Delinea

WHITEPAPER

State of Ransomware 2024

Anticipating the battle and strengthening your defenses

Executive Summary

The battle against ransomware in 2024 requires a comprehensive and multi-layered defense strategy.

In the past year, ransomware adopted a more insidious approach, with greater emphasis on data exfiltration and increased stealth. Cybercriminals are strategically extracting sensitive data without necessarily delivering the destructive encryption payloads that we have seen in the past. This stealth enhances attackers' ability to operate without raising alarms and without disrupting the victim's business operations. Ransomware victims must pay to prevent the exposure of confidential information.

In our annual ransomware study, 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. We compared year-over-year results to see how attitudes and strategies have changed. In this report you'll learn how organizations are adopting proactive measures to detect, mitigate, and prevent ransomware attacks, enabling you to make informed choices for your own security program.

Key takeaways from the study:

1. **Ransomware and its impact are rising after a decrease in the previous year**
   - The number of ransomware victims has significantly increased
   - More victims are agreeing to pay ransoms
   - Revenue loss is the biggest negative consequence

2. **A larger security budget doesn't guarantee better security**
   - Almost all respondents have a dedicated ransomware budget
   - Fewer companies received a post-attack budget bump
   - Top executives and boards are clearly concerned

3. **Stealth attacks require multi-layered defenses**
   - Attackers' techniques shift to data exfiltration
   - Cloud and applications overtake email as the top attack vectors
   - Investment in Privileged Access Management (PAM) significantly increases
   - Incident response plans are more commonly adopted and used

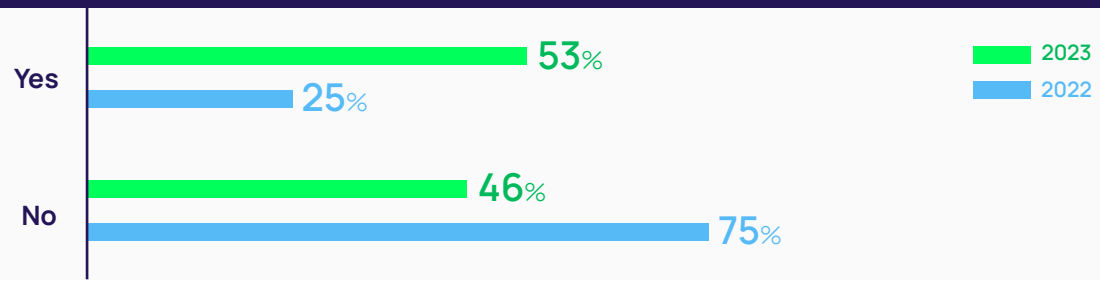
Read on for details of the survey findings, along with context and analysis of what they mean for your business. See how your peers are adjusting their behaviors so you can benchmark your ransomware strategies. What you learn will help you prioritize your cybersecurity, incident response, and crisis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

Key Finding 1

Ransomware and its impact are rising after a decrease the previous year

The number of Ransomware victims have significantly increased in the past year. Based on the findings of this survey, just over half of companies were impacted by ransomware in the last 12 months. This is double the percentage compared with the previous year's report indicating a steep rise in ransomware victims, and a return to the year-over-year increase in ransomware incidents we've seen prior to 2022.

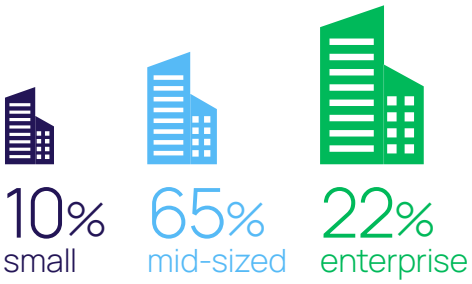
Figure 1 | Has your company been the victim of a ransomware attack in the last 12 months?



Among survey respondents this year, ransomware attacks affected a higher percentage of mid-sized companies (65%) compared with small business under 50 employees (10%), and enterprises over 500 employees (22%).

Based on these findings and additional sources, 2023 has been a boon year for ransomware. Many sources report an increase in ransomware over 2022. BlackFog's monthly ransomware report found that publicized attacks increased 49% in the first half of the year. By October of 2023, the number of ransomware victims reported to Corvus Insurance had already exceeded the total for 2022, representing a 70% YoY increase.

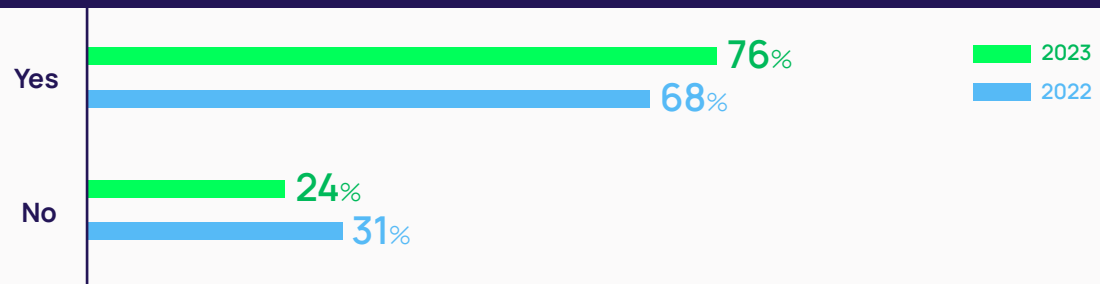
Businesses affected by ransomware attacks in 2023



More victims are agreeing to pay

Faced with the potentially crippling consequences of ransomware, companies are opting to meet ransom demands as a pragmatic response to mitigate the impact.

Figure 2 | If your company has been the victim of a ransomware attack in the last 12 months, did your company pay the ransom?

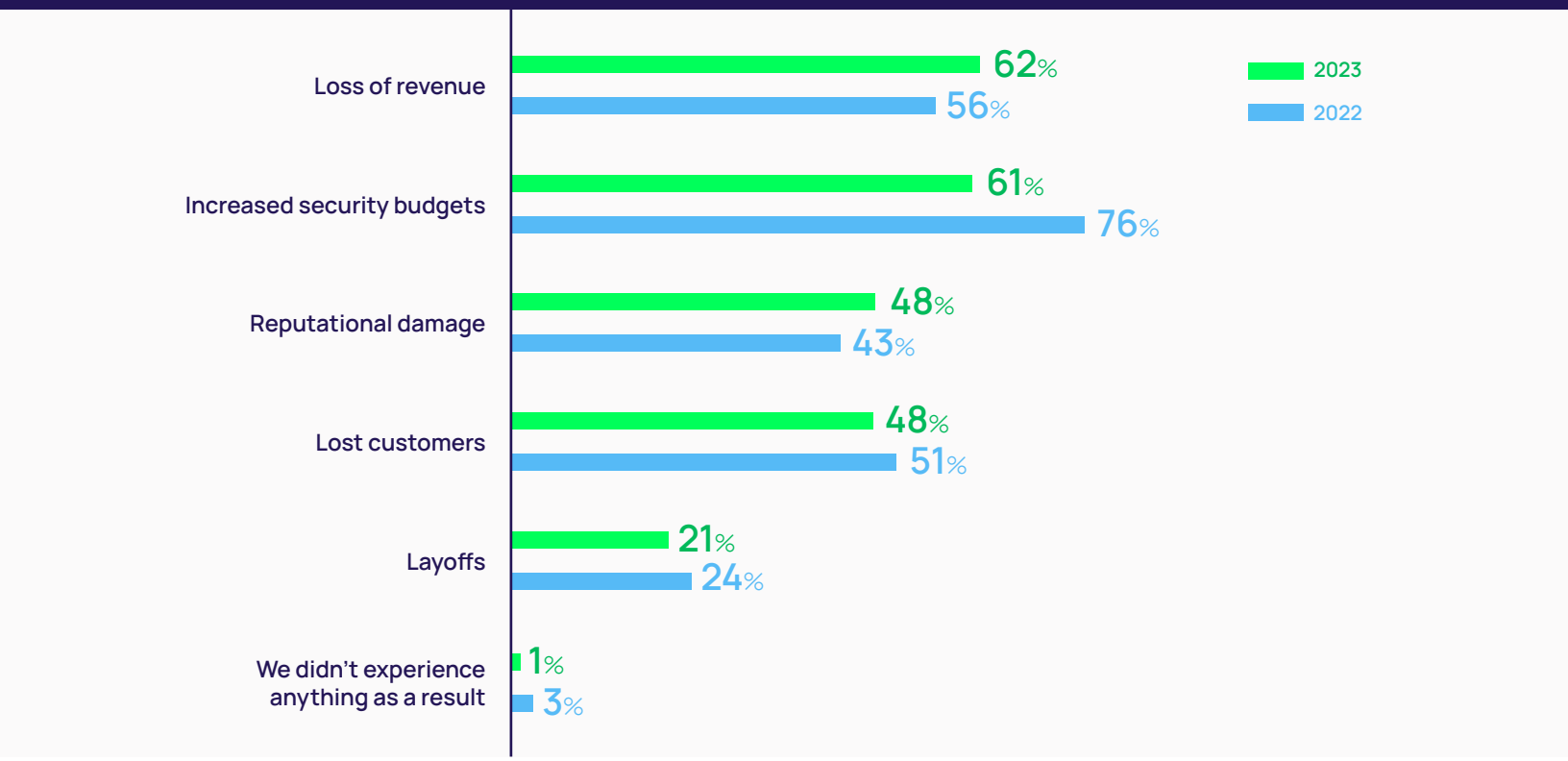


One reason for the willingness to pay may be the rise of cyber insurance. Insurance has provided organizations with a financial safety net, offering coverage for ransom payments and associated costs, thereby influencing the decision-making process.

Revenue loss is the biggest negative consequence

Regardless of whether ransomware payments were covered by cyber insurance or company savings, the cost of ransomware is high, with long-term impact for those affected. Almost all ransomware victims surveyed had some negative result to their business.

Figure 3 | 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)?



Most respondents tie the impact of ransomware directly to loss of business revenue. Businesses lost revenue due to disruptions in operations and inability to deliver services. Ransomware attacks often paralyze critical systems, leading to extended periods of unproductivity and revenue loss as organizations work to recover. But that's not all –reputational damage that deters customers and partners also has a future impact on revenue.

The strain imposed by ransomware incidents, coupled with the financial ramifications, leads some organizations to reduce their workforce. Though least common among the consequences reported by survey participants, the number of layoffs is significant, with one in five organizations streamlining their workforce as a direct consequence of ransomware attacks.

Most companies increased their security budgets following a ransomware attack. That said, a smaller percentage of companies received a post-attack budget bump than last year. There could be many reasons for this decline. It may be an unfortunate but necessary result of economic uncertainty and contraction. This change could also be a recognition that although budgets increased last year, that alone didn't stop the tide of ransomware.

Costs of ransomware attacks

Ransomware costs can be difficult to discern, especially as many attacks go unreported. At the end of 2023, SEC disclosure requirements for public companies have increased transparency, giving the cyber community more information on costs and the material impact of ransomware incidents. Redmond and BlackFog recently reported the following:

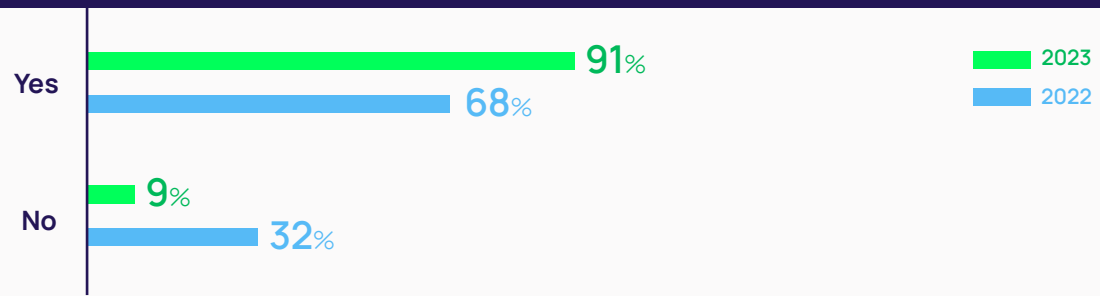
- **Clorox** had a $350M ransomware incident.
- **MGM** incurred over $100M in costs, plus $10M in clean-up fees.
- **Capita**, a British outsourcing company, was hit by a ransomware attack that cost up to $25M for recovery and remediation, as well as additional security investments. Their share price dropped 12%.
- **Dallas City Council** approved $8.6M for services relating to their ransomware attack, including credit monitoring for potential identity theft victims.

Key Finding 2

A larger security budget doesn't guarantee better security

Almost all survey respondents (91%) have a dedicated budget to protect against ransomware, a much higher percentage than 2022. For some, that budget may be a result of their post-attack increase from last year.

Figure 4 | Is your company allocating budget to protect against ransomware in its annual budget?

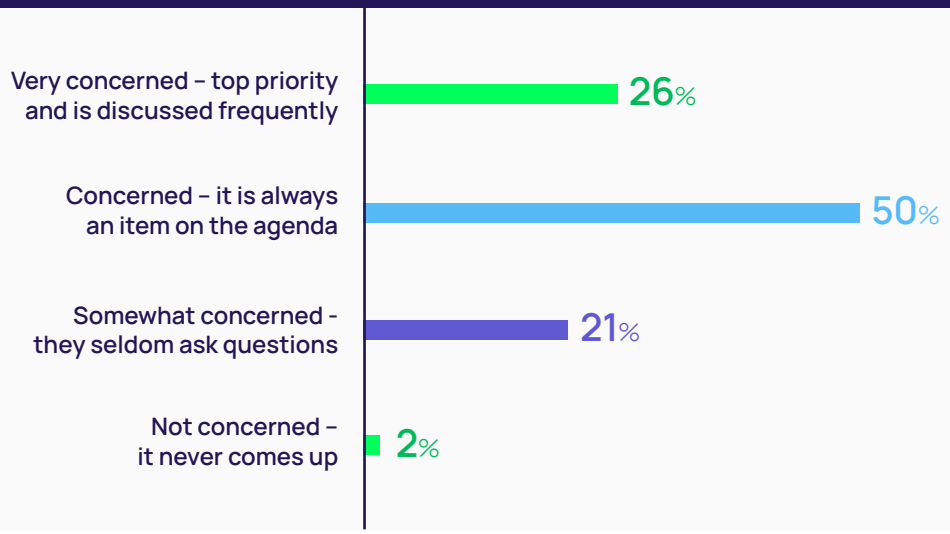


As we can see from the increased incidence of ransomware attacks, having more money doesn't mean better security. Security comes down to whether you spend that money wisely on the right cybersecurity strategy. Ransomware prevention in today's cybersecurity landscape goes beyond simply allocating more budget; it hinges on cultivating a comprehensive and strategic defense approach, and that starts at the top.

Executives and Boards are listening but not all are acting

Survey respondents resoundingly report that their leadership is concerned about ransomware. It's a top priority for one-quarter of leadership teams and an ongoing item on the agenda for half.

Figure 5 | Which statement below best describes your board and executive leadership team's concerns about ransomware targeting your organization?



Interestingly, cybersecurity and information security team members perceive that the ransomware topic is much higher on the executive agenda than do their counterparts in IT functions.

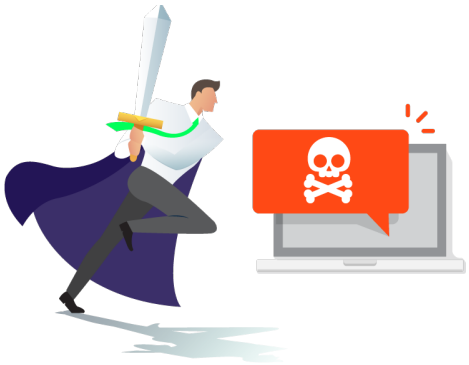
However, having ransomware on the agenda doesn't necessarily mean all parties understand the risk, or that actions are taken. In some cases, this doesn't happen until an organization becomes a victim.

An effective ransomware prevention strategy centers on a proactive cybersecurity program that emphasizes detection and resiliency. This approach not only safeguards against immediate threats but also builds a foundation for long-term security, making it increasingly clear that the quality of cybersecurity measures matters as much as the quantity of the budget allocated.

The highest levels of an organization should be aligned on the risk of ransomware, as well as the plan should an attack take place. Ransomware incident response should be a regular part of your company's business continuity and disaster recovery planning.

Security leaders have the responsibility to ensure leadership agrees on the answers to key questions, such as:

- How much risk are you willing to take on?
- Which assets and data represent the highest risk to your organization?
- At what point would a ransomware attack become "material"?
- Who can make the decision to pay or not pay a ransom demand?



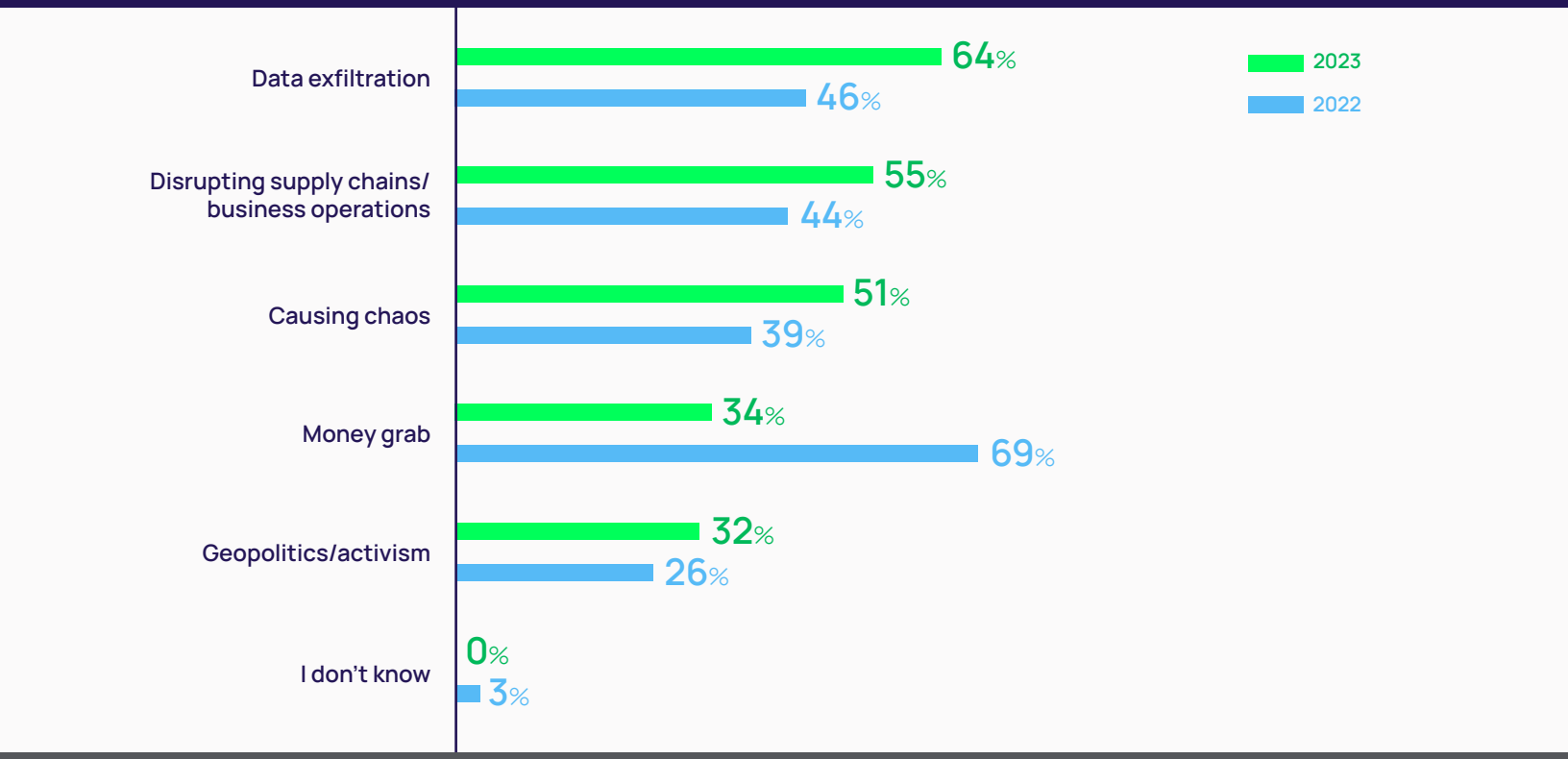
Key Finding 3

Stealth attacks require multi-layered defenses

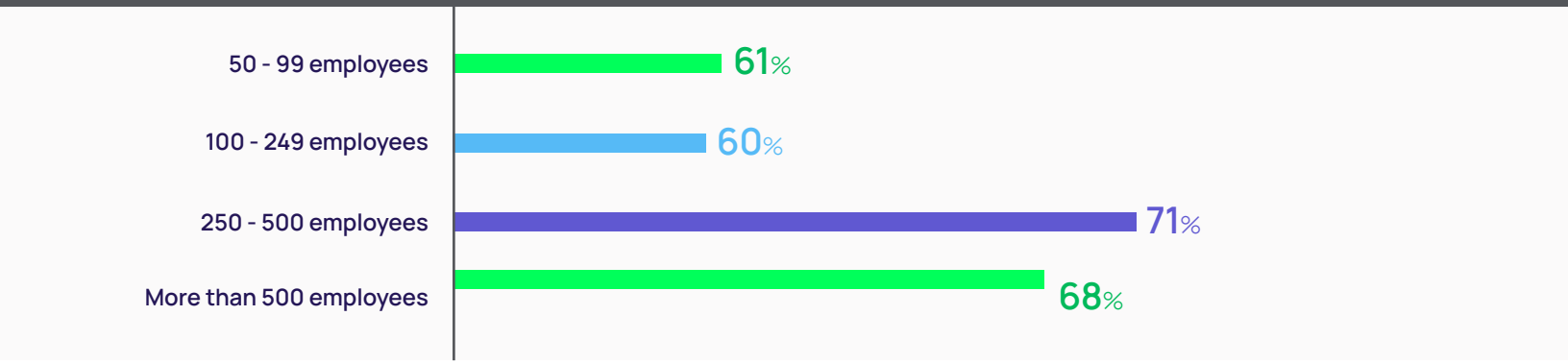
Attackers' motivations shift to data exfiltration

Survey respondents believe attackers' motivations have changed in the past year, from a straightforward money grab toward data exfiltration. The larger the organization, the more concerned they are about losing control of private and sensitive data.

Figure 6 | What do you consider the most prominent motivation for ransomware attacks today? (Tick up to three)



Data Exfiltration a reported motivation by Company Size



In a traditional ransomware scenario, an attacker delivers a payload that encrypts files and only provides the decryption key after the victim pays up. In a data exfiltration scenario, the attacker has opportunities to make money by either forcing the victim to pay the attacker to not disclose the data or by selling the data on the darknet.

In an attack that involves data exfiltration (criminals' access to sensitive data) — often intellectual property, personal information, or other sensitive, protected data — and transfer it to a remote system under criminal control. They can threaten to expose the data publicly unless the victim pays, and/or they can sell the data to other criminals who will weaponize it for alternative crimes. Some criminals release a bit of data at a time, which creates additional pressure for the victim to pay as the breach becomes public.

Data exfiltration tactics stay under a cybersecurity team's radar more easily than a sudden shutdown of operations. Covert data exfiltration tactics give attackers continuous access, enabling them to ramp up the damage when they choose.

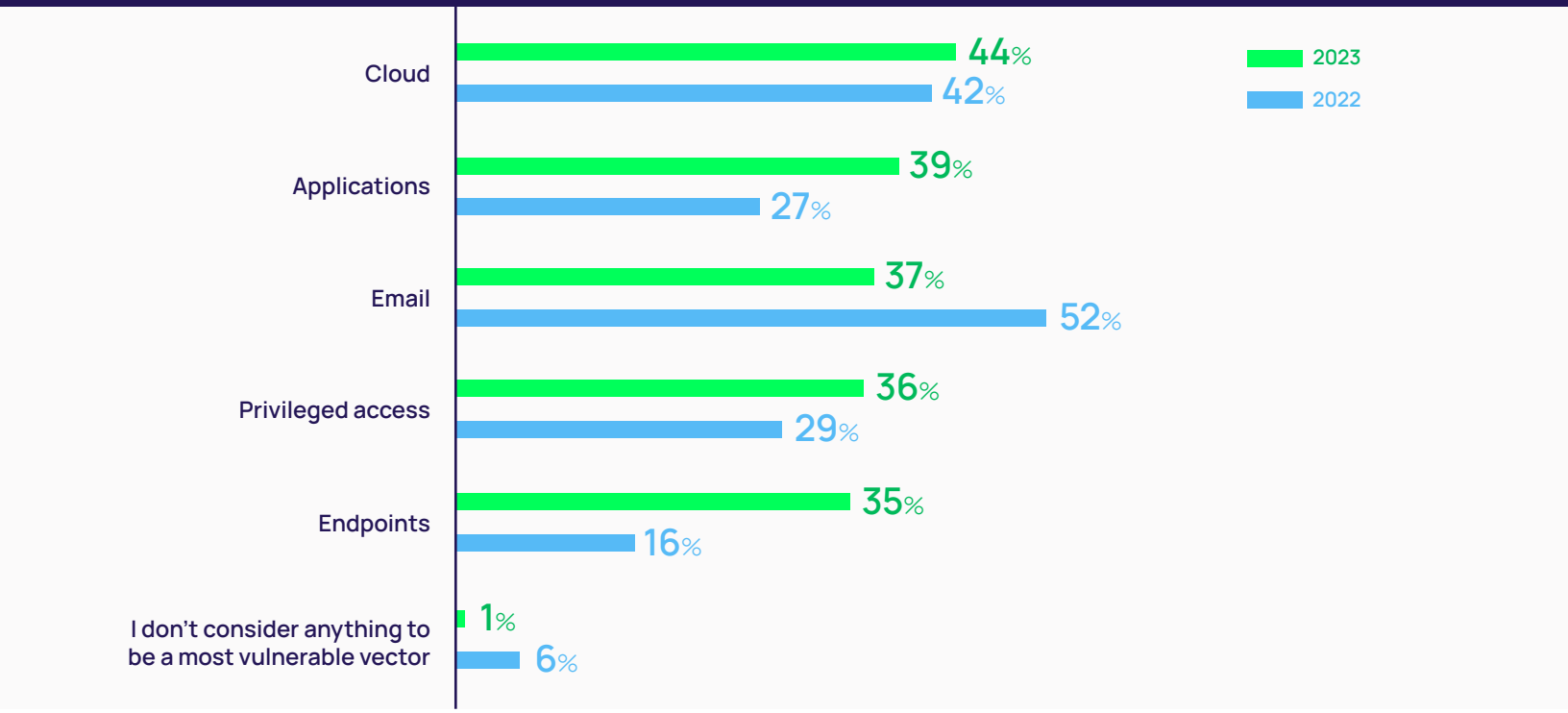
Data exfiltration can be just as costly as other types of ransomware attacks. While a money grab would have an immediate impact on an organization, data exfiltration may take place over time having both short and long-term consequences. Not only would an organization need to pay the ransom demand in the short term to prevent the data being disclosed, but they may also face compliance and regulatory fines further down the line depending on whether they had sufficient cybersecurity controls in place.

We saw several ransomware attacks involving data exfiltration during 2023. Variants such as Maze and DopplePaymer were used to add the threat of data exfiltration to a ransomware attack. The ransomware group Cl0P made headlines by leaking document excerpts and/or screenshots as 'proof' of compromise followed by the periodic release of stolen data. Looking ahead to 2024 and beyond, we'll be keeping an eye on AI-enabled data exfiltration strategies that help ransomware gangs operate in real time and at scale.

Cloud and applications overtake email as the top attack vectors

This year, respondents say they are most concerned about ransomware attacks on cloud infrastructure and applications. Worries about privileged access and endpoints increased, while email concerns decreased.

Figure 7 | What, if anything, do you consider the most vulnerable vectors for ransomware attacks? (Tick up to two)



This collective concern underscores the multi-faceted nature of the ransomware threat, with criminals strategically focusing on critical components of a modern IT environment.

As organizations become more reliant on the cloud for everything from software development to delivery of core services, it's no surprise that they are more concerned with cloud security. Exponential growth in applications for every business function, plus the reliance on APIs to pull those applications together, underscores the need for organizations to scrutinize and fortify their software ecosystems.

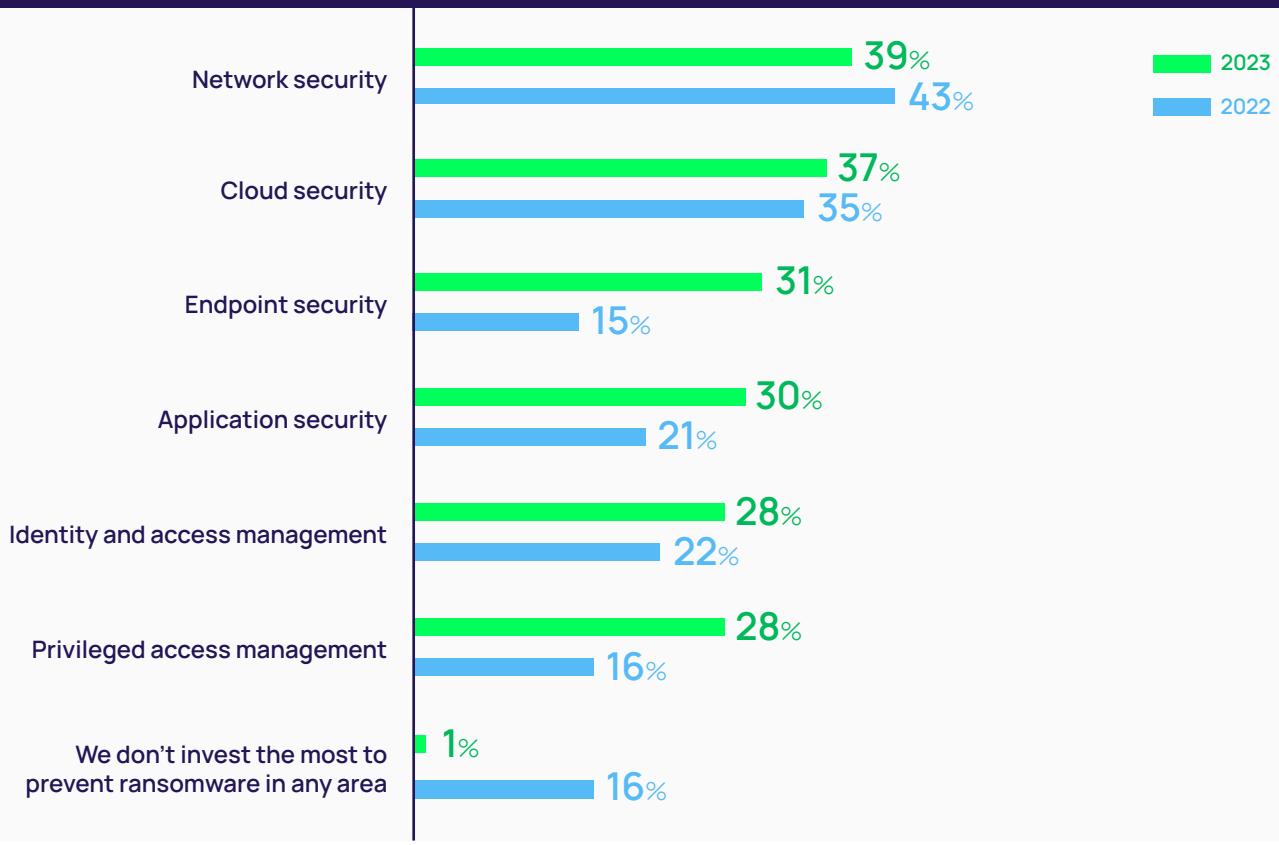
Privileged access is a lucrative target for ransomware gangs. As part of the ransomware ecosystem, access brokers sell compromised credentials that provide entry to IT environments so their affiliates can conduct criminal activities, including data encryption, data exfiltration, and malware that slows or shuts down IT systems.

While endpoints are at the bottom of the vulnerabilities list this year, concerns about their vulnerability have more than doubled since 2022. As remote work and reliance on remote third parties continue, security teams are right to keep an eye on insecure endpoints. In particular, insecure RDP access that allows remote access from endpoints sitting outside the company network have been one of the common entry points reported for ransomware attacks.

Increased Investment in Privileged Access Management

In tandem with the rising concern about privileged access noted above, spending on Privileged Access Management (PAM) has also increased. The number of respondents who said their investment in PAM has increased has nearly doubled.

Figure 8 | In what area, if any, do you invest the most to prevent ransomware? (Tick up to two)



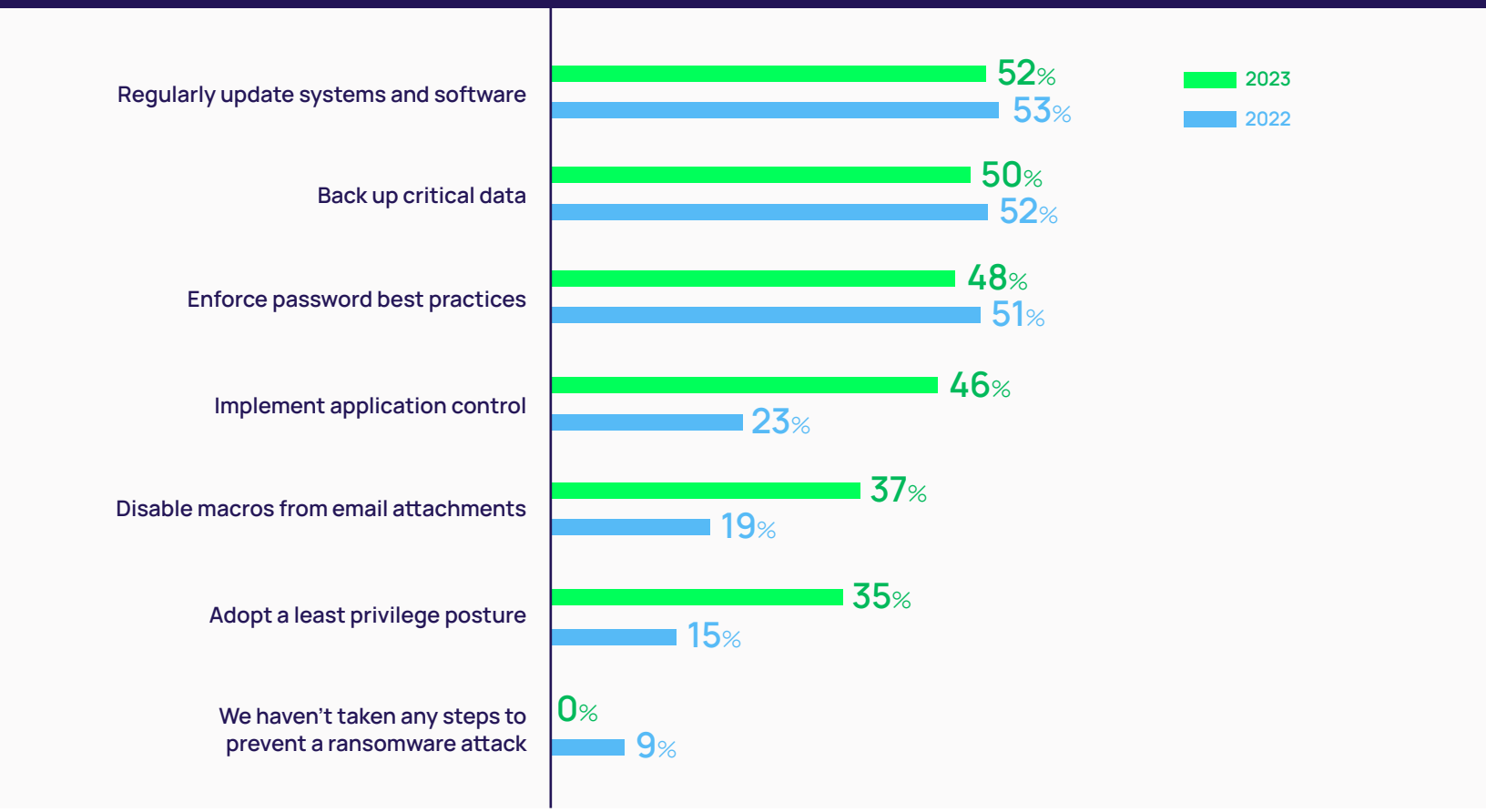
PAM enforces password best practices and enhances defenses by restricting and monitoring access to critical systems and applications, reducing the potential for malicious actors to exploit high-level credentials. As part of PAM, Multi-Factor Authentication (MFA) adds a layer of security, mitigating the risk of unauthorized access even in the event of compromised credentials. PAM is a critical cybersecurity strategy to align with the Principle of Least Privilege, vital to a zero trust strategy, which ensures people have access only to the systems, applications, and capabilities necessary for their jobs.

The increase in both PAM investment and focus over the past year underscores the growing recognition of the critical role privileged access plays in the overall cybersecurity posture.

When it came to which group was most likely to recognize the importance of PAM in preventing ransomware attacks, respondents in cybersecurity and infosec roles ranked highest compared to those in the IT workforce (31% vs. 27%). This potentially indicates a need for more education in the broader IT community.

As ransomware attackers increasingly target privileged access and credentials, organizations are prioritizing PAM strategies in the fight against ransomware. Compared with last year, more companies are focused on adopting a least privilege posture and enforcing application control to improve their zero trust strategy.

Figure 9 | What, if any, steps have you taken to prevent a ransomware attack? (Tick all that apply)



Just as ransomware threat vectors are evolving, so are measures to fend off an attack.

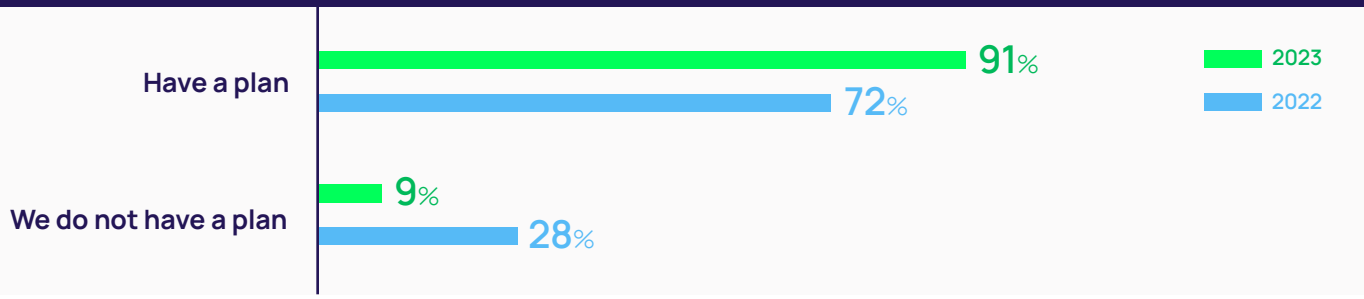
The rise of data exfiltration attacks means that data backups, though vital to ransomware protection and recovery, aren't a comprehensive strategy to mitigate the risk of ransomware attacks. Rather, strategies that help you monitor and control the egress of outbound large data transfers, especially via third-party applications, will become important to reduce the risks from data exfiltration ransom attacks.

Security teams must continue the focus on reducing shadow IT and enabling sanctioned applications for storage and file sharing. Establish an allow list that only executes approved applications, a deny list for known malicious applications, and sandbox those that are unknown until they can be analyzed.

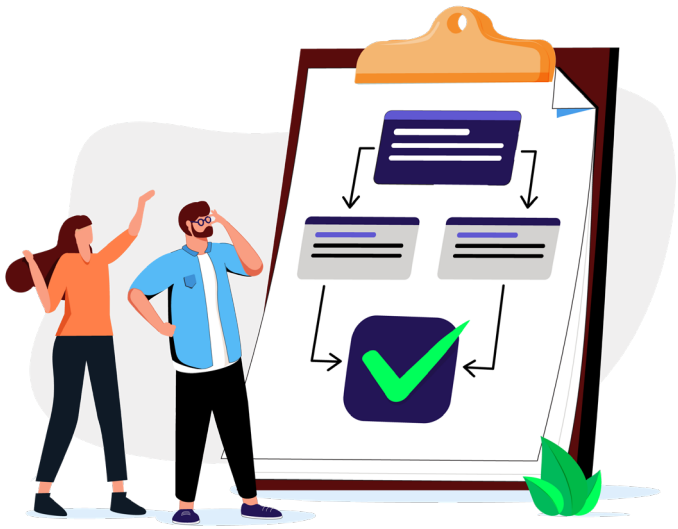
More companies invest in incident response plans

Faced with the escalating threat of ransomware attacks, organizations are recognizing the critical importance of incident response strategies. Over 90% have invested in developing incident response plans. These plans, designed to effectively navigate and mitigate the impact of cyber incidents, are now facing rigorous testing as attack methods change. Their efficacy relies on their adaptability and the ability of organizations to stay ahead of the evolving threat landscape.

Figure 10 | Does your company have an incident response plan in place?



As part of an incident response plan, specialized vendors play a crucial role in assisting companies in the aftermath of an attack, helping recover encrypted data, identify vulnerabilities, and fortify security controls to reduce the risks of future incidents. The commitment to robust incident response is pivotal in not only containing the impact of ransomware attacks but also in fostering a culture of preparedness and resilience.



Conclusion and Next Steps

As the data shows, companies of all sizes are likely to experience ransomware. You can't waste any time developing your defense and recovery plans.

Establishing strong cybersecurity fundamentals is the best way to reduce your risk. Following best practices such as the Principle of Least Privilege to limit the number and scope of admin rights means that even if attackers gain entry to your IT environment, their ability to install payloads, exfiltrate data, and cause damage can be limited.

Limiting privileges does not need to limit productivity. Companies that adopt Privileged Access Management (PAM) solutions can secure access to on-premise and cloud environments, even for remote workers and third parties. Advanced threat protection strategies, such as endpoint security and application controls, provide additional layers of visibility and security.

Align with your leadership on the risk of ransomware and your ability to withstand an attack. Make sure everyone is on the same page in terms of the incident response plan — and practice it — so that if an attack happens, you know exactly how to detect, respond, and mitigate.

For more recommendations and techniques to fight ransomware, download **Delinea's Ransomware Defense Toolkit**.

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**

 STRAN-WP-0124-EN