White Paper, sponsored by Kyndryl | December 2023

IDC RANSOMWARE STUDY:

Organizations Are Less Prepared than They Believe to Recover from Ransomware Attacks

Johnny Yu
Research Manager,
Storage and Computing, IDC

Frank Dickson
Program Vice President,
Cybersecurity Products, IDC

Phil Goodwin
Research Vice President,
Infrastructure Systems, Platforms
and Technologies Group, IDC

Table of Contents

CLICK ANY HEADING TO NAVIGATE DIRECTLY TO THAT PAGE.

IDC Opinion

Organizations are less prepared to recover from a ransomware attack than they realize.

IDC recently conducted a survey focusing on the current state of ransomware impact on business as well as the cyber-resilience efforts deployed by IT and security teams. The survey questions were therefore split into two general categories: one category about the outcomes of cyberattacks and another category about the tools, services, and practices respondents were using.

The survey found that cyberattacks — and ransomware attacks in particular — result in significant losses of data or money for most organizations. Around 70% of respondents indicated they were hit by a successful ransomware attack in the past year. However, 14% declined to answer, indicating this number could be higher.

Within the group of ransomware victims:

- **Two out of three** chose to pay the ransom.
- **Twenty-eight percent** said they were able to recover their encrypted data from backup using the tools they had.
- **Ninety percent** said data was exfiltrated.
- **Forty-six percent** indicated the attackers tried to delete their backups, and the attackers were successful in about half of these cases.

There is no indication that companies aren't making concerted efforts at cyber-resilience. The research found malware scanners and backup and recovery software are widely adopted, each with more than an 83% deployment rate among respondents. The survey found most organizations frequently test their disaster recovery (DR) capabilities, run adversary exercises, and perform cyber-risk assessments. Most are also cognizant of and actively adopting zero trust measures where they can.

It is therefore IDC's conclusion that organizations are struggling to recover from ransomware attacks not because of lack of technology but because of a lack of knowledge and standardization. The survey found organizations know to engage DR as a starting point for their cyber-recovery response but are unsure how to create a complete cyber-recovery plan from there. Most organizations don't formally develop separate plans for normal DR versus cyber-recovery, even though they have indicated they are aware the two scenarios require different data recovery methods. Hence, IDC concludes there is general recognition that cyber-recovery is DR with additional steps, yet there is little consensus on what exactly those extra steps are.

IDC believes market leaders can help organizations by formalizing the differences between DR and cyber-recovery and delivering tools and services that focus on the latter. The services component is especially important, as the research indicated companies have the tools they need, but not the expertise or talent to weave them together into a finely tuned system for cyber-resilience.

Less than a quarter of organizations (22%) said they have enough in-house expertise to handle cyber-recovery without engaging third parties such as retainers, as-a-service offerings, and other outside experts. However, the survey indicated organizations are often willing to use trusted third parties to fill in their knowledge gaps.

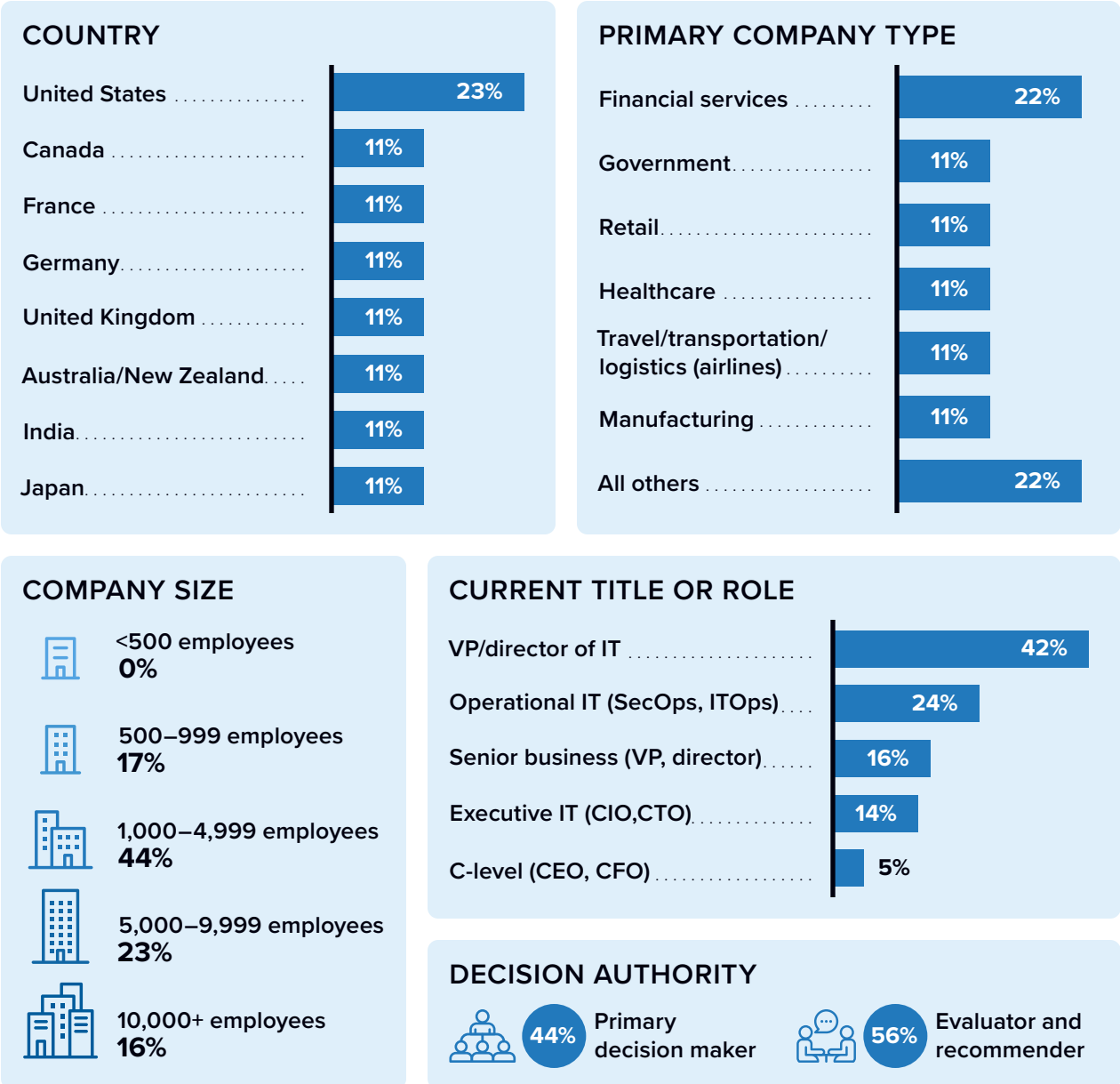
Therefore, organizations are looking for vendors, partners, or service providers that can bring expertise, guidance, and talent for cyber-recovery. This includes not only experts on retainer that can help during recovery scenarios or managed services focused on detection and response but also services that provide support and expertise before a major incident, such as risk assessment and attack.

Methodology

This study included a primary research survey with the following demographics as depicted in **Figure 1**.

FIGURE 1

Survey Sample Demographics



n = 928; Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

Situation Overview

The goal of IDC's study is to examine the level of preparedness as well as the technologies and services organizations use for cyber-resilience. Cyber-resilience, for the purposes and scope of this study, is defined as the ability for an organization to minimize the impact of outages caused by cyberattacks. Other outages such as those from power failure or natural disasters are not within the scope of this study.

Cyber-resilience requires the efforts of IT and security teams, and the research reflects practices used by both. Furthermore, a portion of the survey questions was divided into the five pillars of the NIST Cybersecurity Framework (identify, protect, detect, respond, and recover) to convey a complete, holistic approach to cyber-resilience. This division also helped pinpoint areas organizations found especially challenging.

It is important to note that this white paper does not include the full results of the IDC survey and instead only focuses on the key findings. These data points should help technology buyers assess their own cyber-resilience posture, compare them to other IT organizations, and make better decisions on the technology and services they should adopt to improve their standing.

Survey Findings

Figures 2–15 (pages 7–20) in the sections that follow depict total survey results as well as results broken down by industry.

Finding 1: Most Victims Pay the Ransom

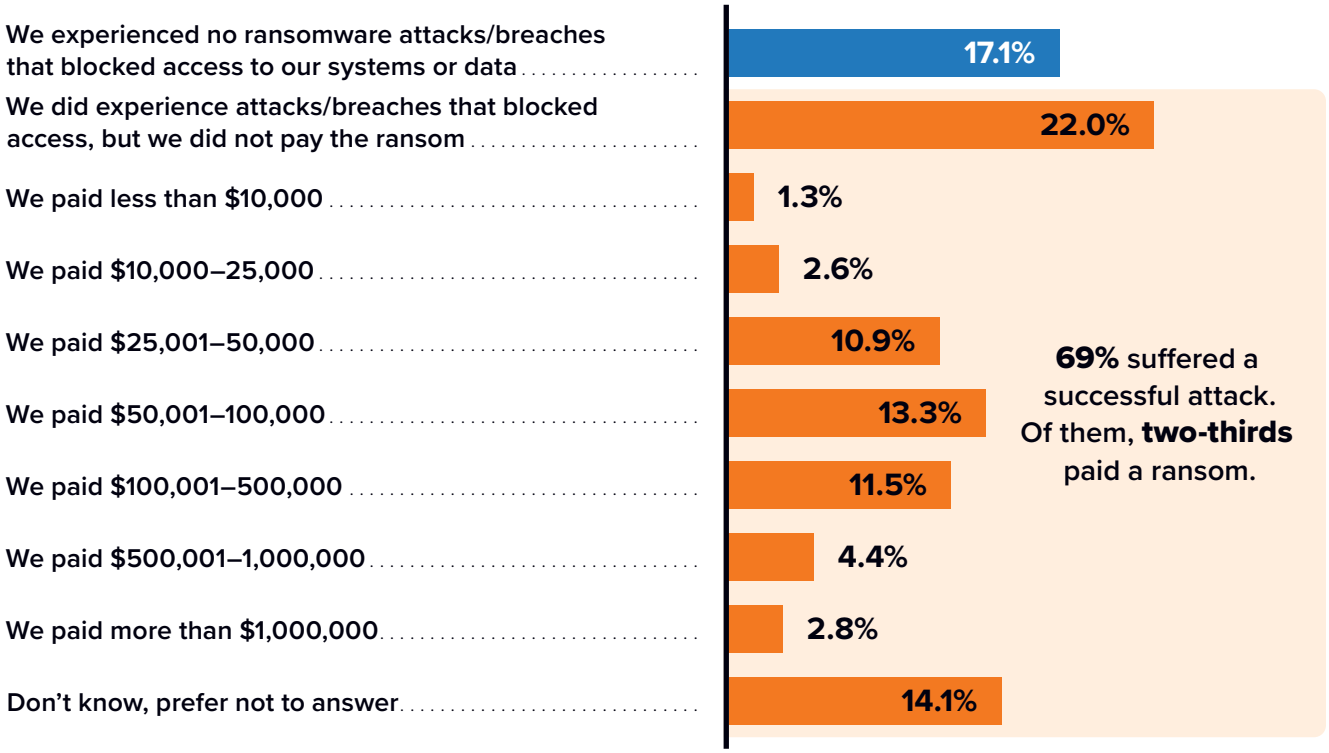
Nearly half of the total respondents surveyed indicated they paid a ransom within the last year. The majority of respondents said they suffered an attack that blocked access to their systems or data, and 22% said they did not pay the ransom, indicating they either were able to recover by themselves or simply didn't recover the compromised systems at all.

The cost of ransomware payments most typically ranges from $25,000/year to $500,000/year, with the most common response from $50,000 to $100,000. Coupled with the relatively high chance that victims will pay, there is little doubt how lucrative the ransomware business is and how costly it is for organizations.

FIGURE 2

Ransoms Paid

If your organization paid a ransom in the past 12 months to regain access to systems or data, how much was paid? Please include the total amount if multiple ransoms were paid.
(Percentage of respondents)

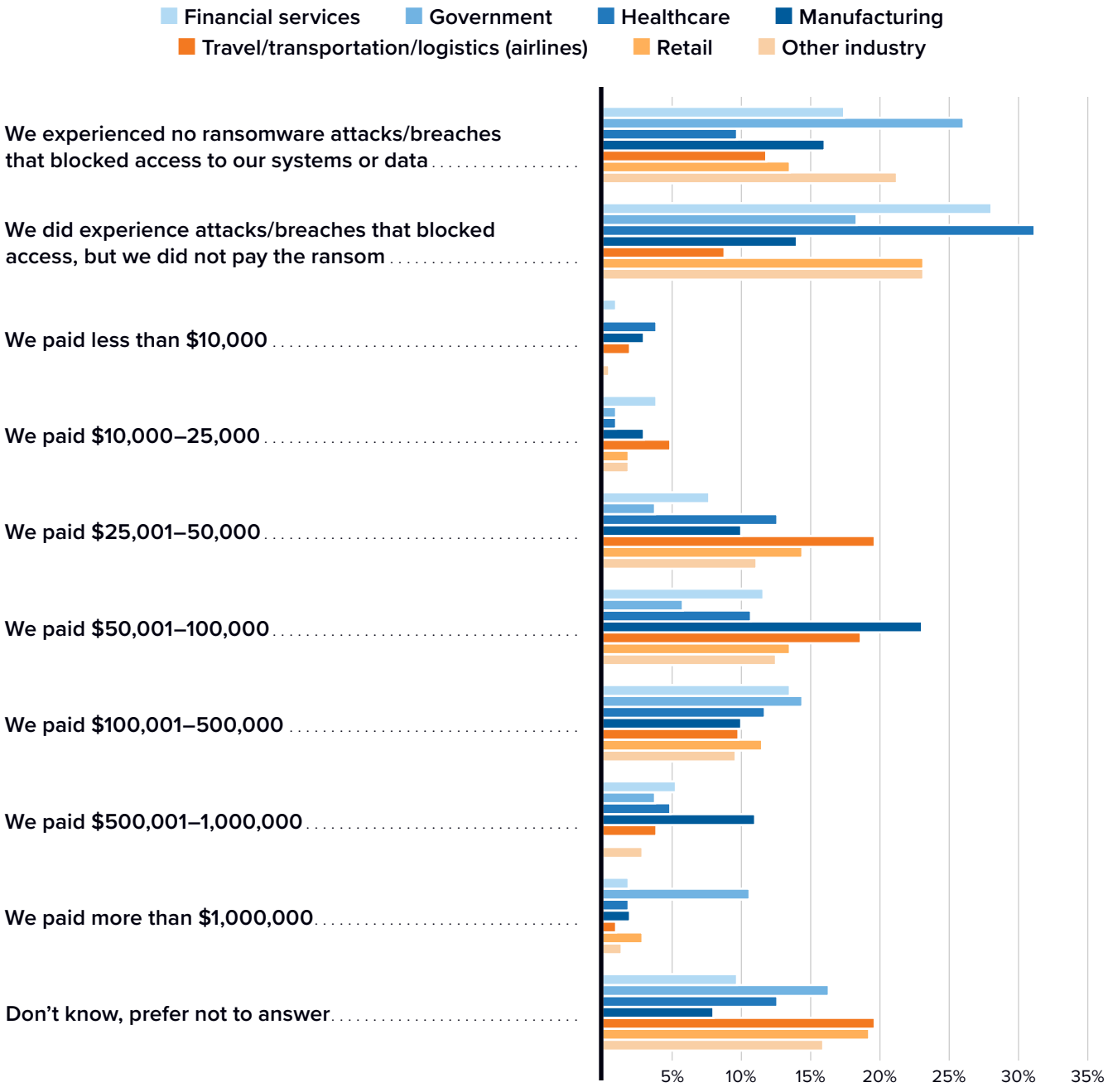


n = 928, Base = all respondents; Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

FIGURE 3

Ransoms Paid by Industry

If your organization paid a ransom in the past 12 months to regain access to systems or data, how much was paid? Please include the total amount if multiple ransoms were paid.
(Percentage of respondents)



n = 207 (financial services), n = 104 (government), n = 103 (healthcare), n = 100 (manufacturing), n = 102 (travel/transportation/logistics [airlines]), n = 104 (retail), n = 208 (other industry); Base = all respondents; Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

For an accessible version of the data in this figure, see Figure 3 Supplemental Data in the Appendix.

Finding 2: Few Organizations Can Recover on Their Own

When the scope is narrowed to just the respondents that suffered a successful ransomware attack, it becomes clear how frequently ransom is paid. Among respondents, 28.2% indicated they avoided paying a ransom because they were able to recover using their backup systems, 67.7% resorted to paying the ransom, and most of them reported that their decryption key worked. Unfortunately, 4.4% paid the ransom but couldn't decrypt their data.

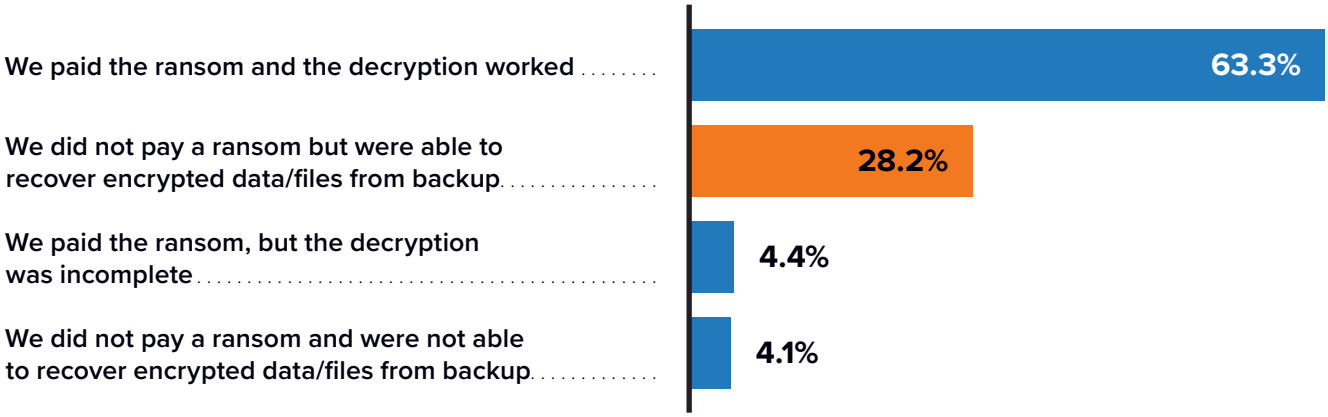
Although the chances of successful recovery after paying a ransom appear exceedingly high, it should not be construed as a good way to recover. As decryption software from criminals is often unoptimized, it is by no means a "quick fix" nor is there any assurance that the decryption key isn't hiding malware. Furthermore, paying the ransom without fixing the vulnerabilities that allowed it in the first place leaves the door open for future attacks.

FIGURE 4

Recovery Rates for Paying or Not Paying the Ransom

For your most recent ransomware incident that blocked access to systems or data, which of the following occurred?

(Percentage of respondents)



Fewer than 30% of respondents could recover without paying ransom.

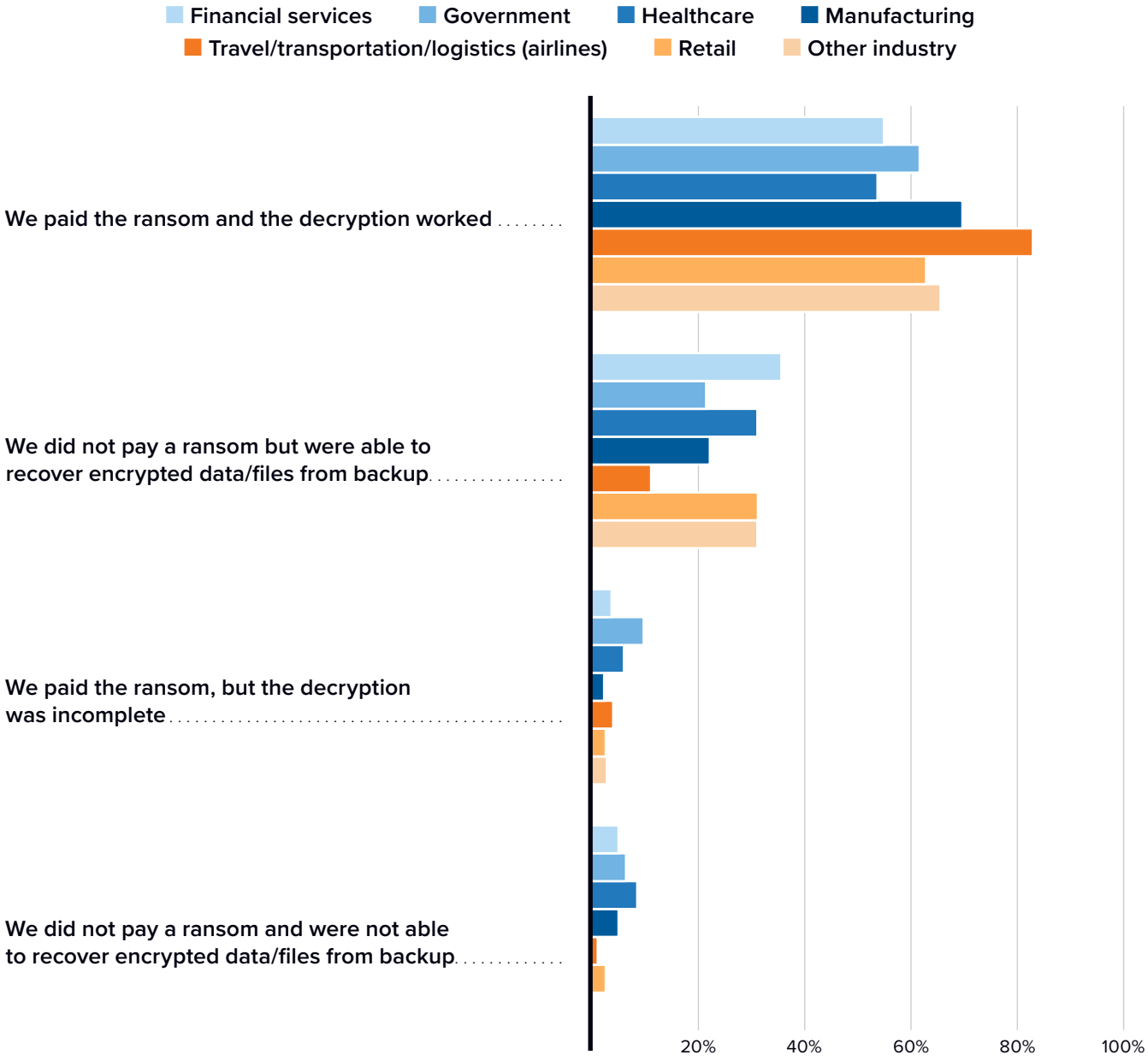
n = 638, Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

FIGURE 5

Recovery Rates for Paying or Not Paying the Ransom by Industry

For your most recent ransomware incident that blocked access to systems or data, which of the following occurred?

(Percentage of respondents)



n = 638, n = 151 (financial services), n = 60 (government), n = 80 (healthcare), n = 76 (manufacturing), n = 70 (travel/transportation/logistics [airlines]), n = 70 (retail), n = 131 (other industry); Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

For an accessible version of the data in this figure, see Figure 5 Supplemental Data in the Appendix.

Finding 3: Nearly All Ransomware Attacks Result in Data Exfiltration

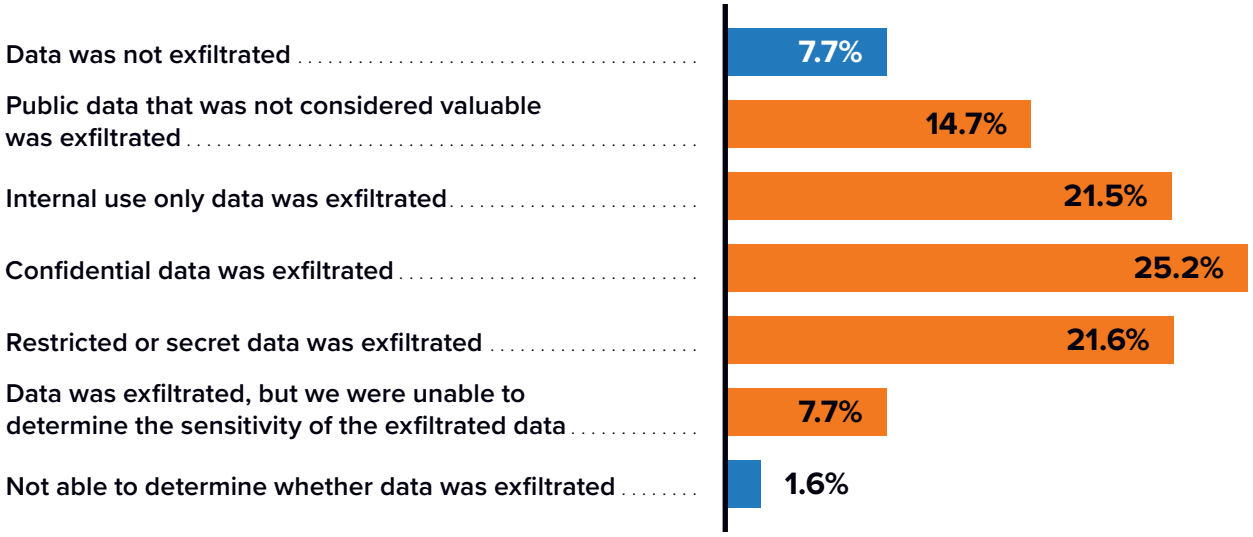
Most successful ransomware attacks result in data being stolen. Among the 90.7% of the respondents that indicated they paid a ransom in the last year reported data was stolen when they were attacked. This allows criminals to extort them further by threatening to release any sensitive data they have gotten a hold of.

Frustratingly, this method of extortion can't be thwarted by recovery efforts, meaning some organizations that can orchestrate a successful cyber-recovery still may end up paying a ransom regardless. In addition, 7.7% of respondents indicated they don't know the sensitivity of the exfiltrated data. This puts more pressure on victims to pay the ransom, as they have no way of knowing if the criminals took anything of value nor can they gauge the risk exposure the data poses.

FIGURE 6

Successful Ransomware Attacks Lead to Data Exfiltration

For your most recent ransomware incident that blocked access to systems or data, which of the following occurred?
(Percentage of respondents)



Of the respondents, 7.7% don't know the sensitivity of the data taken, and 90.7% of victims reported data was exfiltrated.

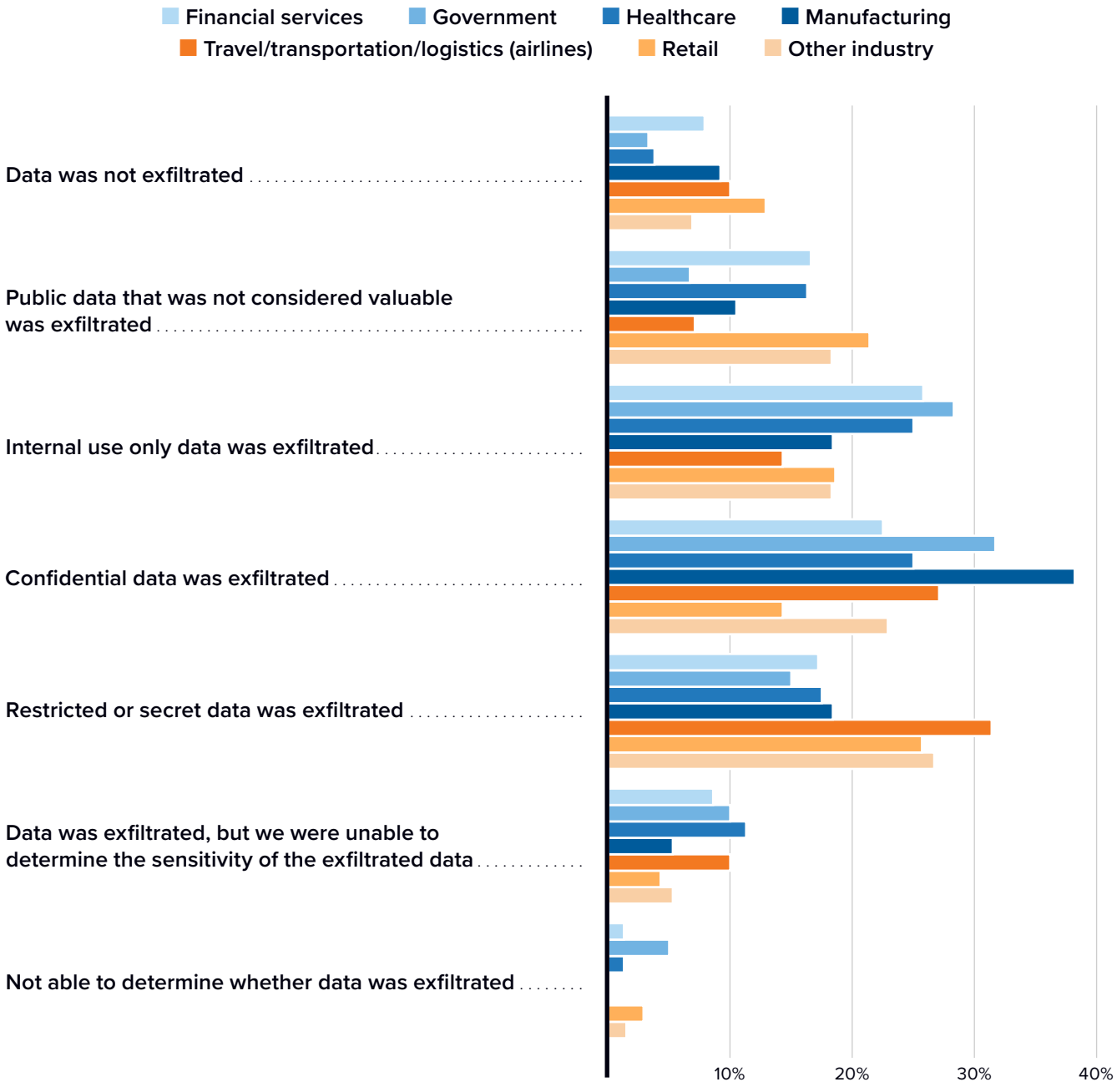
n = 638, Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

FIGURE 7

Successful Ransomware Attacks Lead to Data Exfiltration by Industry

For your most recent ransomware incident that blocked access to systems or data, which of the following occurred?

(Percentage of respondents)



n = 638, n = 151 (financial services), n = 60 (government), n = 80 (healthcare), n = 76 (manufacturing), n = 70 (travel/transportation/logistics [airlines]), n = 70 (retail), n = 131 (other industry); Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

For an accessible version of the data in this figure, see Figure 7 Supplemental Data in the Appendix.

Finding 4: Backups Are at Risk

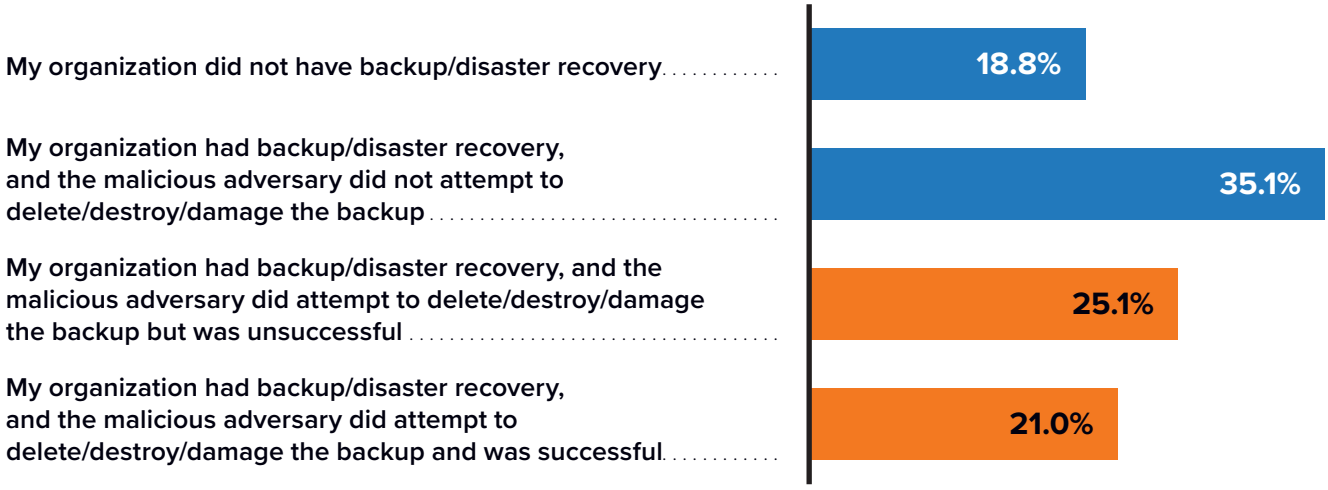
In 46% of cases of successful ransomware attacks, respondents reported the threat actors attempted to delete or disable their backups. The purpose of this is to remove organizations' ability to recover, making it more likely they will have to pay a ransom. This survey found that backup deletion attempts are successful almost half the time.

The frequency of backup deletion illustrates the importance of securing backup data and backup repositories against intrusion. Anti-ransomware measures for backup deletion attacks include data encryption, immutable storage, and air-gapped storage. This survey found that of those three measures, storing backup data in an air-gapped environment had the most impact on preventing deletion. However, it is ideal to build a layered defense consisting of multiple anti-ransomware measures.

FIGURE 8

Adversaries Specifically Target Backups

For your most recent ransomware incident that blocked access to systems or data, what is your organization's stance regarding backup/disaster recovery?
(Percentage of respondents)



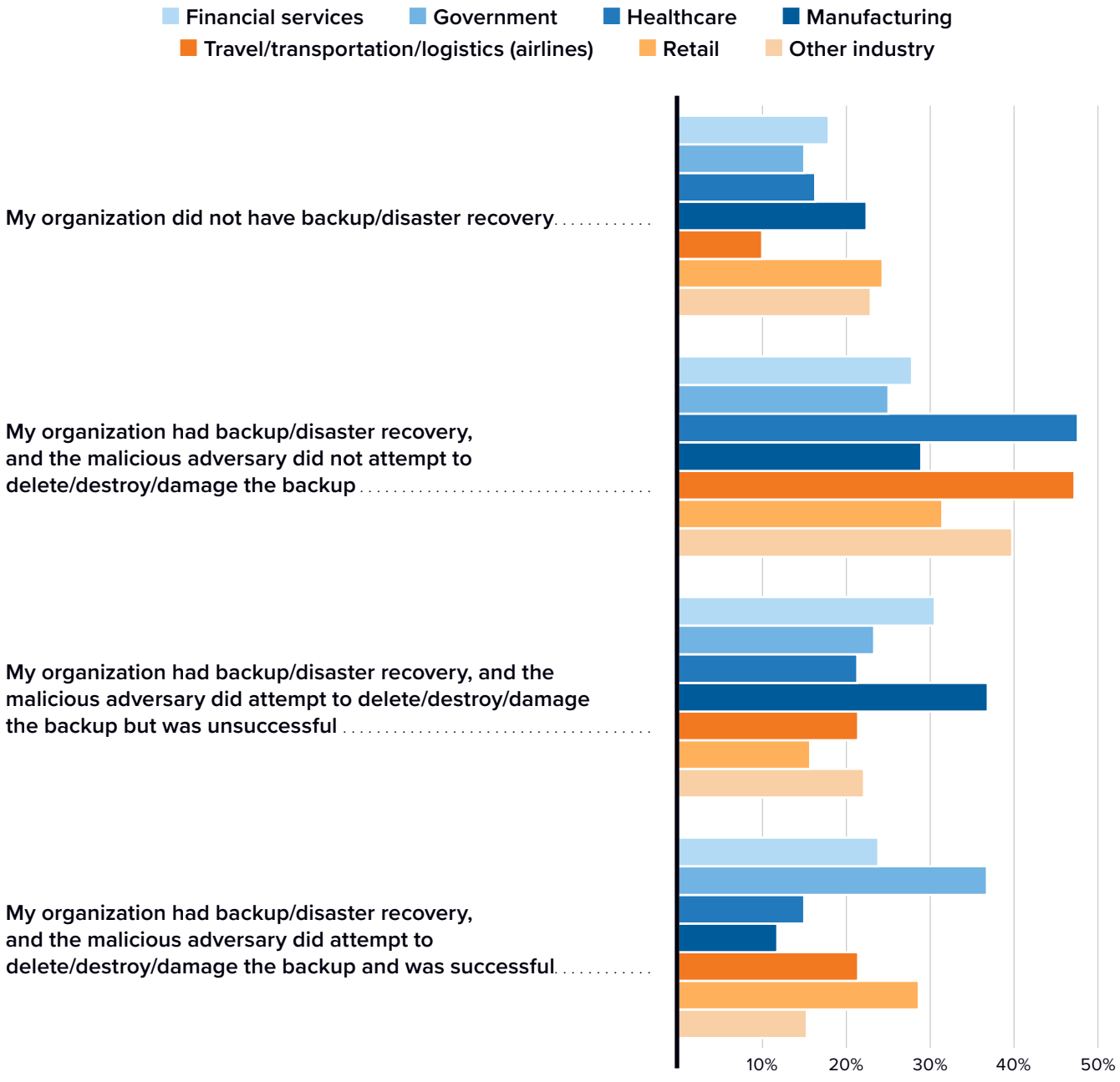
Ransomware still commonly targets backups.

n = 638, Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

FIGURE 9

Adversaries Specifically Target Backups by Industry

For your most recent ransomware incident that blocked access to systems or data, what is your organization's stance regarding backup/disaster recovery?
(Percentage of respondents)



n = 638, n = 151 (financial services), n = 60 (government), n = 80 (healthcare), n = 76 (manufacturing), n = 70 (travel/transportation/logistics [airlines]), n = 70 (retail), n = 131 (other industry); Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

For an accessible version of the data in this figure, see Figure 9 Supplemental Data in the Appendix.

Finding 5: Downtime

Ransomware attacks lead to significant downtime for organizations. The survey found only about 22% of companies can get up and running in a day or less after a ransomware incident, and about 50% are disrupted for a week or longer. For some businesses, downtime is only measured in the time it takes for their cyber-recovery plan to complete, but for others, it will unfortunately include time spent calling in legal experts, negotiating with the criminals, or waiting for the decryption key to work.

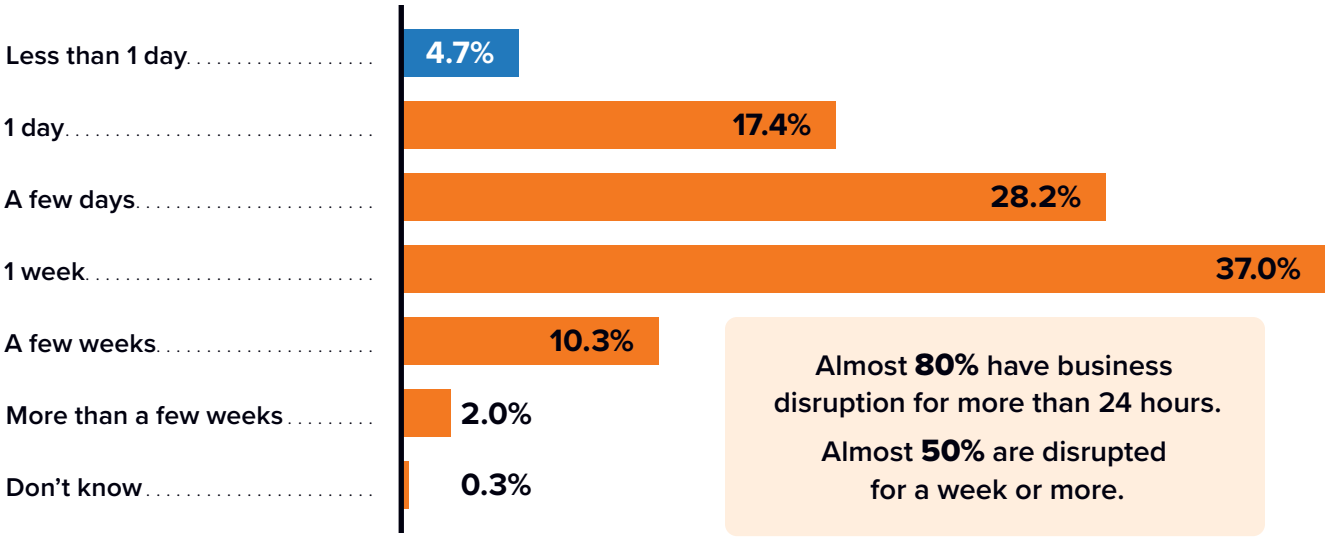
These hours of disruption add up. Another IDC study focused on downtime costs found businesses experience approximately 206 hours of downtime each year at an average cost of $2,800 per hour for on-premises workloads and approximately 161 hours of downtime each year at an average cost of $3,275 per hour for off-premises, public cloud workloads. Days or weeks of downtime can easily cost organizations hundreds of thousands of dollars.

FIGURE 10

Days of Business Disruption

For your most recent ransomware incident that blocked access to systems or data, how many days was business disrupted?

(Percentage of respondents)



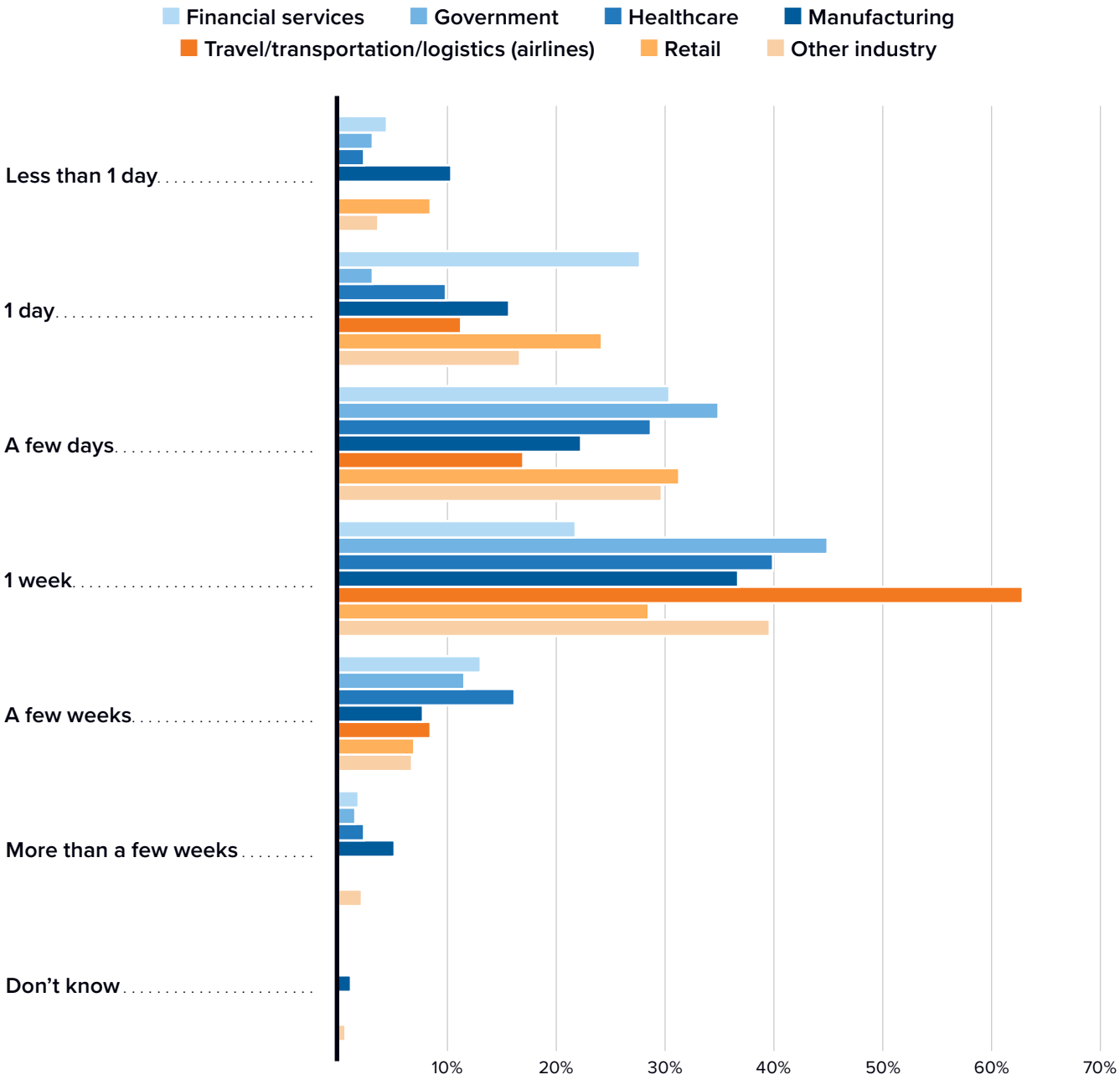
n = 638, Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

FIGURE 11

Days of Business Disruption by Industry

For your most recent ransomware incident that blocked access to systems or data, how many days was business disrupted?

(Percentage of respondents)



n = 638, n = 151 (financial services), n = 60 (government), n = 80 (healthcare), n = 76 (manufacturing), n = 70 (travel/transportation/logistics [airlines]), n = 70 (retail), n = 131 (other industry); Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

For an accessible version of the data in this figure, see Figure 11 Supplemental Data in the Appendix.

Finding 6: Turning to Third Parties

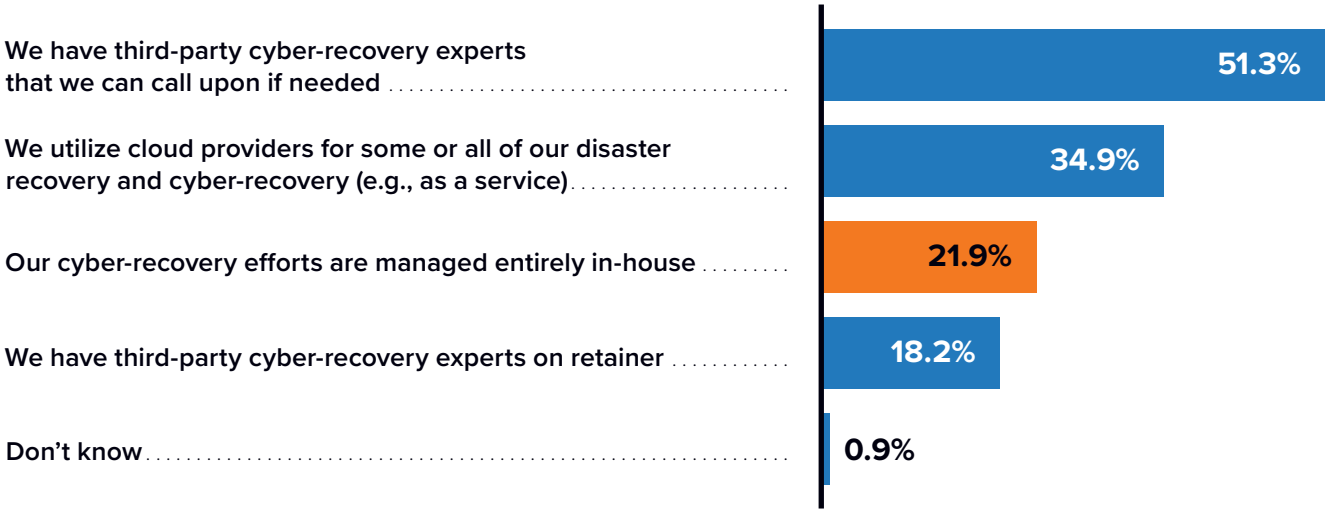
The survey found most organizations do not have the expertise to handle cyber-recovery and instead employ third parties for help. These third parties could be cyber-recovery experts they keep on retainer, cyber-recovery experts from vendors or service providers, or cyber-recovery services provided by cloud providers in an as-a-service manner.

With only about 22% of respondents indicating they manage cyber-recovery efforts entirely in-house, it is clear the vast majority of organizations lack enough cyber-recovery expertise. This survey data heavily suggests that while more robust technology and wider education will be helpful, most of the market impact and opportunity will come from vendors that can provide cyber-recovery services.

FIGURE 12

Who Handles Cyber-Recovery?

How are your cyber-recovery efforts structured?
(Percentage of respondents)



Only about 22% of companies have enough in-house expertise to handle cyber-recovery without outside assistance.

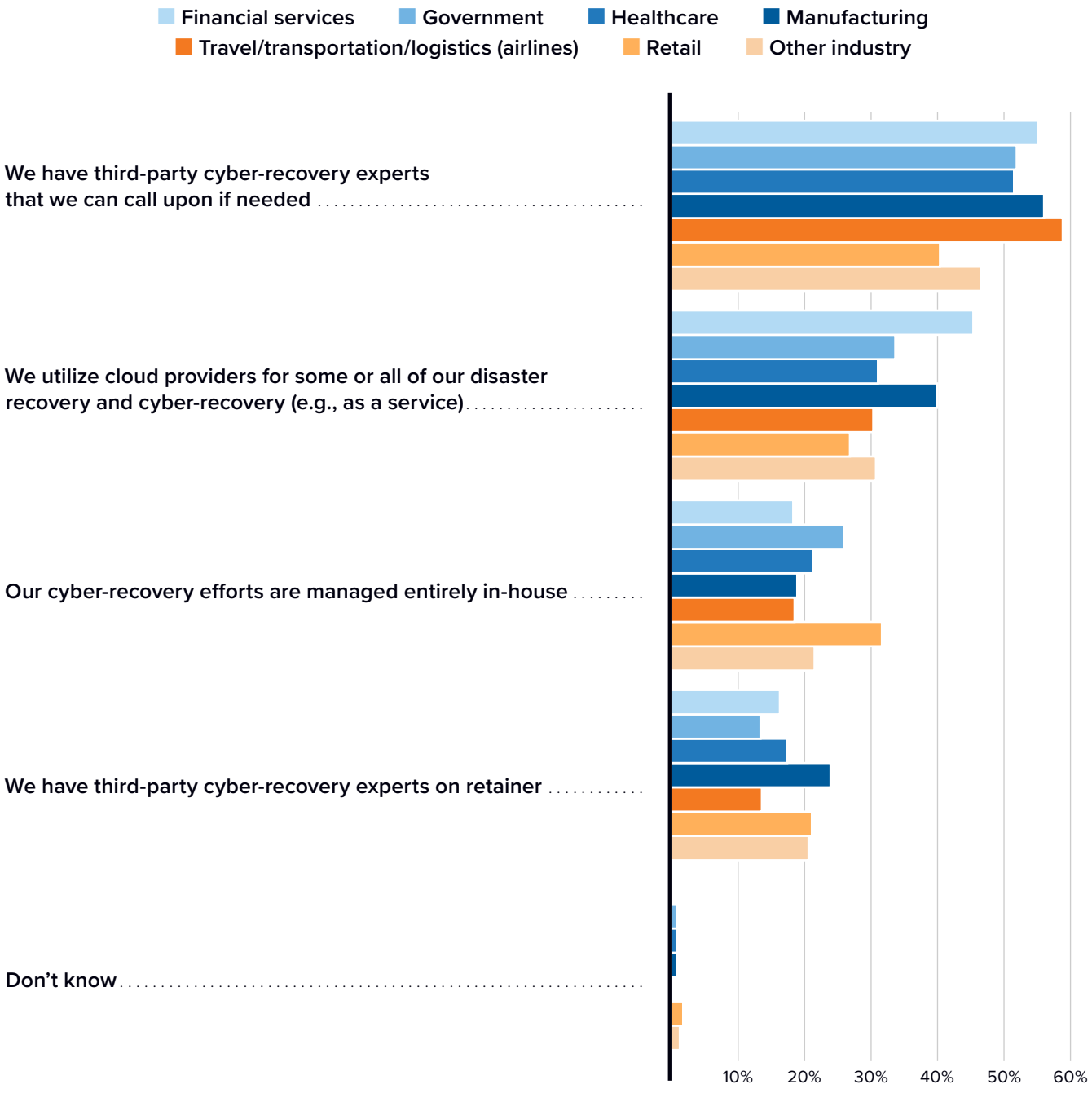
n = 928, Base = all respondents; Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Multiple responses were allowed. Use caution when interpreting small sample sizes. Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

FIGURE 13

Who Handles Cyber-Recovery? — By Industry

How are your cyber-recovery efforts structured?

(Percentage of respondents)



n = 928, n = 207 (financial services), n = 104 (government), n = 103 (healthcare), n = 100 (manufacturing), n = 102 (travel/transportation/logistics [airlines]), n = 104 (retail), n = 208 (other industry); Base = all respondents; Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Multiple responses were allowed. Use caution when interpreting small sample sizes. Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

For an accessible version of the data in this figure, see Figure 13 Supplemental Data in the Appendix.

Finding 7: Addressing Compliance

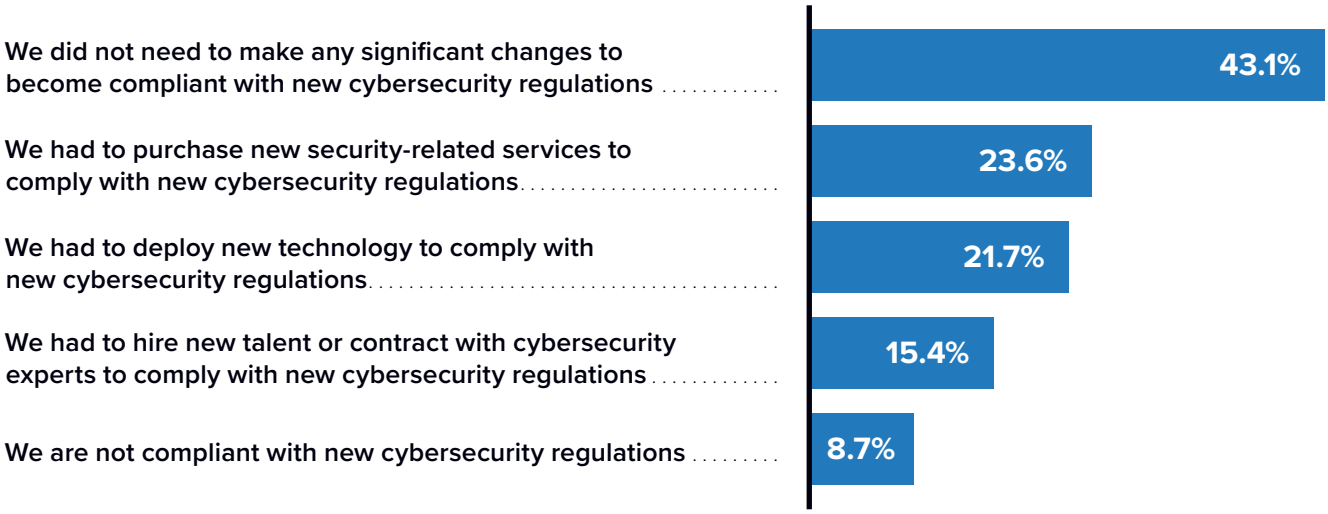
The IDC survey data indicated respondents are encountering challenges achieving compliance with new cybersecurity regulations. Among respondents, 43% said they didn't need to make any significant changes to stay compliant, leaving nearly half making major investments in technology, services, and talent to meet regulatory requirements. The remainder aren't compliant and haven't yet invested in becoming so.

These results punctuate the lack of cybersecurity expertise among organizations and highlight the importance of third-party services to help fill this knowledge gap. As new rules and regulations emerge and as existing ones change, organizations will need help determining what security technology and services they must deploy to stay compliant.

FIGURE 14

Compliance with Cybersecurity Regulations

What changes did your organization make to comply with new cybersecurity regulations such as DORA and the NIS2 Directive?
(Percentage of respondents)



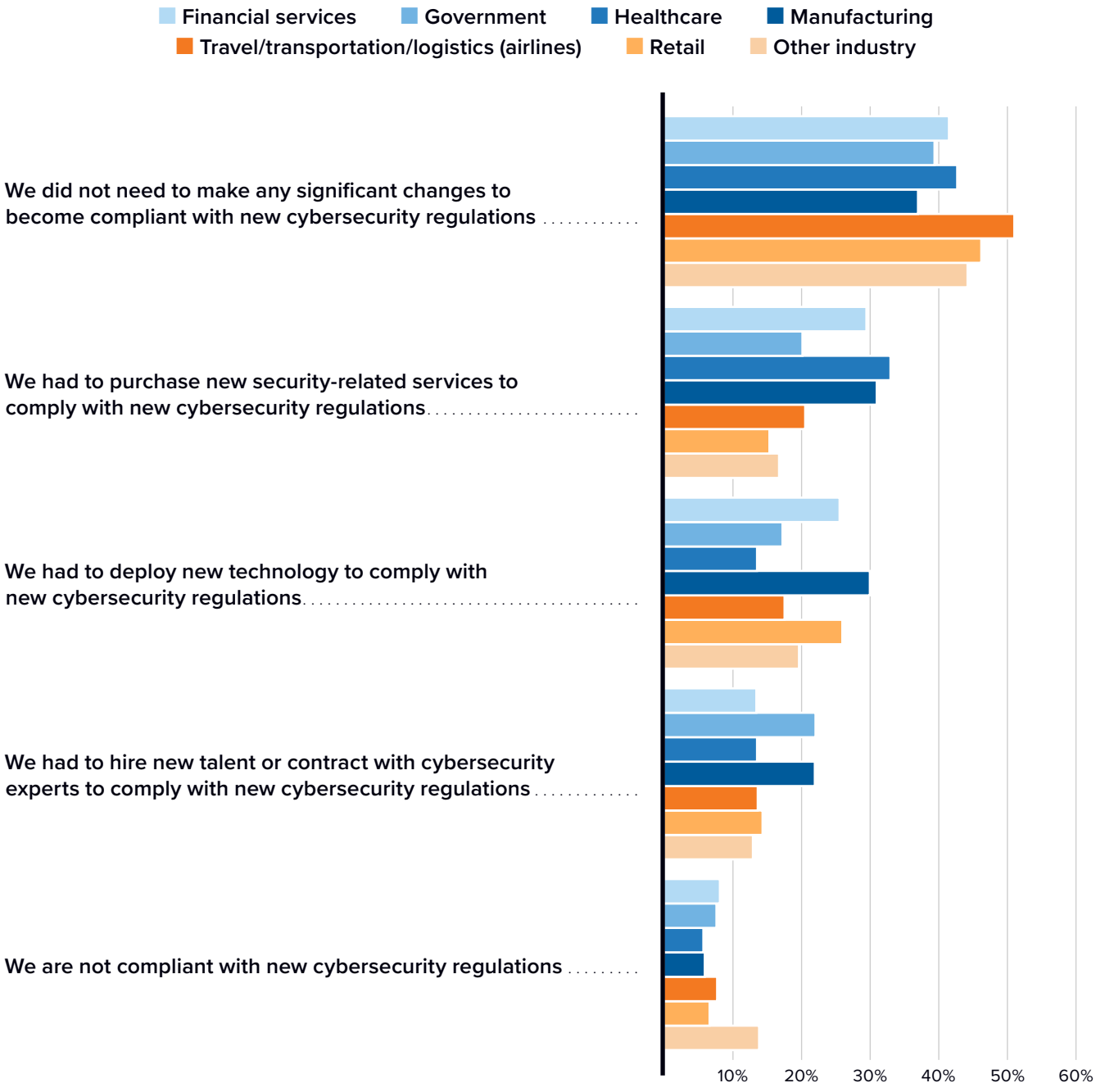
n = 928, Base = all respondents; Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Multiple responses were allowed. Use caution when interpreting small sample sizes. Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

FIGURE 15

Compliance with Cybersecurity Regulations by Industry

What changes did your organization make to comply with new cybersecurity regulations such as DORA and the NIS2 Directive?

(Percentage of respondents)



n = 928, n = 207 (financial services), n = 104 (government), n = 103 (healthcare), n = 100 (manufacturing), n = 102 (travel/transportation/logistics [airlines]), n = 104 (retail), n = 208 (other industry); Base = all respondents; Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Multiple responses were allowed. Use caution when interpreting small sample sizes. Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

For an accessible version of the data in this figure, see Figure 15 Supplemental Data in the Appendix.

Conclusion

Even as the data protection products improve and incorporate security features to counter the ever-evolving ransomware threat, organizations are still struggling to avoid paying ransom. Less than a third of organizations that are attacked can recover their data on their own, and most resort to paying the ransom. This is made worse by data exfiltration and extortion, leading some organizations to pay ransom regardless of successful recovery.

This struggle is happening despite organizations following what are believed to be best practices around backup and recovery, DR, and security. Most organizations run DR tests twice a year or more often, perform adversary exercises twice a year or more, and have cyber-risk assessments that are fewer than six months old. However, each of these best practices are centered around their respective use cases and not specifically for recovering from a ransomware attack.

Therefore, IDC concludes the poor ransomware outcomes aren't a result of weakness in best practices or technology but from a lack of knowledge and standardization around cyber-recovery. IDC's survey found most organizations have already deployed the tools for building a cyber-recovery solution, but they need guidance putting it together.

Tech buyers are encouraged to work with vendors that can provide that guidance. Building a system that can quickly recover data on a large scale without reintroducing infection, exposing backups to attacks, or allowing unauthorized access to sensitive data is a significant task — one that very few organizations can accomplish with internal resources. Tech vendors are encouraged to fill in those expertise gaps with service offerings that help buyers assess and reduce risk, maintain compliance, and bolster their cyber-resilience.

Appendix: Supplemental Data

This appendix provides an accessible version of the data for any complex figures in the document. Click "Return to original figure" to get back to the original data figure.

FIGURE 3 SUPPLEMENTAL DATA

Ransoms Paid by Industry

	Financial services	Government	Healthcare	Manufacturing
We experienced no ransomware attacks/breaches that blocked access to our systems or data	17.4	26.0	9.7	16.0
We did experience attacks/breaches that blocked access, but we did not pay the ransom	28.0	18.3	31.1	14.0
We paid less than $10,000	1.0	0.0	3.9	3.0
We paid $10,000–25,000	3.9	1.0	1.0	3.0
We paid $25,001–50,000	7.7	3.8	12.6	10.0
We paid $50,001–100,000	11.6	5.8	10.7	23.0
We paid $100,001–500,000	13.5	14.4	11.7	10.0
We paid $500,001–1,000,000	5.3	3.8	4.9	11.0
We paid more than $1,000,000	1.9	10.6	1.9	2.0
Don't know, prefer not to answer	9.7	16.3	12.6	8.0

	Travel/transportation/ logistics (airlines)	Retail	Other industry
We experienced no ransomware attacks/breaches that blocked access to our systems or data	11.8	13.5	21.2
We did experience attacks/breaches that blocked access, but we did not pay the ransom	8.8	23.1	23.1
We paid less than $10,000	2.0	0.0	0.5
We paid $10,000–25,000	4.9	1.9	1.9
We paid $25,001–50,000	19.6	14.4	11.1
We paid $50,001–100,000	18.6	13.5	12.5
We paid $100,001–500,000	9.8	11.5	9.6
We paid $500,001–1,000,000	3.9	0.0	2.9
We paid more than $1,000,000	1.0	2.9	1.4
Don't know, prefer not to answer	19.6	19.2	15.9

n = 207 (financial services), n = 104 (government), n = 103 (healthcare), n = 100 (manufacturing), n = 102 (travel/transportation/logistics [airlines]), n = 104 (retail), n = 208 (other industry); Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

Return to original figure

Appendix: Supplemental Data (continued)

FIGURE 5 SUPPLEMENTAL DATA

Recovery Rates for Paying or Not Paying the Ransom by Industry

	Financial services	Government	Healthcare	Manufacturing
We paid the ransom and the decryption worked	55.0	61.7	53.8	69.7
We did not pay a ransom but were able to recover encrypted data/files from backup	35.8	21.7	31.3	22.4
We paid the ransom, but the decryption was incomplete	4.0	10.0	6.3	2.6
We did not pay a ransom and were not able to recover encrypted data/files from backup	5.3	6.7	8.8	5.3

	Travel/transportation/ logistics (airlines)	Retail	Other industry
We paid the ransom and the decryption worked	82.9	62.9	65.6
We did not pay a ransom but were able to recover encrypted data/files from backup	11.4	31.4	31.3
We paid the ransom, but the decryption was incomplete	4.3	2.9	3.1
We did not pay a ransom and were not able to recover encrypted data/files from backup	1.4	2.9	0.0

n = 638, n = 151 (financial services), n = 60 (government), n = 80 (healthcare), n = 76 (manufacturing), n = 70 (travel/transportation/logistics [airlines]), n = 70 (retail), n = 131 (other industry); Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

Return to original figure

Appendix: Supplemental Data (continued)

FIGURE 7 SUPPLEMENTAL DATA

Successful Ransomware Attacks Lead to Data Exfiltration by Industry

	Financial services	Government	Healthcare	Manufacturing
Data was not exfiltrated	7.9	3.3	3.8	9.2
Public data that was not considered valuable was exfiltrated	16.6	6.7	16.3	10.5
Internal use only data was exfiltrated	25.8	28.3	25.0	18.4
Confidential data was exfiltrated	22.5	31.7	25.0	38.2
Restricted or secret data was exfiltrated	17.2	15.0	17.5	18.4
Data was exfiltrated, but we were unable to determine the sensitivity of the exfiltrated data	8.6	10.0	11.3	5.3
Not able to determine whether data was exfiltrated	1.3	5.0	1.3	0.0

	Travel/transportation/ logistics (airlines)	Retail	Other industry
Data was not exfiltrated	10.0	12.9	6.9
Public data that was not considered valuable was exfiltrated	7.1	21.4	18.3
Internal use only data was exfiltrated	14.3	18.6	18.3
Confidential data was exfiltrated	27.1	14.3	22.9
Restricted or secret data was exfiltrated	31.4	25.7	26.7
Data was exfiltrated, but we were unable to determine the sensitivity of the exfiltrated data	10.0	4.3	5.3
Not able to determine whether data was exfiltrated	0.0	2.9	1.5

n = 638, n = 151 (financial services), n = 60 (government), n = 80 (healthcare), n = 76 (manufacturing), n = 70 (travel/transportation/logistics [airlines]), n = 70 (retail), n = 131 (other industry); Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

Return to original figure

Appendix: Supplemental Data (continued)

FIGURE 9 SUPPLEMENTAL DATA

Adversaries Specifically Target Backups by Industry

	Financial services	Government	Healthcare	Manufacturing
My organization did not have backup/disaster recovery	17.9	15.0	16.3	22.4
My organization had backup/disaster recovery, and the malicious adversary did not attempt to delete/destroy/damage the backup	27.8	25.0	47.5	28.9
My organization had backup/disaster recovery, and the malicious adversary did attempt to delete/destroy/damage the backup but was unsuccessful	30.5	23.3	21.3	36.8
My organization had backup/disaster recovery, and the malicious adversary did attempt to delete/destroy/damage the backup and was successful	23.8	36.7	15.0	11.8

	Travel/transportation/ logistics (airlines)	Retail	Other industry
My organization did not have backup/disaster recovery	10.0	24.3	22.9
My organization had backup/disaster recovery, and the malicious adversary did not attempt to delete/destroy/damage the backup	47.1	31.4	39.7
My organization had backup/disaster recovery, and the malicious adversary did attempt to delete/destroy/damage the backup but was unsuccessful	21.4	15.7	22.1
My organization had backup/disaster recovery, and the malicious adversary did attempt to delete/destroy/damage the backup and was successful	21.4	28.6	15.3

n = 638, n = 151 (financial services), n = 60 (government), n = 80 (healthcare), n = 76 (manufacturing), n = 70 (travel/transportation/logistics [airlines]), n = 70 (retail), n = 131 (other industry); Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

Return to original figure

Appendix: Supplemental Data (continued)

FIGURE 11 SUPPLEMENTAL DATA

Adversaries Specifically Target Backups by Industry

	Financial services	Government	Healthcare	Manufacturing
Less than 1 day	4.6	3.3	2.5	10.5
1 day	27.8	3.3	10.0	15.8
A few days	30.5	35.0	28.8	22.4
1 week	21.9	45.0	40.0	36.8
A few weeks	13.2	11.7	16.3	7.9
More than a few weeks	2.0	1.7	2.5	5.3
Don't know	0.0	0.0	0.0	1.3

	Travel/transportation/ logistics (airlines)	Retail	Other industry
Less than 1 day	0.0	8.6	3.8
1 day	11.4	24.3	16.8
A few days	17.1	31.4	29.8
1 week	62.9	28.6	39.7
A few weeks	8.6	7.1	6.9
More than a few weeks	0.0	0.0	2.3
Don't know	0.0	0.0	0.8

n = 638, n = 151 (financial services), n = 60 (government), n = 80 (healthcare), n = 76 (manufacturing), n = 70 (travel/transportation/logistics [airlines]), n = 70 (retail), n = 131 (other industry); Base = respondents indicated their organization paid a ransom in the past 12 months to regain access to systems or data;
Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Use caution when interpreting small sample sizes.
Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

Return to original figure

Appendix: Supplemental Data (continued)

FIGURE 13 SUPPLEMENTAL DATA

Who Handles Cyber-Recovery? — By Industry

	Financial services	Government	Healthcare	Manufacturing
We have third-party cyber-recovery experts that we can call upon if needed	55.1	51.9	51.5	56.0
We utilize cloud providers for some or all of our disaster recovery and cyber-recovery (e.g., as a service)	45.4	33.7	31.1	40.0
Our cyber-recovery efforts are managed entirely in-house	18.4	26.0	21.4	19.0
We have third-party cyber-recovery experts on retainer	16.4	13.5	17.5	24.0
Don't know	0.0	1.0	1.0	1.0

	Travel/transportation/ logistics (airlines)	Retail	Other industry
We have third-party cyber-recovery experts that we can call upon if needed	58.8	40.4	46.6
We utilize cloud providers for some or all of our disaster recovery and cyber-recovery (e.g., as a service)	30.4	26.9	30.8
Our cyber-recovery efforts are managed entirely in-house	18.6	31.7	21.6
We have third-party cyber-recovery experts on retainer	13.7	21.2	20.7
Don't know	0.0	1.9	1.4

n = 928, n = 207 (financial services), n = 104 (government), n = 103 (healthcare), n = 100 (manufacturing), n = 102 (travel/transportation/logistics [airlines]), n = 104 (retail), n = 208 (other industry); Base = all respondents; Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Multiple responses were allowed. Use caution when interpreting small sample sizes. Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

Return to original figure

Appendix: Supplemental Data (continued)

FIGURE 15 SUPPLEMENTAL DATA

Compliance with Cybersecurity Regulations by Industry

	Financial services	Government	Healthcare	Manufacturing
We did not need to make any significant changes to become compliant with new cybersecurity regulations	41.5	39.4	42.7	37.0
We had to purchase new security-related services to comply with new cybersecurity regulations	29.5	20.2	33.0	31.0
We had to deploy new technology to comply with new cybersecurity regulations	25.6	17.3	13.6	30.0
We had to hire new talent or contract with cybersecurity experts to comply with new cybersecurity regulations	13.5	22.1	13.6	22.0
We are not compliant with new cybersecurity regulations	8.2	7.7	5.8	6.0

	Travel/transportation/ logistics (airlines)	Retail	Other industry
We did not need to make any significant changes to become compliant with new cybersecurity regulations	51.0	46.2	44.2
We had to purchase new security-related services to comply with new cybersecurity regulations	20.6	15.4	16.8
We had to deploy new technology to comply with new cybersecurity regulations	17.6	26.0	19.7
We had to hire new talent or contract with cybersecurity experts to comply with new cybersecurity regulations	13.7	14.4	13.0
We are not compliant with new cybersecurity regulations	7.8	6.7	13.9

n = 928, n = 207 (financial services), n = 104 (government), n = 103 (healthcare), n = 100 (manufacturing), n = 102 (travel/transportation/logistics [airlines]), n = 104 (retail), n = 208 (other industry); Base = all respondents; Notes: Data is managed by IDC's Global Primary Research Group. Data is not weighted. Multiple responses were allowed. Use caution when interpreting small sample sizes. Source: IDC and Kyndryl's *The State of Cyber-Resilience Survey*, February 2023

Return to original figure

About the IDC Analysts

Johnny Yu
Research Manager, Storage and Computing, IDC

Johnny Yu is a research manager within IDC's infrastructure software platforms research group. He covers as storage controller software, data replication, protection and archiving, storage device management and container data management, with a focus on how businesses optimize costs and secure their storage environments as their infrastructure expands beyond their data centers.

More about Johnny Yu

Frank Dickson
Program Vice President, Cybersecurity Products, IDC

Frank leads the team that delivers compelling research in the areas of Network Security; Endpoint Security; Cybersecurity Analytics, Intelligence, Response, and Orchestration (AIRO); Identity & Digital Trust; Legal, Risk & Compliance; Data Security; IoT Security; and Cloud Security. Topically, he provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models.

More about Frank Dickson

Phillip Goodwin
Research Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC

Phil Goodwin is a research vice president within IDC's Enterprise Infrastructure Practice, covering research on data management. He provides detailed insight and analysis on evolving industry trends, vendor performance, and the impact of new technology adoption. He is responsible for producing and delivering timely, in-depth market research with a specific focus on cloud-based and on-premises Data Protection, Business Continuity and Disaster Recovery, and Data Availability. Phil takes a holistic view of these markets, and covers risk analysis, service level requirements and cost/benefit calculations in his research.

More about Phillip Goodwin

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.