Delinea

Closing the Cyber Insurance Gap

2023 State of Cyber Insurance Report

WHITEPAPER

Delinea

Executive Summary

Costs, coverage, and trends impacting buyers

The cyber insurance industry is maturing rapidly and trying to right itself after years of escalating cyber incidents and payouts.

Insurers have gathered valuable historical incident and breach data to quantify risk and understand the factors that impact their risk exposure. As a result, they're evolving their risk assessment practices, policies, and prices. They're getting more stringent and prescriptive about the best practice security controls they require before granting coverage.

The demand for cyber insurance is well-established, as reported in Delinea's 2022 survey and other market analysis. In this year's study, we wanted to understand what it takes to get insurance in today's environment, to what degree insurance covers costs in the event of an attack, and how cyber insurers are evolving. To see how buyers are adapting to the changing market, we surveyed over 300 organizations in the United States, including the security, IT, legal, and compliance leaders involved in obtaining insurance policies.

As an insurance policyholder, staying up to date with the latest costs, coverage, and gaps of cyber insurance must be an essential part of the planning and budgeting process.

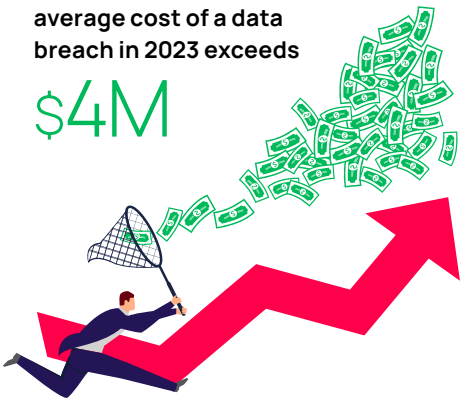
Read on, as this report will help you:

- Benchmark your own experience with cyber insurance
- Prepare for your next insurance negotiation
- Understand the fine print of your insurance policies
- Know what resources to set aside to maintain business continuity

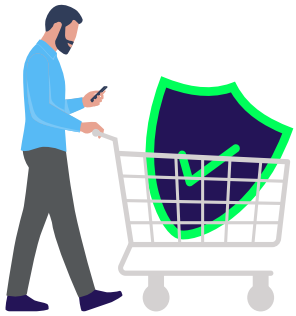
The results uncover many key pieces of information policyholders need to know

average cost of a data breach in 2023 exceeds

$4M



1. **Saving is essential because insurance won't cover all costs or types of cyberattacks**
   - All respondents had at least one exclusion in their policy that would void coverage.
   - All respondents had at least one attack-related expense that wouldn't be paid for by cyber insurance.
   - Considering the average cost of a data breach in 2023 exceeds $4M, it's crucial to set aside a rainy-day fund for situations that won't be covered.



44%

purchased Privileged Access Management (PAM)

2 **Rates are increasing, but the board is still willing to pay**

- 79% saw insurance costs increase, with 67% facing an increase of 50-100%.
- 81% got the budget increase needed to cover it.

3 **Insurance requirements drive additional investments in cybersecurity solutions**

- 96% purchased at least one new security solution before being approved by carriers.
- Almost half (44%) purchased Privileged Access Management (PAM).

4 **The time and effort to obtain cyber insurance is increasing**

- Most alarming, the number of companies requiring 6+ months increased 21X over last year.
- What would your team be able to do with that extra time?

Enterprises with 250+ employees face different challenges than small businesses

1 **Smaller companies are more likely to be denied coverage**

- 28% applied and were denied coverage, versus 8% of large companies.

2 **Larger companies need much more assistance during the application/approval process**

- 63% had to use insurance-provided solutions/appliances.
- 60% were required to pay for an external risk assessment.

3 **Smaller companies are less likely to have insurance that pays for a variety of costs**

- The top reason small companies were denied was the lack of security protocols (40%).
- Large companies were more likely to have claims denied due to human error (47%).

Delinea

The Fine Print

Cyber insurance policies can differ based on several factors, including risk profiles of customers, provider policies, size, risk appetite, and the latest threats. Here are some ways they may vary and why you need to read the fine print in your policy.

- **Coverage scope:** Cyber insurance policies can have vastly different coverage scopes and focus on specific areas of cyber risk, such as data breaches, ransomware attacks, business interruption, liability claims, and more.
- **Policy limits:** The maximum amount an insurer will pay for a covered incident can vary, so you need to assess your organization's risk tolerance and potential financial losses to determine appropriate limits.
- **Deductibles:** Cyber insurance deductibles (the amount you'll pay out of pocket) can vary. Depending on your risk management strategy, you might choose higher deductibles to lower your premiums or vice versa.
- **Risk assessment and underwriting:** Insurance carriers and brokers conduct risk assessments to evaluate cybersecurity practices and infrastructure, which can influence the coverage options, terms, and premiums offered.
- **Industry-specific policies:** Providers may offer specialized policies for sectors with unique risks or regulatory requirements, such as healthcare, finance, or retail. Those policies address industry-specific cyber threats and compliance challenges.
- **Policy exclusions:** Policies typically contain exclusions for specific circumstances, causes, or events.
- **Legal and regulatory requirements:** Cyber insurance policies may need to align with local jurisdictions, including specific requirements or restrictions.
- **Evolving cyber threat landscape:** Cyber threats are constantly evolving, so insurance providers are updating their policies to keep pace with the latest attack scenarios. Renewal of existing policies may include changes to the fine print.

Work closely with insurance providers to select policies that provide adequate coverage and align with your risk management strategies.

Make sure to read the fine print when you renew.

The policy that covered you last year may have changed or may not cover your current needs.

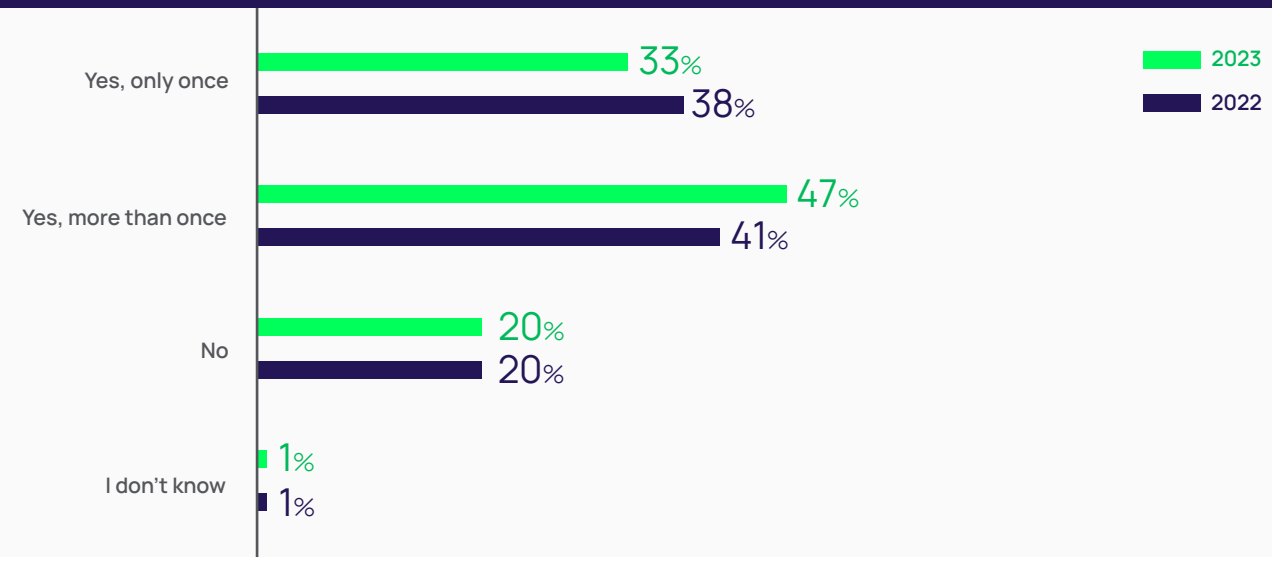
Delinea

Key Finding 1

Insurance doesn't let you off the hook for good security

Companies that have cyber insurance use it — and more than once. This holds true regardless of company size, underscoring the need for insurance at all levels of the market. In fact, the survey found that the percentage of companies that used their cyber insurance more than once increased over the past year, from 41% to 47%.

Figure 1 | Has your organization ever used cyber insurance before?

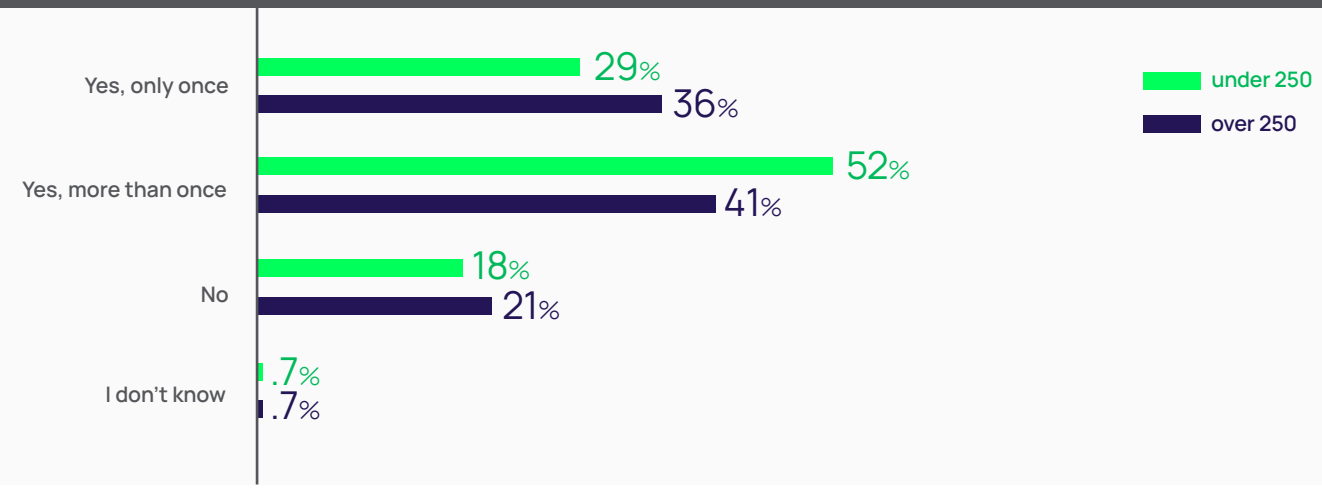


Note that while 42% of companies with over 250 employees used cyber insurance more than once, more than half (52%) of smaller companies used it multiple times.

52%

of smaller companies used cyber insurance multiple times

BY COMPANY SIZE

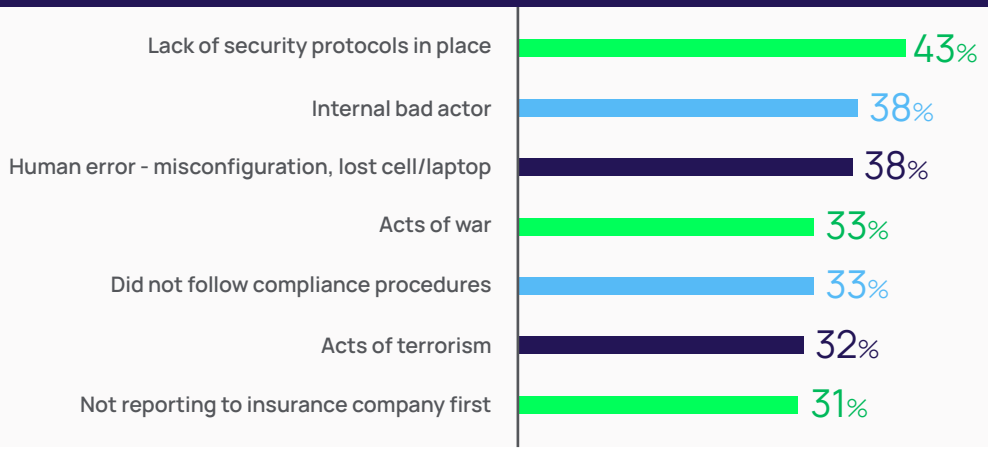


Watch the exclusions!
You need the right pieces in place, or your coverage could be voided

In the early days of the cyber insurance market, carriers were willing to take on risk without truly understanding the drivers behind it so they could capitalize on demand. After several years of learning from their own data, they know what to look for when evaluating a company's ability to prevent or withstand a cyberattack. So, if post-event investigations find you didn't follow cybersecurity best practices, you likely won't get the insurance safety net you expect.

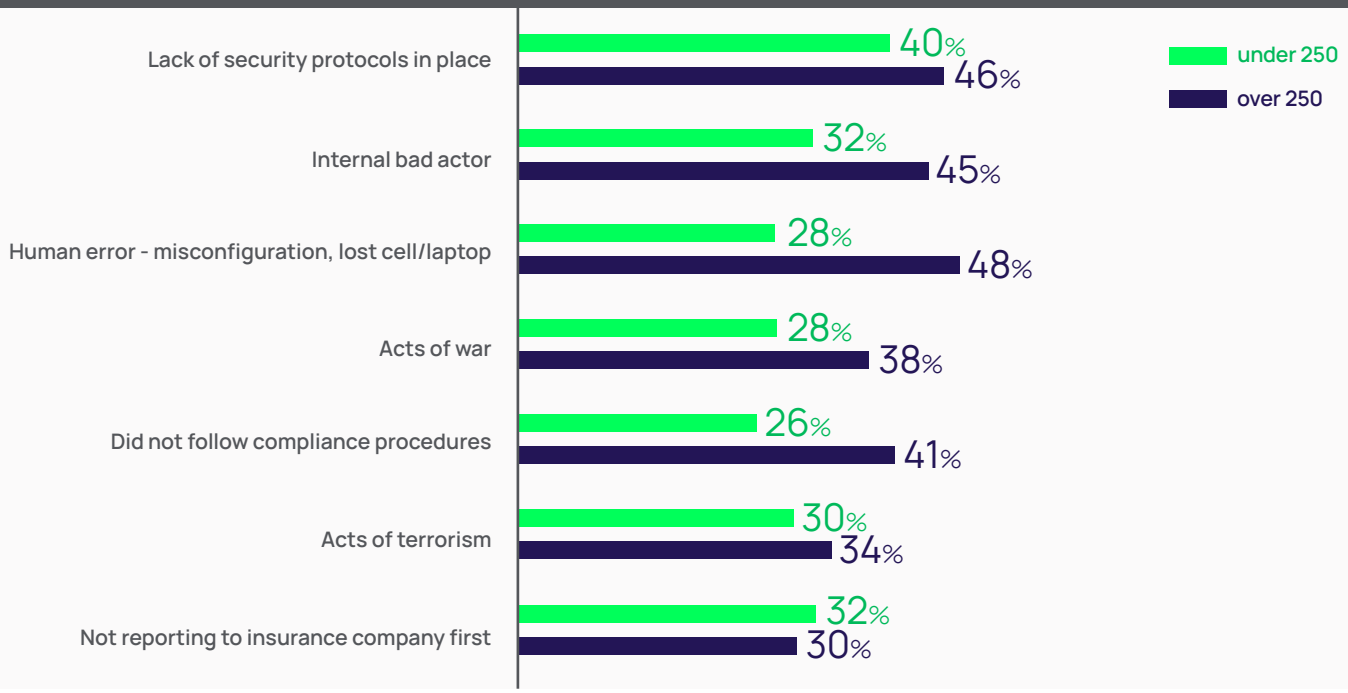
The study found that many issues voided insurance coverage. The top reasons for denials were lack of security controls, internal bad actors, human error, and not following compliance procedures.

Figure 2 | In what situations, if any, would your cyber insurance coverage be void?



The lack of security protocols was the top reason smaller organizations had their claims denied, noted by 40% of respondents. In comparison, the top reason larger organizations had their claims denied, noted by 48% of respondents, was human error.

BY COMPANY SIZE



What's the story behind these common exclusions?

- **Lack of security protocols in place:** Insured organizations are often required to meet certain protocols, such as implementing specific security controls, regularly updating software and systems, or conducting employee training.
- **Internal bad actor:** Illegal or unauthorized activities such as engaging in hacking, cyber extortion, or illegal data acquisition are typically excluded and may lead to a claim being denied.
- **Human error:** Accidents matter. If an incident is caused or worsened by misconfigurations, failure to address known vulnerabilities or other mistakes, the insurer may argue that it could have been prevented or mitigated, leading to claim denial.
- **Acts of war or Acts of terrorism:** Attribution for a cyberattack is tricky, so an exclusion clause related to the source of an attack is a blurry area. High-profile court cases are currently determining whether providers can rely on exclusionary language that attributes an attack as an "act of war" or "act of terrorism" to limit the scope of their payouts in the event of a cybersecurity attack.
- **Not following compliance procedures:** Any evidence of misrepresentation or non-disclosure of material information when applying for cyber insurance may result in the insurer denying coverage.
- **Not reporting incidents to the insurance company:** If you fail to notify the insurer within the specified time frame or provide incomplete information, your claim may be denied.

Insurance won't cover all costs

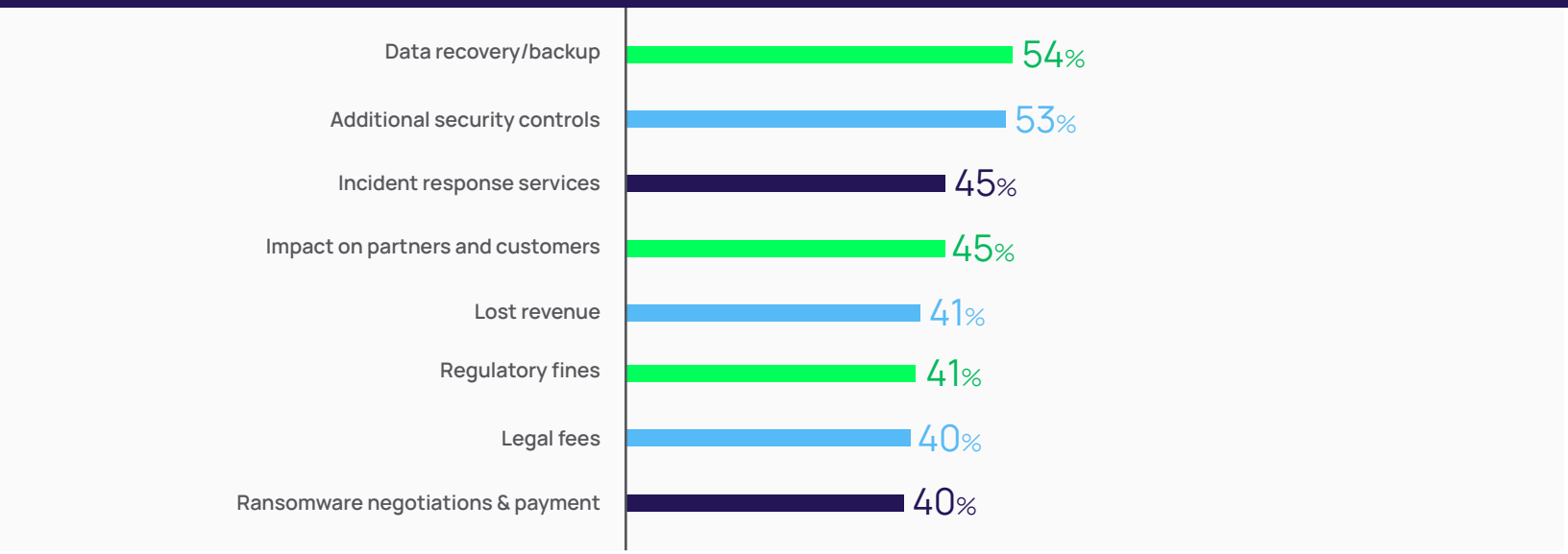
Should a cyberattack hit your organization, you'll have to take responsibility for the consequences — for your own company as well as third parties. Expect to face numerous expenses to get back on track.

Among the options provided, respondents said expenses most likely to be recouped were those spent on data recovery. Consider, however, that "data recovery" can mean different things to different insurers and in different situations. For example, say an attacker is holding your data for ransom. Some insurance companies may say they want to make the decision whether to pay the ransom to recover your data (regardless of your preference).

Almost half of respondents said their policies would pay for incident response. Incident response could include security activities conducted by internal or third-party resources, forensic investigations, and even communications costs for public relations and crisis response. Keep in mind that your policy may only cover a portion of these expenses.

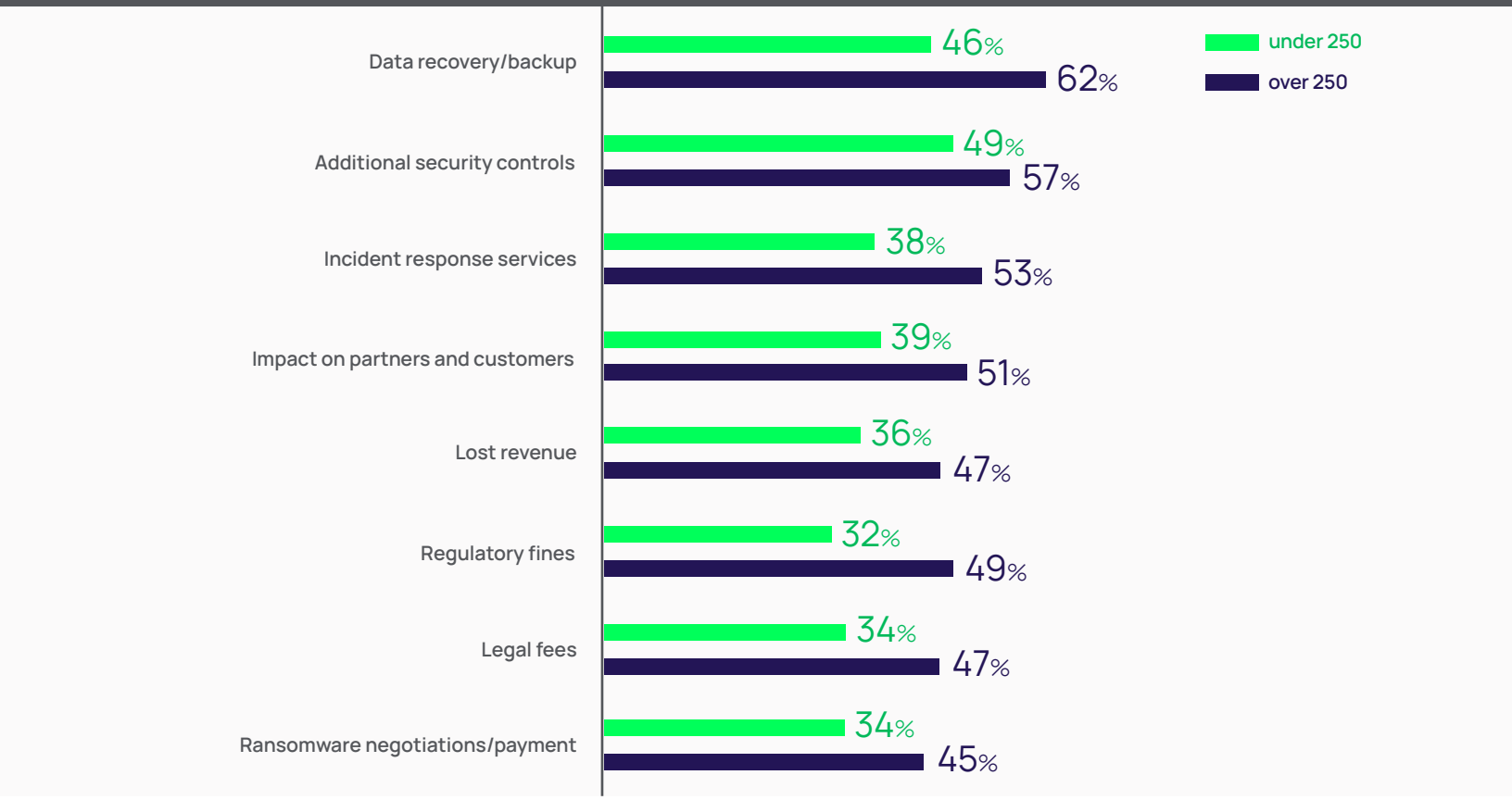
Respondents said that insurance policies are least likely to pay for lost revenue, regulatory fines, legal fees, and ransomware payments.

Figure 3 | What would your cyber insurance policy pay for?



Larger companies were more likely than smaller ones to have insurance coverage that pays for a variety of costs caused by a successful cyberattack.

BY COMPANY SIZE



What to do about it

It's important to review your cyber insurance policies carefully and ensure you meet their requirements. Implementing strong cybersecurity measures and following best practices and timing requirements can help avoid claim denials and ensure proper coverage for cyber incidents.

Focus on what you can control. Regardless of insurance, you still need a robust cybersecurity program, including the right tools and the right people, to make sure you'll be able to count on the coverage you pay for. Having the right security and governance policies in place isn't enough; your employees must know those policies and always follow them.

Don't rely on error-prone manual work or people's best intentions to protect what matters most. Mistakes happen, and they have consequences. Make sure it's seamless for people to follow security best practices so they don't try to skirt them in the name of speed or productivity. Build those practices into their workflow through policies, putting technology behind the scenes, and automating processes where possible.

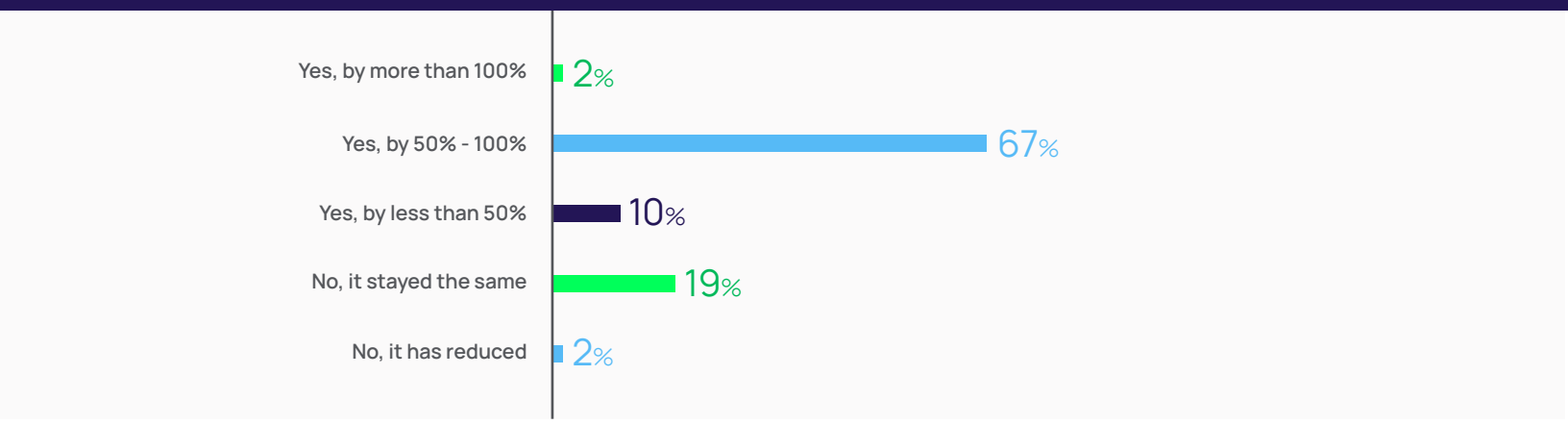
- Third-party damage often isn't covered by insurance, so you'll need to be very confident in your supply chain security controls, including remote access for contractors and vendors.
- Ransomware expenses may not be covered, so you'll need to be extra sure of your privilege escalation controls to block lateral movement for attackers that find their way inside your environment.
- Insider threats (intentional and accidental) put you at risk, so you need granular, ongoing oversight. Make sure your security controls are working as expected, and people are using them correctly. Session monitoring and behavioral analytics keep track of user activities. Most people want to do the right thing, so make it easy for them to do so with usable security.

Key Finding 2

Higher rates call for bigger budgets, and boards continue to 'rain money'

Almost eight out of ten respondents (79%) said their insurance rates increased upon application or renewal. Over two-thirds (67%) report they increased 50-100%.

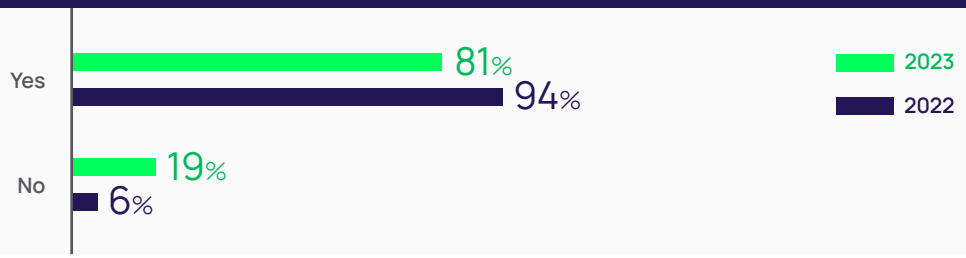
Figure 4 | Have your cyber insurance costs increased since you applied, or since your last renewal?



This year, as in 2022, most companies got a welcome increase to cover policy requirements.

That said, keep an eye on budgets in an uncertain economy. This year's report found a noticeable drop (13%) in the number of organizations that got an increased budget to cover their cyber insurance requirements.

Figure 5 | Were you allocated additional budget in order to meet insurance requirements?



The board is a strong driver for cyber insurance, as are industry-related cyberattacks

Boards of directors are mandating that companies obtain cyber insurance. This is true regardless of company size.

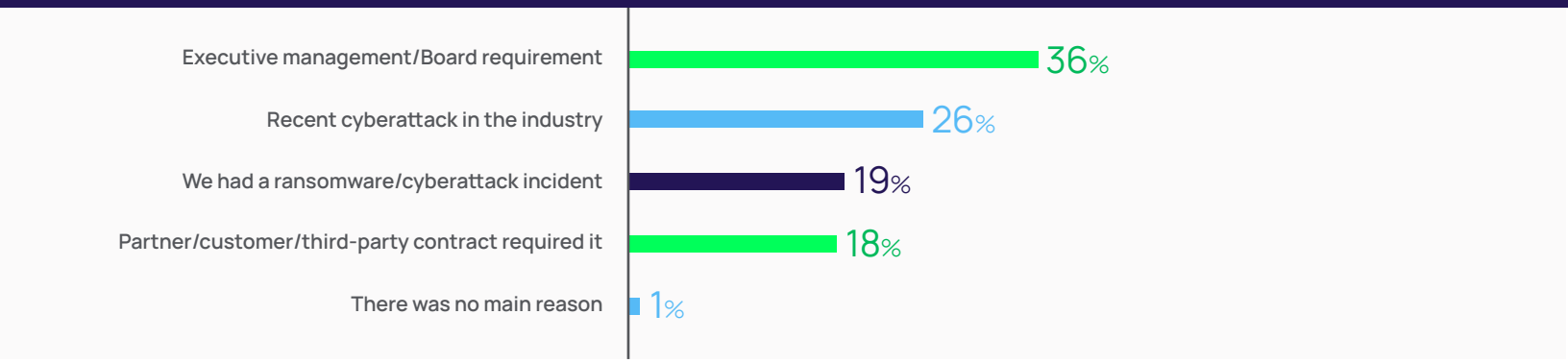
Boards look to insurance as a top strategy for good governance for several reasons:

- While boards can't know all the technical cyber considerations behind cybersecurity strategies, they're keenly interested in ensuring the company can recover if an attack occurs.
- Board members may be held personally responsible for cyber incidents that cause a drop in shareholder value.
- The board and executive team determine the level of risk that the company is willing to take on (its risk tolerance). And ultimately, they approve the budget required for investments in cybersecurity tools and teams. If they can offset the potential loss exposure of a cyberattack by writing a check for insurance, and they can afford to do so, they will.
- A cyber incident can significantly damage an organization's reputation and brand image. Boards want to ensure stakeholder confidence. Insurance reassures customers, partners, and investors that the organization takes cybersecurity seriously and is financially prepared to prevent and handle cyber incidents.

In addition to meeting board expectations this year, companies are also looking at their industry peers. When a breach occurs in their industry, it's a wake-up call, prompting companies to take a hard look at their own cyber resilience strategies and obtain or increase insurance coverage.

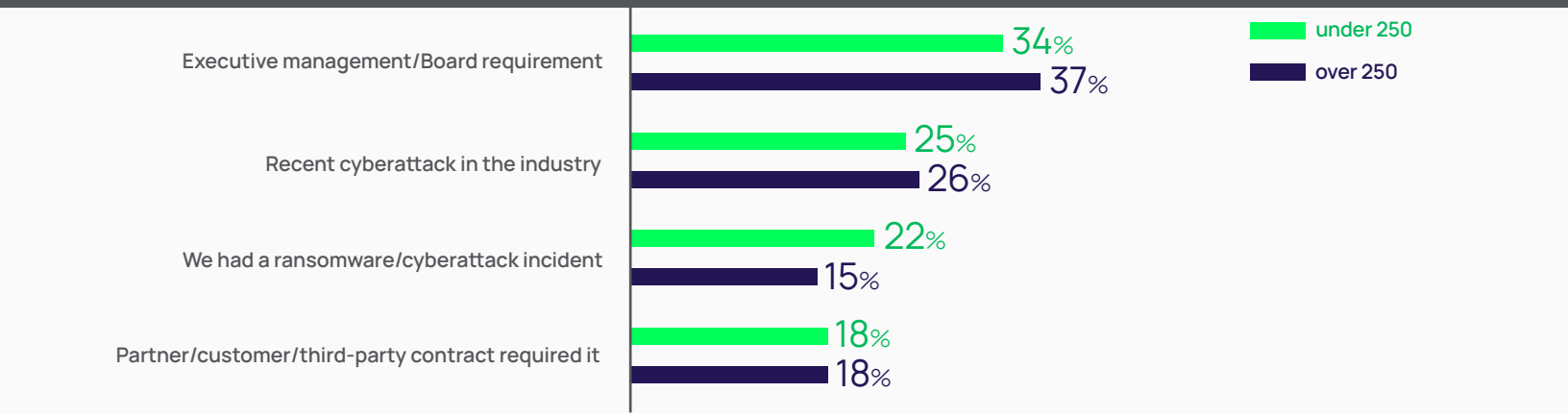
The study also found that contractual agreements with clients, vendors, or business partners prompted them to apply for cyber insurance. Sadly, many organizations needed the impetus of a successful cyber incident at their own organization to apply.

Figure 6 | What was your main reason for applying for cyber insurance, at the time you did?



Smaller companies were more likely to say they sought cyber insurance because they experienced a ransomware attack themselves.

BY COMPANY SIZE



What to do about it

No one has an unlimited budget. Work with your board and executives to determine your organization's risk tolerance so you can budget to cover your loss exposure.

Cybersecurity and cyber insurance are a balancing act. Cyber insurance should be complemented by robust cybersecurity measures to effectively manage cyber risks. You'll want to earmark enough money in the budget to cover the rising insurance costs but not so much that you can't afford to invest in cybersecurity solutions and skilled resources.

Especially if you're among the 19% that aren't allocated additional budget, you'll want to look for opportunities to reduce costs in other places, such as consolidating tools or reducing software licenses.

Plus, you'll still want to reserve a budget to pay for loss and recovery expenses. Simply having insurance doesn't preclude you from experiencing a cyberattack or having to pay for the repercussions.

Key Finding 3

Privileged access security controls are critical for obtaining cyber insurance

Cyber insurance policies typically require or strongly recommend implementing various security solutions to mitigate cyber risks. While specific requirements may vary among policies and insurance providers, the survey uncovered some commonly demanded security solutions you'll need before a policy is granted.

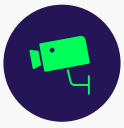
Considering that most cyberattacks involve stolen credentials, it's no surprise that insurance providers require related security controls. Starting with Identity Access Management (IAM) and Privileged Access Management (PAM), insurance companies insist on security controls that prevent credential theft and contain attacks should credentials be stolen or used for unauthorized access.

Identity and Access Management (IAM) manages and controls user access to critical systems, applications, and data. Implementing robust IAM practices can reduce the risk of unauthorized access, data breaches, and insider threats.

Privileged Access Management (PAM) focuses on securing privileged accounts with extensive access rights, which are highly sought after by attackers. Proper management of these accounts minimizes the risk of unauthorized access and potential misuse. PAM solutions are designed to control, monitor, and audit privileged access to critical systems and applications. They reduce your attack surface and mitigate the impact of security breaches or insider threats associated with privileged accounts.

Password complexity and rotation requires regularly rotating passwords, so they are continually changing and complex, and hard to guess. Many organizations use a password vault for this type of functionality, taking highly privileged administrative accounts and passwords out of the direct control of IT staff and end users. In some cases, passwords are never even seen by users, further reducing the risk of sharing, repetition, and theft.

Multi-Factor Authentication (MFA) adds an extra layer of authentication for user access to critical systems and applications, reducing the risk of unauthorized access due to stolen or compromised credentials. Rather than just asking for a username and password, MFA requires one or more additional verification factors. You can choose to implement MFA at multiple points in the attack chain, including login, privilege elevation, password/secret checkout, etc. MFA can also be applied dynamically based on context or level of risk.

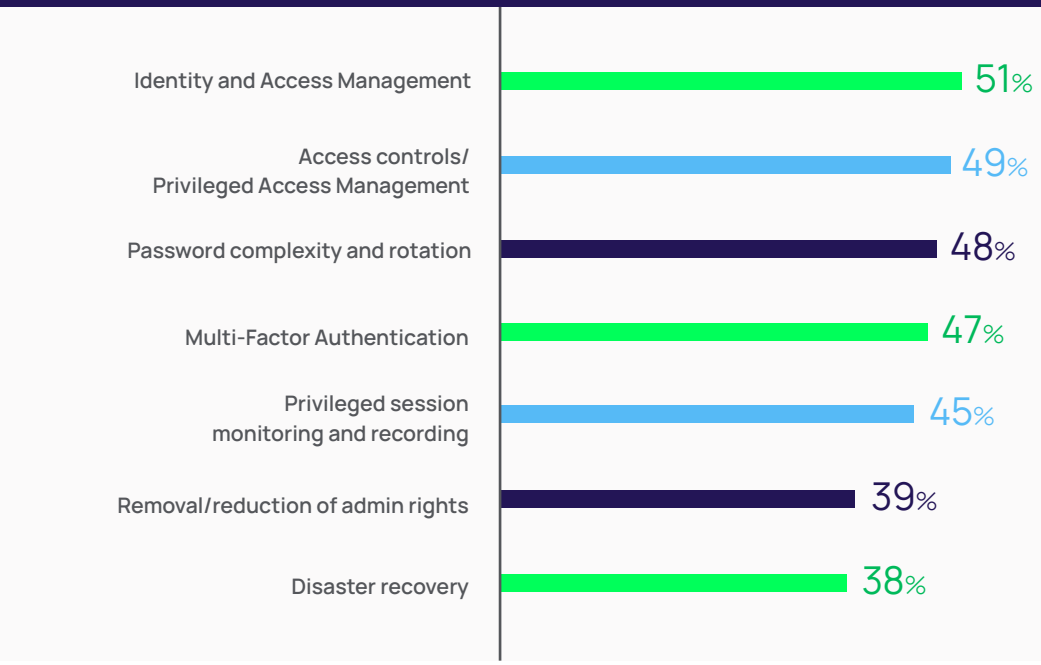


Privileged session monitoring and recording includes the ability to record videos of privileged sessions and log keystroke activity. It even makes it possible for someone to review sessions live or shut the session down if the user is doing something harmful.

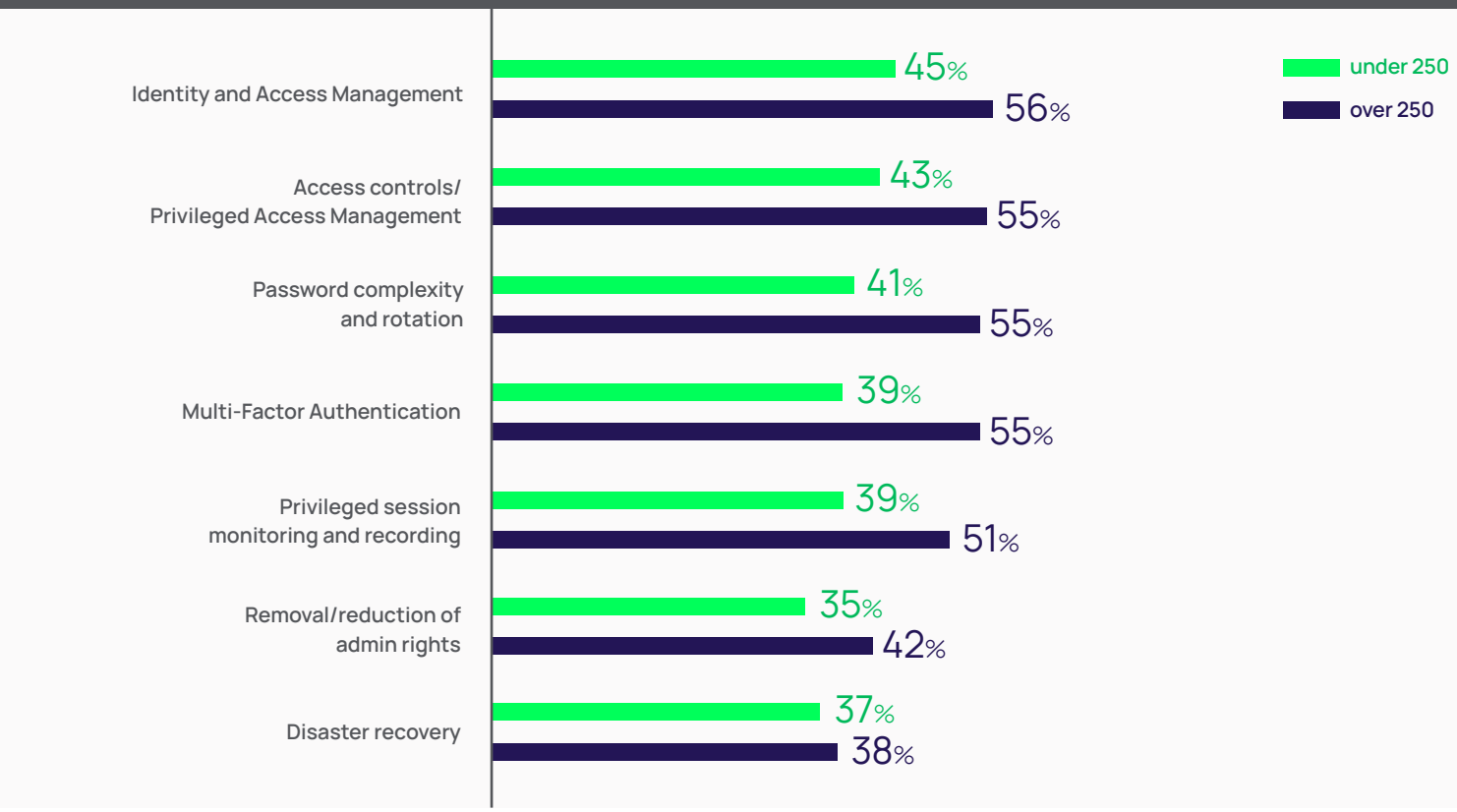
Removal/reduction of admin rights is a critical security practice that reduces your attack surface. Instead of providing standing admin rights, you limit privileges only to those who need them when they need them. This means removing local admin rights from workstations and providing just-in-time domain-level privileges.

Larger enterprises tend to have many more security requirements to meet than their SMB counterparts, but both groups must demonstrate the same top controls – IAM and PAM – to insurance providers.

Figure 7 | What security controls, activities, and processes are required by your cyber insurance policy?



BY COMPANY SIZE



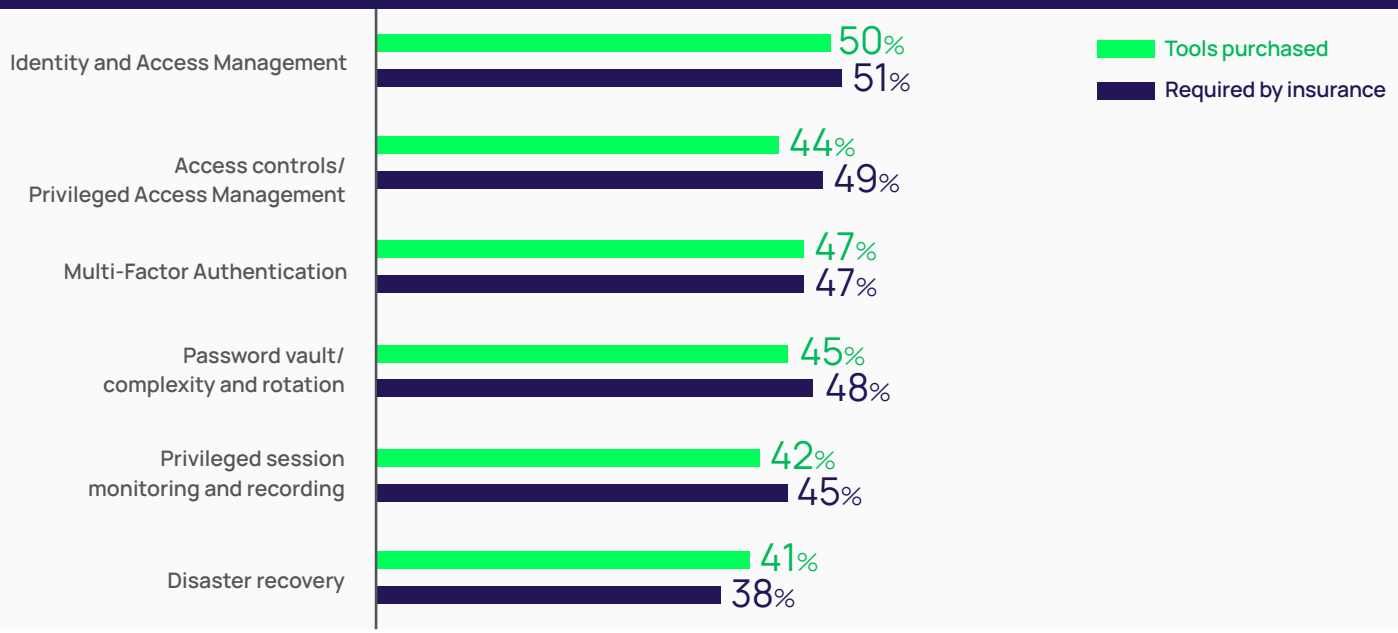
Delinea

Most companies purchased solutions to meet insurance requirements

Insurance requirements drive additional investments in cybersecurity solutions. Virtually all respondents (96%) had to purchase at least one new security solution before an insurance carrier or broker would grant them a policy.

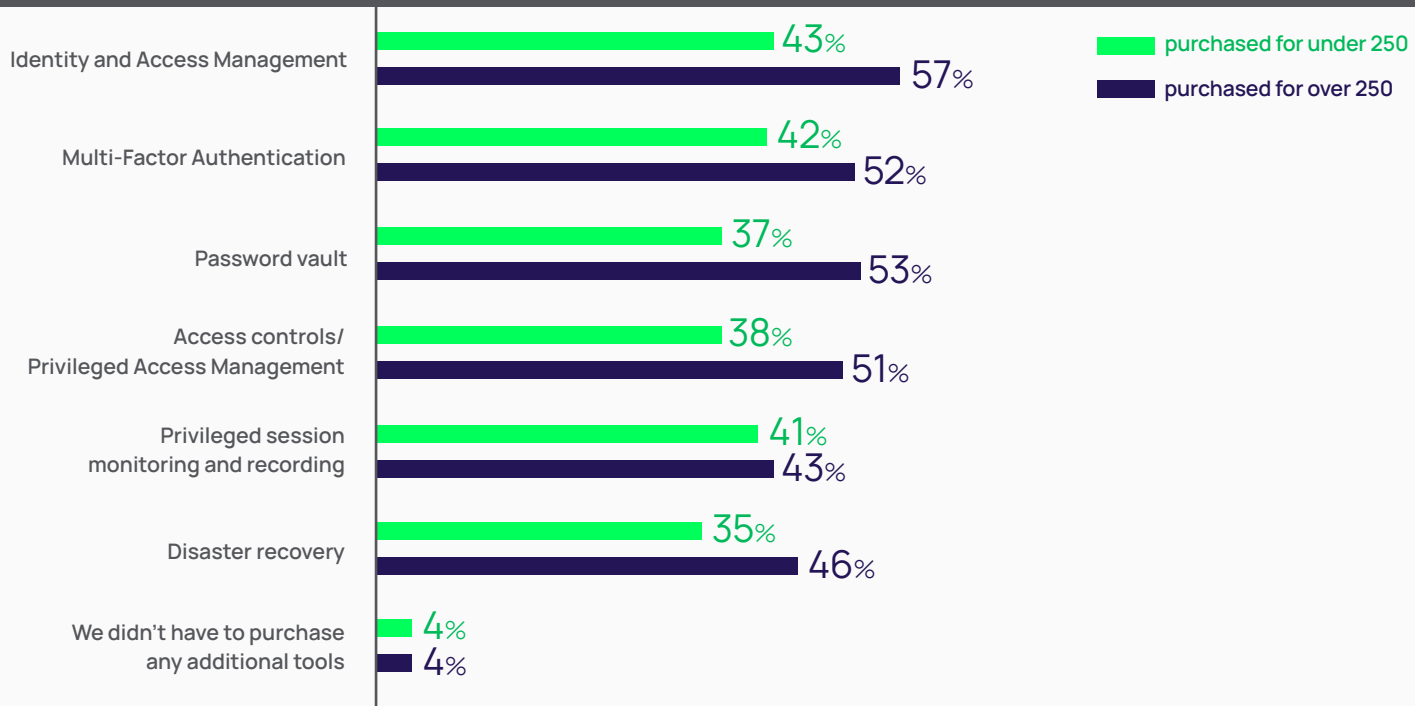
What did they buy?

Figure 8 | What additional tools did you have to purchase to obtain/renew your policy? What security controls, activities, and processes are required by your cyber insurance policy?



Again, large companies were more likely than small ones to make a variety of purchases to meet the requirements of insurance companies.

BY COMPANY SIZE



Both control requirements and solution investments have increased year-over-year

Compared to the results of our 2022 study, insurance requirements for IAM and PAM increased dramatically this year, while MFA requirements were static.

When it comes to purchasing solutions, companies were more likely to add IAM, PAM, and MFA to their security arsenal this year than last.

	IAM		PAM		MFA	
	2022	2023	2022	2023	2022	2023
Control required	35%	**51%**	29%	**49%**	47%	**47%**
Solution purchased	35%	**50%**	24%	**44%**	36%	**47%**

What to do about it

If you don't already have these solutions, it's time to implement them before you shop for or try to renew your cyber insurance. They're essential controls to add to your toolbox, along with the basics like anti-malware software, data encryption, firewall and intrusion detection, patching, and vulnerability management.

The good news is that you don't need to purchase multiple, single-purpose software (e.g., a standalone password vault, role-based access controls, a unique MFA solution, etc.) to meet the security controls insurance companies require. In fact, purchasing a lot of disconnected tools could lead to higher costs and more complexity, with multiple interfaces to learn and data to reconcile.

You can address these requirements in a unified and centralized Privileged Access Management (PAM) platform. A robust PAM tool provides password management and vaulting, identity consolidation and MFA for authentication, access controls for authorization, session recording for oversight, and more. Plus, PAM solutions make reporting easy so you can demonstrate to cyber insurance companies that security controls they expect are in place and working.

Delinea

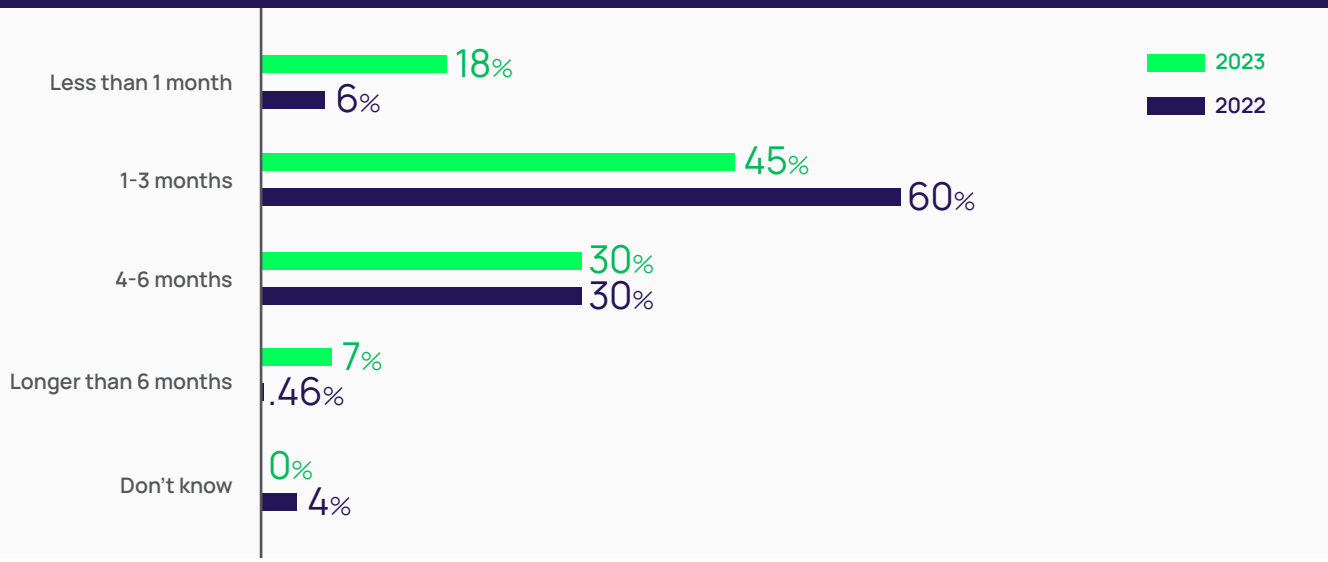
Key Finding 4

More scrutiny from insurance companies = more time and work for you

Some organizations may be able to get coverage relatively quickly, as shown by the increase in respondents saying it takes less than one month. Quick turn, online applications may be sufficient for a basic policy or a straightforward renewal for an organization that hasn't changed much in the past year.

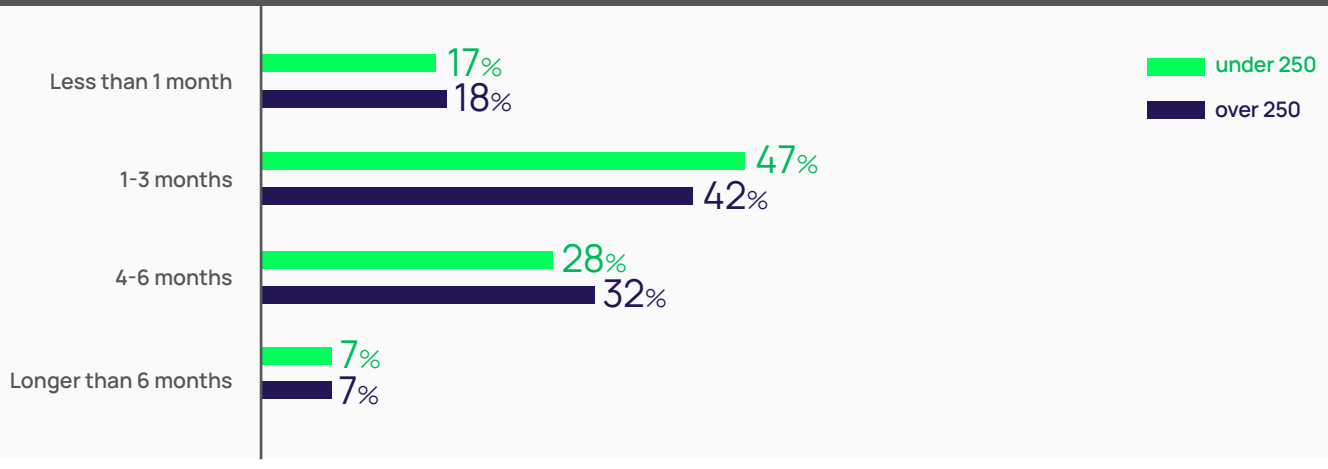
However, on the other end of the spectrum, the time and effort to obtain cyber insurance is increasing for many. Note that the percentage of respondents reporting that the process to get cyber insurance took more than six months increased significantly from 0.46% in 2022 to 7% in 2023.

Figure 9 | How long did the process take you, or do you anticipate it will take you, to obtain/renew your cyber insurance?



Larger organizations, however, such as enterprises with more than 250 employees, are a different matter. They represent significant risk and often experience significant changes in their attack surface and business structure between renewals.

BY COMPANY SIZE



The IT team bears the burden

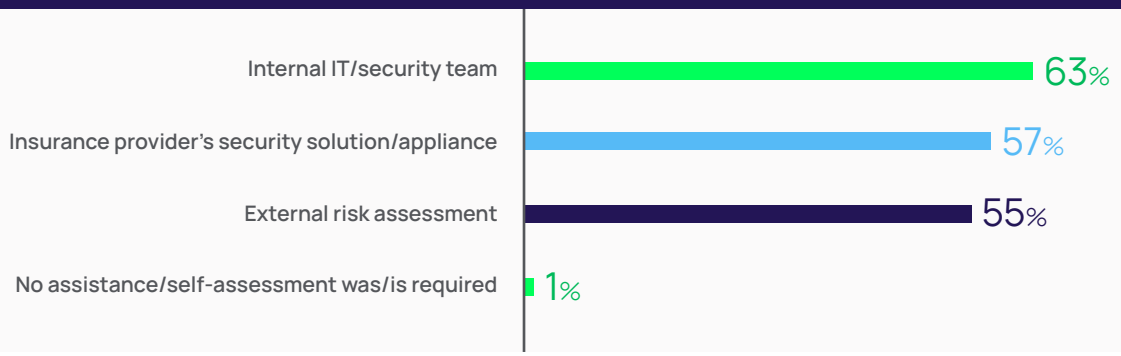
Insurance questionnaires and calls with risk analysts require knowledge of your IT systems, including their functionality, dependencies, sensitive data, and security controls. People will need to take time away from keeping business-critical systems running and supporting employees and customers to answer them. Consider what else those valuable people could be doing instead of chasing down data and building reports.

Providers require solutions for risk assessment

Despite the effort it takes, internal-only assessments may not be good enough for insurance companies to take on your risk.

To reflect how the insurance market is maturing, we added an option in this year's survey to ask about the support companies needed in obtaining cyber insurance. More than half reported that providers require them to conduct an external evaluation, and 55% said they had to use a provider-approved solution. In fact, some providers have their own appliances which they want to install in a company's IT environment. While these types of solutions provide an unbiased, outside-in perspective, they can also be costly and time-consuming.

Figure 10 | What assistance, if any, was/is required in obtaining your cyber insurance policy?



What to do about it

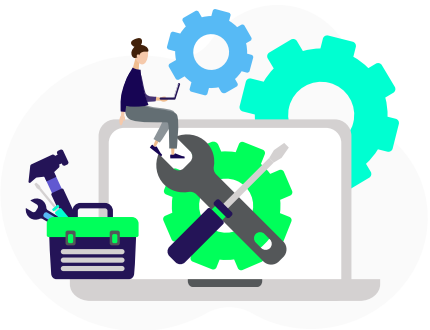
Time is of the essence. Every day you don't have the right security controls, and you don't have insurance coverage increases your risk.

Do the pre-work. Prepare for insurance questionnaires by understanding what they ask.

Know what the most high-risk assets are in your IT environment and how they're protected by security controls. Spend the time now to find out what you don't know.

Toolkits can offer insight into what you may be missing.

Conduct regular risk assessments on your own, using a standard framework like NIST CSF. In addition to internal audits, you could provide limited-time, isolated access to an external auditor or pen tester to evaluate your security posture.



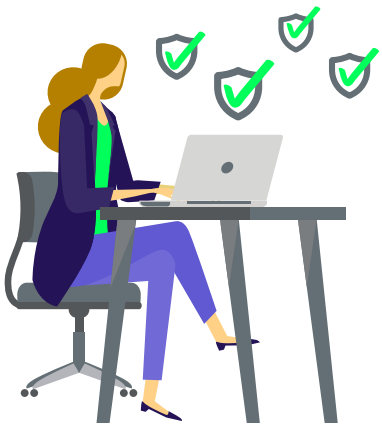
Conclusion

Cyber insurance is a safety net that allows you to transfer risk so it becomes acceptable to your organization. With cyber insurance, even if the worst happens, you'll have the financial means to continue to operate, serve customers, and recover. But cyber insurance is not cybersecurity — it's an important distinction that cyber insurers and organizations seeking cyber insurance are beginning to understand more clearly.

Based on the results of this survey, it appears that the drivers putting pressure on the cyber insurance market will continue into the next year and likely beyond. Organizations are looking to buy insurance, driven by their board, industry peers, and the unabating pace of cyberattacks and ransomware.

Yet, the obstacles they face are increasing. The bar for security controls is higher than ever, which requires a budget for purchasing technical solutions and hiring skilled resources. Identity and access controls, password vaults, and MFA are must-haves for any organization seeking insurance.

At the same time, economic pressure means more companies must find the money for increasing insurance rates from within their existing budgets. And, the whole process takes significant time and diverts attention away from other priorities that might do more to help organizations reduce their risk.



Even if you can obtain a policy, the "gotchas" abound as insurance companies tighten the reigns. You may not be able to use the same policy with the same coverage as last year. If you're renewing a policy, don't just rubber stamp it, as conditions and exclusions have likely changed, and so may have your requirements. Make sure you review any policies carefully to understand what types of incidents will and won't be covered, and what internal mistakes could render policies void.

The more effective security controls you have in place and the more preparation you do before shopping for insurance, the easier the review process will go. You can check out an at-a-glance cyber insurance checklist to get you started, and a more detailed analysis of cyber insurance questionnaires to make sure you have the answers to questions insurers are sure to ask.

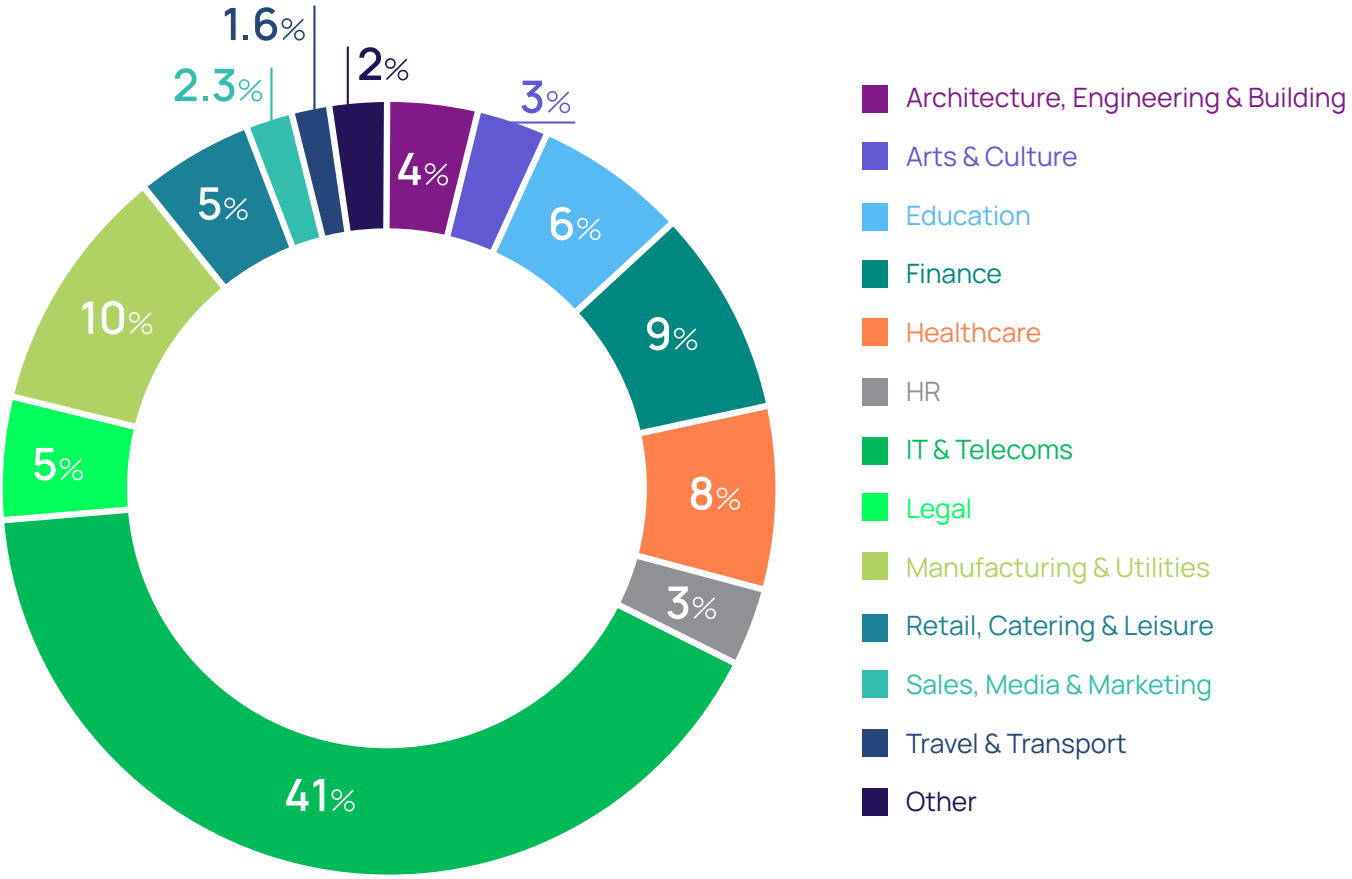
Always remember that cyber insurance is just one component of a comprehensive cybersecurity program. It should be complemented by robust cybersecurity measures, including employee training, strong security protocols, regular vulnerability assessments, and incident response plans.

Methodology

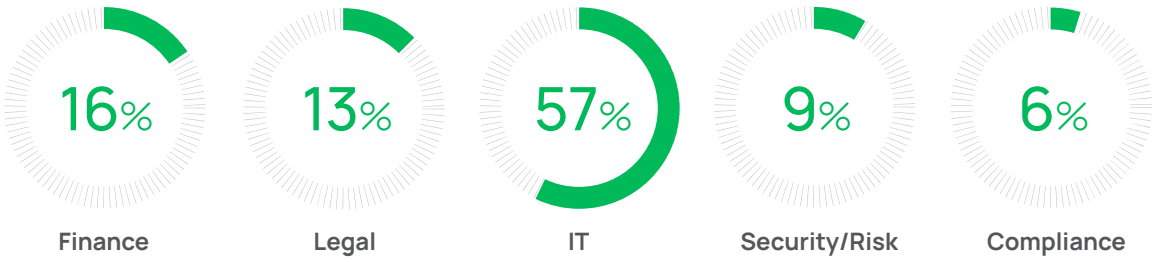
This online survey was conducted on behalf of Delinea by Censuswide, who in June 2023 surveyed 300 leaders with visibility into their organization's cyber insurance application or renewal process. All respondents were presented with the same set of questions, and the answer options were randomized. Results were not weighted.

Breakdown of respondents

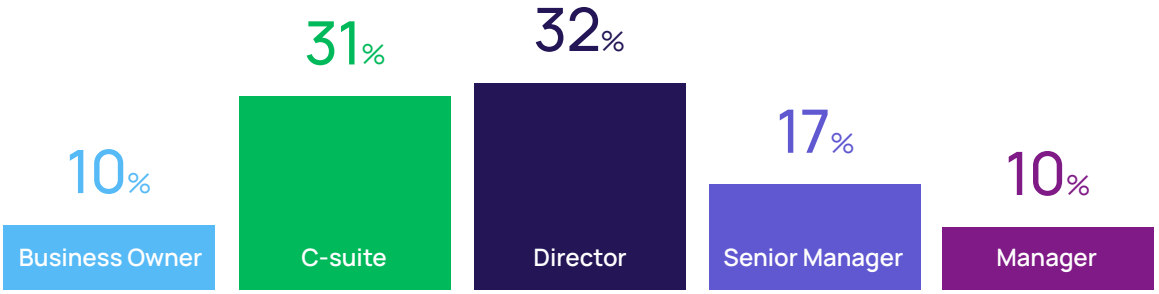
Industry



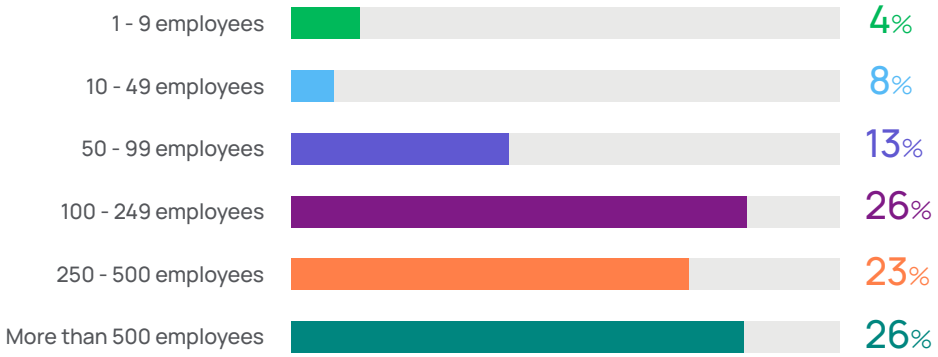
Roles



Titles



Company size



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**

 SCIR-WP-0823-EN