Delinea

2025 Cyber Insurance Research Report:

Identity Security Controls Become Non-Negotiable for Coverage

As cyber insurance premiums rise, claims surge, and insurers scrutinize organizations with unprecedented rigor, one truth remains clear: **The quality and affordability of cyber insurance coverage will be directly proportional to the care an organization puts into adopting a strong set of identity-first security controls.**

Delinea partnered with Censuswide to survey more than 750 security leaders to understand the state of their cyber insurance coverage and claims practices. The survey results provide some compelling benchmarks for organizations regarding how their security controls and identity security practices can affect their insurability in 2025 and beyond.

Key takeaways include:

▶ **Insurability is now measured by control maturity.** A near unanimous 99.5% of respondents stated that at least some level of security controls, activities, or processes had to be in place to secure coverage.

▶ **Cyber insurance claims are on the rise, and so is insurer pricing and scrutiny.** The number of respondents who filed a claim in the last year rose 10 points to 72% this year. And 70% of organizations said their insurance costs rose this year. Almost all respondents had to undergo insurer assessments to get coverage, and 51% needed to use an insurance provider's preferred security solution or appliance.

▶ **CISOs can't assume coverage safety simply because they have a policy; gaps must be identified and managed.** Only 33% of policies cover lost revenue, and just 45% cover ransomware negotiations or payment. Approximately 45% of organizations said their policy could be deemed void due to a lack of security controls.

▶ **Identity-first controls are the new requirements that insurers now demand.** About 97% of respondents reported that identity-related controls influenced their premium or coverage terms in some way at renewal. The most commonly cited factor was Privileged Access Management (PAM), a core element of identity security, which influenced terms at 41% of organizations.

▶ **AI offers both risks and rewards when it comes to insurance.** A significant 86% of respondents said that their insurers offered them premium reductions or credits for their use of AI in security controls. But weaknesses in broader AI adoption could also trigger exclusions: 42% said their policies had AI misuse and liability as an exclusion in their cyber insurance policy language.

The findings of this report offer CISOs and other risk leaders a roadmap for navigating a cyber insurance landscape fraught with exclusionary pitfalls and potential coverage obstacles. It provides data for organizations that can help prove their insurability, justify identity security investments, and anticipate how AI and regulation are reshaping coverage.

Finding 1:

Insurability is now measured by control maturity

Cyber insurance is no longer seen as simply a stopgap measure for cyber risk. Our study indicates it is increasingly becoming an integral component of risk management and compliance strategies.

An overwhelming 84% of organizations reported that they have expanded their cyber insurance coverage over the last 12 months with either new policies or new areas of coverage. Companies with revenue over $10 billion per year were slightly less likely than the overall pool to have grown their coverage, with 72% reporting expansion. This is likely an indication that these larger enterprises

are at the front end of the maturity scale, with many of them having already determined the exact amount of coverage needed to buy down risk in line with their risk appetite.

The pressure for establishing and expanding coverage areas is coming from many different directions: regulators, executive management, partners, and threat activity. The survey revealed that no single factor was an overwhelmingly dominant driver for purchasing cyber insurance policies, with regulatory requirements narrowly surpassing board requirements to claim the top spot.

What were your main reasons for applying for cyber insurance at the time you did?

Reason	%
Compliance/regulatory requirements	37%
Executive management/board requirement	36%
Recent cyberattack in the industry	27%
Our risk profile changed/rose above our risk threshold	27%
We had a ransomware/cyberattack incident	25%
Partner/customer/third-party contract required it	24%

As more companies increasingly seek broader coverage to address risk gaps, they're facing the reality that cyber insurance cannot replace a lack of controls. Cyber insurers are growing more savvy by the day about the cybersecurity market, and their underwriting processes are more tightly aligned with control requirements than ever.
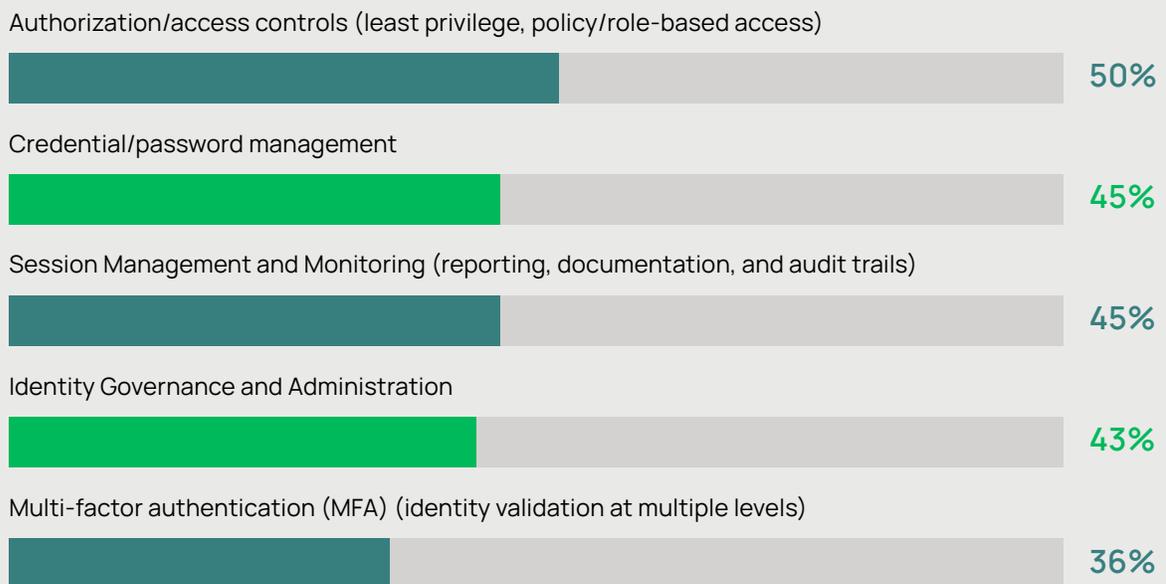
Our survey demonstrates that insurability is now measured by control maturity. A near-unanimous 99.5% of respondents stated that at least some level of security controls, activities, or processes had to be in place to secure coverage. More than half of respondents said their cyber insurance policy required a threat detection and incident response/resilience plan as well as authorization/access controls. And in every category, required

99.5%

of respondents stated that at least some level of security controls, activities, or processes had to be in place to secure coverage.

security controls have grown year over year, with some areas especially emphasized by insurers. Threat detection requirements increased from 40% last year to 53% this year, and authorization/access controls rose from 40% to 50% during the same period. Credential/password management and secure remote/third-party controls both increased from 35% to 45%.

The study showed that identity and access management controls are particularly significant litmus tests for cyber insurance underwriters:

Authorization/access controls (least privilege, policy/role-based access)

50%

Credential/password management

45%

Session Management and Monitoring (reporting, documentation, and audit trails)

45%

Identity Governance and Administration

43%

Multi-factor authentication (MFA) (identity validation at multiple levels)

36%

Delinea

Finding 2:

Cyber insurance claims are on the rise, and so is insurer pricing and scrutiny

As more organizations purchase cyber insurance policies and an increasing number are hit by breaches and cyber incidents, it logically follows that cyber insurance claims would also rise. Our study corroborates broader industry statistics about the increase in cyber insurance claims in 2025.
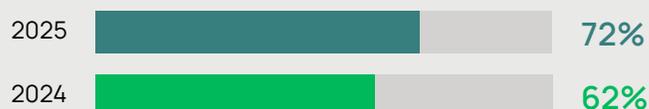
The number of respondents who reported they'd filed a claim in the last 12 months rose to 72% this year, compared to 62% last year. The ratio of organizations that have filed multiple claims in the previous year is also on the rise — 37% this year compared to last year's 27%.

Larger organizations were more likely to rely heavily on their cyber insurance policies for support. At the same time, 45% of organizations with headcounts over 3,000 filed multiple claims in the last 12 months, just under a third of organizations with under 250 employees reported the same.

Insurers are in the business to make money, so it should come as no surprise that the rise in claims has spurred coverage pricing increases. The increased costs of payouts are also driving cyber insurers to grow more sophisticated in the types of controls they require from insureds and also the level of scrutiny they apply to determining where and how those controls have been applied.

Overwhelmingly, 70% of respondents reported that costs have risen since they applied for or renewed their cyber insurance policy. This is a

The number of respondents who reported they'd filed a claim in the last 12 months

2025	72%
2024	62%

Organizations that have filed multiple claims in the previous year

2025	37%
2024	27%
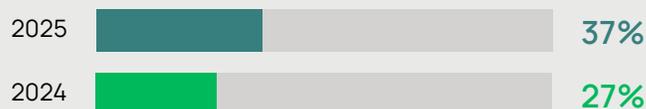
sharp increase from the previous year, when only 50% of respondents reported rising costs. A scant 2% reported their costs had decreased. Interestingly, although larger organizations are more likely to have reported multiple claims in recent years, the smaller organizations are more likely to report increased policy costs. 73% of organizations with $50M or less in revenue reported increased costs compared to just over half of respondents with $10B or more in revenue.

This could be correlated with controls maturity, as big-budget enterprises tend to have more controls in place than their smaller counterparts and could be reaping the benefits of discounted rates as a result.
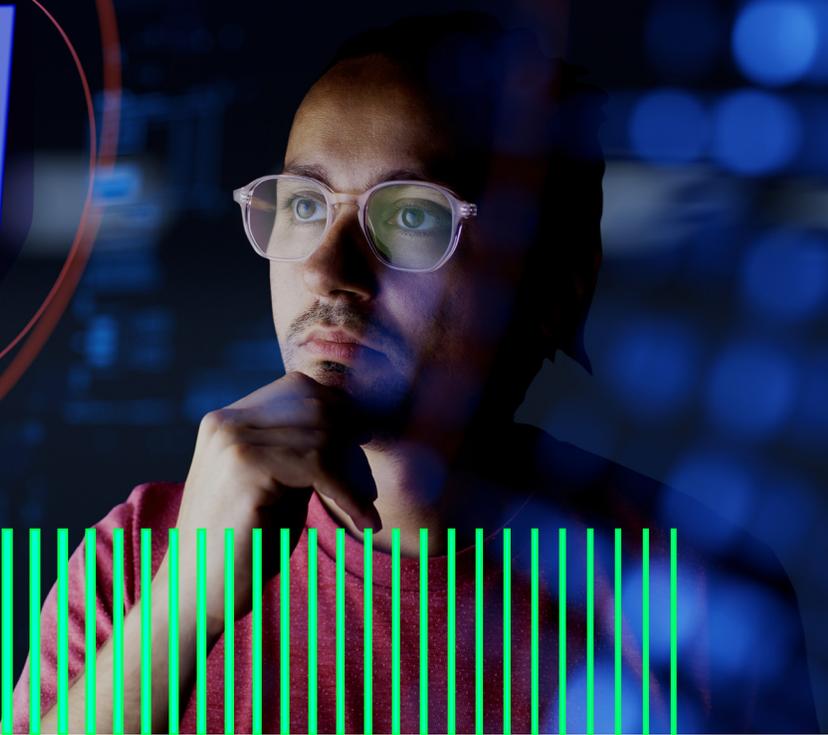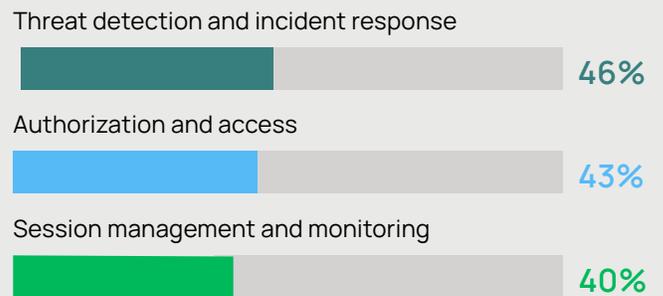
In addition to the increase in claims driving cyber insurance cost increases, multiple factors are at play. Approximately 68% of organizations cited increased complexity in their IT environment as a factor in rising insurance prices, and 50% said it was due to an increase in risk profile. More than a third of organizations also cited compromised privileged accounts or a lack of security controls in place as a contributing factor.

In addition to spending more on the policies themselves, almost all organizations have had to step up their investment in some sort of new or updated security tooling to obtain or renew their policies. Less than 5% of organizations reported not needing to purchase additional tools for their latest coverage.

Nevertheless, many organizations were able to satisfy escalating controls requirements at least partially through existing software or internal work across part of their security stack. For example, while 45% of respondents said that their policies required secure remote/third-party controls, only
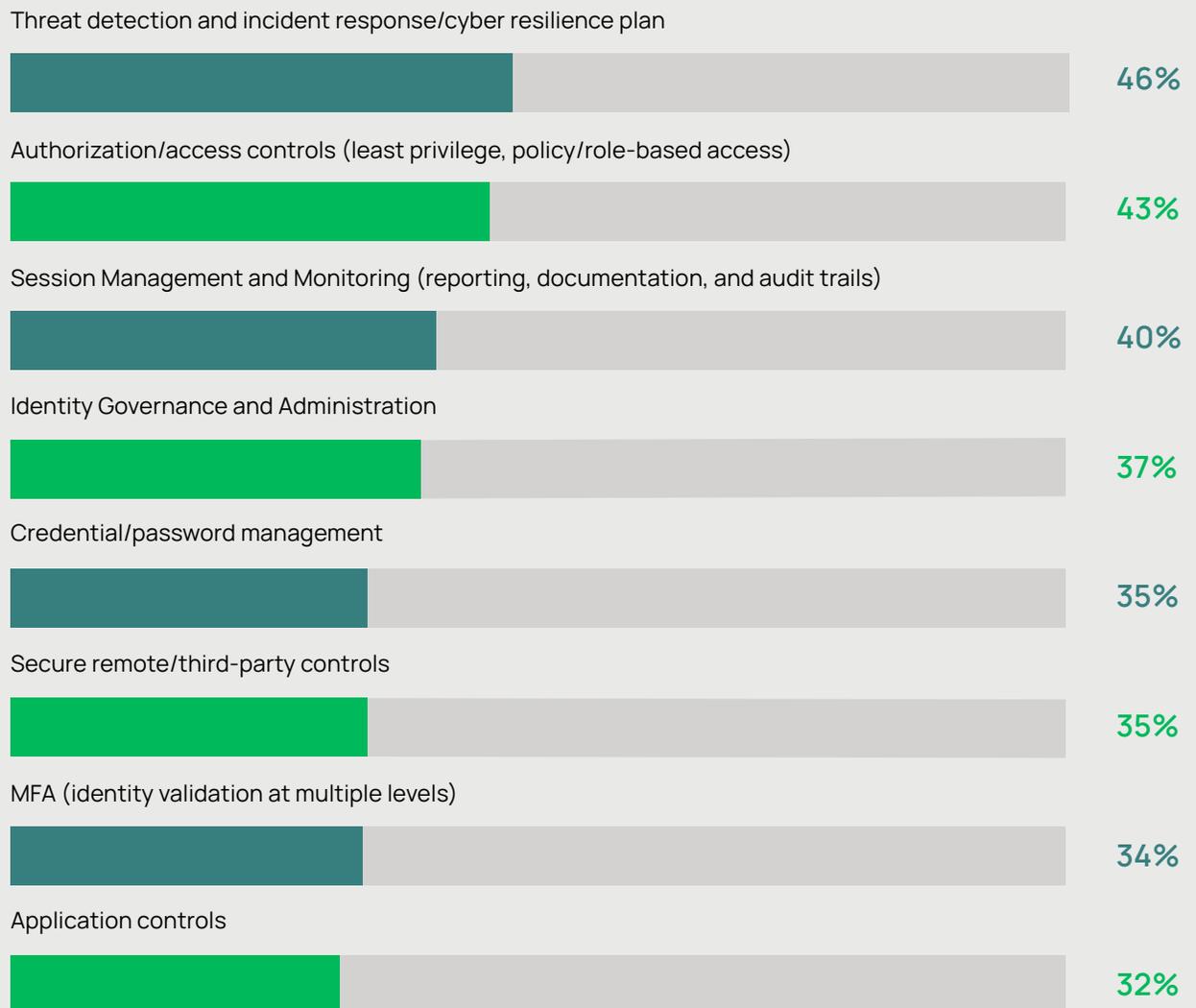
The most commonly cited new tools

Threat detection and incident response

46%

Authorization and access

43%

Session management and monitoring

40%

35% reported having to purchase new tools to satisfy those controls requirements.

The additional tools respondents had to purchase to account for added policy requirements grew sharply year over year. Threat detection and incident response saw the largest increase, rising from 33% to 46%, while MFA grew from 26% to 34%. The most commonly cited new tools were threat detection and incident response (46%), authorization and access (43%), and session management and monitoring (40%).

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

Threat detection and incident response/cyber resilience plan

46%

Authorization/access controls (least privilege, policy/role-based access)

43%

Session Management and Monitoring (reporting, documentation, and audit trails)

40%

Identity Governance and Administration

37%

Credential/password management

35%

Secure remote/third-party controls

35%

MFA (identity validation at multiple levels)

34%

Application controls

32%

Cyber insurers are increasingly scrutinizing their insureds before issuing policies. The percentage of insurers requiring internal and IT security team review increased significantly to 77% from 56% last year. And, insurers are less likely to take these internal assessments as the last word in certifying risk levels. The use of insurance provider security solutions and appliances has reached a tipping point, with 51% of organizations now reporting that they must comply with this type of oversight. That's up from 42% last year. Additionally, 50% of organizations reported that they are subject to external risk assessment, up from 42% last year.

Finding 3:

CISOs can't assume "coverage safety" just because they have a policy — gaps must be identified and managed

Cyber insurers are managing their costs by constantly tightening policy language for when and how much certain losses are covered. Plus, they are raising prices and barriers to entry for issuing new policies and renewals. Cyber insurance customers must be cautious of coverage limitations and policy exclusions for incidents such as acts of cyberwarfare. Additionally, organizations must be aware of lapses in controls and processes that could void their coverage when it is needed most.

33% of organizations report that their policy covered lost revenue

Our study revealed that while 60% of cyber insurance policies cover data recovery, only about half of these policies also cover lost revenue from cyber events. Just 33% of organizations report that their policy covered that. Startlingly, less than half of policies covered incident response services or additional remediative security controls necessary to recover from an incident. The

percentage of policies that cover legal fees related to incidents dropped from 44% last year to 39% this year.

Less than half (45%) of policies cover ransomware negotiations and payments. Given that 1 in 5 organizations reported a ransomware incident as the reason for expanding their coverage, there may be a discrepancy between the expectations and the reality of what an insurance policy actually covers when things go wrong.
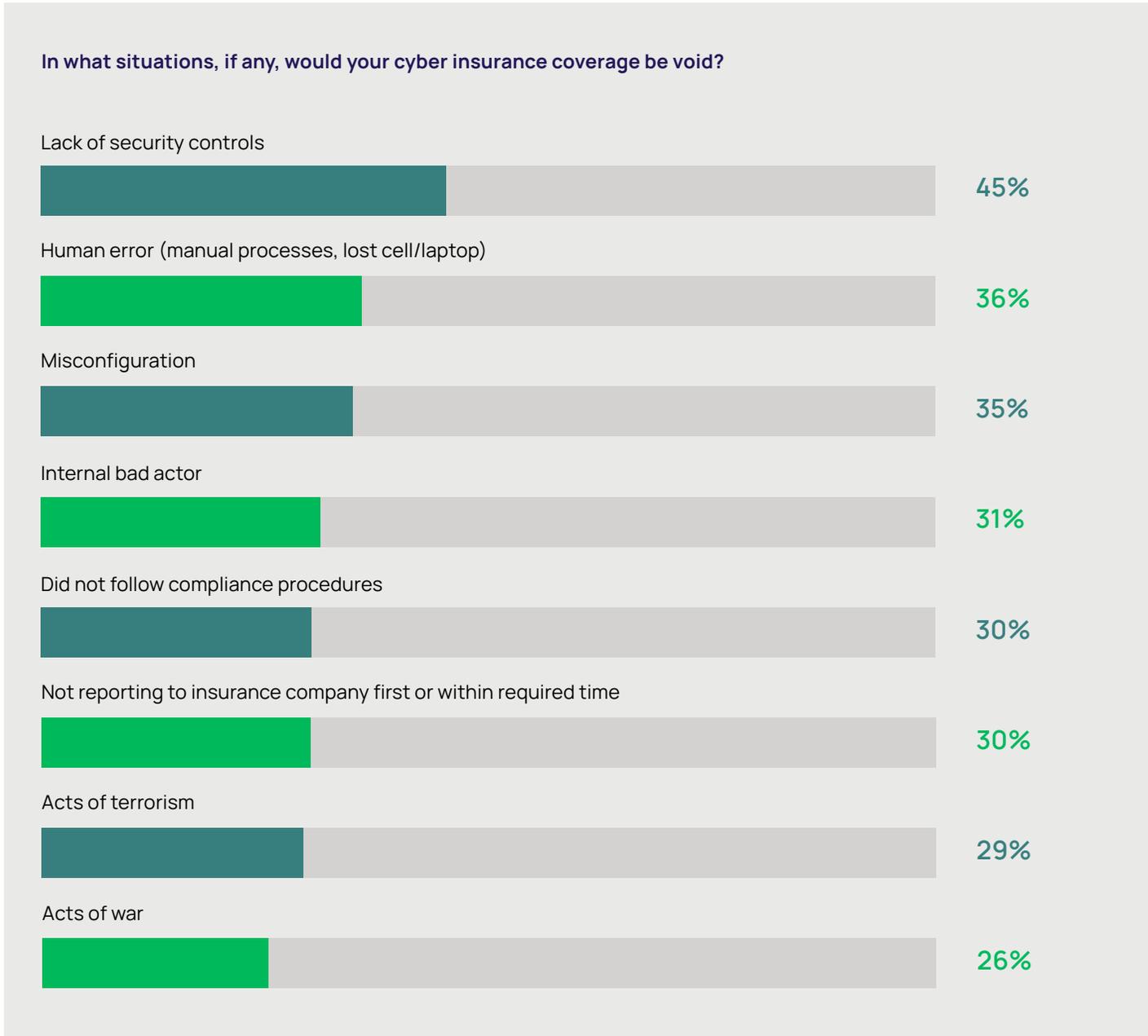
Larger organizations tend to have more comprehensive coverage, though. For example, 42% of respondents had lost revenue coverage, and these respondents reported having four separate items covered by their policies on average.

But even without significant coverage gaps, a policy may not hold up for organizations if they aren't careful about policy terms that void coverage. **Insurance adjusters are on the lookout for a range of controls lapses that could get their companies off the hook for paying a claim.**

According to our respondents, these types of conditions are increasingly making their way into cyber insurance policies. Only 8% of respondents reported that no situation exists in their policy that would cause it to be void.

The number one reason adjusters can void policies is a lack of security controls. The percentage of organizations stating that this language exists in their policies rose year over year by eight points to 45%, while the number reporting misconfigurations as a potential contract nullification increased by nine points to 35%.

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

Lack of security controls

45%

Human error (manual processes, lost cell/laptop)

36%

Misconfiguration

35%

Internal bad actor

31%

Did not follow compliance procedures

30%

Not reporting to insurance company first or within required time

30%

Acts of terrorism

29%

Acts of war

26%

Policies for larger organizations with over $10B in revenue tend to be stricter than those for smaller organizations. For instance, while only about 33% of organizations with $10M-$50M in revenue would have their policy declared void for human error or misconfiguration, 44% of over $10B revenue organizations would have their policy declared void.

Finding 4:

Identity security-first controls are the new requirement that insurers demand

Amid tightening policy restrictions, rising prices, and exclusion pitfalls, it might seem at first that the cards are stacked against organizations to get a good ROI out of their cyber insurance policy. This may even be true for organizations that view cyber insurance as a pass to avoid investing in modern cybersecurity controls. But our survey indicates there's plenty of opportunity to secure affordable insurance plans you can rely on—provided you continually improve your cybersecurity risk management practices.

Organizations that can prove cyber risk management maturity typically end up securing better premiums, coverage, and claims outcomes. Identity security can play an outsized role in how insurers assess their customers' progress up the maturity scale.

When asked whether identity-related controls influenced their premium or coverage terms at renewal, only a slim 2.5% of respondents said it had no influence. Diving into the identity controls that matter most, 41% of respondents most commonly cited PAM as the top difference maker for how the underwriters viewed their insurability. That was followed by identity governance and administration (IGA) (38%) and third-party and vendor access controls (32%).

These numbers are logical when analyzed in the context of the primary cyber incident causes leading organizations to file claims in the past year. We followed up with claimants to ask for the most detrimental factors that led to the claims-related incident, and 46% of organizations said the incidents were either identity-related or caused by a privileged account compromise. Meanwhile, the most common single factor behind claims was those incidents involving suppliers and vendors, which were reported by 29% of respondents and 39% among large organizations with over $10B in revenue.
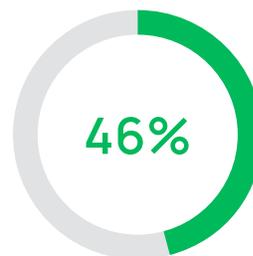
46% of organizations said the incidents were either identity-related or caused by a privileged account compromise

Insurers are closely following these kinds of root cause statistics and are taking notice of the controls that can reduce the most common risks.

Finding 5:

AI offers rewards and risks for insurability

AI adoption is shifting the cyber insurance landscape—both as a risk reducer and an additional exposure point.

Respondents reported that AI-powered defense tools are earning organizations premium reductions. **As security teams utilize AI-embedded controls, they're becoming more effective, which insurers recognize.**
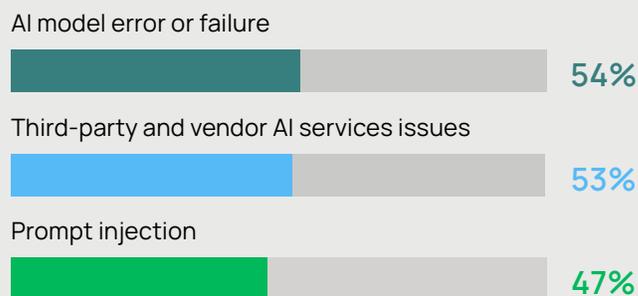
Of all respondents, 86% reported that insurers offered them premium reductions or credits for their use of AI in defense. According to those respondents who said their overall cyber insurance costs have decreased in the last year, a striking 64% reported that they leveraged AI to bring these costs down. This cyber insurance trend has been on the uptick since last year, when that ratio was about 50%.

When asked which specific AI capabilities they're adopting to lower premiums, 63% reported AI-powered threat detection and monitoring as the most common premium influencer, followed closely by behavioral analytics and auditing, which was named by 59%. Half of organizations reported that anomaly detection using plain language AI query capability is reducing rates, while 41% cited contextual and adaptive MFA.

At the same time, cyber risk professionals say that AI-related vulnerabilities across the enterprise are driving new policy exclusions and coverage complications. When asked which emerging risks

they believed insurers would focus on most in the next one to two years, AI misuse and liability was the number one factor, named by 42% of respondents. Number two was data sovereignty and compliance failures, named by 38%, which is often closely tied to AI usage.

Three biggest exclusionary events related to AI

AI model error or failure

54%

Third-party and vendor AI services issues

53%

Prompt injection

47%

Less than one in ten survey respondents reported that they hadn't yet seen any exclusions related to AI added to their policies. The three biggest exclusionary events related to AI were AI model error or failure (54%), third-party and vendor AI services issues (53%), and prompt injection (47%). These three common AI weaknesses are likely to be the battleground of the next generation of claims legal battles, and organizations will be called by their insurers to balance AI adoption to avoid introducing uninsured risks to their infrastructure.

Final Insights

Cyber insurance is a maturing market for the insurance industry. As such, it is still undergoing significant changes as insurers tweak their coverage, pricing, and exclusions to rationalize the market for their bottom line. Many traditional insurers are still refining their expertise and statistical risk models for cyber incidents, which means cyber policies tend to be more in flux at each renewal than standard business liability policies.

98% of respondents expressed confidence that their organization could obtain the same or better coverage in the next year

The good news is that cybersecurity remains a win-win proposition for insurers and insureds under the right circumstances. When we asked respondents how confident they were that their organization could obtain the same or better coverage in the next year, an overwhelming 98% expressed confidence. The trick, of course, is to make that happen at the lowest cost possible while ensuring their controls meet policy requirements, thereby guaranteeing coverage withstands adjuster and legal scrutiny in the event of incidents.

As cyber executives incorporate insurance into their broader strategy, they must recognize the distinct financial implications of deploying

controls and demonstrating their security posture to insurers. As risk professionals consider what these survey findings mean to them, they should consider two additional insights based on our analysis of the data and our observations of cyber insurance market dynamics.

Regulatory mandates are now an insurance factor

Because the cyber insurance market is still maturing, policy language and coverage options can vary widely from insurer to insurer — and even policy to policy. One of the challenges that organizations face is in the interpretation of policy requirements. While policy exclusions tend to be fairly clear-cut (i.e., exclusions around acts of war or nation-state activity), the language around controls requirements can sometimes remain vague.

The good news is that the cybersecurity industry itself is much farther along on the maturity scale of determining what "good" looks like in terms of tech and process deployment. The prevailing trend is that regulatory requirements can serve as an authoritative arbiter in determining whether an organization is engaging in responsible cyber risk management activities.

In general, requirements set out by comprehensive and stable laws, regulations, and frameworks, like the NIST CSF, the PCI DSS, and the EU NIS2 Directive, are going to be a superset of anything an insurer would come up with in its baseline list of requirements. If an organization can prove its compliance with established sets of regulatory standards, it'll also be able to prove its compliance with insurer expectations.

Underwriters are increasingly aligning their requirements with regulatory mandates when evaluating risk and seeking reasons to void a policy upon claims. In this way, regulatory posture is as important as specific technical controls when securing coverage.

Cyber insurance is a board-level proof point

Boards of directors and CEOs are demanding higher levels of accountability for cyber risk because they are being held accountable by shareholders, the SEC, and other regulators. For directors with extensive enterprise risk backgrounds in different areas of the business, insurance is one of the most obvious vehicles for minimizing risks of unpreventable outlier events. They know that they must keep facilities updated and safe,

but that general liability can shield them from unusual circumstances that could cause fires or other catastrophes. They understand the importance of keeping their employees well-trained, but also recognize that insurance against errors and omissions can help mitigate the risk of costly mistakes. They also understand that if an insurer refuses to offer coverage or significantly increases its rates due to unsafe conditions, changes need to be made.

In this way, **cyber insurance coverage and terms can offer a shorthand language for CISOs to demonstrate program proficiency to even the most tech-adverse boards and executives.** The ability to obtain favorable terms and coverage can stand as a proof point to boards, regulators, and investors that security strategies are meeting baseline expectations and working as expected.
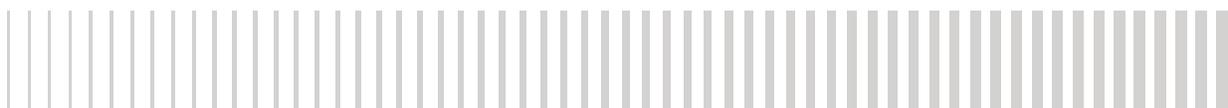
As CISOs and risk leaders take action on these insights, consider the following best practices:

▶ **Never assume your organization is fully covered**
Cyber insurance policy language is fraught with exclusions, limitations of coverage, and conditions that will void a policy. It is incumbent upon risk leaders to collaborate with executive management and the board to identify how existing controls weaknesses could jeopardize their insurability and to utilize gap analysis for prioritizing investments.

▶ **Prioritize identity security investments**
This survey offers data-backed evidence that insurers are looking closely at the kinds of access and authorization controls organizations put in place, as well as the identity governance policies and practices. Focusing on identity-first controls can improve insurability because underwriters are increasingly understanding that they can improve long-term security outcomes.

▶ **Understand the AI risk-reward equation**
Insurers are realistic about both the risks and rewards of their customers' use of AI in security defenses and across business applications. Take advantage of AI credits and rate reductions by employing AI-powered controls encouraged by insurers. And minimize risks of exclusions by bolstering AI governance and monitoring.

▶ **Secure the supply chain**
Supply chain risks are named as one of the leading causes of cyber insurance claims. While third-party risk management monitoring can help minimize risk, organizations also must consider how to interrupt the flow of supply chain attacks. One of the most critical factors in reducing the severity and spread of such events is through good security hygiene, which is facilitated by strong remote access and guest access controls.

As the cyber insurance landscape evolves, insurance carriers and brokers will become increasingly stringent. To help understand what they may be looking for, download our Insights into Enhanced Cybersecurity Insurance Requirements whitepaper.

If you can't demonstrate the appropriate policies and procedures, you may not be able to obtain or renew your policy. Delinea provides Privileged Access Management controls for cyber insurance that can help you quickly and comprehensively demonstrate compliance and best practices to cyber insurance providers.
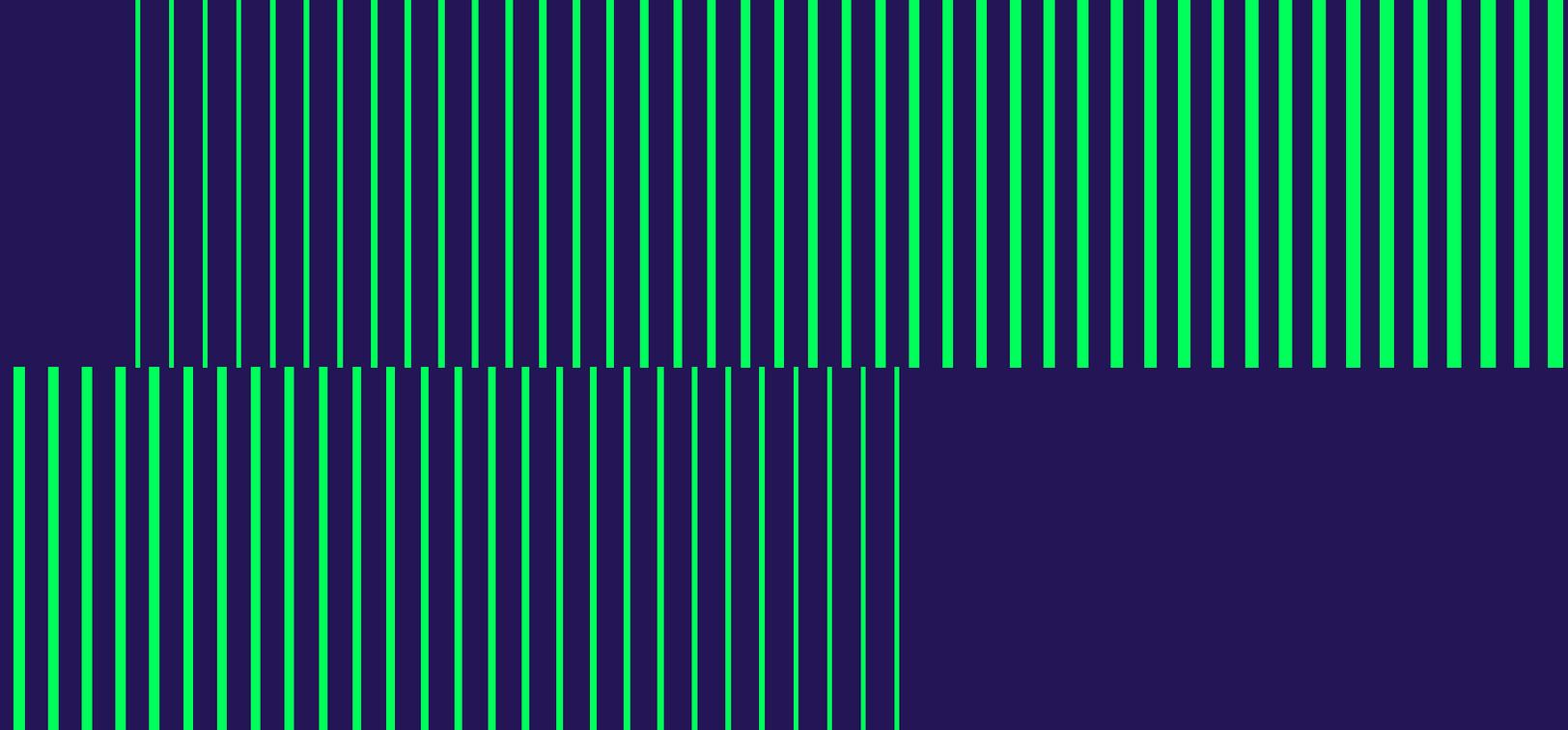
Delinea.

Securing identities at every interaction

Delinea is a pioneer in securing human and machine identities through intelligent, centralized authorization, empowering organizations to seamlessly govern their interactions across the modern enterprise. Leveraging AI-powered intelligence, Delinea's leading cloud-native Identity Security Platform applies context throughout the entire identity lifecycle across cloud and traditional infrastructure, data, SaaS applications, and AI. It is the only platform that enables you to discover all identities — including workforce, IT administrator, developers, and machines — assign appropriate access levels, detect irregularities, and respond to threats in real-time. With deployment in weeks, not months, 90% fewer resources to manage than the nearest competitor, and a 99.995% uptime, the Delinea Platform delivers robust security and operational efficiency without complexity. Learn more about Delinea on **Delinea.com**, **LinkedIn**, **X**, and **YouTube**.