White Paper

Why Rapid Recovery Is Safer than Paying the Ransom

Sponsored by: Veeam

Johnny Yu Jennifer Glenn Phil Goodwin
June 2022

INTRODUCTION

Every minute of downtime can mean thousands of dollars in lost business. When ransomware hits, paying the ransom can be tempting, but it isn't the quick fix organizations are hoping for.

Payment doesn't always guarantee recovery, let alone a timely one. According to IDC's *Worldwide Future Enterprise Resiliency and Spending Survey,* <28% of respondents were able to recover after paying the ransom (see Figure 1).

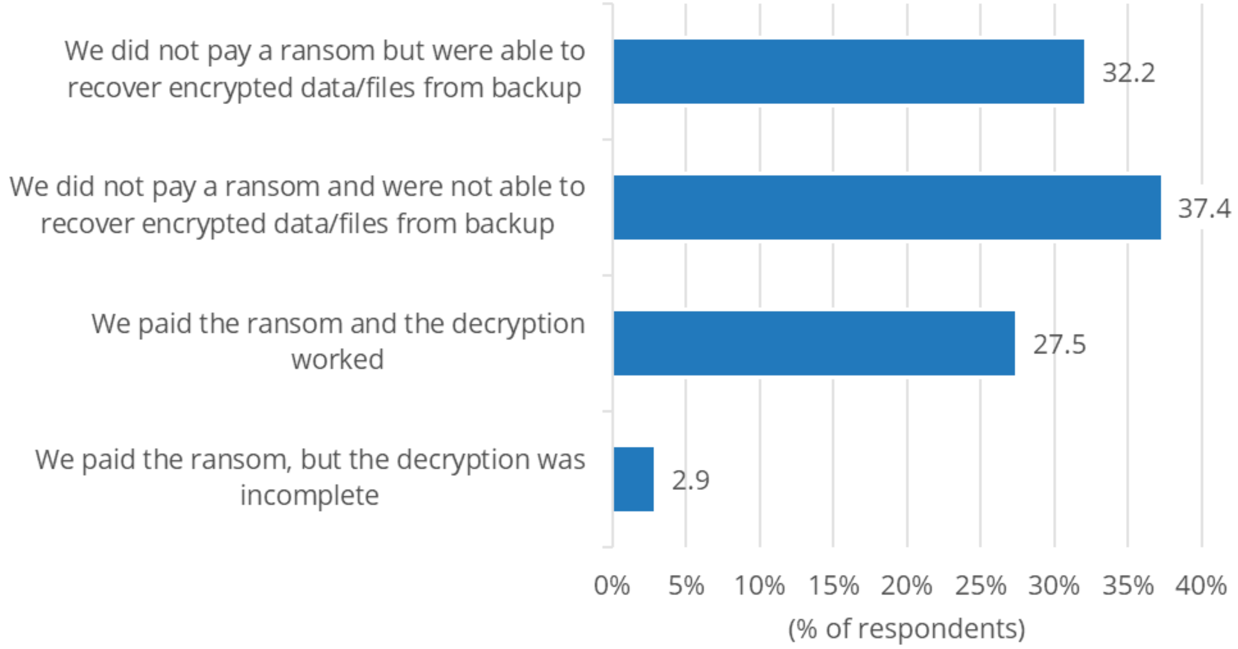
In addition, opting to pay the ransom is not as cut and dried as it seems. When an organization chooses to pay the ransom, leaders must first spend time discussing the decision with the legal team and others that may be impacted. Then the team may spend time negotiating with the attackers. Then more time is spent on the decryption process itself – and as noted in the same survey, the decryption process may not even work in some cases.

Choosing not to pay the ransom has its own risks. The same survey found that fewer than a third of the respondents were able to recover encrypted data from their backup files. However, this number can be bolstered, as the tools and techniques for building a dependable and fast data recovery plan are available now. With these, enterprises can confidently focus their efforts – and precious time – on recovery without spending cycles deciding on whether to pay the ransom.

FIGURE 1

Less than One-Third of Organizations Are Able to Recover on Their Own

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



n = 444

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Worldwide Future Enterprise Resiliency and Spending Survey,* December 2021

Building Rapid, Reliable Recovery

Ransomware is often a collection of attacks that sneak through security defenses to gain access to and take hostage essential information. While preventing ransomware attacks altogether is obviously the best solution for protecting data, it's not always feasible. The demands on digital business for agile service, innovative solutions, and always-on availability mean that security can't impede operations. This also means that relying on protection alone simply isn't enough.

Instead, successful organizations are expanding their data protection efforts to focus on fast and reliable recovery to keep operations moving and information secure. This includes:

- **Detection:** Rapidly identifying and responding to anomalies and security intrusions
- **Protection:** Creating and maintaining clean, immutable copies of essential data
- **Recovery:** Quickly getting essential data and applications back into the hand of the business

The first step in rapid and reliable recovery is immediately knowing when a security incident occurs and stopping it. To do this, organizations have to know where their data lives, the characteristics of that data, who or what has access to it, and how it can be used. Armed with this information, IT and security ops teams can collaborate on the creation of policies that dictate which users or devices can access certain types of data, as well as when and how it can be used.

Once these policies are established, they can be issued to multiple security and data management control points to protect sensitive information from unauthorized access, misuse, or exfiltration/theft. These policies can be tuned or adjusted as new risks emerge or business operations change. They also provide a foundation of data protection that can direct incident response processes and playbooks for any future ransomware attacks that may arise.

The protection component of rapid ransomware recovery involves having clean and quickly accessible backup copies of data to recover from. The tools that make backups difficult to compromise such as encryption, immutable storage, and air gapping have been on the market for the past several years and are likely familiar to data protection practitioners.

Aside from the tools themselves, best data protection practices also need to be implemented. This includes having multiple copies of backup data stored in multiple locations as well as restricting access to who can delete or overwrite backups or initiate a recovery.

The recovery and remediation component for rapid ransomware recovery is similar to any recovery process for unplanned outages, but with a few extra steps. A holistic ransomware response needs to involve security in the recovery process. An initial recovery should be done in an isolated sandbox environment so that security teams can run forensics and scan backup copies for malware or signs of intrusion.

Once a recovery method has been established, it should be regularly tested. This ensures the backup copies are recoverable, and it also provides opportunities for all parties involved to practice their incident response. This repeated drilling enables organizations to time and improve their recovery and confidently refuse to pay any ransom.

By involving security teams into what is essentially a normal disaster recovery (DR) process, organizations can target and remove remnants of a cyberattack and ensure the backup data is clean before it is pushed into production.

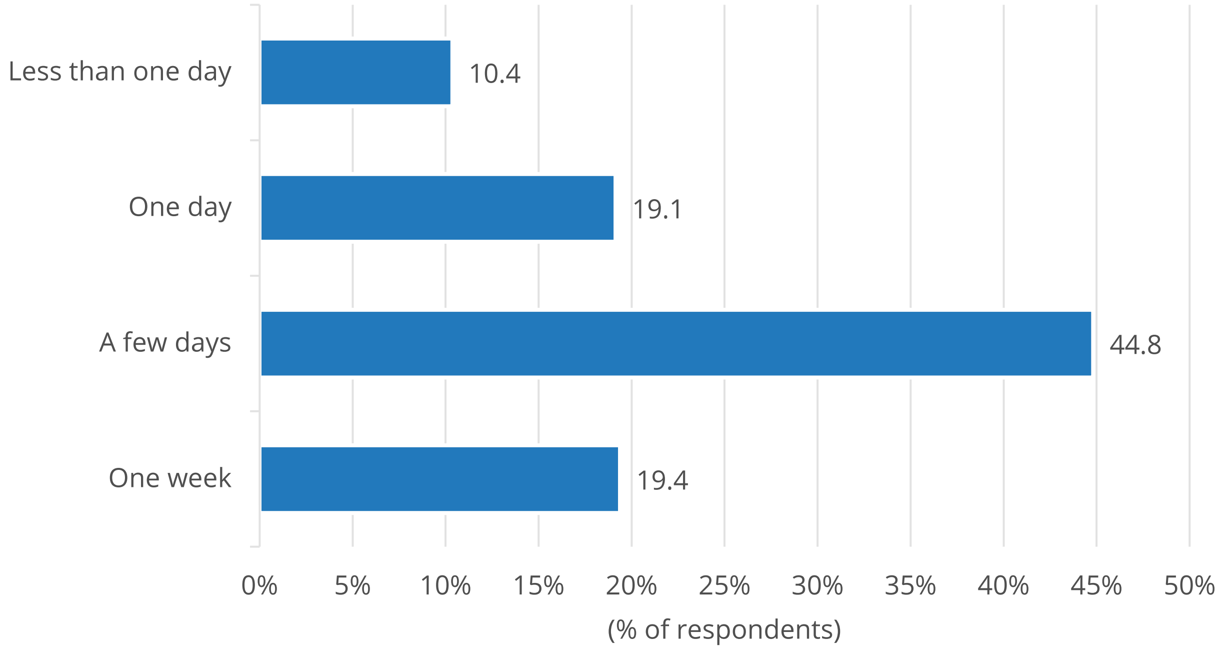
Paying the Ransom Versus Rapid Recovery

According to IDC's December 2021 *Worldwide Future Enterprise Resiliency and Spending Survey,* nearly 45% of respondents that had been affected by ransomware said business was disrupted by a few days. Almost one-fifth of respondents (19.4%) reported disruptions lasting an entire week (see Figure 2).

FIGURE 2

Most Organizations Experience More than One Day of Downtime When Ransomware Hits

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



n = 444

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Worldwide Future Enterprise Resiliency and Spending Survey,* December 2021

As minimizing downtime is one of the major goals of ransomware response, some organizations choose to pay the ransom (see Figure 3). However, the perception that paying the ransom immediately starts a company down the road to recovery is a myth.

The decision to pay the ransom isn't usually immediate. Most organizations will try every data recovery method available to them while senior decision makers and legal teams meet before considering making a payment. A documented and tested disaster recovery plan can shorten this step, and if an organization's recovery capabilities prove insufficient, it must escalate to the next step.

When an organization decides to pay a ransom, cyberinsurance companies and government agencies are brought into the conversation, as well as the attackers themselves. A company must negotiate with all of these entities – to argue that best practices were followed in order to make a successful insurance claim, to prove the company was in compliance with the law, and to lower the criminals' asking price. Every day spent deliberating is another day of downtime.

Once payment has been made and the criminals deliver a decryption key, the recovery process still can't begin until the encrypted data has been decrypted. Decrypters are generally unoptimized software, so the decryption process will take a long time. There's also no guarantee the decryption software isn't itself tainted or will actually work.

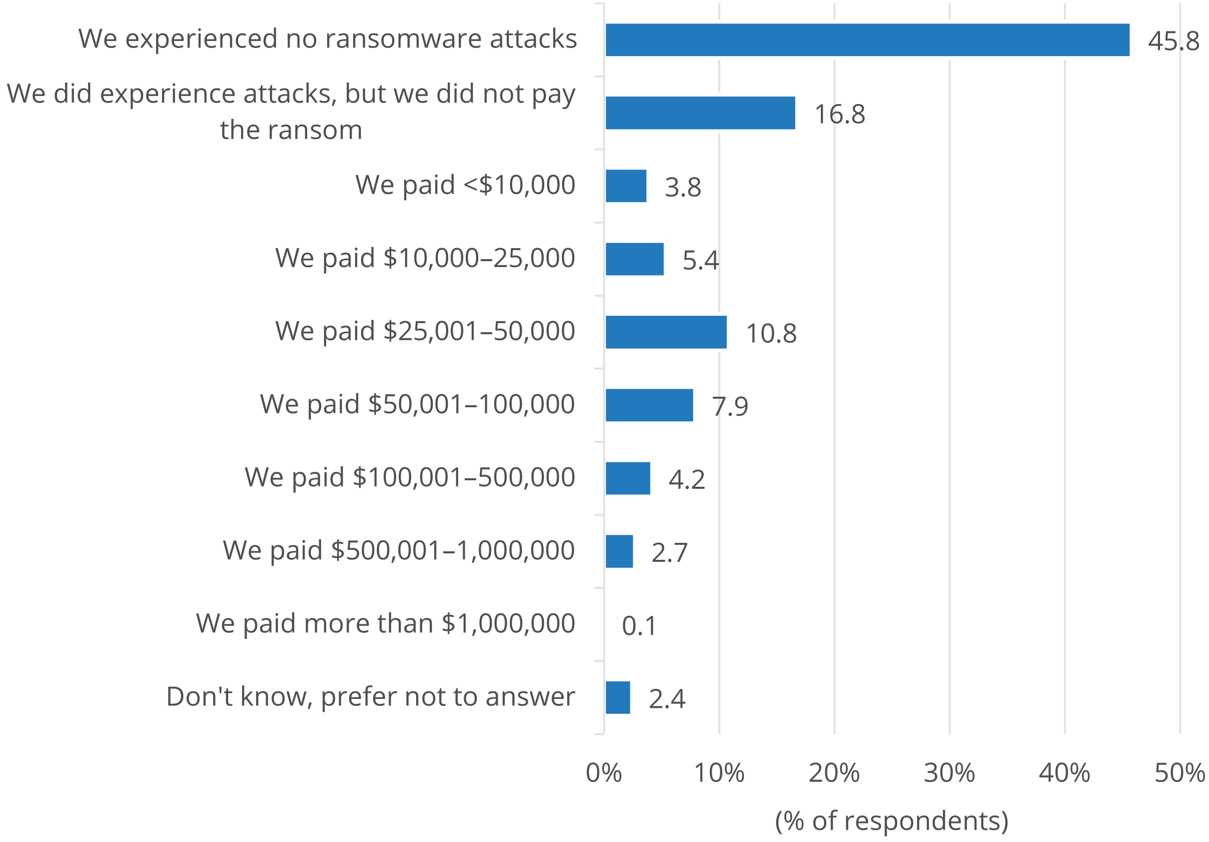
In addition, paying the ransom doesn't block off the method by which the criminals got in in the first place, so an organization could still be vulnerable to the exact same type of attack in the future. And by feeding a criminal business model and showing it is lucrative, paying the ransom all but guarantees that future attacks will happen.

Instead, strengthening the technology and processes for data backups can be instrumental in rapid, reliable recovery. According to IDC's *Worldwide Future Enterprise Resiliency and Spending Survey,* 32.2% of respondents that were affected by ransomware were able to successfully recover their files from backup without paying the ransom (refer back to Figure 1).

FIGURE 3

Ransom Payments Can Cost Tens of Thousands of Dollars or More

Q. If your organization paid a ransom in the past 12 months to regain access to systems or data, how much was paid?



n = 858

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Worldwide Future Enterprise Resiliency and Spending Survey*, December 2021

Since a rapid, reliable recovery system is based on disaster recovery, it is already suited for restoring a business back to a functional state within hours. Allowing extra time for security scans and forensics would still likely lead to a speedier recovery for an organization while avoiding paying any ransom.

In addition, rapid ransomware recovery allows organizations to be proactive, as the strength and reliability of their recovery system are under their control. Organizations that regularly test their recovery will have a solid understanding of their timetable during a ransomware incident and won't need to worry about whether criminals will fulfill their part of the deal once payment has been made.

From a cost perspective, rapid, reliable recovery is more sustainable than paying the ransom every time an attack occurs (refer back to Figure 3). Also, an organization doesn't necessarily have to invest in new tools to build a rapid recovery system, as it can weave its existing backup, disaster recovery, and security assets together.

The cost of downtime can add up significantly. According to IDC's 2020 *Cost of Downtime and the Importance of Support Survey,* the average cost of downtime of on-premises workloads is $2,800 per hour, and for workloads running in the cloud, it's $3,275 per hour. These metrics include costs associated with lost productivity, potential revenue loss, costs to restore, penalties, and other fees. More alarmingly, these are average costs per workload, and ransomware attacks can bring down multiple systems at a time.

In the same survey, respondents also rated the significance of nonfinancial factors caused by downtime. Respondents were concerned that extended downtime would have negative impacts on employee morale, productivity, and company reputation. Downtime caused by ransomware brings additional costs such as potential regulatory action and legal action brought by company shareholders.

FUTURE OUTLOOK

Data protection and data security have become so intertwined that organizations now look for solutions that deliver a holistic approach to prevention, detection, and remediation. Because ransomware is constantly evolving, it is impossible to develop defenses against attack techniques that haven't yet been encountered.

To stay on top of this ever-changing threat, organizations will treat ransomware recovery as a group effort. Unusual backup or encryption activity, file name changes, and data deletion that's detected by data protection software will be shared with security and incident response teams to alert a possible breach. Similarly, threat and unusual data access can help backup admins narrow down when the last good backup copy was.

Over time, organizations will develop a ransomware response that is more proactive than reactive. In addition to a well-practiced response, steps will be taken to ensure security best practices are followed, policies are updated whenever new infrastructure is introduced, and the blast radius of any potential attack can be contained. Vendor tools from both the security and data protection side will be able to share info to assist in these efforts.

CONSIDERING VEEAM

Veeam's platform provides data protection capabilities across on-premises core, cloud, and edge repositories. Although Veeam is best known for its handling of data in virtual environments, its capabilities extend to physical infrastructure and Unix environments as well. Veeam's platform has these core modules:

- **Backup and recovery.** Protect data on premises and in the cloud using Veeam Backup, the hallmark of which is simplicity. Veeam Backup and Recovery is designed to deliver the most stringent service levels while reducing the human labor needed to manage it.

- **Orchestration.** Automate disaster recovery, documentation, testing, and compliance. Many organizations have either no disaster recovery plan or only a partial DR plan largely because of the complexity and cost of implementing a complete one. Orchestration is designed to simplify the process of recovering from a disaster by automating many of the common tasks associated with recovery.
- **Monitoring and analytics.** Using Veeam ONE, organizations can view their entire infrastructure from a single pane of glass. Veeam ONE gives insight into infrastructure optimization as well as rapid identification of data protection gaps and assurance of recovery success.

CHALLENGES AND OPPORTUNITIES

Ransomware attacks are constantly evolving, and defending against them has predominantly been reactionary. IDC believes IT leaders need to be as proactive as possible, and the technology to enable this is available.

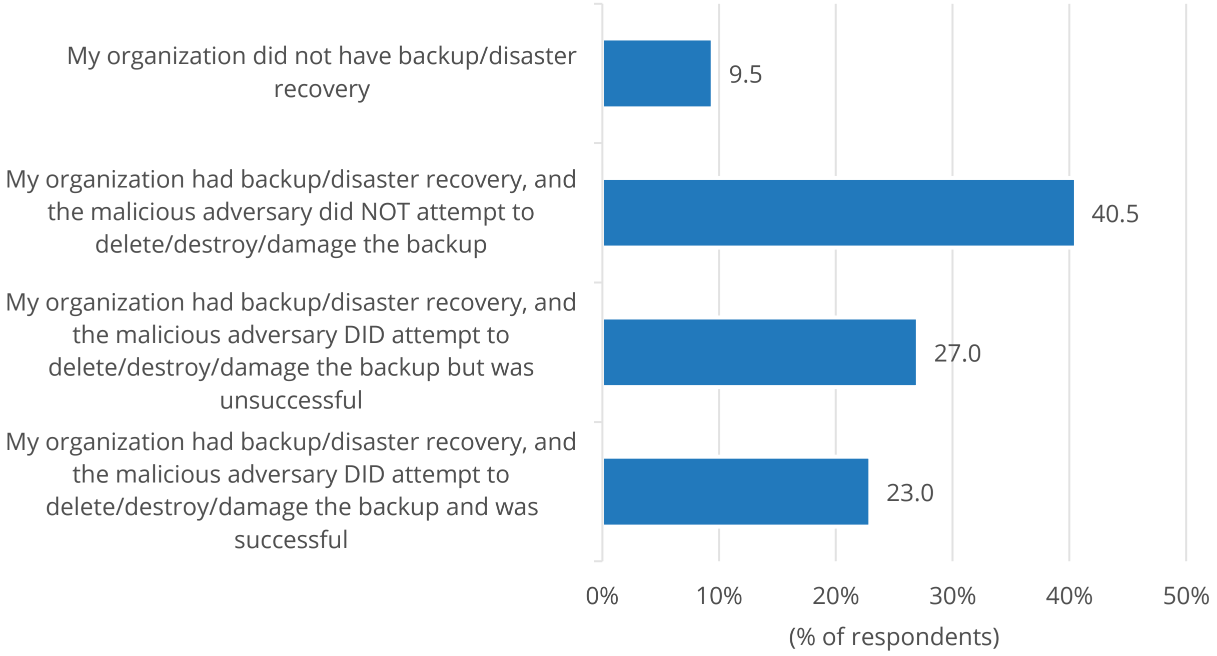
In the past, the market has offered singular products as ransomware solutions, but no single solution can address all aspects of malware and ransomware attacks. Thus IT organizations need to build the total solution and will invariably need products from both data protection and security.

Securing the backups should still be emphasized by data protection vendors, as attempting to delete backups is still a popular attack method. According to IDC's *Worldwide Future Enterprise Resiliency and Spending Survey,* half of the respondents said malicious attackers targeted their backups, and of those attempts, roughly half were successful (see Figure 4).

FIGURE 4

Ransomware Attackers Commonly Try to Disable Backups

Q. *For your most recent ransomware incident that blocked access to systems or data, what is your organization's stance regarding backup/disaster recovery?*



n = 444

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

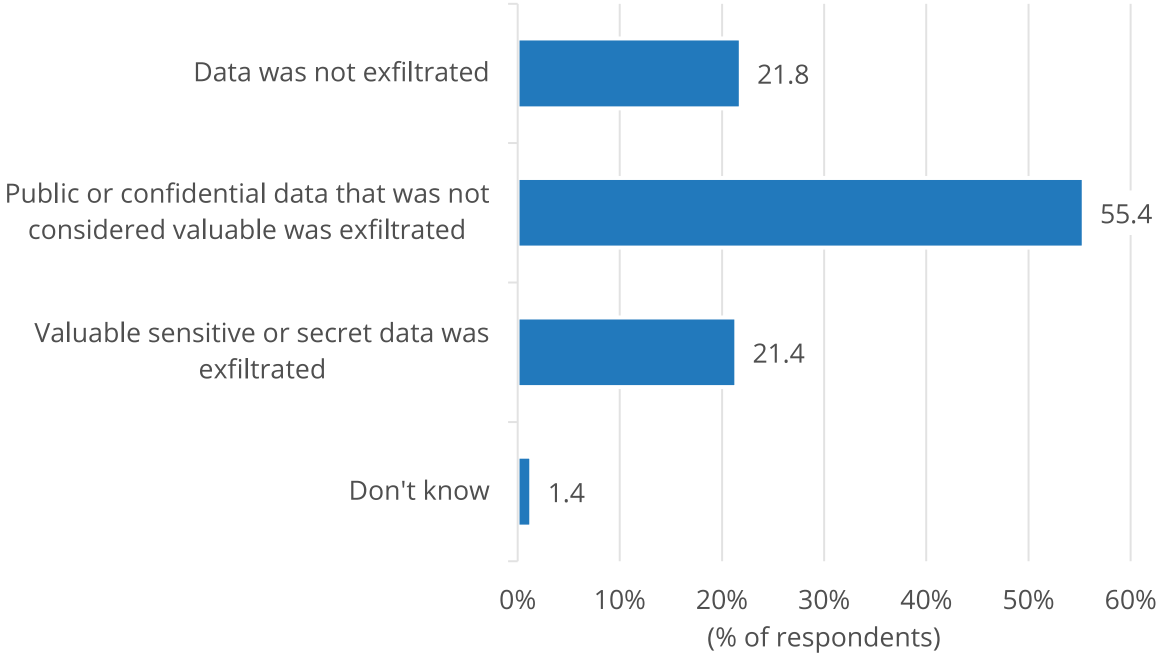
Source: IDC's *Worldwide Future Enterprise Resiliency and Spending Survey*, December 2021

The need for security is further emphasized by the increasing occurrences of data exfiltration. Nearly three-quarters of respondents who suffered a ransomware incident said data was stolen in their most recent attack (see Figure 5). Security's involvement in the data recovery and remediation process could help ensure any data that's stolen is encrypted and useless to criminals, or at least determine if anything important or sensitive was stolen.

FIGURE 5

Data Gets Stolen in More than 75% of Ransomware Incidents

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



n = 444

Notes:

Data is managed by IDC's Quantitative Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Worldwide Future Enterprise Resiliency and Spending Survey,* December 2021

Since ransomware continually evolves and IT organizations are constantly on the defensive, organizations will have to adopt more proactive stances against inevitable attacks. They will be looking to implement zero trust, threat containment, and other practices, and IT suppliers have a market opportunity in helping organizations with these implementations.

CONCLUSION

A small portion of organizations are able to fully recover from ransomware without paying the ransom, and paying the ransom is often viewed as a faster means of restoring business operations to normal. However, simply paying the ransom does not mean organizations can immediately begin recovery, nor does it ensure that data can be fully recovered.

Decryption algorithms are often slow, and time has already been spent consulting with lawyers and government agencies and negotiating with the attackers. All that time could be saved if organizations decide from minute one to start a data recovery process they are confident with.

Organizations need to build a system of assured data recovery based on the principles of detect, protect, and recover. Weaving security into data protection and recovery processes ensures integrity and enables organizations to minimize downtime in a ransomware scenario.

About IDC

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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright Notice