Deloitte. | SailPoint

Insights into Identity Security: SailPoint and Deloitte Survey

January 2025

What does identity security look like in business today? The answer depends on a multitude of factors, some of which seem random. Talk to enough companies, though, and patterns likely emerge.

That's what SailPoint and Deloitte did. We began with a survey of more than 400 executives across a diverse set of industries, mostly based in the United States, and all working in cybersecurity and information technology (IT). Then we followed up with more in-depth interviews of five C-suite executives from multi-billion-dollar companies.

What we learned was eye-opening. Evidently, the benefits of identity security are well known, but the path to realizing those benefits is not.

Read on to learn more about the challenges C-suites face and their optimism around the technology solutions they're seeing—especially when it comes to AI.

Key Points

As threats like phishing, data breaches, and malware continue to plague the cybersecurity landscape, traditional identity security is no longer adequate.

More organizations are moving toward an "identity-first" security strategy, with support at the top of the organizations and across a range of business functions.

Many organizations struggle to implement a robust identity program due to technical challenges, a lack of internal resources, and other barriers.

Interest in artificial intelligence (AI) for identity governance is high, especially when it comes to risk prediction and threat detection.

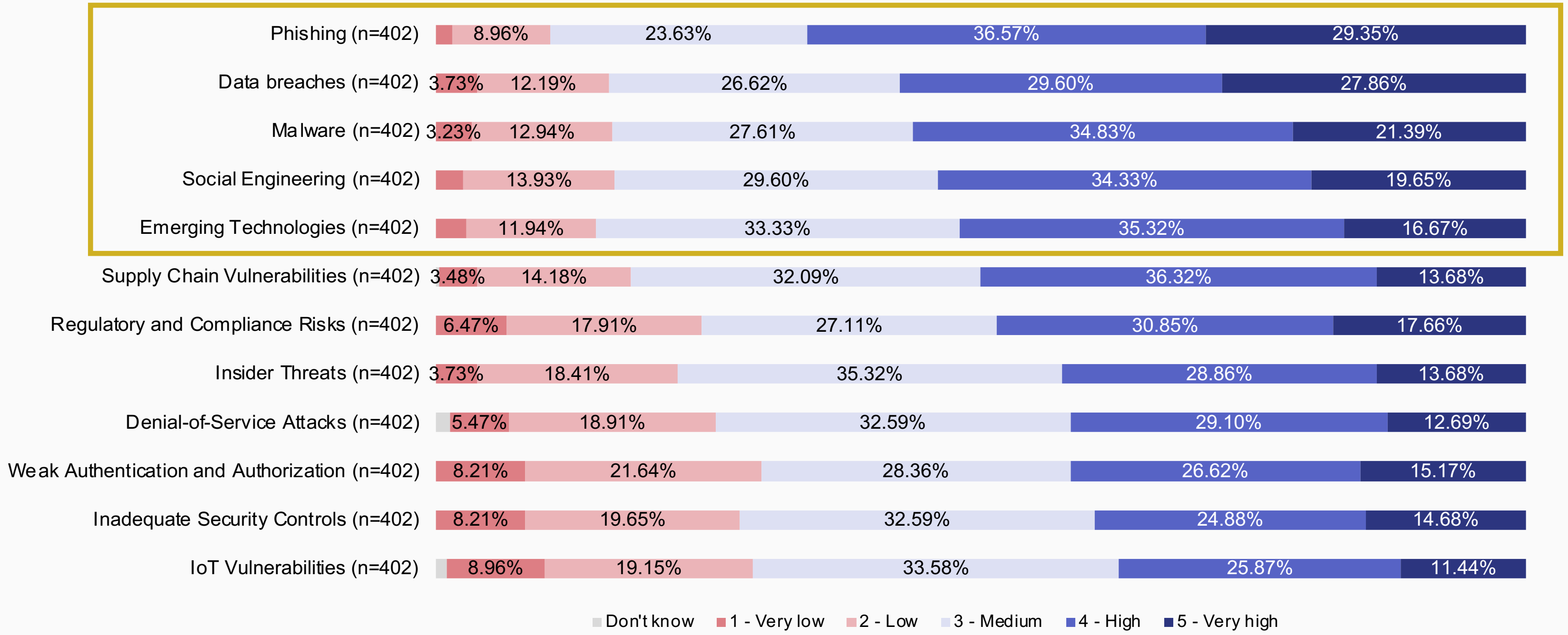
The cybersecurity landscape is shifting

According to respondents, phishing is the number one threat with 66% rating the current risk level as high or very high. Data breaches and malware tie for second with 58% rating the risk level as high or very high. And 71% of respondents rate a list of twelve other cyber threats as moderately risky (Figure 1).

According to a chief information security officer (CISO) of a tech company, the main challenges many companies face when addressing cyberthreats are *"the volume and velocity of threats that continue to increase exponentially, the dawn of AI and its proliferation, and the need to start thinking of [faked or breached] identity as a threat factor."* To this CISO, traditional identity administration is becoming increasingly inadequate.

Conventional identity management focuses on controlling the network's boundary via firewall. Once inside that firewall, though, a user is free to do what they want. But this approach assumes the IT environment is contained in a single location, which is no longer the case for many organizations. Some 97% of respondents have at least part of their IT environment in the cloud, with the largest share—43%—describing their environment as a combination of multi-cloud and on-premises systems.

Figure 1. Perceived levels of cyberthreat risks



Source: SailPoint/Deloitte Identity Security Survey 2024

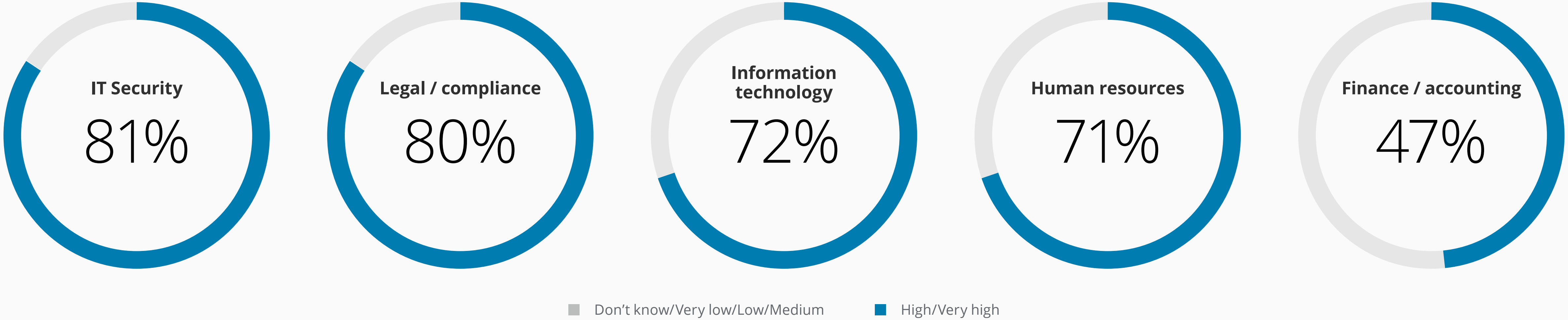
Taking the hybrid route is an increased attack surface, not to mention inconsistent security policies across each environment. The more diversity organizations have in their systems, the more complex it becomes to manage them.

Support for identity security is high and broad

Instead of focusing on network perimeters, an "identity-first" security strategy manages access to digital resources based on user credentials.

While some executives have yet to fully implement an identity-first access management strategy, they say they're familiar with it, with roughly 70%-80% rating their understanding as high or very high (Figure 2). *"Identity security is table stakes today,"* says the chief legal and compliance officer of a manufacturing company. "*In fact, we're moving in the direction of Zero Trust from there.*"

Figure 2. Level of understanding identity security solutions by job function

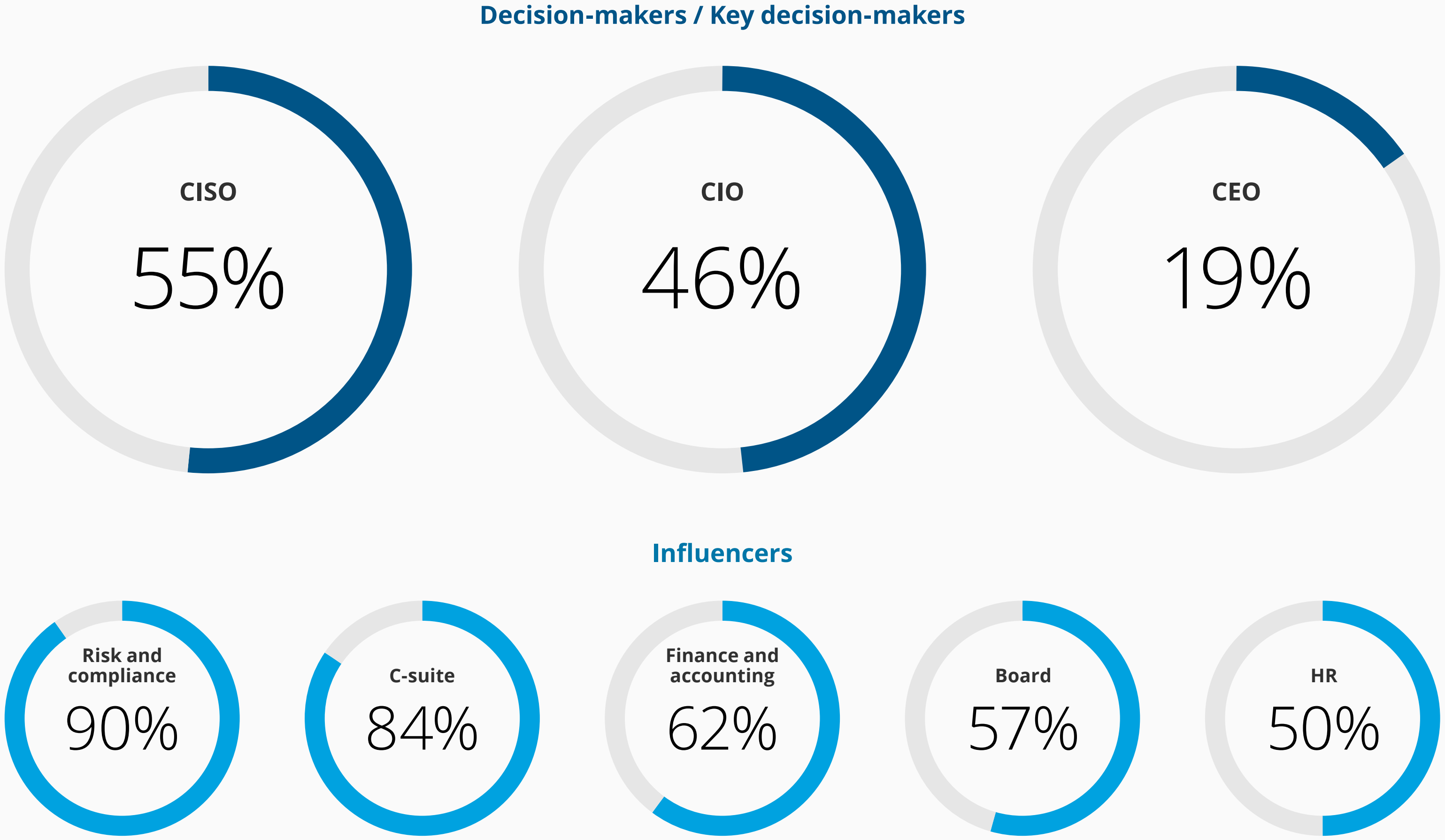


Source: SailPoint/Deloitte Identity Security Survey 2024

Respondents also appear to appreciate what identity security does for their company. Thirty-nine percent rate its effectiveness as medium, while 57% rate it as high or very high. Eighty percent say it increases security across business units and functions, while others commend its cost savings from fewer security breaches (59%) and more efficient processes such as real-time integrated reporting (48%)

Still another indicator of support is the variety of stakeholders involved with cybersecurity decisions. According to our survey, the top stakeholders are the CISO and the chief information officer (CIO). However, 19% of respondents identify the chief executive officer (CEO) as a key decision-maker, indicating that those companies view identity security as a strategic imperative. Then there are stakeholders in other roles—risk and compliance, finance and accounting, and human resources among them—who have at least some influence, pointing to the extent of cross-functional collaboration in cybersecurity decisions (Figure 3).

Figure 3. Stakeholders involved with cybersecurity decisions



See appendix for full data

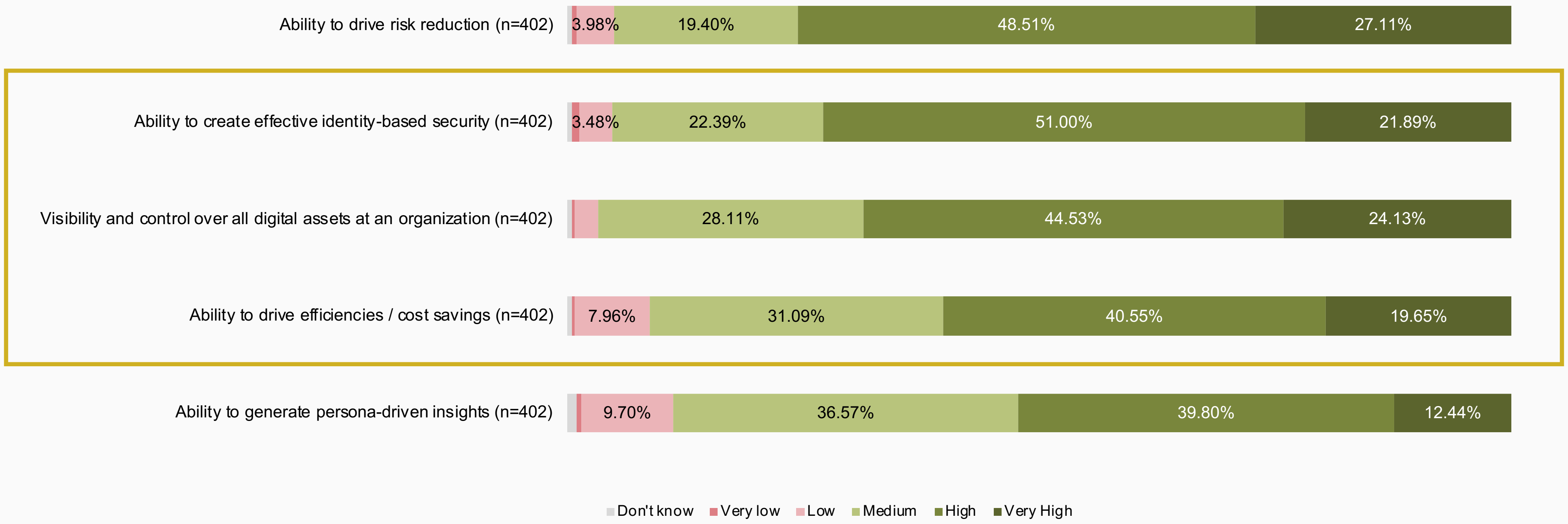
Source: SailPoint/Deloitte Identity Security Survey 2024

Implementation is a struggle

In spite of the support received, many organizations still struggle to execute.

Besides budget limitations, respondents say the biggest difficulties with making identity security implementation decisions are a diverse technology landscape and a lack of technical understanding (Figure 4).

Figure 4. Challenges with making identity security implementation decisions

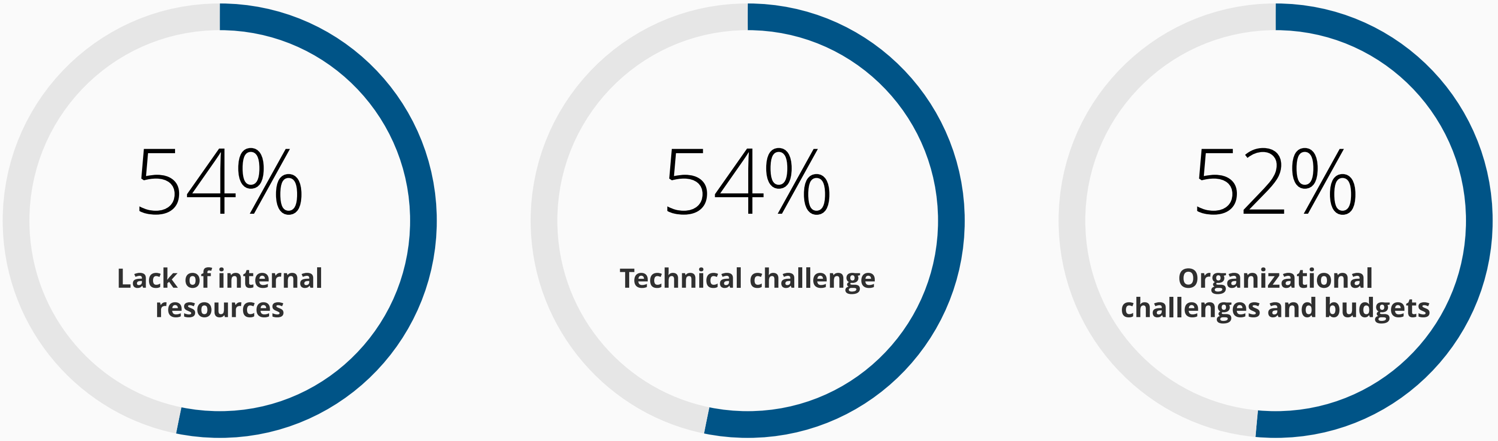


Source: SailPoint/Deloitte Identity Security Survey 2024

More than half (54%) of respondents cite technical challenges and a lack of internal resources as very or extremely relevant to identity security implementation. Nearly as many respondents (52%) say the same about organizational challenges and budgets, while 48% cite a lack of understanding or stakeholder buy-in (Figure 5).

Taking the hybrid route is an increased attack surface, not to mention inconsistent security policies across each environment. The more diversity organizations have in their systems, the more complex it becomes to manage them.

Figure 5. Relevance of barriers to identity security implementation

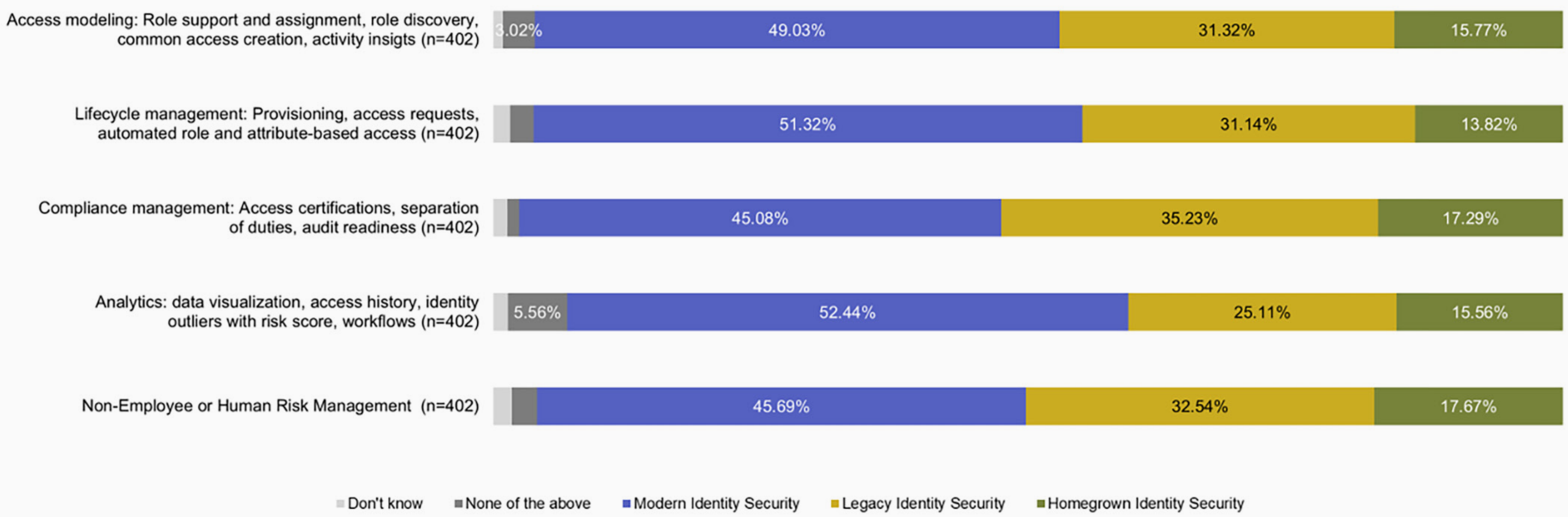


See appendix for full data

Source: SailPoint/Deloitte Identity Security Survey 2024

These barriers may be holding back progress. In our survey, only about half of businesses call their company's identity security program mature. The rest use legacy or homegrown identity security solutions across a range of applications from analytics to compliance and risk management (Figure 6).

Figure 6. Identity security maturity across different use cases



Source: SailPoint/Deloitte Identity Security Survey 2024

When it comes to discovering and managing thousands of applications—and identifying risky access combinations—48% say their company is only somewhat effective, while 10% see little to no effectiveness. What's more, only 12% of respondents say identity security is significantly integrated with their current business processes.

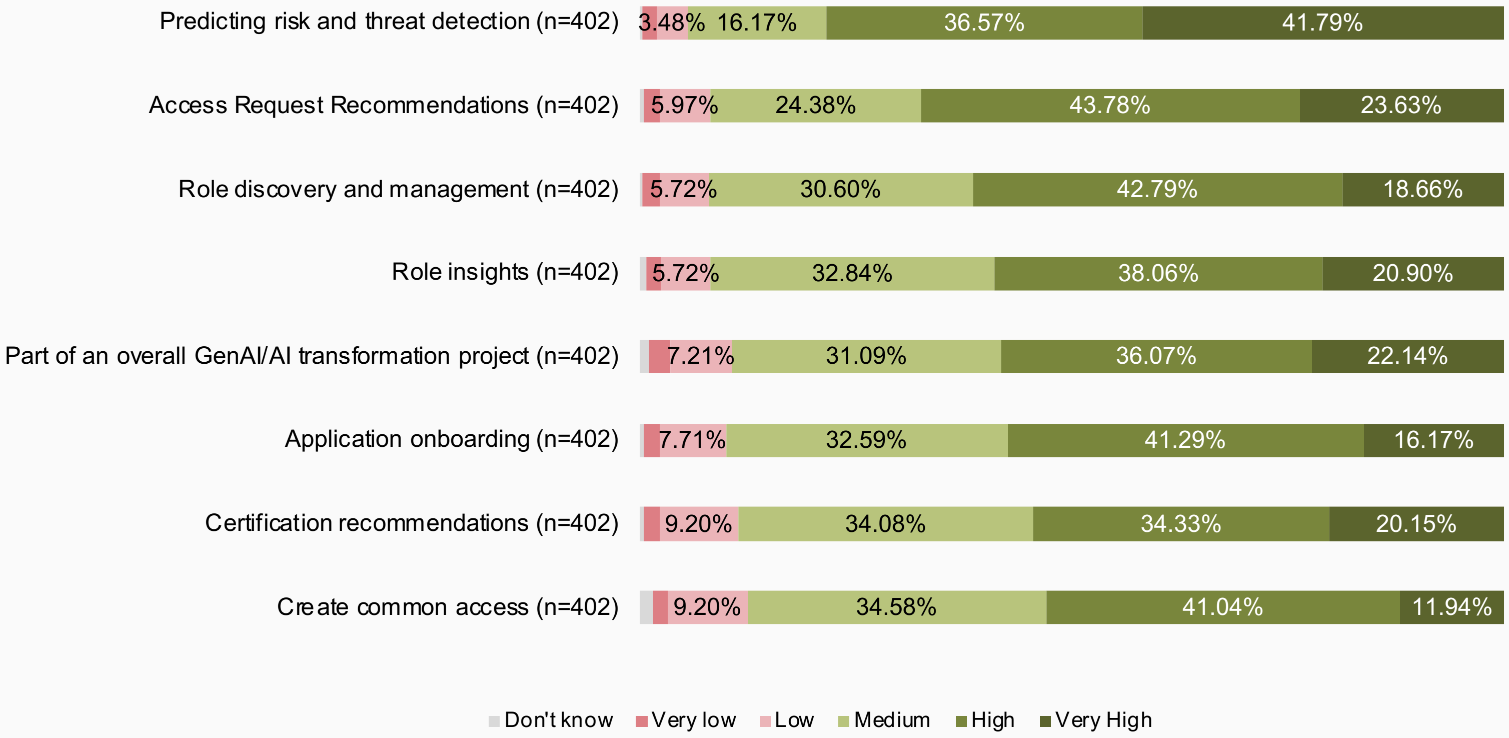
Interest in using AI is high across a range of identity governance processes

Despite the challenges of implementing identity governance, respondents are interested in seeing what AI can do. Risk prediction and threat detection has the highest level of interest, followed by access request recommendations and role discovery and management (Figure 7).

"The notion of AI in the context of identity security gets people both excited and worried," says a chief of manufacturing legal and compliance. *"It holds promise—or already shows value—in terms of efficiency and accuracy in basic identity management, like in airports or onboarding processes."*

Among other benefits, respondents expect AI to enhance automation and workflows (36%), reduce manual effort (24%), and boost the accuracy of access assignments (23%). Three-quarters of survey participants say they're likely or very likely to adopt an AI-driven solution that provides strategic identity management recommendations tailored to their company.

Figure 7. Interest in implementing AI by identity governance process



Source: SailPoint/Deloitte Identity Security Survey 2024

The cybersecurity landscape is shifting

Enterprises used to rely on firewalls to safeguard applications and data while keeping attackers at bay, but this approach has outlived its utility.

In the wake of rising threat levels and the migration of applications to the cloud, many have started to view identity as the new firewall. For example, implementing least privilege models and eliminating standing privileges wherever possible can help reduce access to applications and data.

Between internal complexities and an evolving landscape, organizations may find themselves far from identity security maturity. But identity security is a journey, not a destination. A programmatic approach can better position companies to mitigate the impact of breaches while folding in new capabilities as technologies continue to advance.

The cybersecurity landscape is shifting

Enterprises used to rely on firewalls to safeguard applications and data while keeping attackers at bay, but this approach has outlived its utility.

The right execution strategy can make all the difference. SailPoint and Deloitte have developed one based on three pillars:

1. Modernize via accelerated migration from legacy systems

2. Scale with faster onboarding

3. Innovate by adopting AI-driven identity security solutions

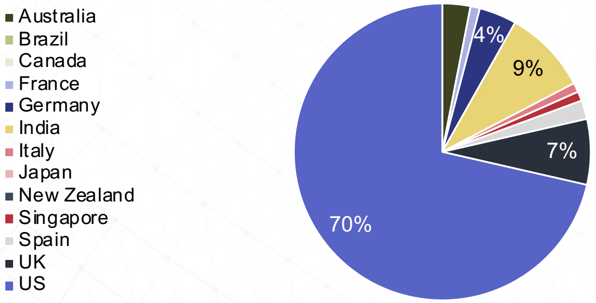
Each pillar applies the knowledge our team has gathered from helping organizations with their own identity security implementations.

In future articles, we'll explore more about what it takes to stand up an effective identity security program amid the realities revealed in our survey. Stay tuned.

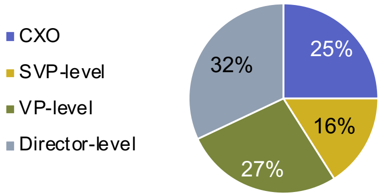
About this survey

The SailPoint–Deloitte Identity Security Survey 2024 took place in September and October 2024. The survey's 402 respondents represent organizations across a half-dozen industries, with 70% primarily operating in the US. Most respondents (68%) are at the vice president level or above, and 75% are in an IT-related role.

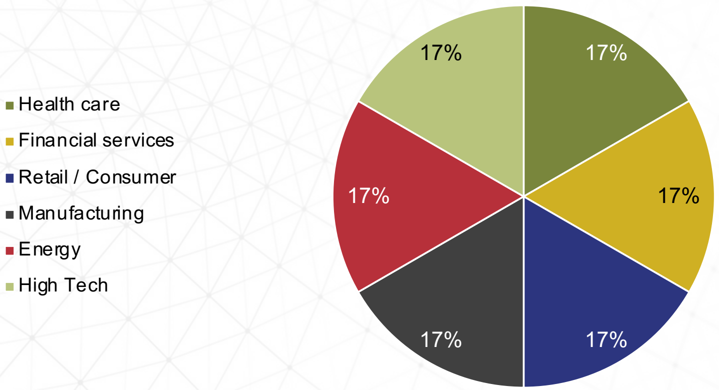
Region of Operation



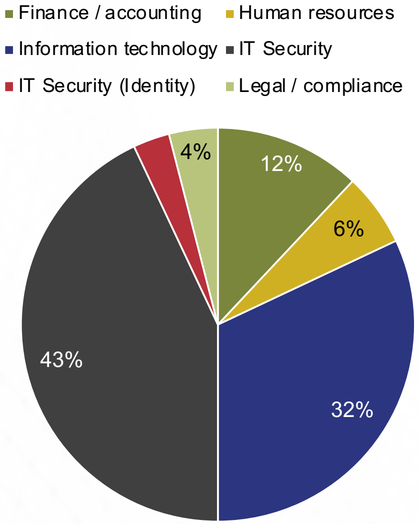
Seniority Level



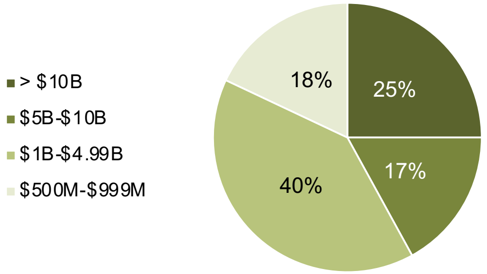
Industry



Job Function



Annual Revenue



100% of respondents have a set budget allocated for Identity Security

If you have any further questions or to learn more about our relationship visit
Deloitte.com/us/en/pages/financial-advisory/articles/deloitte-and-sailpoint-alliance.html

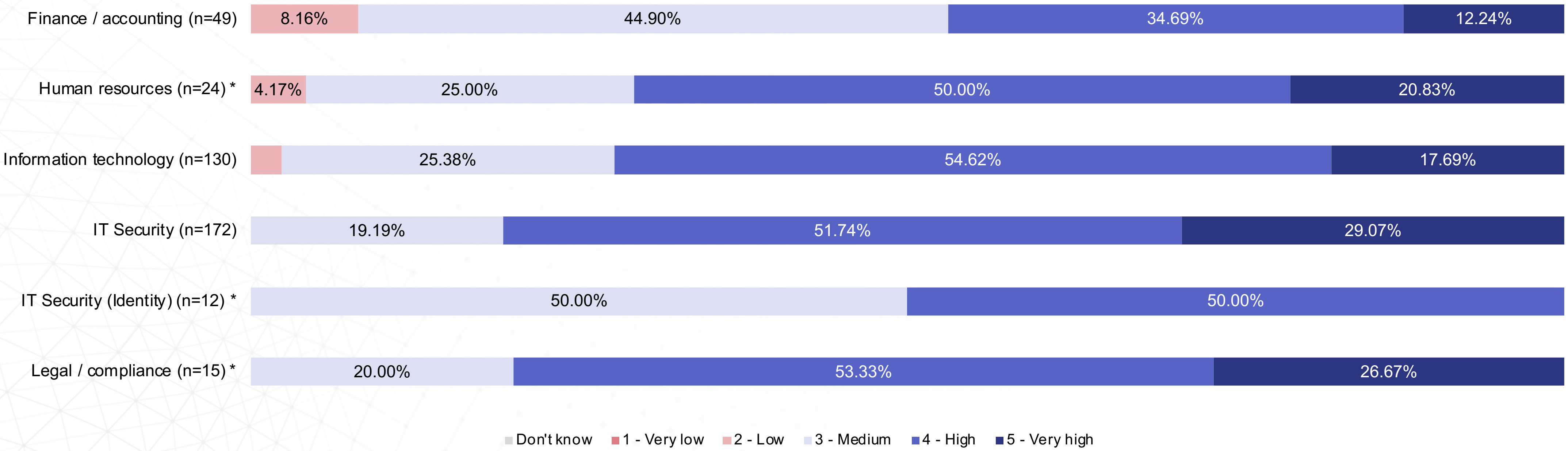
Contact

Chris Gossett
Senior Vice President, Technology Services
SailPoint
Chris.gossett@sailpoint.com

Amit Chhikara
Principal
Deloitte & Touche LLP
achhikara@deloitte.com

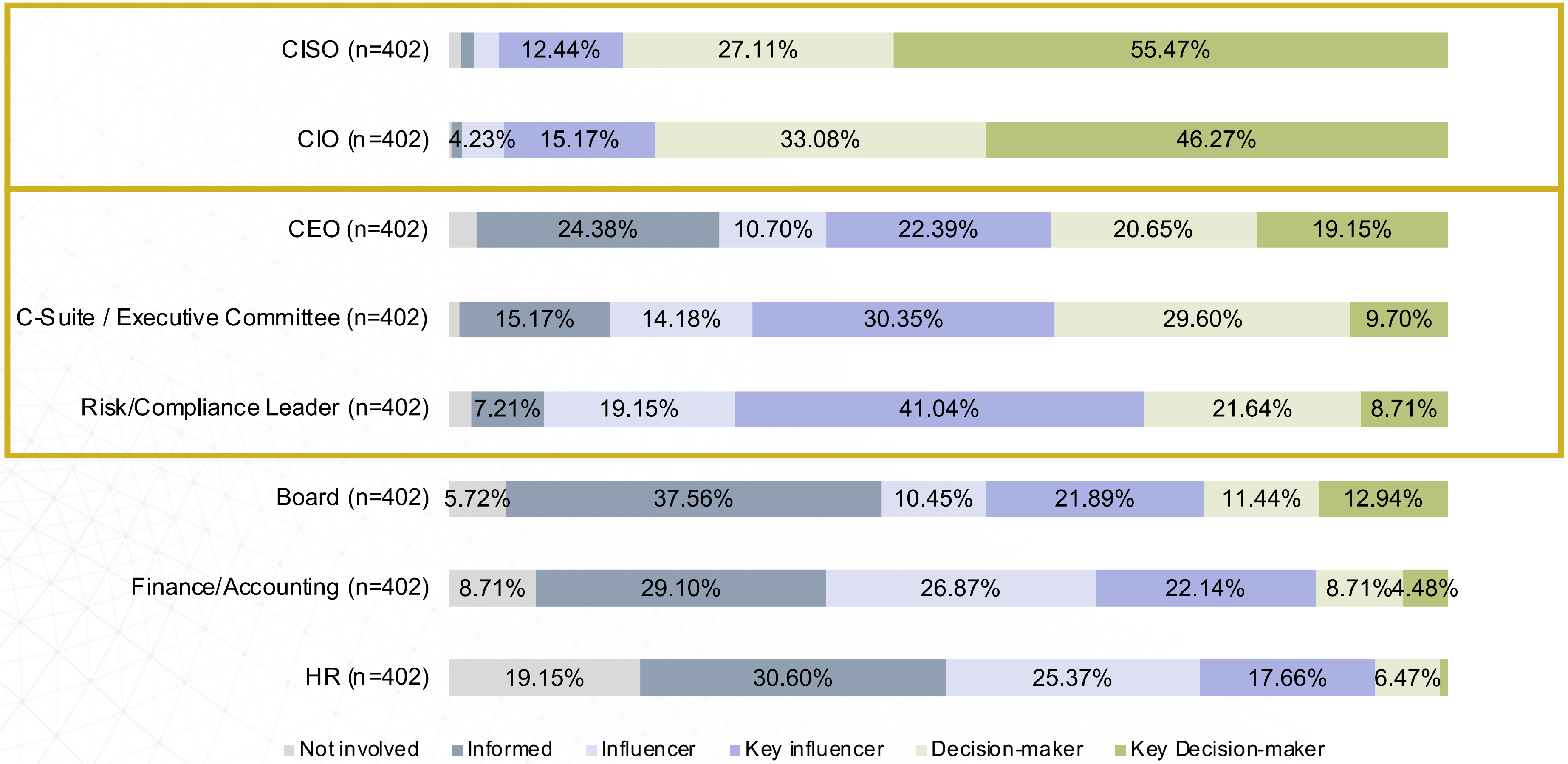
Appendix

Figure 2. Understanding identity security solutions by job function



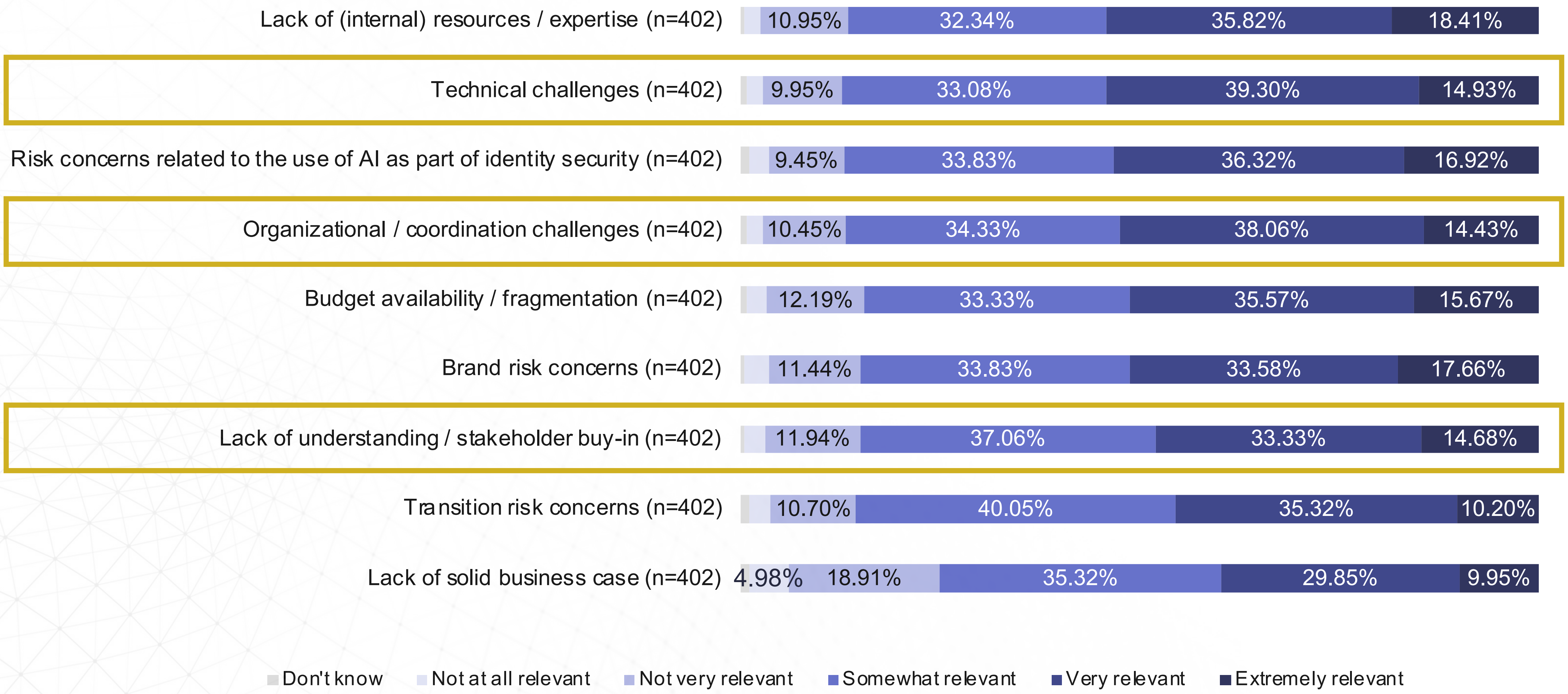
Source: SailPoint/Deloitte Identity Security Survey 2024

Figure 3. Stakeholders involved with cybersecurity decisions



Source: SailPoint/Deloitte Identity Security Survey 2024

Figure 5. Relevance of barriers to identity security implementation



Source: SailPoint/Deloitte Identity Security Survey 2024

Deloitte.

About Deloitte

This document contains general information only and Deloitte and SailPoint are not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. In addition, this document contains the results of a survey conducted by Deloitte & SailPoint. The information obtained during the survey was taken "as is" and was not validated or confirmed by Deloitte or SailPoint.

Deloitte and SailPoint shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

About SailPoint

SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data through the lens of identity – at speed and scale. As a category leader, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps many of the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation