10-point scale, please rate how confident your organization is on a scale from 1 = not confident to 10 = highly confident that these MSSPs and service providers can assist in mitigating the risk of a ransomware attack?	Global
1 or 2	19%
3 or 4	23%
5 or 6	20%
7 or 8	20%
9 or 10	18%
Total	100%

Q3. Are these MSSPs and service providers held accountable for complying with regulations.	Global
Yes	34%
No	66%
Total	100%

Q4. Using the following 10-point scale, please rate how confident your organization is on a scale from 1 = not confident to 10 = highly confident in employees' ability to detect social engineering lures that could result in a ransomware attack?	Global
1 or 2	19%
3 or 4	22%
5 or 6	20%
7 or 8	24%
9 or 10	16%
Total	100%

Q5 What cybersecurity controls do you have in place to combat ransomware? Please select all that apply.	Global
Email security/scanning	28%
Firewalls/NGFW	26%
IPS/IDS	31%
Endpoint security	23%
Anti-malware	22%
Web security	19%
Security awareness training	25%
Segmentation/microsegmentation	27%
Incident response tools/services	24%
Multi-factor authentication	37%
Automated patching/updates	36%
Total	299%

Q6. Using the following 10-point scale, please rate how concerned your organization is that it may experience an AI-generated ransomware attack from 1 = not concerned to 10 = extremely concerned.	Global
1 or 2	16%
3 or 4	14%
5 or 6	19%
7 or 8	24%
9 or 10	27%
Total	100%

Q7a. Has your organization adopted AI to help combat ransomware?	Global
Yes	42%
No (please skip to Q8a)	58%
Total	100%

Q7b. What are the benefits of AI in reducing ransomware risks? Please select all that apply.	Global
Prevents ransomware from getting in	42%
Detects ransomware activity within the environment	44%
Responds to and resolves ransomware incidents	41%
Increases overall SecOps efficiency	46%
Total	174%

Q8a. Using the following 10-point scale, please rate the seriousness with which your organization treats ransomware from 1 = not serious to 10 = extremely serious.	Global
1 or 2	11%
3 or 4	15%
5 or 6	23%
7 or 8	25%
9 or 10	27%
Total	100%

Q8b. Using the following 10-point scale, please rate your organization's concern about the impact of data leakage related to ransomware attacks from 1 = no concern to 10 = highly concerned.	Global
1 or 2	11%
3 or 4	15%
5 or 6	23%
7 or 8	24%
9 or 10	28%
Total	100%

Q8c. Using the following 10-point scale, please rate your organization's concern about the risk your supply chain poses to your organization as it relates to ransomware from 1 = no concern to 10 = highly concerned.	Global
1 or 2	10%
3 or 4	13%
5 or 6	22%
7 or 8	27%
9 or 10	29%
Total	100%

Q8d. Using the following 10-point scale, please rate how confident your organization is on a scale from 1 = not confident to 10 = highly confident that third parties such as suppliers, cloud providers, and other partners have the necessary privacy and security practices in place to reduce the risk of a data breach involving your organization's sensitive and confidential information.	Global
1 or 2	10%
3 or 4	20%
5 or 6	23%
7 or 8	25%
9 or 10	22%
Total	100%

Q9. Using the following 10-point scale, please rate how vulnerable your organization is to ransomware attacks over the next 12 months from 1 = not vulnerable to 10 = highly vulnerable.	Global
1 or 2	10%
3 or 4	14%
5 or 6	19%
7 or 8	27%
9 or 10	31%
Total	100%

Q10. Who in your organization is most responsible for addressing the threat of ransomware?	Global
Business owner	7%
Senior executive	9%
CIO/CTO	21%
CISO	21%
Backup and disaster recovery team	9%
Incident response team (CSIRT)	10%
Business unit management	8%
Managed security service provider (MSSP)	9%
No one person or function	8%
Total	100%

Q11. Which areas of your organization's network are most vulnerable in a ransomware attack? Please select all that apply.	Global
Endpoint	45%
Data center/on-premise IT	43%
Cloud	49%
Operational technology (OT)	43%
Total	180%

Q12. Has your company experienced one or more ransomware attacks?	Global
Yes, within the past 3 months	27%
Yes, within the past 4 to 6 months	27%
Yes, within the past 7 to 12 months	21%
Yes, more than 12 months ago	13%
No (please skip to Q37)	12%
Total	100%

Q13. How many ransomware incidents do you think your company has experienced in the last 12 months?	Global
1 to 2	34%
3 to 5	30%
6 to 10	19%
Greater than 10	17%
Total	100%
Extrapolated average	5.4

Q14. In a typical month, how many attempted ransomware attacks do you suspect trigger an alert through one or more security controls but remain undetected? Your best guess is welcome.	Global
Less than 1	36%
1 to 5	32%
6 to 10	19%
Greater than 10	13%
Total	100%
Extrapolated average	4.3

Q15. Using the 10-point scale, how effective were your organization's ransomware-protection measures in mitigating the risk of a ransomware attack on a scale from 1 = not effective to 10 = highly effective?	Global
1 or 2	10%
3 or 4	16%
5 or 6	22%
7 or 8	27%
9 or 10	26%
Total	100%

Q16. Which extortion tactic did the attackers use to exert pressure?	Global
Data encryption	43%
Data exfiltration	47%
DDoS	45%
Communication with stakeholders/customers	34%
Total	168%

Q17. How was the ransomware unleashed?	Global
RDP compromise	32%
Phishing	45%
Software vulnerability	19%
Other (please specify)	4%
Total	100%

Q18. What type of device(s) was compromised by ransomware? Please select all that apply.	Global
Desktop/laptop	50%
Mobile device	15%
Server	31%
Other (please specify)	4%
Total	100%

Q19. Which factors made it more difficult to respond to the ransomware attack? Please select all that apply.	Global
Lack of visibility through the organization's hybrid cloud environment	35%
Lack of network security policies in place	26%
Inability to respond quickly to identify and contain the attack	44%
Insider negligence	50%
Lack of in-house expertise	33%
Total	188%

Q20. What percentage of critical systems were affected?	Global
Less than 5%	5%
5% to 10%	9%
11% to 15%	11%
16% to 20%	22%
21% to 25%	24%
26% to 50%	17%
More than 50%	11%
Total	100%
Extrapolated average	24.9%

Q21. What was the length of downtime for these critical systems?	Global
Less than 1 hour	11%
1 hour to 5 hours	21%
6 hours to 10 hours	26%
11 hours to 24 hours	23%
More than 24 hours	19%
Total	100%
Extrapolated average	11.94

Q22. Did the compromised device infect other devices in the network (e.g., lateral infection)?	Global
Yes	55%
No (please skip to Q24)	45%
Total	100%

Q23. Which techniques were used for lateral movement and privilege escalation? Please select all that apply.	Global
Local administrator weaknesses	35%
Cached credential attacks (mimikatz, etc.)	48%
Weak passwords on high-privileged accounts such as service and administrative accounts	47%
Missing patches	52%
Other (please specify)	4%
Total	187%

Q24. Was sensitive data exfiltrated during the attack?	Global
Yes	56%
No	41%
Not sure	3%
Total	100%

Q25. How much in Bitcoin or other currency was demanded?	Global
Less than $25,000	5%
$25,000 to $49,000	9%
$50,000 to $100,000	12%
$100,000 to $250,000	14%
$250,001 to $500,000	13%
$500,001 to $1,000,000	15%
$1,000,001 to $2,000,000	12%
$2,000,001 to $5,000,000	10%
More than $5,000,000	7%
Other (please specify)	3%
Total	100%
Extrapolated average	1,225,018

Q26. Did your company pay the ransom?	Global
Yes (Please skip to Q28)	51%
No	49%
Total	100%

Q27. If you did not pay a ransom, why not? Please select all that apply.	Global
Effective backup strategy	48%
Company policy	47%
Law enforcement advice	40%
Lack of trust in the provision of decryption key	46%
Compromised data wasn't critical	49%
Other (please specify)	4%
Total	234%

Q28. If you paid the ransom, why did you do so?	Global
We have cyber insurance	41%
We cannot afford downtime	47%
We didn't want our data leaked	47%
All of the above	40%
Total	175%

Q29. If you paid, did the cybercriminals provide a decryption key?	Global
Yes	45%
No	55%
Total	100%

Q31. Did the attacker demand further payment or threaten more attacks?	Global
Yes	32%
No	68%
Total	100%

Q32. Was the data leaked and/or misused by the attacker after paying the ransom?	Global
Yes	40%
No	60%
Total	100%

Q33a. Did you report the ransomware incident to law enforcement?	Global
Yes (please skip to Q34)	28%
No	72%
Total	100%

Q33b. If not, why?	Global
Did not feel the extortion was exorbitant	24%
Did not want to publicize the incident	39%
We were up against a payment deadline	38%
Fear of retaliation	38%
Other (please specify)	5%
Total	143%

Q34. Approximately how many hours were spent (per person) dealing with the containment and remediation of your organization's largest ransomware incident? Please include all personnel and third parties involved in the incident.	Global
5 to 10	8%
11 to 25	10%
26 to 50	17%
51 to 100	17%
101 to 200	20%
201 to 300	19%
More than 300	10%
Total	100%
Extrapolated average	132

Q35. How many people from your organization and/or a third party were involved in the detection, escalation, containment, and remediation of the attack?	Global
Less than 5	6%
5 to 10	19%
11 to 15	20%
16 to 20	23%
21 to 30	21%
More than 30	11%
Total	100%
Extrapolated average	17.5

Q36. What were the consequences of the ransomware attack? Please select all that apply.	Global
We had to shut down for a period	58%
We lost customers	41%
We had to eliminate jobs	40%
We lost significant revenue	40%
Our brand was damaged	35%
We had to invest in new security technologies	35%
Demoralized employees	30%
Other (please specify)	5%
Total	282%

Q37. Do you think having a full and accurate backup is a sufficient defense against ransomware?	Global
Yes, backups are sufficient if done right	52%
No, backups alone aren't enough	44%
Not sure	4%
Total	100%

Q38. Does your organization have a cyber insurance policy that covers ransomware attacks?	Global
Yes	52%
No (please skip to Q40)	48%
Total	100%

Q39. Has your organization's cyber insurance provider modified its ransomware protection over the past year resulting in decreased coverage?	Global
Yes	44%
No	56%
Total	100%

Q40. Approximately what range best defines your organization's expected 2024 IT security budget?	Global
< $1 million	3%
$1 to 5 million	4%
$6 to $10 million	7%
$11 to $50 million	9%
$51 to $100 million	10%
$101 to $250 million	12%
$251 to $500 million	18%
$501 to $750 million	12%
$751 million to $1 billion	14%
More than $1 billion	13%
Total	100%
Extrapolated average	439,920,833

Q41. Approximately what percentage of the IT security budget will be allocated to staff and technologies meant to prevent, detect, contain, and resolve ransomware attacks?	Global
< 1%	4%
1% to 2%	5%
3% to 5%	5%
6% to 10%	7%
11% to 15%	11%
16% to 20%	10%
21% to 30%	12%
31% to 40%	11%
41% to 50%	18%
More than 50%	19%
Total	100%
Extrapolated average	29.1%

Q42. Following are six cost categories caused by a ransomware attack. Please rank each category based on the financial impact to your organization. 1 = most significant financial impact and 6 = least significant financial impact.	Global
Cost of technical support, including forensics and investigative operations	3.86
Cost of users' idle time and lost productivity because of IT security failure	4.42
Cost resulting from the organization's response to information misuse or theft	2.92
Cost associated with legal and regulatory actions	2.21
Revenues or income lost because of IT security failure	2.59
Cost associated with reputation and brand damage because of IT security failure	2.18
Average	3.03

D1. What organizational level best describes your current position?	Global
Business owner	7%
Executive/VP	8%
Director	9%
Manager	17%
Supervisor	16%
Technician	15%
Staff	13%
Consultant	8%
Contractor	5%
Other	3%
Total	100%

D2. Who do you report to within the organization?	Global
Board of Directors	4%
CEO/Business Owner	5%
Chief Financial Officer	3%
General Counsel	5%
Chief Information Officer	17%
Chief Information Security Officer	12%
Compliance Officer	13%
Human Resources VP	10%
Chief Security Officer	9%
Data Center Management	5%
Chief Risk Officer	6%
No one, I am the boss	8%
Other	3%
Total	100%

D3. What industry best describes your organization's focus?	Global
Agriculture & food services	2%
Communications	4%
Consumer products	4%
Education & research	3%
Energy & utilities	7%
Entertainment & media	6%
Financial services	15%
Health & pharmaceuticals	7%
Hospitality	7%
Industrial/manufacturing	9%
Professional services	5%
Public sector	5%
Retail	8%
Services	9%
Technology & software	7%
Transportation	5%
Total	100%

D4. What is the worldwide headcount of your organization?	Global
Less than 200	8%
200 to 500	9%
501 to 1,000	11%
1,001 to 3,000	16%
3,001 to 5,000	15%
5,001 to 8,000	14%
8,001 to 10,000	17%
More than 10,000	10%
Total	100%