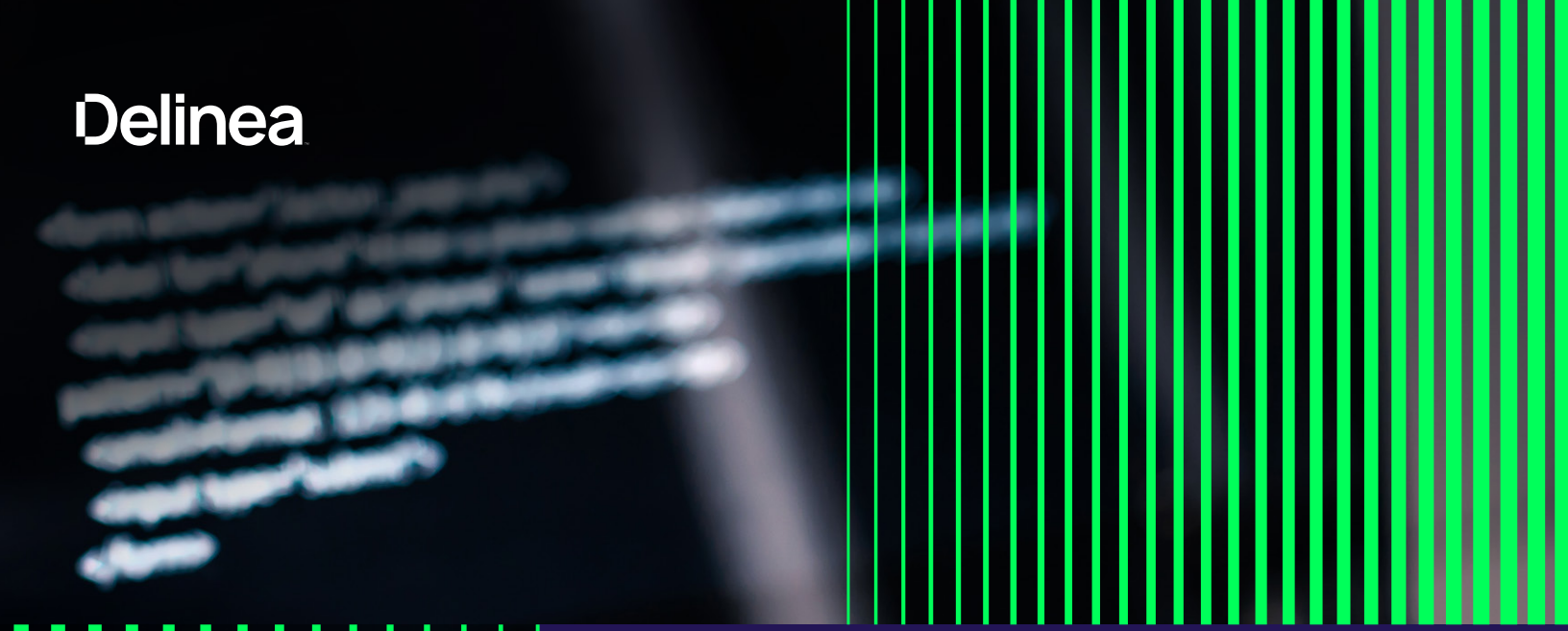
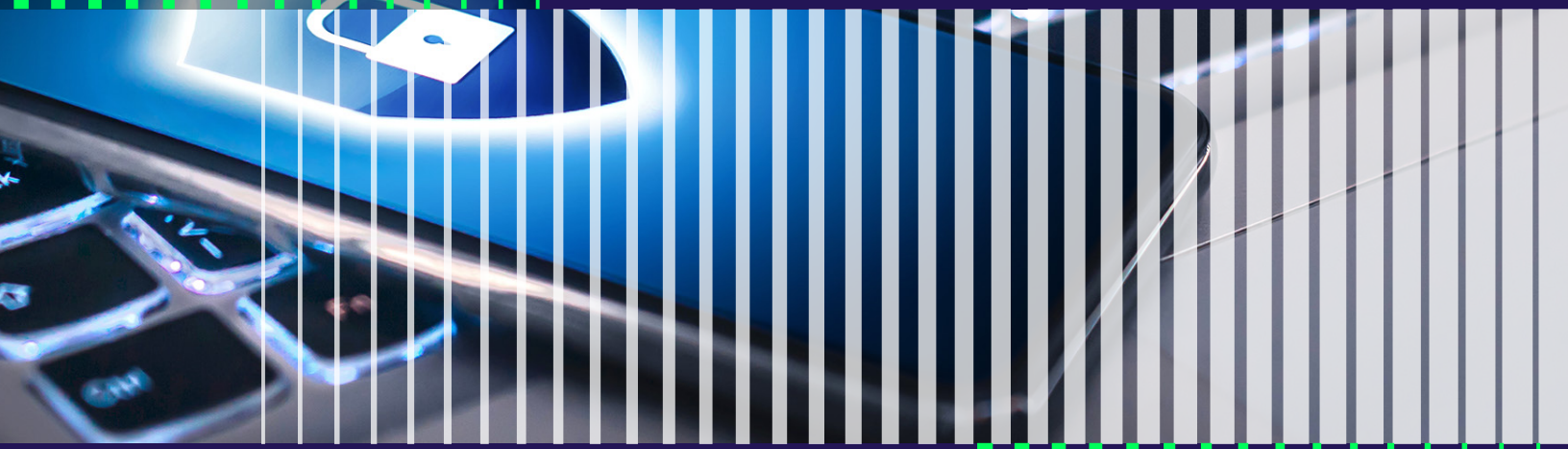
Delinea



State of Ransomware Survey Report

Making the Hard Choices for Ransomware Readiness and Response



WHITEPAPER

Executive Summary

For IT and security leaders, the moment you realize your organization has been hit with ransomware is likely one of the worst moments of your career. While it's widely understood that no organization is immune to ransomware, no one expects an attack when it happens to them.

When a ransomware attack does happen, you swing into action. You've got to figure out what systems are affected and how your business and customers are impacted. From a technical perspective, you need to uncover which security controls failed or need to be fortified. Depending on regulatory requirements, you may need to report the attack and inform the impacted victims.

The worst part of all this is you must decide whether to pay the ransom.

This is the scenario we envisioned when we set out to understand how IT and security leaders grapple with the tough decisions surrounding ransomware. In our second annual ransomware research report, we surveyed over 300 IT and security decision-makers across the United States from a variety of industries to get insights from the folks in the trenches of ransomware preparedness and incident response. We compared year-over-year results to see how things have changed from 2021 to 2022.

We found that just as ransomware tactics are evolving, so are perspectives on the best way to prepare and respond.

Key takeaways from the study:

1. **Ransomware is decreasing — but don't start celebrating yet**
2. **Diverse ransomware motivations make every organization a potential victim**
3. **More companies are saying no to ransomware payments, even as business suffers**
4. **Companies are stagnating or backsliding in the ransomware fight**
5. **Support for making ransomware payments illegal has steeply declined**

Read on for details of the survey findings, along with context and analysis of what they mean for your business. See how your peers are adjusting their behaviors so you can benchmark your ransomware strategies. What you learn will help you prioritize your cybersecurity, incident response, and crisis management plans.

Types of ransomware

Crypto ransomware, such as WannaCry and Petya, encrypts your data so it's unreadable. The perpetrator extorts money from compromised users in exchange for a decryption key.

Exfiltration, also known as doxware or leakware, is when a malicious actor steals sensitive data and threatens to release it publicly, unless they're paid a ransom.

Distributed denial-of-service (DDoS) ransomware attacks target your network services, not your data. Spurious connection requests flood your servers to bring them to a standstill.

Screen lockers prevent access to a computer or device (not your data) until you meet the attacker's ransom demands.

KEY FINDINGS 1:

Ransomware is decreasing — but don't start celebrating yet

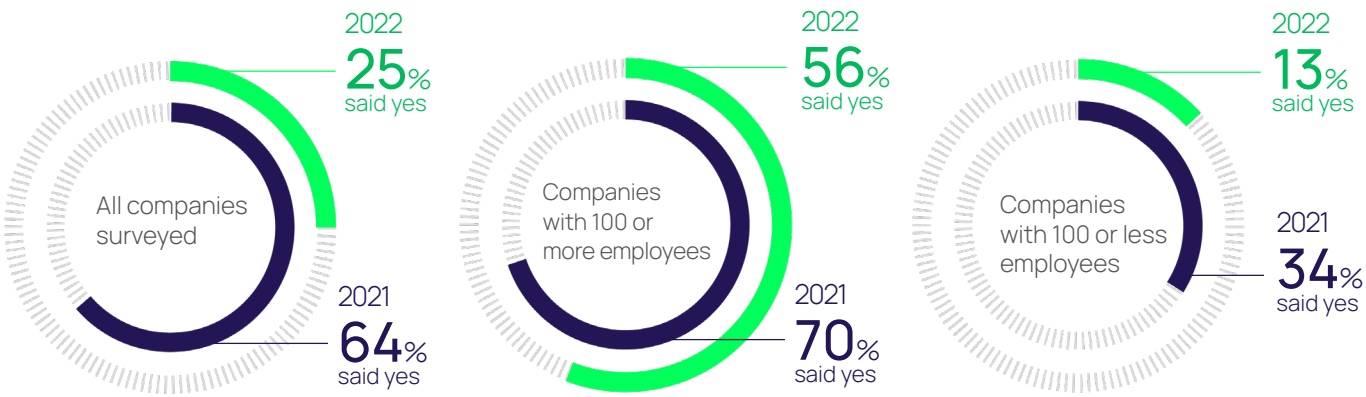
Only 25% of respondents in this year's survey said they were victims of ransomware over the past 12 months. This is a sharp decrease from last year's overall ransomware attack rate of 64%.

The larger the company, the more likely they were to be victimized.

Companies with 100 or more employees experienced ransomware attacks at a rate of 56% in 2022, compared with 70% in 2021 (a decrease of 14 percentage points).

Meanwhile, 13% of companies with less than 100 employees said they were victims of ransomware this year, compared with 34% in the previous survey (a decrease of 21 percentage points).

Q. Has your company been the victim of a ransomware attack in the last 12 months?



Behind the numbers

There are many potential reasons for the recent decrease in ransomware attack volume. One contributor may be the disbanding of prominent ransomware group Conti. It's also possible that ransomware-preventing security control implementations have been at least somewhat successful in deterring or blocking attacks. The cynical among us might say that it's the number of companies that *admit* to ransomware attacks which is declining.

The fact is these findings support primary cyber industry research indicating a slowdown in ransomware attacks toward the end of 2022. GuidePoint Research, for example, reported a 35% slowdown in ransomware attacks in the second quarter of 2022 compared to the first quarter.[i] Digital Shadows, which conducts daily monitoring of ransomware groups, reported a 10% decline from the second quarter of 2022 to the third.[ii]

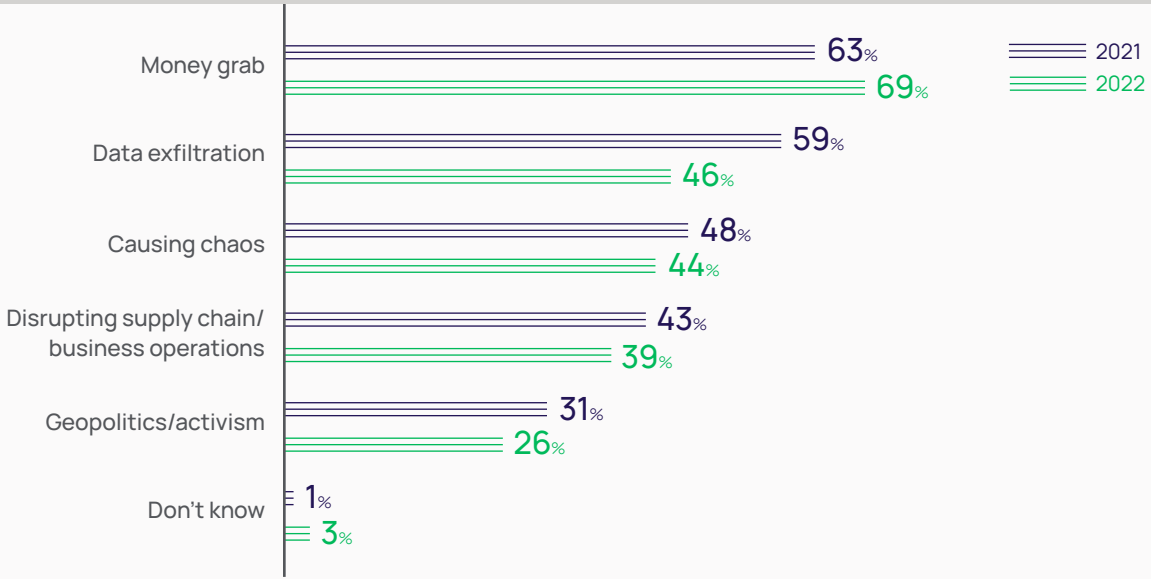
It's important to note that while the volume of attacks appears to be decreasing, the average ransomware payment is increasing. The payments in cases worked by Unit 42 incident responders were nearly $1 million in the first five months of 2022, a 71% increase over the same period the previous year. On top of payments, companies are also paying for remediation expenses, downtime, and reputational harm.[iii]

The cybersecurity industry will be keeping a close eye on this trend. Though the decline in attack volume is good news in the short term, this period of decline may simply represent a gap in activity as ransomware groups gather their resources. The fourth quarter of the year is historically a peak period of ransomware activity, as cybercriminals take advantage of the increase in e-commerce activity around the holidays, so it's important for companies of all industries and sizes to stay on guard.[iv]

KEY FINDINGS 2:
Diverse ransomware motivations make every organization a potential victim

Survey respondents recognize multiple motivations for ransomware attacks. In addition to the desire for financial reward, they believe perpetrators are looking to create problems for businesses and society.

Q. What do you consider the most prominent motivation for ransomware attacks today? (Check up to 3)



Behind the numbers

To achieve these diverse goals, cybercriminals aren't just after corporations with deep pockets. They may target government agencies or organizations with agendas they don't agree with. They may take down infrastructure or public services. Some worry that Russia's war in Ukraine has increased the threat of cyberattacks against U.S. targets, as many ransomware operators are based in Russia.[v]

Other perpetrators may not even have specific targets for their criminal activity. Take Non-Petya, for example, this attack method wasn't considered "ransomware" in the strictest sense because there was no decryption key and thus nothing was held for ransom. The malware was released indiscriminately, purely with the intention of causing widespread chaos and destruction.

A more recent example is Azov Ransomware, a data wiper that intentionally destroys victims' data and infects other programs. It was distributed worldwide with the goal of causing mass chaos, rather than monetary gain. In this case, the ransom note told victims to contact security researchers and journalists to frame them as developers of the ransomware.

The bottom line is that as ransomware spreads, everyone is at risk.

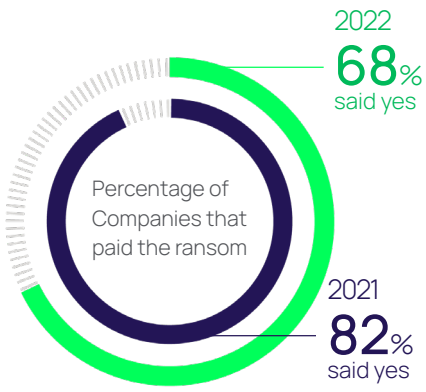
KEY FINDINGS 3:
More companies say no to ransomware payments, even as business suffers

Most ransomware victims do end up paying so they can get back control of their data and systems. However, according to the survey, an increasing percentage of companies are refusing to pay their attackers.

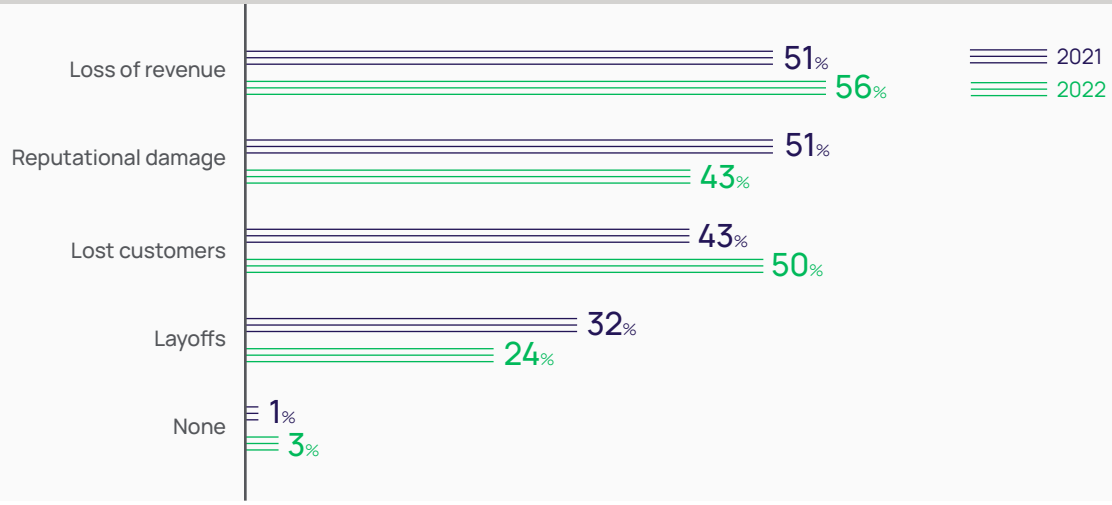
Sixty-eight percent of companies that experienced a ransomware attack in the past 12 months paid the ransom. In the industry that experienced the most ransomware attacks – IT/technology – 77% paid up. In contrast, last year 82% of companies said they paid the ransom and no industry surveyed had less than a 72% payment rate.

Even as willingness to pay decreased this year, the business impact of ransomware attacks continues to be wide-ranging.

Q. If your company has been the victim of a ransomware attack in the last 12 months, did your company pay the ransom?



Q. If your company has been the victim of a ransomware attack in the last 12 months, what, if anything, did your company experience as a result? (check all that apply)



Even as willingness to pay decreased this year, the business impact of ransomware attacks continues to be wide-ranging.

Behind the numbers

With such varied impacts, why are fewer companies paying up? There are a few potential reasons.

Perhaps companies are beginning to follow advice from the FBI, which is raising the alarm that paying a ransom doesn't guarantee data will be returned. The government also warns that capitulating to perpetrators encourages them to target more victims and offers an incentive for others to conduct this type of illegal activity.[vi]

Smart investment in data backup strategies may also help companies combat ransomware that encrypts data and/or locks up systems. If you're able to recover critical data quickly, you don't need to capitulate to an attacker to keep your business running.

Thirdly, reliance on cyber insurance may be helping organizations transfer the risk of ransomware, as they'd rather rely on their insurance to cover the costs than pay the ransom. This strategy is far from certain, however, as some insurance companies refuse to pay for ransomware costs and/or may not cover all costs involved.

KEY FINDINGS 4:
Companies are stagnating or backsliding in the ransomware fight

Last year, 94% of organizations said they had an incident response plan. In this year's survey, only 71% said they had one in place.

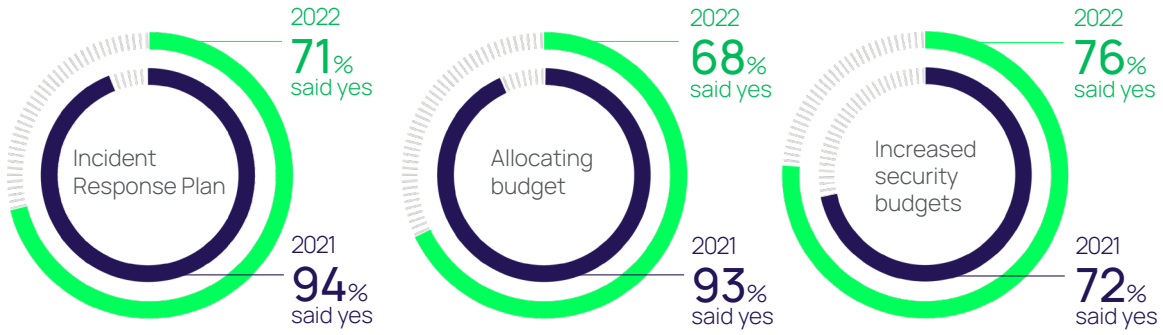
What's more, only 68% of companies said they're currently allocating budget to protect against ransomware. This is in sharp contrast to the 93% of respondents who said they were allocating budget to protect against ransomware in 2021.

After suffering a ransomware attack, however, 76% of companies increased security budgets as a result. This is similar to last year's finding that 72% of companies received a bump in their budget following an attack.

This finding underscores the results of Delinea's recent cyber insurance survey, which found that companies often receive more budget for security resources and tools after they've suffered a cyberattack.[vii]

This lack of preparedness is alarming, especially considering the many attack vectors IT and security leaders surveyed recognize that may let ransomware into their organization.

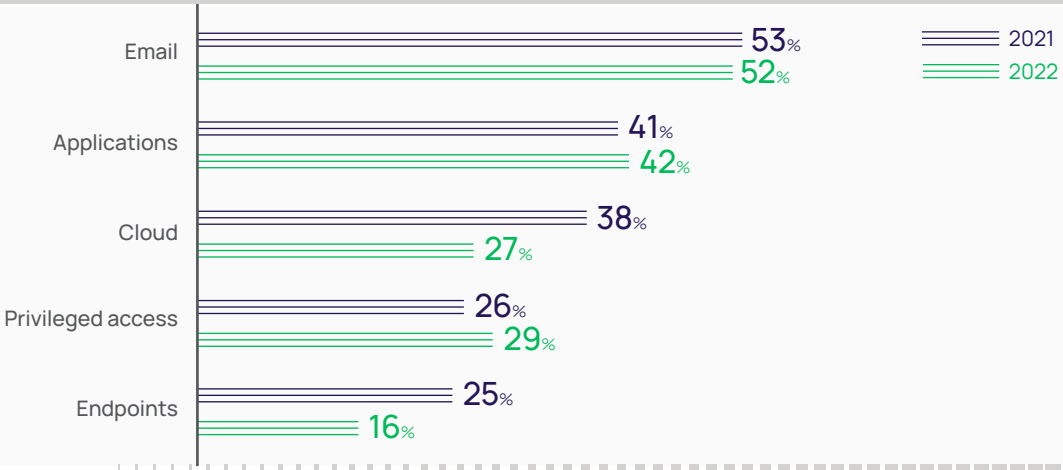
Q. Is your company allocating budget to protect against ransomware in its annual budget?



Dangers lurk on many fronts

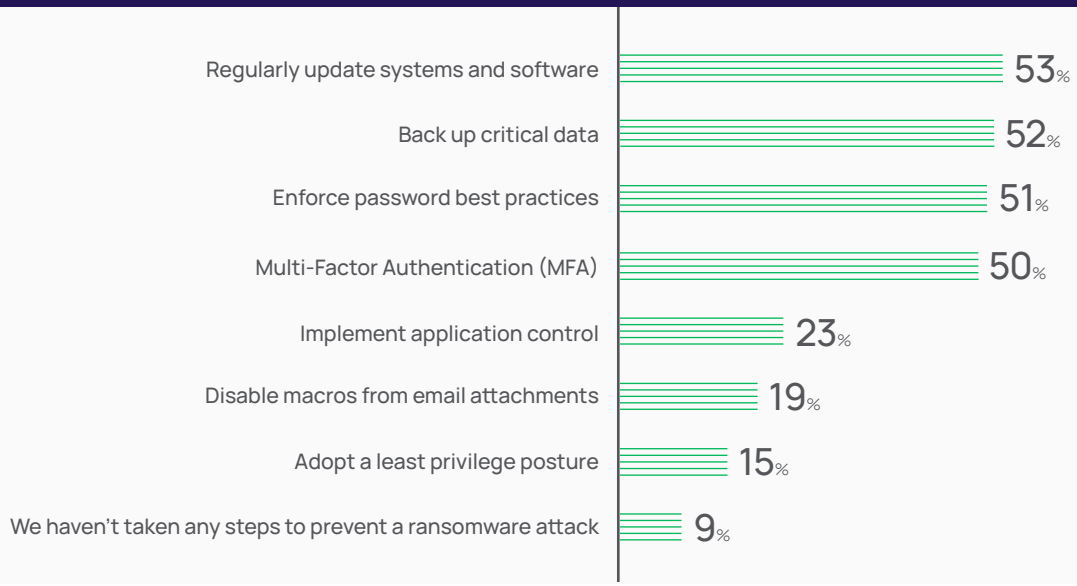
Respondents worry about vulnerabilities throughout their organizations. Awareness of privileged access as an attack vector has increased slightly, while respondents are less concerned about cloud platforms and endpoints than they were last year.

Q. What, if anything, do you consider the most vulnerable vectors for ransomware attacks? (Check up to 2)



Delinea

Q. What, if any, steps have you taken to prevent a ransomware attack?



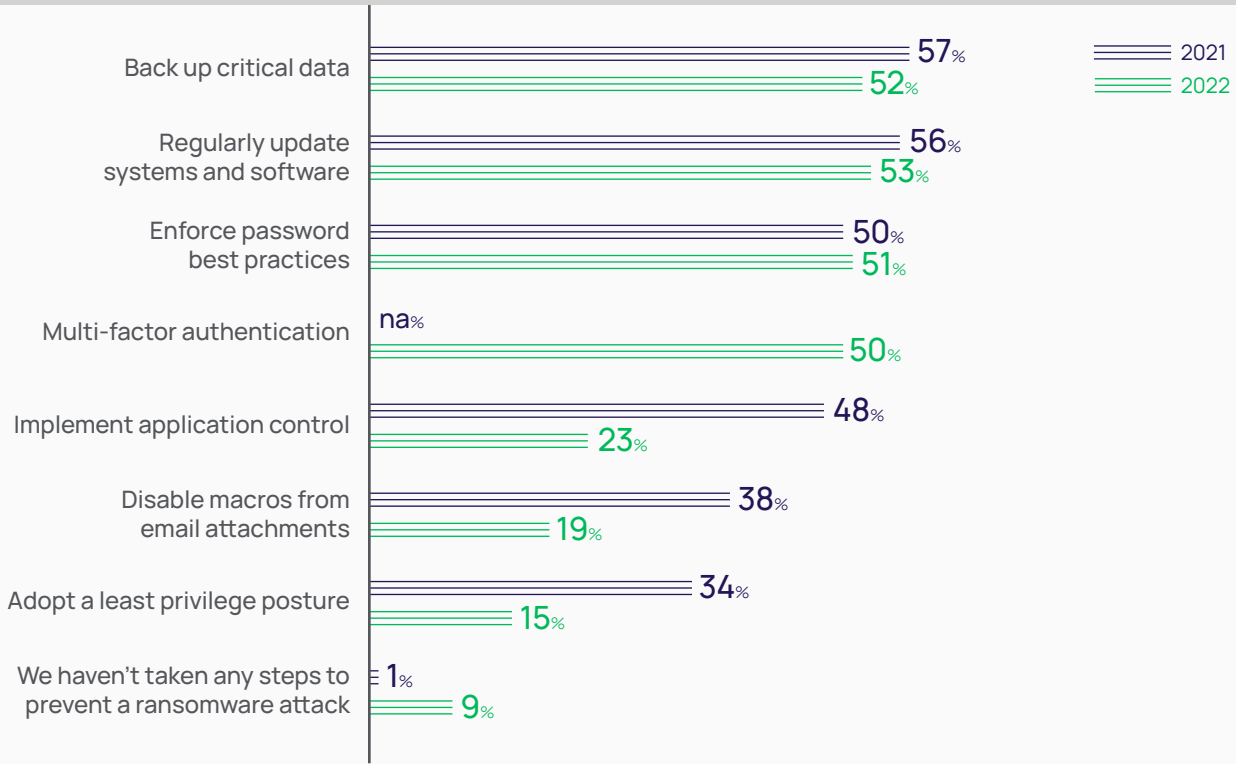
Gaps in security strategies make companies vulnerable to ransomware attacks

Similar to last year, only slightly more than half of organizations say they back up data, regularly update systems, or enforce password best practices. This year we asked about Multi-Factor Authentication (MFA) and learned that only half of the organizations are implementing it for ransomware protection.

Other cybersecurity strategies, such as application control, disabling macros from email attachments, and least privilege policies, have dropped in popularity, with less than a quarter of organizations now leveraging them.

According to the findings, least privilege becomes a more popular security strategy as companies grow larger. More than one third of larger companies follow least privilege best practices, approximately 3x the rate of smaller companies.

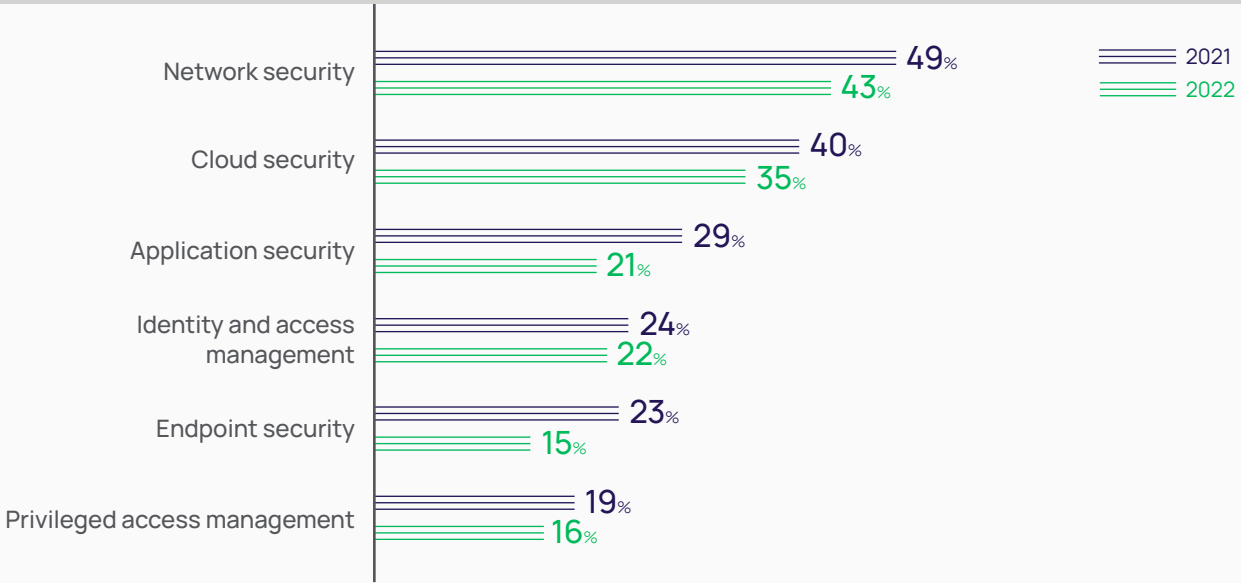
Q. What, if any, steps have you taken to prevent a ransomware attack? (Check all that apply)



Investments in ransomware prevention are declining

In terms of investment size, security strategies decreased slightly but overall remain roughly the same as last year. The largest percentage of companies reporting that network security represents their biggest investment.

Q. In what area, if any, do you invest the most to prevent ransomware? (Check up to 2)



Evolution of ransomware as a team sport

Ransomware-as-a-Service has enabled experts to specialize in specific areas of the ransomware supply chain, making it easy for cybercriminals to target victims and deploy ransomware.

Today, all a cybercriminal needs to launch a successful ransomware attack is an internet connection and the right friends/affiliations.

The ransomware supply chain involves gangs of criminals who pool their skills and share in the profits. A gang will typically include encryption specialists, black hat cybercriminals who gain access and sell it, hands-on keyboard attackers who abuse stolen access, and the criminal who negotiates the ransom and manages the payment distribution.

Behind the numbers

Traditionally, network protection has been a primary choice for cyber protection as it consists of a clearly defined network perimeter which made it easier to keep the bad guys out and the good guys in. Today, however, business activity takes place inside, outside, and across networks, as more organizations continue remote workstyles and partner with third-party organizations.

Based on the findings of this survey, Privileged Access Management (PAM) is a key ransomware prevention strategy that is often underutilized. It provides more bang for the buck as it's less expensive and easier to implement than many of the other strategies listed above.

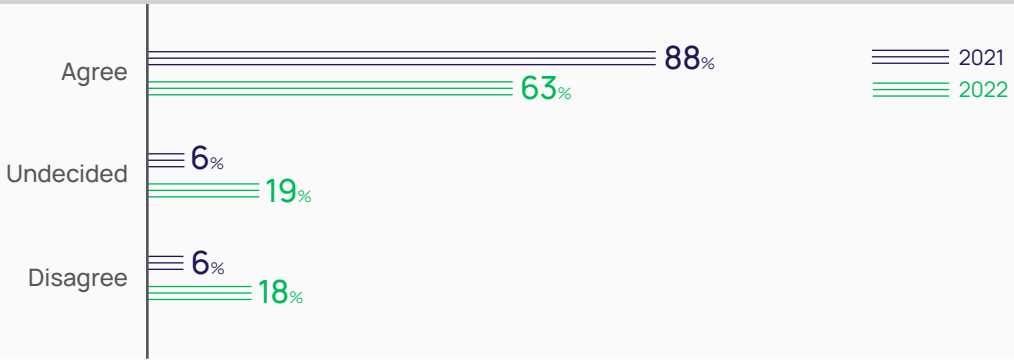
Following the principle of least privilege should not be an optional security strategy. By providing users only with the privileges they need, when they need them, you immediately limit the damage that a malicious insider or cybercriminal can do. Limited privileges mean that even if ransomware gains access to your organization, the damage can be quickly contained.

Having a plan for incident response is key. Create a plan, test it, and refine it so that you can move fast. The faster you can detect ransomware and take action, the less damage will be done.

KEY FINDINGS 5:
Support for making ransomware payments illegal has steeply declined

Last year, we found that support for making ransomware payments illegal was extremely high, with 88% of respondents agreeing or strongly agreeing with the idea. This year, that number dropped to 63%.

Q. To what extent do you agree or disagree that it should be illegal for companies to pay ransom?



Behind the numbers

The implications of making ransomware payments illegal are widely debated, with convincing arguments on both sides. On one hand, a legal ban may appeal to organizations that want to remove the responsibility of the decision from their shoulders. However, faced with the very real possibility of ransomware gangs holding their data and systems hostage, some companies feel caught between a rock and a hard place: refuse to pay the ransom and risk losing their business, or pay the ransom AND suffer the legal consequences.

During the past year, the way governments legislate ransomware response has been evolving. In March 2022, Congress gave the U.S. Federal government much greater visibility into hacking efforts that target private companies by requiring that affected companies must report when they've paid a ransom. In addition, The U.S. Treasury Department recently warned that it could punish anyone who pays ransom to individuals or organizations that are on its sanctions list. Several U.S. states have recently moved to ban local and state agencies, along with related organizations from paying ransoms. Still, legislation has not gone as far as the EU, which says member states can impose fines for paying ransoms under the Security of Network and Information Systems Directive.

Keep an eye out for more changes as governments contend with the ongoing threat of ransomware. Gartner has predicted that the percentage of countries passing legislation to regulate ransomware payments, fines and negotiations will rise to 30% by the end of 2025, compared to less than 1% in 2021.[viii]

Conclusion and next steps

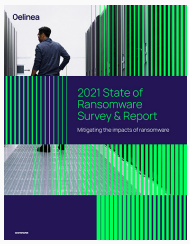
Though ransomware has become the norm, businesses can't afford to become complacent. Government action and cyber insurance offer no guarantees for recovery. Cyber resilience is essential for customer trust and business growth.

The ransomware landscape is evolving rapidly as criminals, enterprises, and governments test new strategies to reach their goals. Attack motivations and techniques are changing, which means your preparedness and response must change as well.

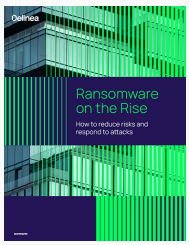
To combat ransomware, it's critical to fortify your defenses, including endpoint protection and access control. Having a backup strategy that enables you to recover quickly can help you avoid paying a ransom and allow you to get back to business as usual. Get your incident response plan in place, test it, and refine it. With these strategies in place, when an attack occurs, instead of panicking, you can act with confidence.

Resources to combat ransomware

Ransomware

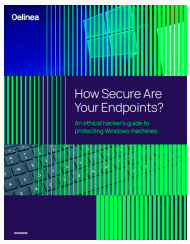


Ransomware Survey Report 2021



Ransomware on the Rise Whitepaper

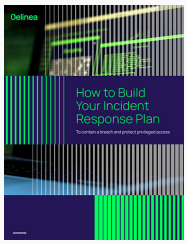
Endpoint protection



Guide to Securing Windows Endpoints

Least Privilege Discovery Tool

Incident response



Incident Response Plan Checklist

Customizable Incident Response Template

Cyber Insurance

Cyber Insurance Checklist

Cyber Insurance Survey Report

Cyber Insurance Webinar

Endnotes

i. https://www.guidepointsecurity.com/newsroom/ransomware-attacks-slowing-as-2022-wears-on/

ii. https://www.digitalshadows.com/blog-and-research/ransomware-in-q3-2022/

iii. https://www.paloaltonetworks.com/blog/2022/06/average-ransomware-payment-update/#:~:text=The%20numbers%20are%20startling%3A%20The,rose%2071%25%20from%20last%20year.

iv. https://darktrace.com/newsroom/darktrace-reports-30-more-ransomware-attacks-targeting-organizations-during-the-holiday-period-e

v. https://www.usatoday.com/story/news/nation/2022/03/08/ukraine-war-could-mean-russian-attacks-us-cyber-networks/9431219002/?gnt-cfr=1

vi. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

vii. https://delinea.com/resources/cyber-insurance-survey-report-results

viii. https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio#

Delinea

Defining the boundaries of access

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**