Delinea

WHITEPAPER

Identity Security is Critical to Obtaining and Maintaining Cyber Insurance

2024 Cyber Insurance Research Report

Executive Summary

Cyber insurance is a critical component of a cyber risk management program to ensure resilience and recovery. Now that having cyber insurance has become standard practice for organizations of all types, the focus has shifted to maintaining insurability even as risk factors change.

As cyber incidents have rattled the industry, insurers are engaging in detailed risk assessments, and it's increasingly difficult for cyber leaders to prove the value of their security program and get robust coverage. Organizations must provide relevant evidence to make sure their insurance continues and increases or adjusts as necessary. For complex, hybrid organizations with changing risk profiles, collecting accurate, up-to-date information can be incredibly cumbersome and time-consuming work.

In this research study of 300 decision-makers, we analyze how companies are addressing these challenges to obtain and maintain cyber insurance. In particular, we explore how organizations are adopting newer technologies like Artificial Intelligence to increase efficiency, scale quickly, and lower costs.

Key takeaways:

1. **Gaps in identity security are the most common cause of cyber incidents that result in insurance claims. Identity and privilege compromises account for 47% of attacks that lead to insurance claims.**

2. **Insurance companies want evidence of identity security before granting a policy. Over 40% of insurance companies require least privilege access controls/authorization before granting a policy. Virtually all (95%) of U.S. companies had to invest in identity security solutions before obtaining a policy.**

3. **Although overall cyber insurance costs are increasing, AI is providing leverage for policyholders. Half of U.S. companies are using AI-supported threat detection and monitoring to reduce their cyber insurance premiums.**

Read on to benchmark your own identity security practices and cyber insurance strategies. What you learn will help you prepare for your next cyber insurance assessment and identify innovative ways to reduce your effort and costs.

47%

Identity and privilege compromises account for 47% of attacks that lead to insurance claims

Key Finding 1

Gaps in identity security are the most common cause of cyber incidents that result in insurance claims.

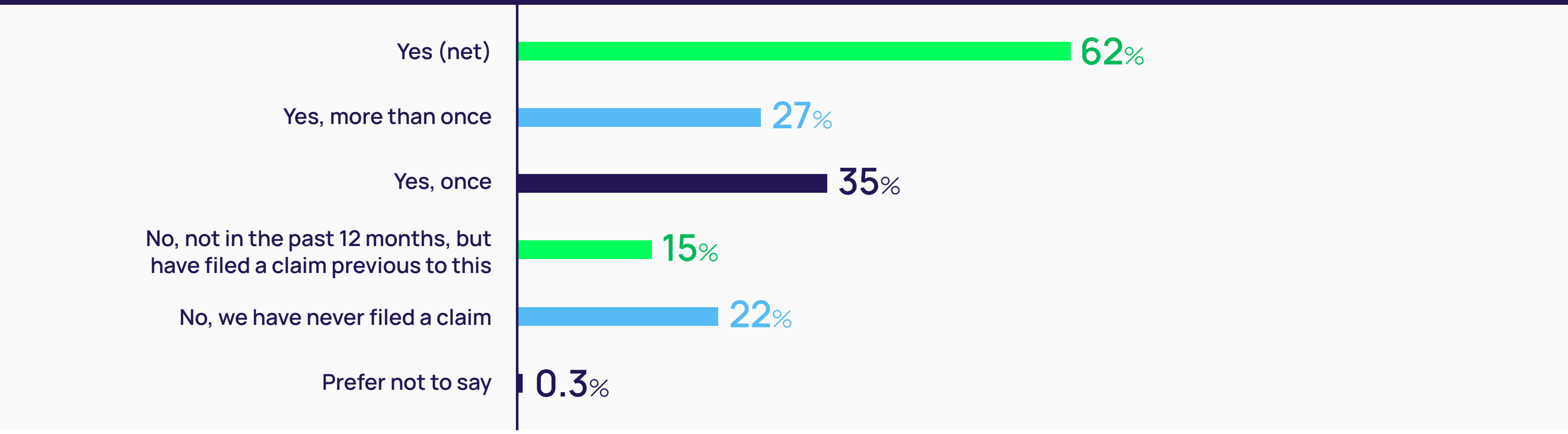
The frequency of cyber insurance claims remains high.

Once companies have cyber insurance, they use it.

The data shows that 77% of companies with insurance have previously filed a claim. This is consistent with the results of Delinea's 2023 survey, in which 79% of respondents said they had used cyber insurance in the past.

In the last 12 months alone, 62% of companies filed a claim. It's been a particularly bad year for more than 27% of companies, who filed more than once during the previous 12-month period.

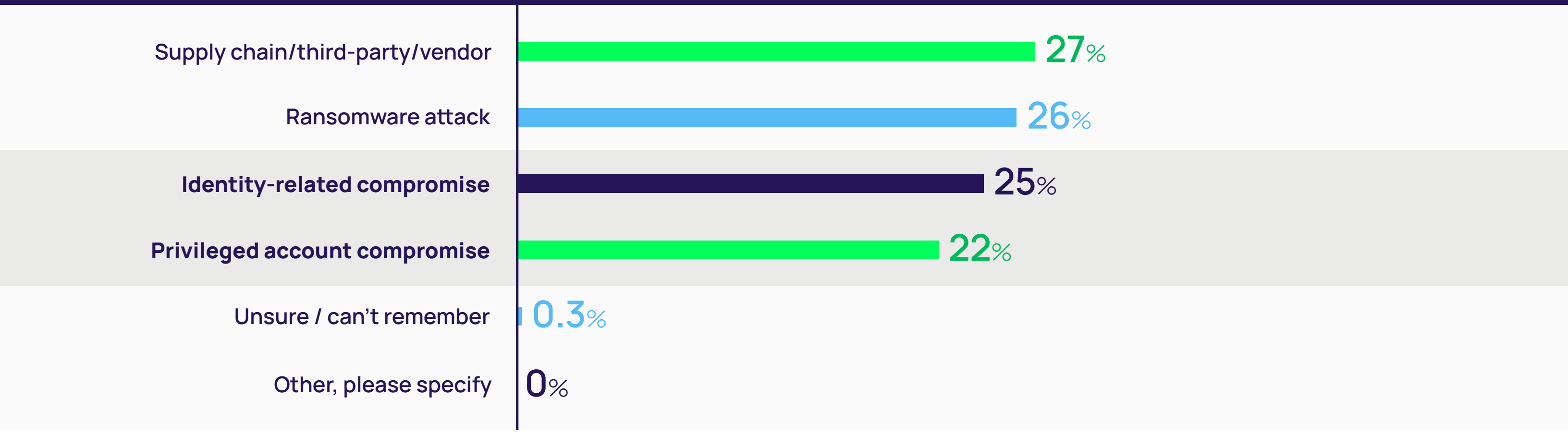
Figure 1 | Has your organization filed a cyber insurance claim in the past 12 months?



Attack techniques exploit identities and privileged accounts.

Taken together, two identity attack vectors, identity-related compromise and privileged account compromise, cause over 47% of attacks that lead to insurance claims.

Figure 2 | What caused the cyber incident related to the cyber insurance claim?



These days, most cyber attackers don't need to break in — they simply login. Identity-related attacks typically begin when an attacker uses valid credentials they have stolen or purchased. They may use those credentials to impersonate an authorized identity or utilize a privileged account so they can unlock access to protected resources. Depending on the level of access attached to that identity or privileged account, the attacker may be able to download malware, manipulate data, shut down systems, or more, all of which lead to a potential claim being filed with the insurer.

As part of the supply chain, third parties such as contractors, vendors, and partners often have access to sensitive data and IT systems. For example, IT operations teams often outsource tasks like troubleshooting, and engineering teams commonly scale using external developers. These users may access resources using a shared privileged account or an individual identity. Too often, these types of users operate without sufficient oversight, and access remains in place long after projects are complete, leaving vulnerabilities that bad actors will exploit, resulting in a potential payout for insurers.

Ransomware often gains a foothold through social engineering or phishing, encouraging users with local privileges to click on a link that downloads malware. Once they gain a foothold, an attacker can encrypt data and demand a ransom for the encryption key, or exfiltrate data and threaten to release it unless a ransom is paid.

Companies get cyber insurance coverage to support their compliance requirements and ensure business continuity.

We asked companies why they sought insurance coverage *at the time they did.* Triggers include compliance with regulatory requirements, directives from executive management or the Board of Directors, and reactions to recent cyberattacks, either within their industry or directly affecting their organization.

Respondents report that compliance/regulatory requirements are the *#1 driver* to get cyber insurance. The point here isn't that regulations such as PCI, HIPAA, and other compliance frameworks require that covered entities have cyber insurance. Neither is the point that cyber insurance is an effective strategy to pay for non-compliance fines, at least for most companies; the reality is that regulatory fines are the ***least common*** expense cyber insurance will pay for.

Figure 3 A | What were your main reasons for applying for cyber insurance, at the time you did?

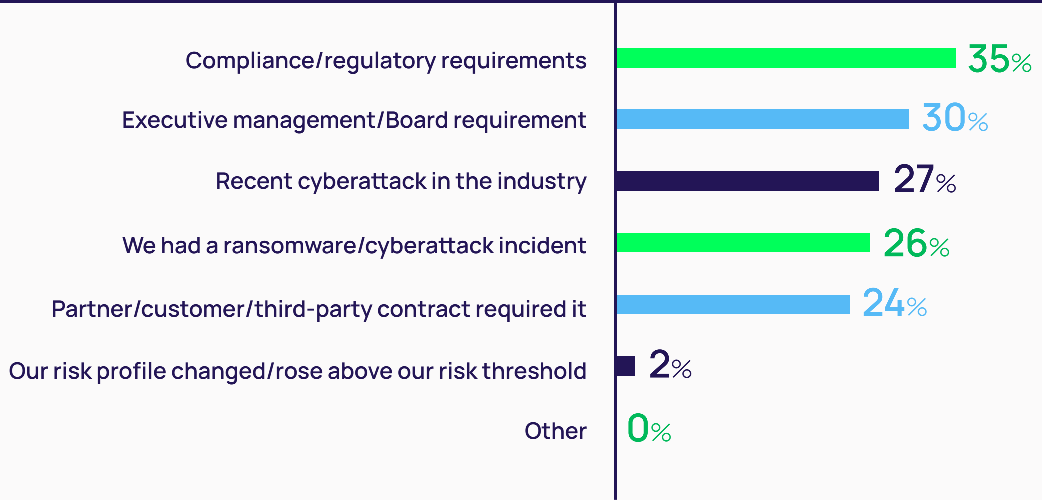
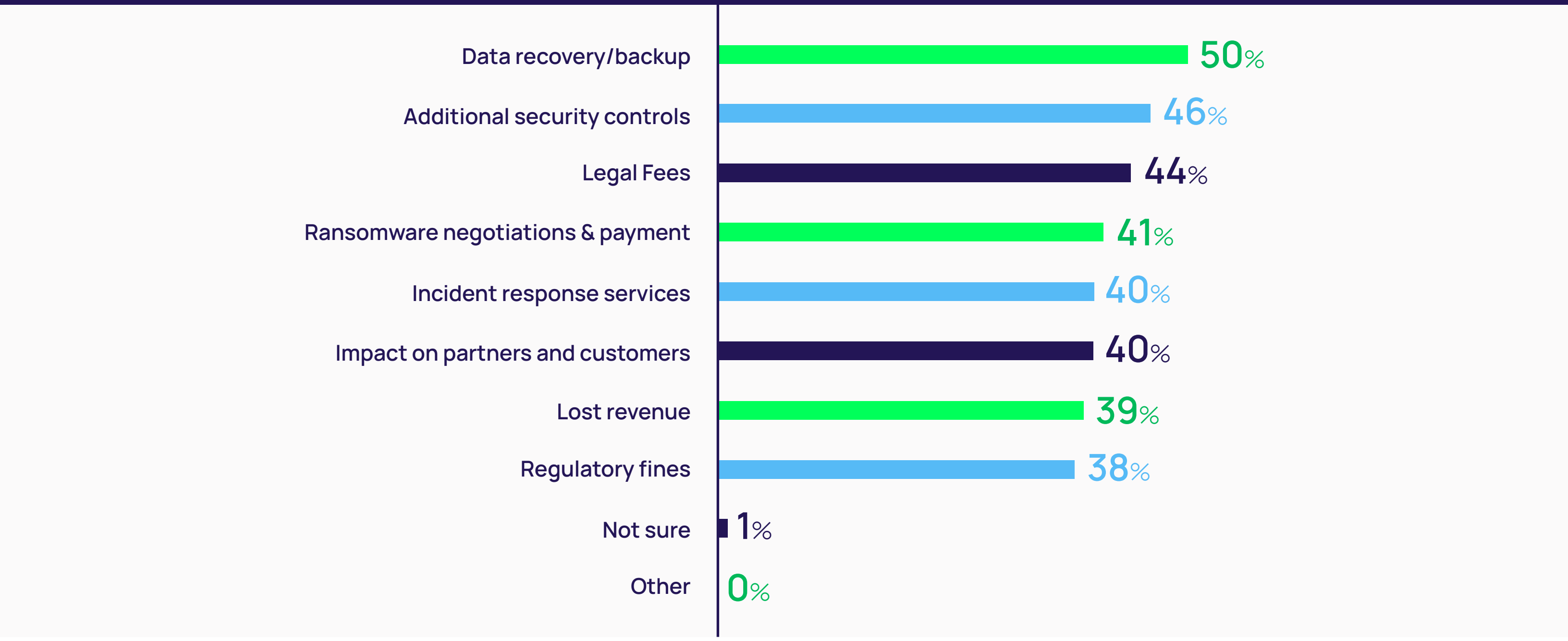


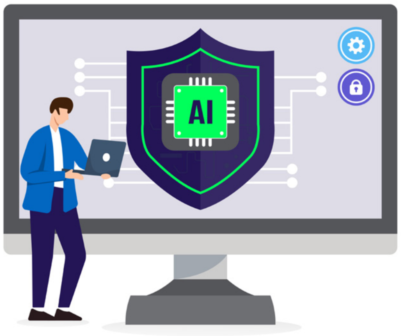
Figure 3 B | What would your cyber insurance policy pay for?



More likely, companies that are governed by industry regulations face stringent non-compliance fines regarding data protection. Quick recovery and backup can help avoid fines and other costs associated with non-compliance following a data breach because they allow you to quickly recover and secure data .

Cyber insurance focuses heavily on data recovery and backup services because they are essential for minimizing downtime and financial losses after a cyber incident. By covering these services, insurers support rapid recovery and business resilience, which benefits both the insured and the insurer.

Also consider that insurance is a risk management strategy, not a cybersecurity strategy. Many companies use compliance or cybersecurity frameworks like NIST to guide their security programs, even if they aren't covered entities. These frameworks call for evidence of security controls, as will insurance companies, because they are proven to reduce risk. If you put these controls in place, you'll be able to satisfy both regulators and insurance companies. Even if you're not bound by regulations that carry potential fines, you can't just skip this part and expect to pass your next audit or insurance assessment.



Half of U.S. companies are using AI-supported threat detection and monitoring to reduce their cyber insurance premiums

Key Finding 2

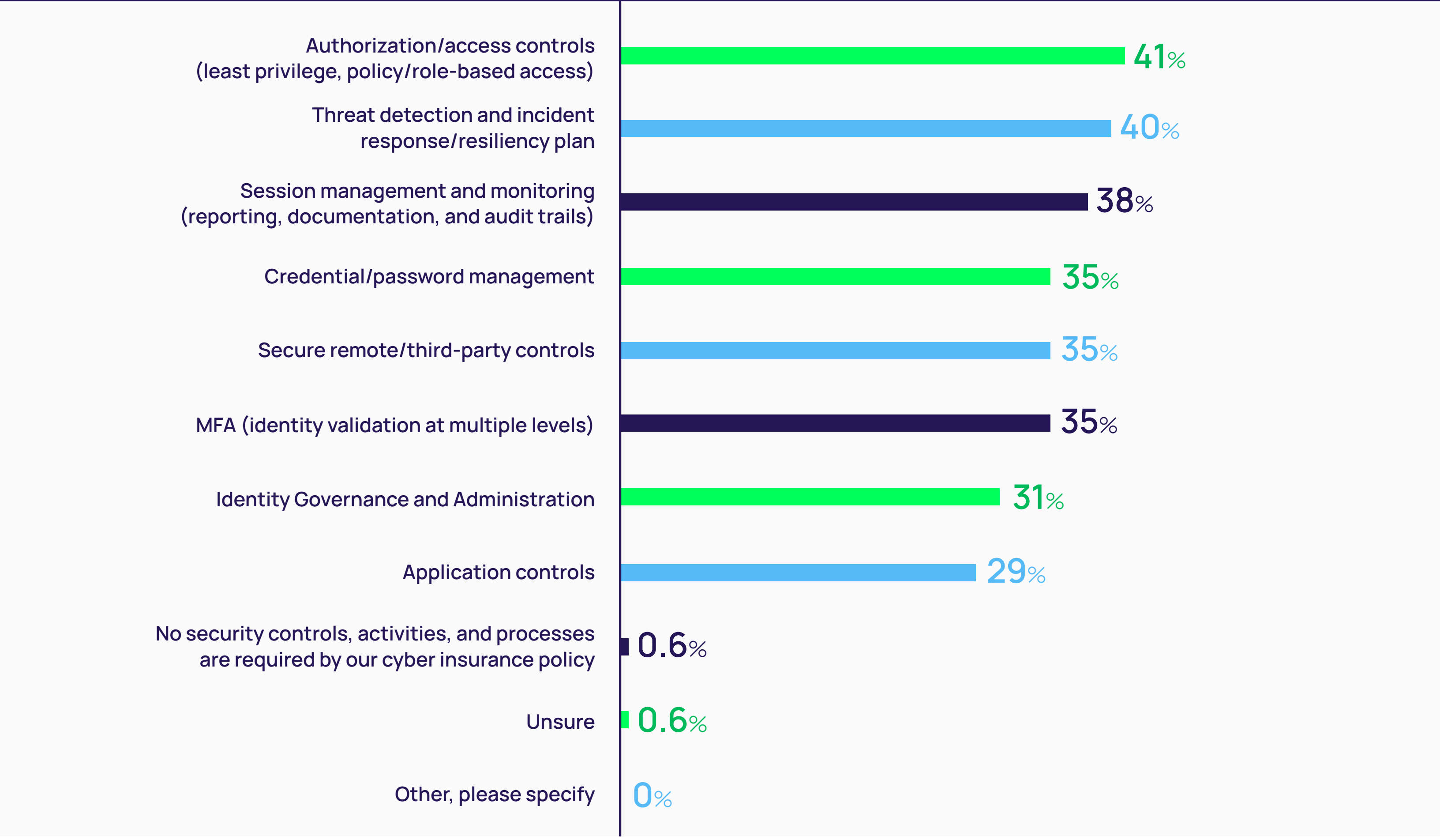
Insurance companies want evidence of identity security before granting a policy, with 41% requiring authorization controls.

Insurers require identity security controls, activities, and processes.

Now that they have more historical data pointing to the cause of cyberattacks, many insurance companies have requirements for policyholders to minimize the likelihood and impact of cyber incidents, reducing their potential payouts on claims. Nearly all respondents have some form of identity security requirement mandated by their cyber insurance provider. Most of those who were surveyed say cyber insurance policies require multiple identity security controls.

Insurers commonly require policyholders to establish controls related to authorization/least privilege access, followed closely by threat detection and response.

Figure 4 | What security controls, activities, and processes are required by your cyber insurance policy?



These controls align with industry best practices and regulatory requirements. Effective security controls not only help prevent incidents but also ensure that organizations can respond quickly and effectively, reducing downtime and financial losses. By requiring comprehensive security controls, insurers can better manage and predict potential losses, leading to more stable and predictable premiums for policyholders.

Required identity security controls defined

Access controls/ authorization

Access controls authorize what systems and data an identity can access and what they can do with that access. Companies typically manage authorization through policies such as role-based access controls or attribute-based access controls. Least privilege best practices require that identities have only the permissions necessary to perform their job functions, only when they need them.

Application controls

Application controls help you balance least privilege best practices and user productivity. Trusted applications are added to allow lists for automatic installation or execution, while known malicious applications (malware) are added to deny lists and blocked. Unknown applications can be sandboxed until they have been reviewed and approved.

Credential/password management

Credentials include usernames, passwords, tokens, and other secrets that unlock access to your systems and data. Cyber attackers use methods such as credential stuffing and password cracking to steal credentials. They may also buy credentials from access brokers on the dark web. To prevent theft, credentials should be difficult to guess and always secured. You can store credentials in a military-grade encrypted vault. Ongoing credentials management, such as rotation and expiration, ensures credentials have limited lifespans.

Identity Governance and Administration (IGA)

IGA controls permissions for identities throughout their lifecycle, including when users join, move, or leave and enables oversight of all the identities in your organization (human and machine) making it easy to demonstrate that oversight to auditors, cyber insurance companies, and compliance bodies.

Multi-factor Authentication (MFA)

Multi-factor authentication validates human identities by requiring people to provide something they have (such as a code on a phone or fingerprint) or something they know (such as challenge questions). Best practices call for identity validation at every interaction that carries high risk, including initial log in and privilege elevation.

Secure remote/ third-party controls

These controls allow remote employees and third parties to securely access the exact resources they need to complete their work, while still being closely monitored for ongoing oversight.

Session management and monitoring

Session management and continuous monitoring detect anomalies in identity activities and events, aiding in proactive incident prevention and rapid response. Audit trails allow you to identify patterns, useful for predicting risks and speeding post-event forensic analysis. In addition, granular reporting allows you to track improvements in your identity security posture, ensure accountability, and demonstrate evidence of controls to cyber insurance companies.

Threat detection and incident response

Effective threat detection and incident response are critical for cyber resilience and business continuity. Controls include mechanisms to detect threats and a structured response plan to proactively mitigate risks and contain and remediate incidents in progress. This includes redundancies to ensure minimal to no disruptions during an incident.

The importance of identity security is echoed by security and cyber insurance experts

CJ Dietzman
Senior Vice President of
Alliant Insurance Service

“

When I think about insurance carriers’ and underwriters’ expectations, identity security has become table stakes. The way cyber insurance companies measure risk is based on incidents, law, and claims. As we reverse engineer cyberattacks, often-times there were soft spots in identity management. You must have a good narrative of integrated controls and a holistic story on how you’re mitigating unauthorized access risk and protecting identities.”

“

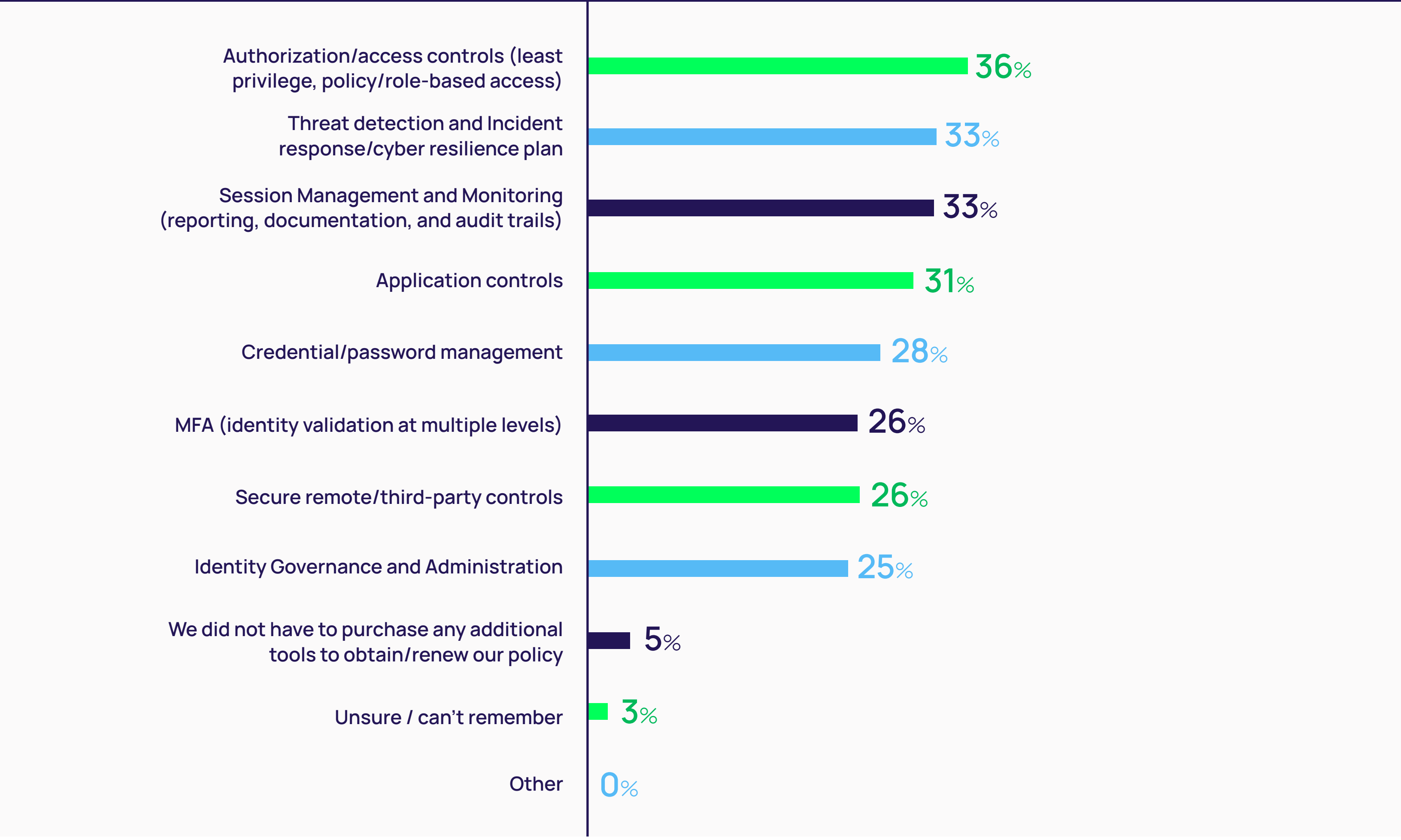
The greater portion of cybersecurity incidents that have reached the level of a claim are root-caused back to harvesting a credential, compromising an insider, using a third party that had access to your systems, etc., so when organizations are being evaluated for renewals, these are the questions that are asked.”

Myrna Soto
CEO of Apogee Executive Advisors
and an expert in cybersecurity and
risk management

The majority of companies surveyed had to invest in identity security solutions before obtaining or renewing their policy.

To satisfy the security requirements noted above, organizations say they can't simply present manual processes to potential insurance providers and expect to receive a policy. Instead, they needed to purchase identity security solutions as part of their security technology stack.

Figure 5 | What additional tools did you have to purchase to obtain/renew your policy?

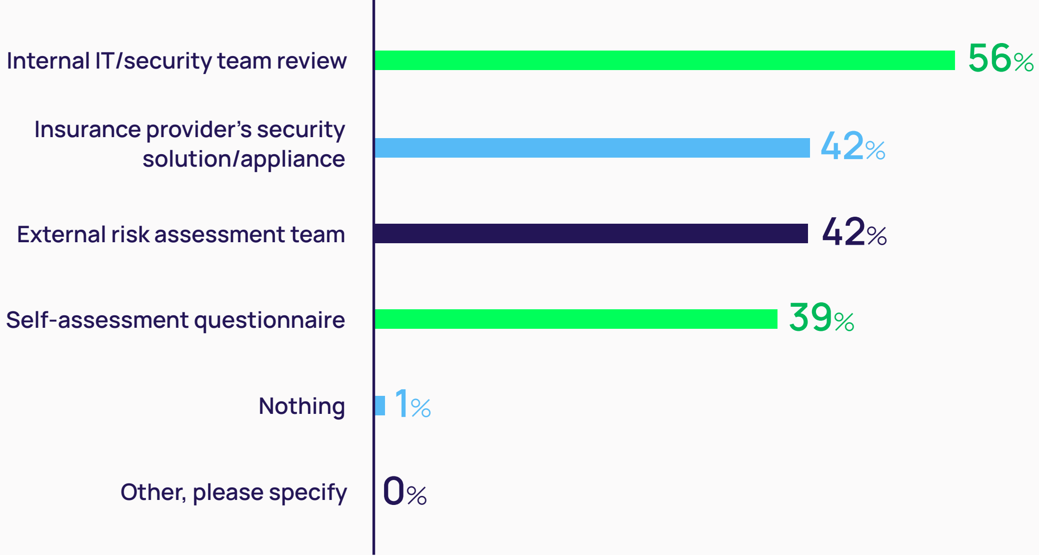


These results highlight organizations' diverse security needs and varying levels of preparedness regarding cybersecurity infrastructure.

Assessments evaluate security posture before policies are granted.

Reflecting the increasing maturity of the cyber insurance industry, insurers now require detailed assessments of security posture. Most respondents choose to conduct these assessments on their own. Others bring in a third-party risk assessment team to supplement their internal skillset and provide an unbiased view of a company's security posture.

Figure 6 | What types of assessments did you have to do to obtain your cyber insurance policy?



Whether you conduct these assessments on your own or rely on a third party, expect that they will take skilled IT and security team members away from their day-to-day work and more strategic projects.

41%

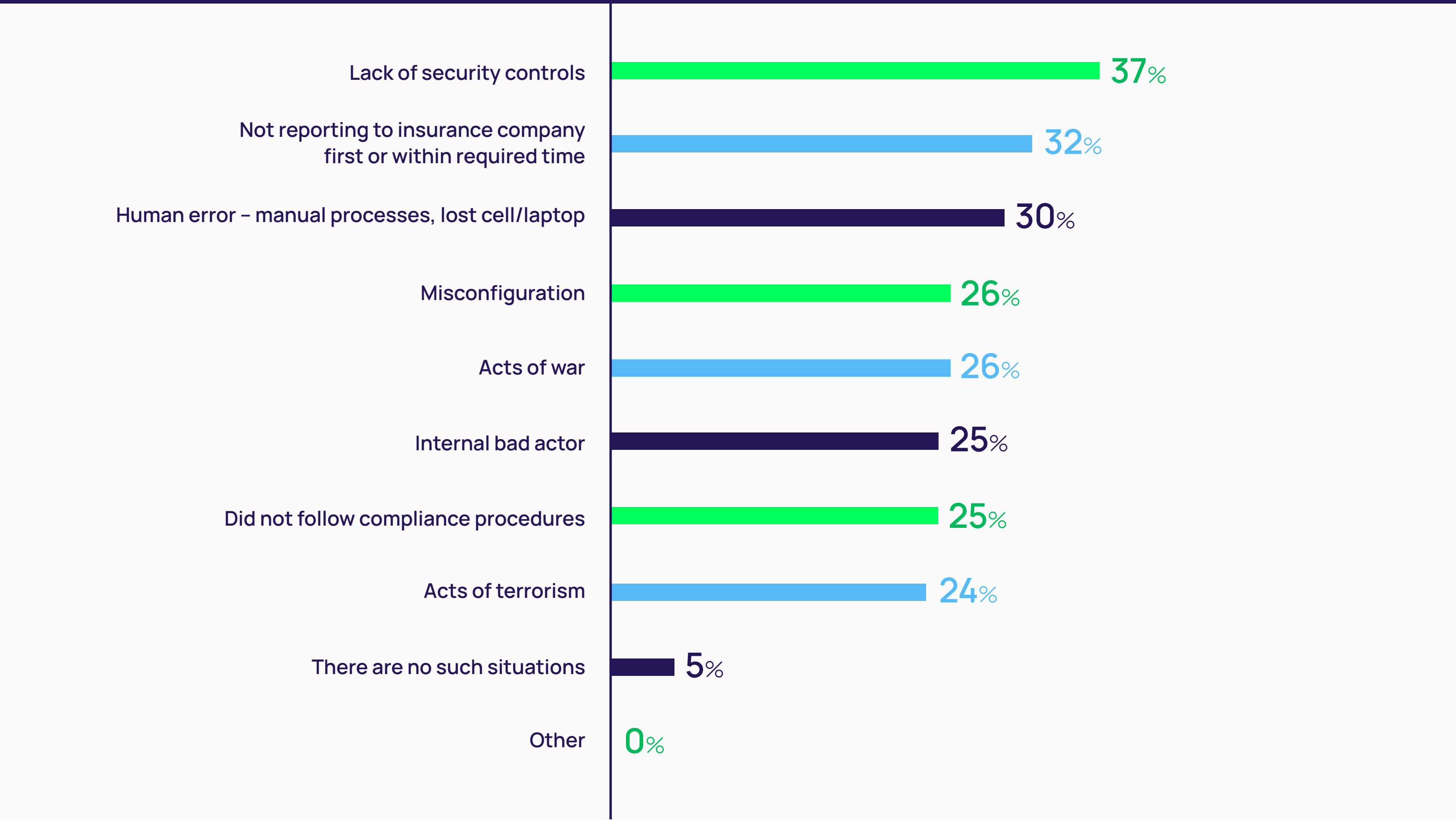
41% of insurance companies require least privilege access controls/ authorization before granting a policy

Requirements don't stop after policies are granted. You must maintain effective security controls if you expect claims to be paid.

Great news, you purchased identity security solutions, you demonstrated controls, and you passed your assessment. Your insurance policy has been granted!

However, the results of this survey show that if you don't keep those security controls in place and use them properly, you're likely to have an insurance claim denied. As respondents shared, you must make sure you're checking that security controls are applied to your changing organization, configured correctly, and working as expected.

Figure 7 | In what situations, if any, would your cyber insurance coverage be void?



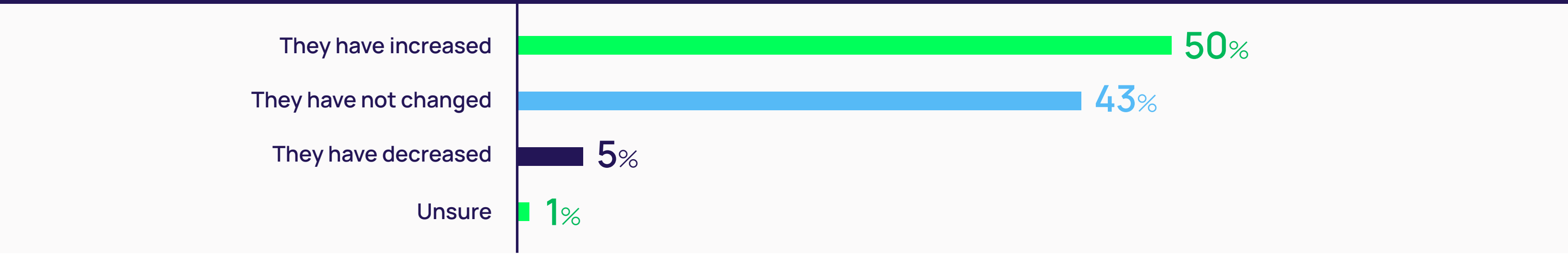
Your security posture isn't 'set it and forget it.' Your risk is always changing as your IT environment becomes more complex and people join, change roles, and leave the organization. The truth is that enterprises don't always follow the policies they proudly share with an insurance provider on their application.

Key Finding 3

Though overall cyber insurance costs are increasing, new technology like AI is reducing premiums.

Insurance costs continue to rise for many organizations.

Figure 8 | How, if in any way, have your cyber insurance costs changed since you applied or since you last renewed?



Though more than half report an increase, a year-over-year comparison shows that the increase is slowing. Last year, 79% of companies said that insurance costs increased since their latest application or renewal.

Why the rise for some?

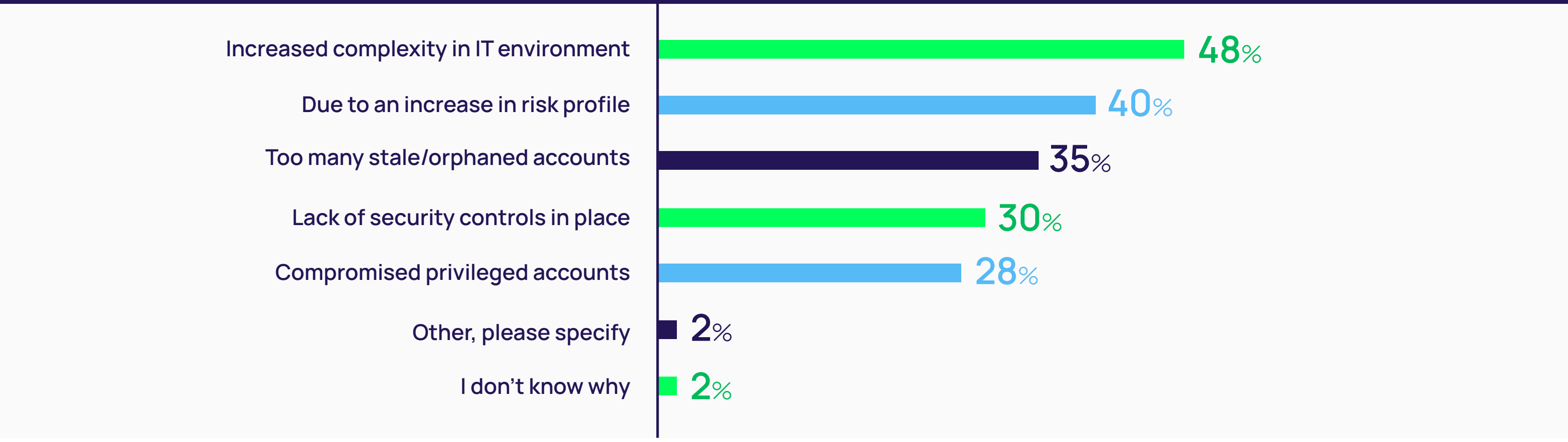
Consider the total cost of resources it takes to complete insurance assessments, address gaps, and demonstrate evidence of effective cybersecurity in a modern, hybrid IT environment.

Respondents point to IT complexity as a driving factor for rising costs. As the number of identities increases, more resources are required to accomplish these tasks. Complexity in the IT environment makes cyber insurance security assessments harder to complete, with disjointed audit and reporting solutions making it difficult to aggregate the details and measure risk.

Rising costs could mean that policyholders are requesting higher limits of coverage due to an increased risk profile. They recognize the business impact they'll need to shoulder if they experience a cyberattack and want to transfer that risk.

Based on IT complexity and risk profile, insurance companies may be raising prices for all policyholders to ensure sufficient liquidity in case a number of claims come in at once.

Figure 9 | Why did costs increase?



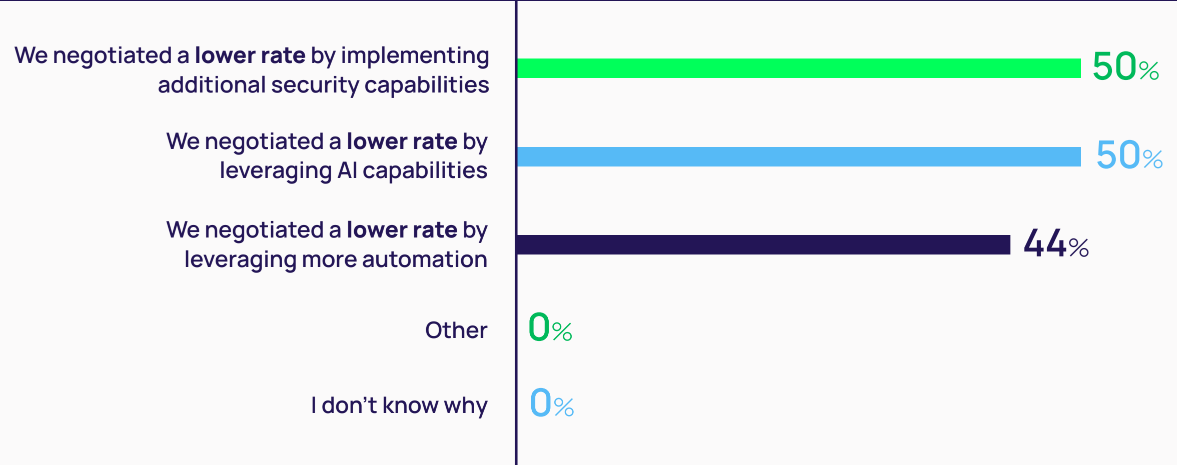
Cybersecurity solutions that quickly and comprehensively assess a complex IT environment and deliver risk-based reports you can share with insurance providers are effective means to lower your cyber insurance costs.

AI and security controls helped forward-looking companies decrease insurance rates.

Not everyone gets the same insurance rate. Your rate is determined based on how risky the insurance company views you — your risk profile. In the case of cyber insurance, your risk is influenced by factors such as your technology stack, security controls, and history. If you can demonstrate visibility and controls that make you a lower risk, you may be able to successfully lower your rates and, thus, your costs.

The survey results show that forward-thinking companies are reaping the benefits of AI to negotiate lower rates and, therefore, costs. The majority, however, still need to focus on adopting and implementing the foundations of strong identity security.

Figure 10 | Why did your insurance costs decrease?

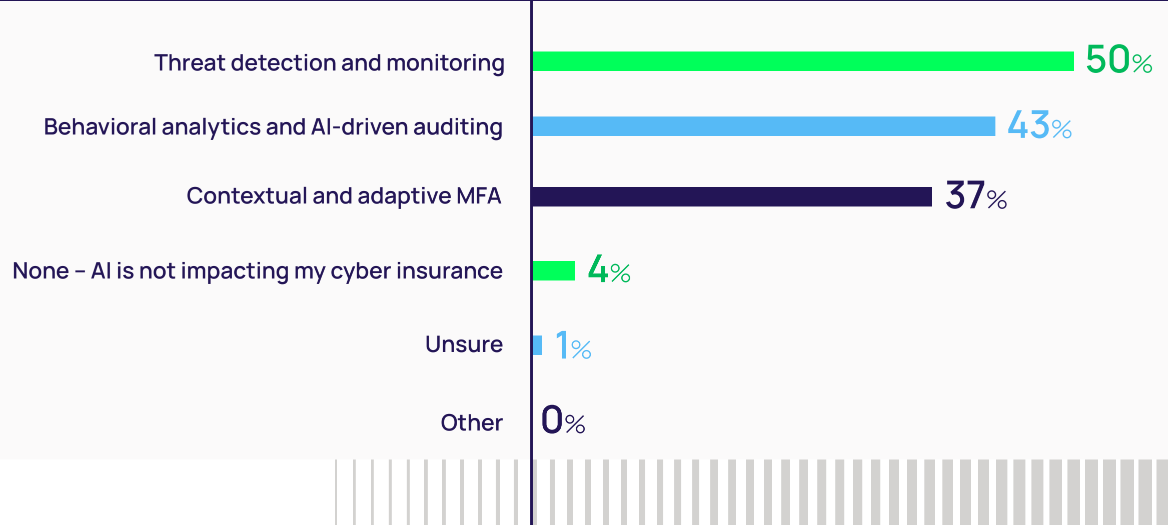


Artificial Intelligence, especially for threat detection and monitoring, is effective to reduce cyber insurance premiums

Premiums, the amount of money a business pays to keep an insurance policy active, are determined by the type of insurance you get, your policy limits, and your deductible, among other factors. The more confident you are in your security posture and controls, the better you can select the right insurance for you and negotiate lower premiums.

Companies are adopting Artificial Intelligence (AI) to ensure cybersecurity solutions and policies are working as expected and to contain incidents in progress so that they can reduce the dwell time of threat agents and blast radius of attacks, which in turn may lower your risk profile.

Figure 11 | What AI capabilities, if any, are you adopting to reduce your cyber insurance premiums?



Conclusion

While insurance is an essential tool for cyber resilience, you'll never be able to transfer all your risk. Cyber insurance needs to work in concert with robust, reasonable, defensible cyber security controls and processes.

In particular, insurance providers expect to see identity security policies and effective solutions before granting a policy. You'll need to share evidence of identity security controls in action and ensure you maintain these controls as your attack surface changes and your risk profile increases.

AI is helping organizations capture the knowledge of subject matter experts and act as "SOC assistant" to pinpoint identity-related threats faster, ultimately reducing dwell time, limiting the blast radius of an attack, and reducing risk. Based on the results of this survey, AI is poised to deliver even greater benefits as companies negotiate policies with insurance carriers

As part of their risk assessments, underwriters are going to want to know how you're embedding AI in your digital transformation efforts, including product development, coding, development, QA testing, etc. You should also expect questions that scrutinize how your security team is using AI for things like identity management, authorization, detection, and response. Any AI-based controls must be easily explainable, so that your team, auditors, and insurance providers are confident in how they work to reduce risk.

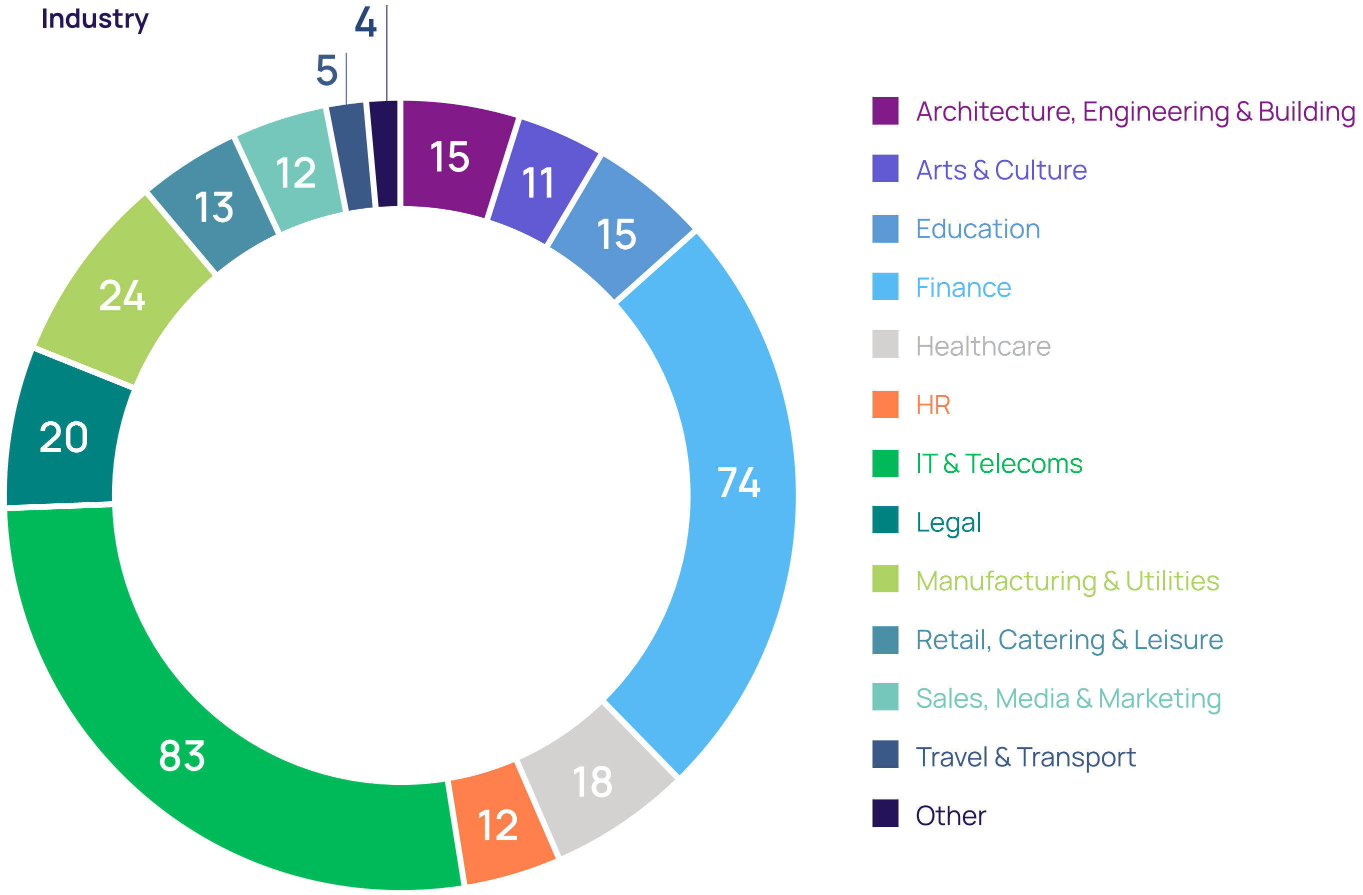
Most U.S. companies surveyed had to invest in identity security solutions before obtaining a policy

Methodology

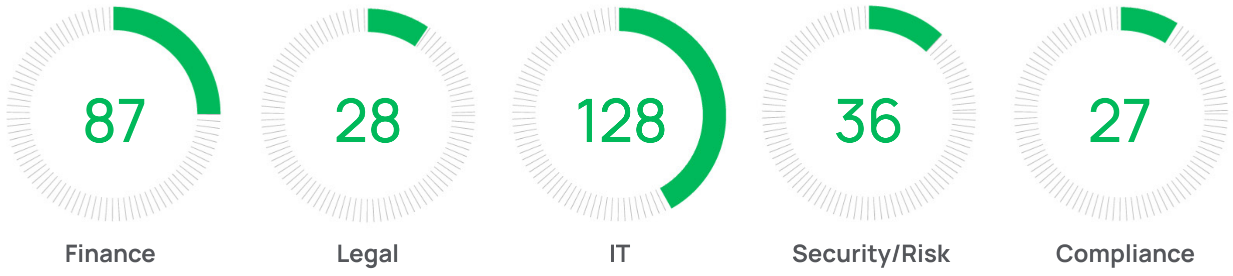
This online survey was conducted on behalf of Delinea by Censuswide, who, in June 2024, surveyed 306 leaders with visibility into their organization's cyber insurance application or renewal process. All respondents were presented with the same set of questions, and the answer options were randomized. Results were not weighted.

Breakdown of 306 respondents by counts

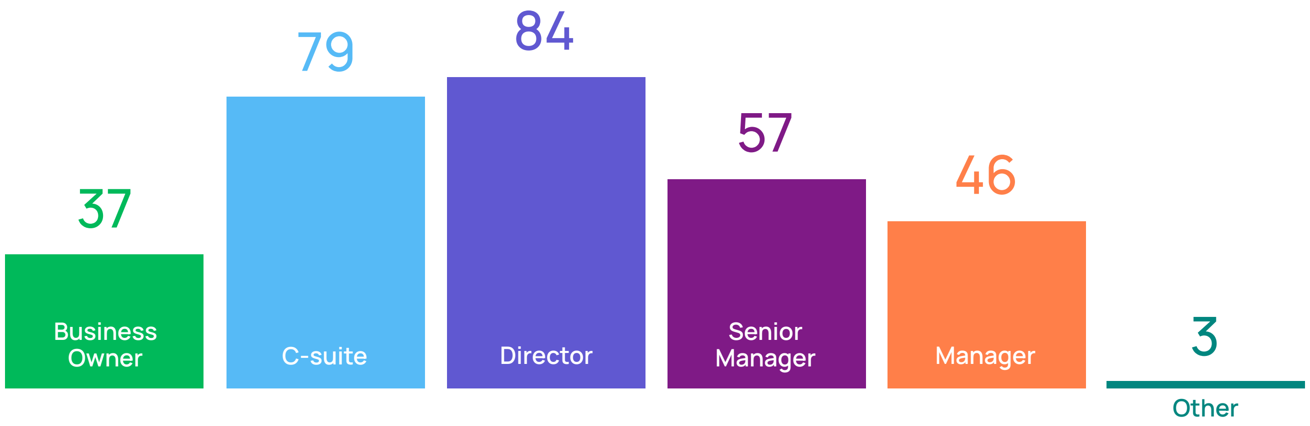
Industry



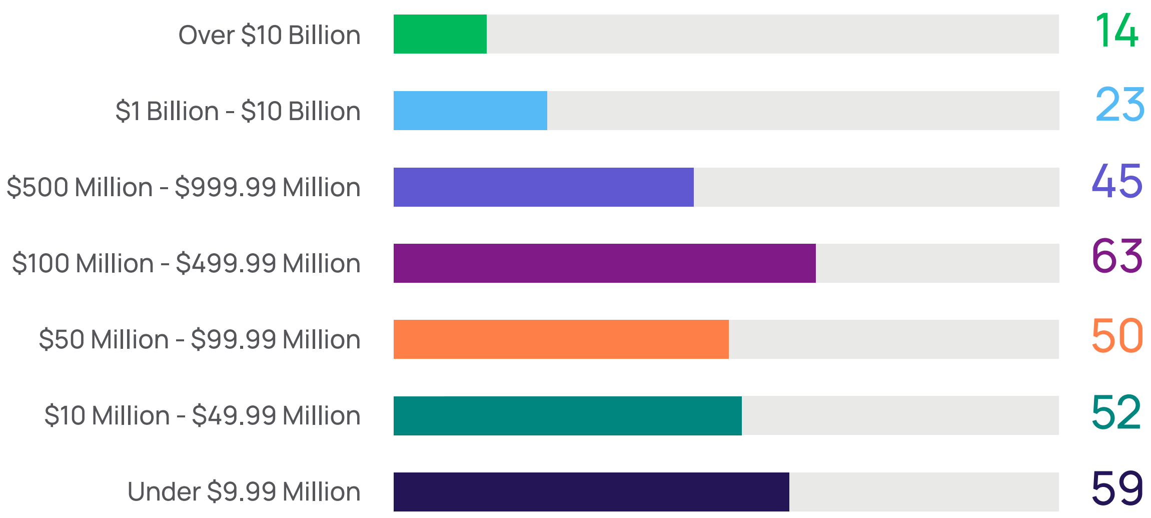
Roles



Titles



Company size



| Related Resources

WEBINAR

The Future of Cyber Insurance: Navigating the Impact of AI on Policy Holders

Hear what cybersecurity and insurance experts say about evaluating policy language to make sure you understand your coverage, exclusions, and how your provider will support you should an incident occur.

Watch Now

WHITEPAPER

Insights into Enhanced Cybersecurity Insurance Requirements

This report aggregates questionnaires from leading insurance companies and highlights the common questions. Specifically, it examines increasingly stringent insurer requirements for identity security, including multi-factor authentication (MFA), password management, access control, privilege elevation, session management, least privilege, and zero trust policies.

Download Now

PODCAST

Cyber Insurance Trends for Risk Management with Joe Carson of Delinea and Dara Gibson of Optiv

Learn how to have conversations about cyber insurance with your board.

Listen Now

Delinea

Defining the boundaries of access

Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across the modern enterprise. Delinea allows organizations to apply context and intelligence throughout the identity lifecycle across cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. With intelligent authorization, Delinea provides the only platform that enables you to discover all identities, assign appropriate access levels, detect irregularities, and immediately respond to identity threats in real-time. Delinea accelerates your teams' adoption by deploying in weeks, not months, and makes them more productive by requiring 90% fewer resources to manage than the nearest competitor. With a guaranteed 99.99% uptime, the Delinea Platform is the most reliable identity security solution available. Learn more about Delinea on **delinea.com**, **LinkedIn**, **X**, and **YouTube**.