

March 2024

Navigating the identity security minefield

Practitioners share lessons learned so others can move forward

CRA | Business Intelligence
A CRA Resource

Sponsored by:

 **SAVVY**

Contents



THE STATE OF IAM
Organizations get serious about IAM in 2024



IAM STRATEGY AND TACTICS
Respondents warming to the potential for AI-driven IAM solutions



IAM CHALLENGES
Costs, staffing, user acceptance, and technical challenges hinder IAM adoption

ALSO IN THIS REPORT

| | |
|---|----|
| Foreword | 3 |
| Survey Methodology | 24 |
| Other CRA Business Intelligence Reports | 25 |
| About CyberRisk Alliance | 26 |

FOREWORD

In the digital-first world, identity rules all.

From key fobs and SIM cards to passwords and biometric readers, there's a vast digital ecosystem governing what each of us can or cannot access at every single moment. The machinery behind this system – what's known as identity and access management (or IAM) – is critical to safeguarding the trust and integrity of these transactions.

So, of course, there are those who want to tear it all down.

Headline after headline tells us that identity-based cyber attacks are on the rise. Phishing, social engineering, deepfakes, password cracking, and Kerberoasting are just some of the many methods that criminals are using to gain access and move laterally through networks.

How are security teams faring in this battle? That's what we wanted to find out. This report presents the findings of a survey of more than 200 IT security professionals and leaders who have the pulse on their organizations' IAM tools and policies.

Many reported progress in implementing IAM in the last 12 months. Many were also significantly more concerned about unauthorized access than ever before. Some were excited to see how AI and automation could open up new applications in IAM security. And all were outspoken in the type of practices and action steps they'd like to see moving forward.

Our hope is that this report spurs new discussion about how IT departments can secure their employees and data in the year ahead, and the challenges they need to overcome to make IAM effective. The organizations that can marshal resources, strategize appropriately, and prioritize IAM investments in this identity-centric age will be the bane of attackers everywhere.

Dave Bowman: Open the pod bay doors, HAL.

HAL: I'm sorry, Dave. I'm afraid I can't do that.

Dave Bowman: What's the problem?

HAL: I think you know what the problem is just as well as I do.

Dave Bowman: What are you talking about, HAL?

HAL: This mission is too important for me to allow you to jeopardize it.

– KUBRICK, S. (DIRECTOR) (1968).

2001: A Space Odyssey [Film]. Metro-Goldwyn-Mayer.

Identity and Access Management 101

Purpose: IAM is a set of security policies and controls used to verify the identity and permission rights of an entity seeking to access an organization's network, systems, or data. The purpose is to permit the right users to access the right information under the right conditions, while preventing the wrong users from gaining unauthorized access. The IAM policy should follow the principle of least privilege, meaning that users are prescribed the minimum level of access that is needed to perform their job.

Methods: There are different tools to manage identity and access. Multifactor authentication (or MFA) requires a user to submit two or more forms of verification to authenticate their identity, such as a PIN code, security token, or knowledge-based input. Other IAM examples include single sign-on, role-based access control, federated identity, and active monitoring of user behaviors and transactions. It is important for organizations to deploy these tools in a way that does not hinder productivity or disrupt the user experience.

Context: The cybersecurity threat landscape has evolved significantly in the last decade, making IAM essential for protecting employees and data. A spike in hybrid and remote work setups means that security must extend beyond the office firewall to ensure the integrity of any entity accessing the company network. Cybercriminals have become much more adept at exploiting endpoint vulnerabilities and stealing credentials to move undetected through networks. Without strong IAM enforcement, organizations are leaving the door wide open.



“Start. Somewhere. You’ll never accomplish anything if you wait for your plan to be perfect. Get the framework set, aligned and agreed upon. Determine testing and champion groups to explore the impacts of policy, standards or technology changes, and then turn them into evangelists. Top-down support helps, but equally important is the feedback from peers. Find a partner that will enable you to grow with them. Be realistic. It will take twice as long as you plan.”

– SURVEY RESPONDENT



Four key findings from the survey:

1.

IAM adoption rose substantially in the last year, but so too did fears of improper access.

Sixty-four percent of respondents report full or partial implementation of IAM policies, a considerable uptick over the 44% from [our 2023 IAM study](#). However, three in four respondents were also more concerned about unauthorized access than they were 12 months ago.

2.

Only one in four respondents are highly confident their organization provides users the bare minimum level of access to perform their jobs.

Among those with little confidence, at least half believe their employer grants excessive privileges to up to a quarter of their entire workforce.

3.

Multifactor authentication and single sign-on policies predominate among IAM practices, reflecting the need for secure granular access that comes with minimal interference.

More sweeping, macroscopic policies and tools (such as ITSM, zero trust architecture, and AI-powered analytics) have yet to become a fixture in most IAM strategies.

4.

Besides the high costs associated with IAM investments, respondents are wary of identity tools that could negatively impact users or fail to integrate with existing IT infrastructure.

Even though many consider themselves competent managers of IAM tools, confusion persists about how IAM should be introduced, incorporated, and communicated effectively.

1

THE STATE OF IAM

Organizations get serious about IAM in 2024

In the second half of 2023, organizations rolled up their sleeves and got serious about securing identity and access. The percentage of those reporting partial or full IAM implementation spiked to 64% in 2024 from 44% in 2023, a whopping 20-point increase in a 10-month span.

However, many feel it's too early to celebrate just yet. Seventy-four percent of respondents are actually more concerned now about the threat of unauthorized access than they were 12 months ago – with one in four expressing significantly more concern.

Some of those concerns likely stem from difficulties assigning users appropriate access within new IAM policies or systems. "We have many staff members who shouldn't need all the access rights they have," writes one respondent. "Some users do not understand the security implications of allowing them to have more access than they need."

Growing pains may also be a factor. Fifty-one percent of respondents only started using IAM in the last three years, and most are split on how they manage their IAM solutions: in-house versus outsourcing some degree of upkeep to a provider. It may take a couple more years for organizations to smooth out the kinks, but the uptick in IAM adoption this past year is encouraging.

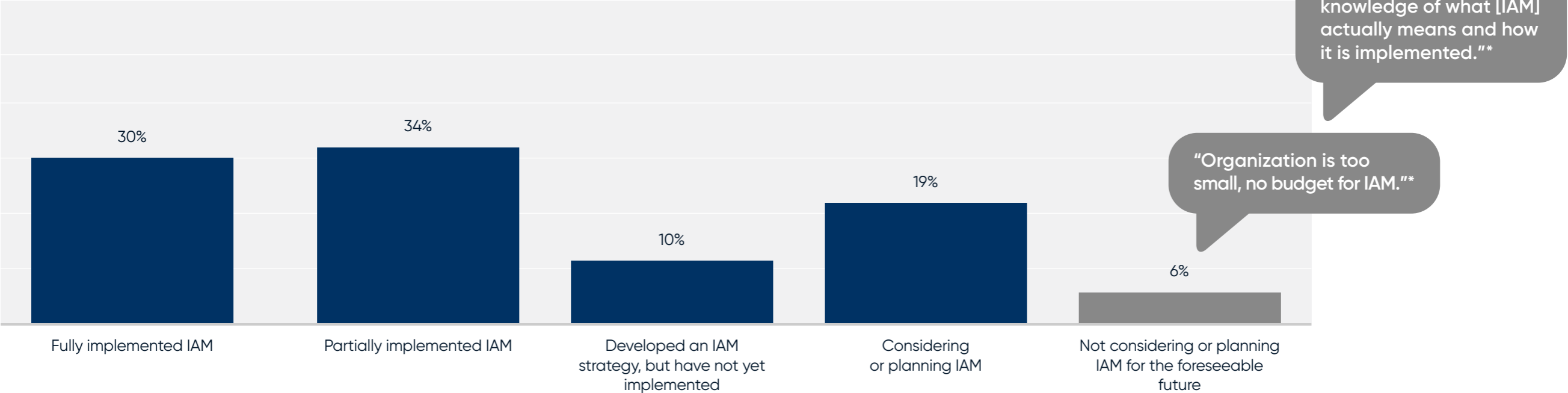


64%

are currently implementing
IAM at some level

Nearly two-thirds of respondents report their organization has partially or fully implemented IAM.

Q: What is your organization's status in implementing IAM?



Base: All respondents (n=202).
*Those not considering/planning IAM were asked to describe their reasons in a follow-up question.
Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.

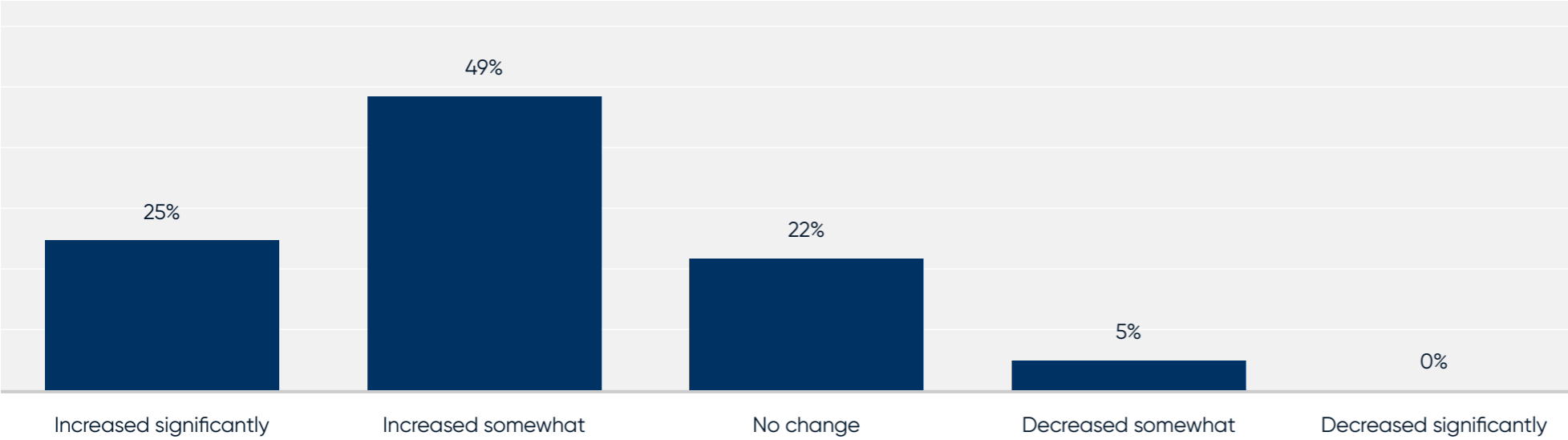
Three out of four respondents report increased concerns about unauthorized access to sensitive information in the past 12 months.

“Start ASAP. Do not let business pressure push risk acceptance in high threat areas. Assess cloud current and future state when planning.”

– SURVEY RESPONDENT



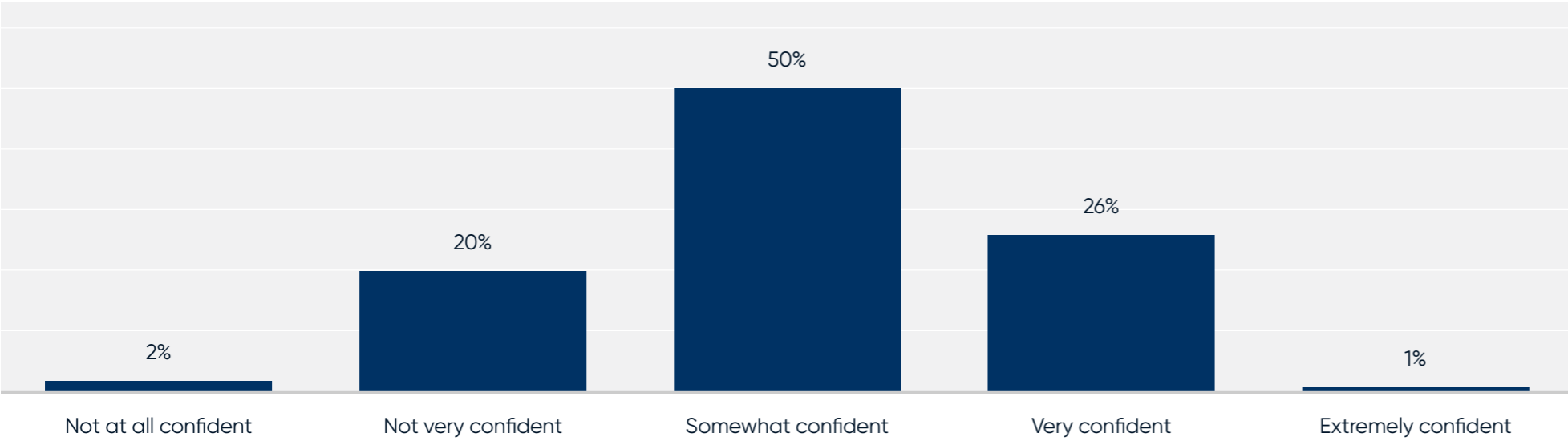
Q: How has your organization's level of concern regarding unauthorized access to sensitive information changed over the last 12 months?



Base: All respondents (n=202).
Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.

Only 27% have high confidence that their organizations' users are provided with the absolute minimum level of access to perform their job.

Q: How confident are you that users in your organization are only provided with the absolute minimum level of access privileges necessary to perform their job?



Base: All respondents (n=202).
Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.

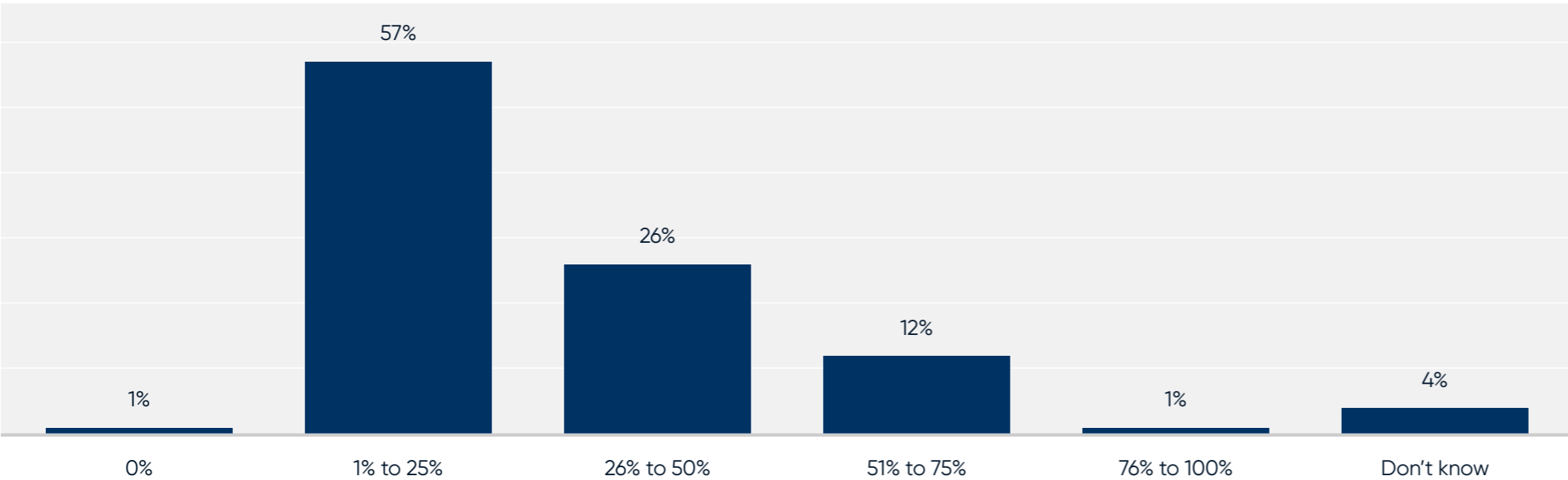
“Before assigning any IAM roles, take the time to review business workflows and map all required user access. Then build appropriate user groups based on workflows. Use this mapping as the guide to architect IAM setup, then apply and stick to the plan.”

– SURVEY RESPONDENT



Among those with low to moderate confidence in their organization's allocation of privileged access, most (57%) indicate that up to one-quarter of their users are granted access beyond what is required to do their job.

Q: Roughly, what percent of users at your organization have access privileges beyond what is required to perform their job?



Base: Respondents who are not confident or only somewhat confident about their organization's access privileges practices (n=147).
Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.

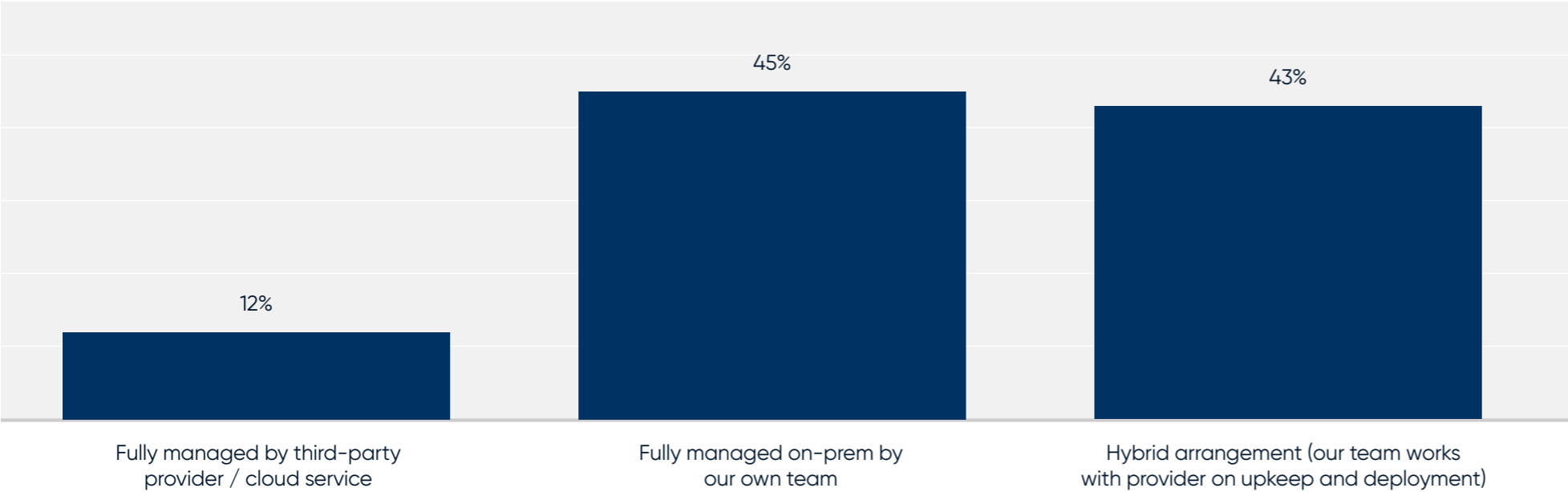
“Try to map out the current and potential future app landscape, and when creating roles do your best to have granular application responsibilities as it makes it easier to remove access to them in the future. Minimize overlap – don't have 12 roles that share five responsibilities and a sixth that is unique. Create one for the five and then 'a la carte' the other unique requirements.”

– SURVEY RESPONDENT



Most respondents report their organization either fully manages their IAM internally or as a hybrid arrangement with a third-party provider.

Q: Which of the following best describes how your organization manages IAM?



Base: Respondents whose organizations are currently implementing IAM (n=129).
Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.

“It is very helpful to develop a partnership with your IAM provider and to dedicate budget dollars and IT time to ensure a successful deployment of your IAM program. Don’t try to cut corners and don’t try to go it alone.”

– SURVEY RESPONDENT



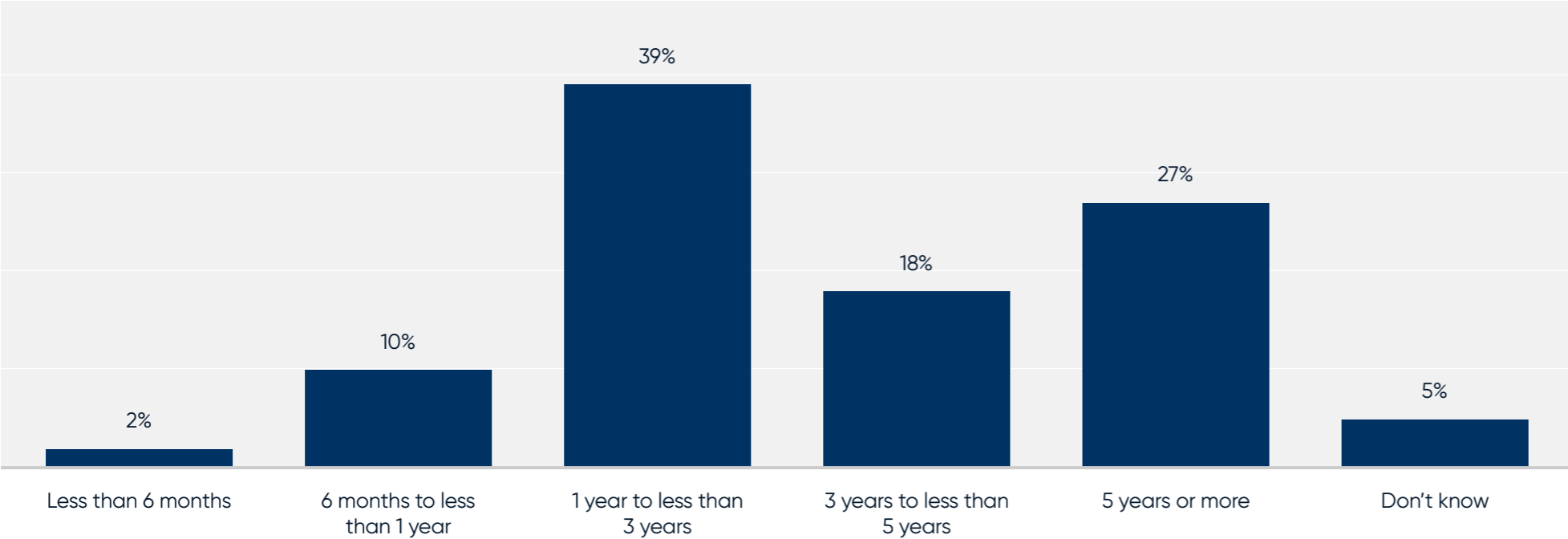
About one-quarter of all respondents have been implementing IAM for five years or more.

“Start with role-based access as a foundation and build on it.”

– SURVEY RESPONDENT



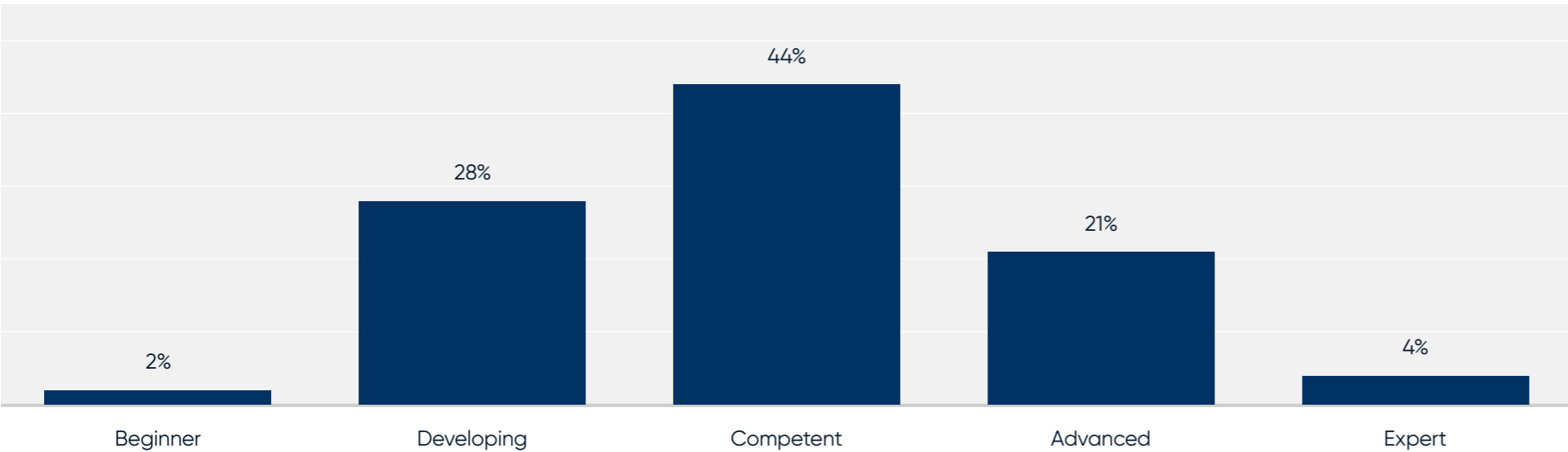
Q: How long has your organization been implementing IAM?



Base: Respondents whose organizations are currently implementing IAM (n=129).
Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.

About three in four respondents characterize their organizations' proficiency in IAM management as less than advanced.

Q: How would you describe your organization's overall proficiency in managing its IAM program?



Base: Respondents whose organizations are currently implementing IAM (n=113; "Don't know" excluded).
Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.

"A clear strategy is critical, [and] the distinction between employee, partner, and customer identities is important to implement and scale the right identity solutions."

– SURVEY RESPONDENT



2

IAM STRATEGY AND TACTICS

Respondents warming to the potential for AI-driven IAM solutions

It's no mystery why so many organizations aggressively expanded their identity and access toolkit last year. Data breaches, data breaches, and data breaches. From **Okta** and **Xfinity**, to **Microsoft** and **PJ&A**, companies have been rocked by identity-based attacks and leaks resulting from negligent enforcement policies. These incidents, say 58% of respondents, provided sufficient motivation to get serious about IAM.

But what does that look like in practice? There's a broad range of tactics under the IAM banner, but MFA and SSO are by far the most common practices, followed by federated identity, password self-service, and role-based access control.

AI-driven analytics that can support IAM functionality is still a rarity, but respondents are warming to it. Among the possible use cases for AI/IAM overlap, its ability to automate threat response in instances where identity is being abused, make continuous authentication more adaptive and less intrusive, and enforce IAM policies more consistently garnered the most support from respondents.

68%

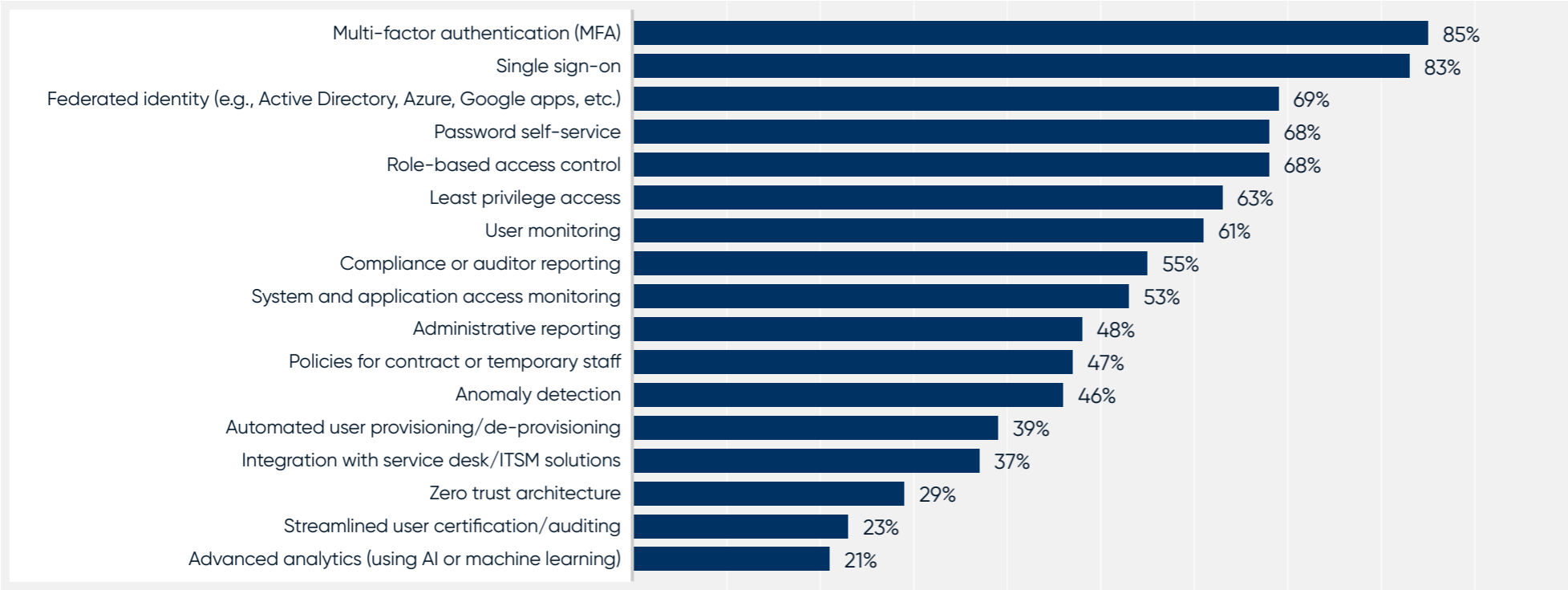
believe automated enhanced threat response is a top benefit of AI/ML-enhanced IAM

MFA and single sign-on are commonly included in IAM programs, whereas advanced analytics, simplified user certification, and zero trust architecture are much less likely to be implemented.

“Find a way to automate MFA being activated rather than relying on someone to manually activate it. Too many users slip through the cracks.”

– SURVEY RESPONDENT

Q: Which of the following are currently included in your organization's IAM strategy or program?

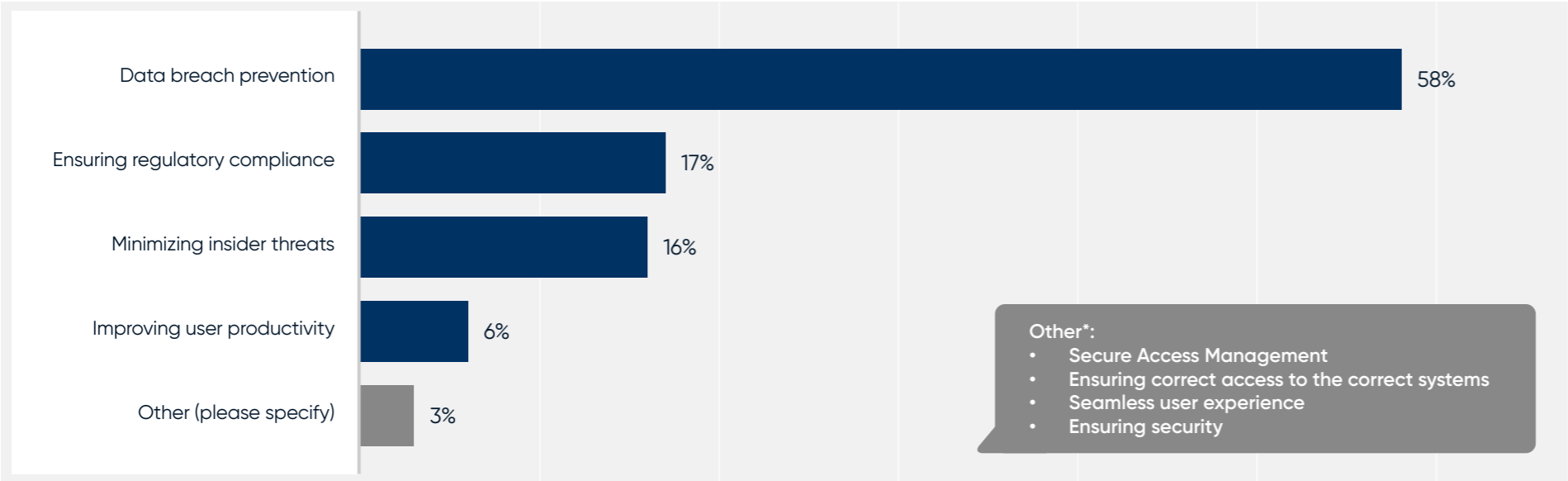


Base: Respondents whose organizations are either currently implementing IAM or have an IAM strategy but not yet implementing IAM (n=150).
Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.



Data breach prevention is, by far, a predominant IAM objective among respondents.

Q: Which of the following is your primary IAM objective?



“Do a thorough assessment of your IAM needs and prioritize those needs before starting the vendor selection process. This enables your vendor comparison research to be more effective because you can find the best fit solution for your highest needs and will be less influenced by distracting features that matter little to your organization.”

– SURVEY RESPONDENT



Base: Respondents whose organizations are either currently implementing IAM or have an IAM strategy but not yet implementing IAM (n=150).

*Other, specify open-ended responses.

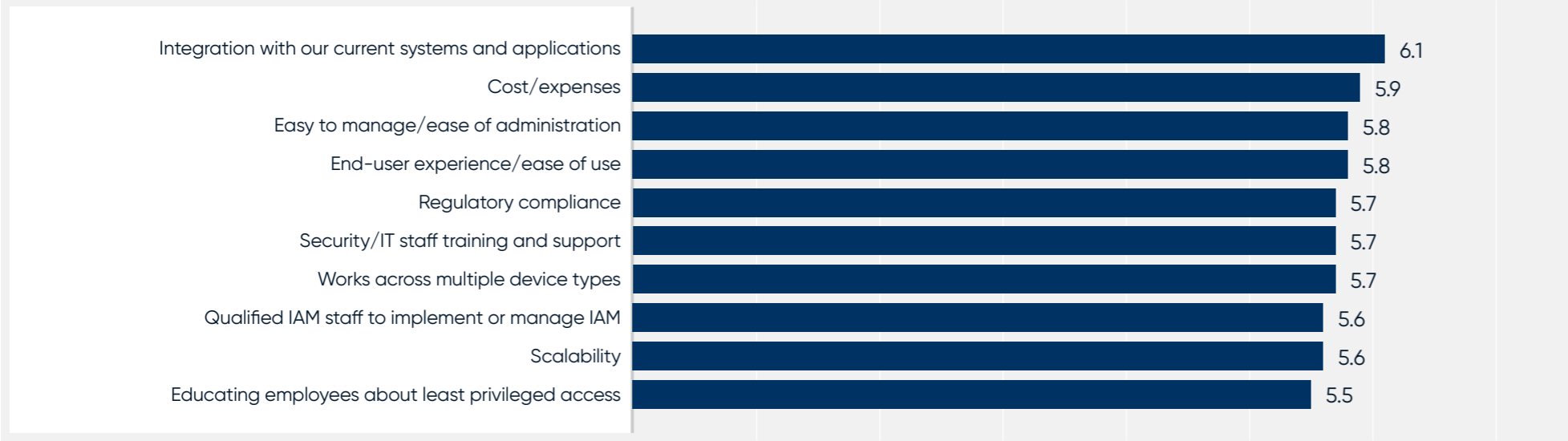
Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.

According to respondents, the most important factor in evaluating their organizations' IAM requirements is the integration with existing systems and applications.

“Make sure that the business processes that IAM relies on are well-defined and consistent. A bad process automated is still a bad process.”

– SURVEY RESPONDENT

Q: How important are each of the following criteria when evaluating how to address IAM needs for your organization?



Notes: Respondents were asked to rate each on a scale from 1 to 7, where 1 is “Not at all important” and 7 is “Extremely important.”
Chart shows mean scores (out of 7).
Base: Respondents whose organizations are implementing IAM, have developed an IAM strategy, or considering/planning IAM (n=189).
Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.

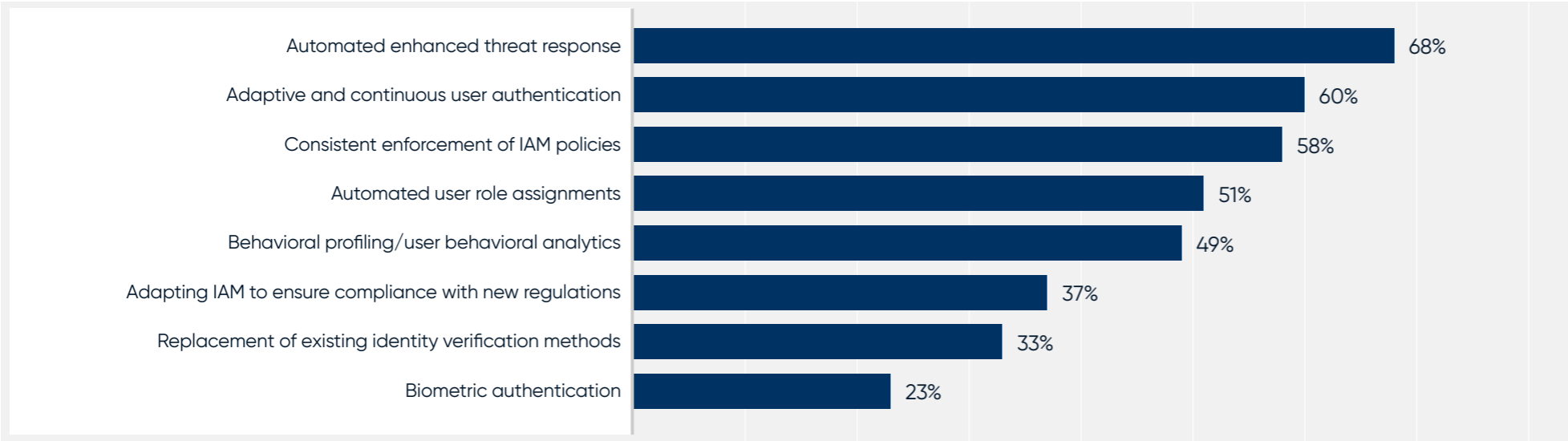
Automated enhanced threat response (e.g., real-time alerts, detailed notifications, locking malicious activities, isolating affected systems, initiating incident response workflow, etc.) is considered a top benefit of including AI/ML capabilities with IAM.

“Be prepared for some pain, but the end result is worth it!”

– SURVEY RESPONDENT



Q: When thinking about the potential benefits of including AI/ML capabilities with IAM, which of the following capabilities do you consider to be the most important for your organization?




Notes: Respondents were asked to select up to 5 choices.
Base: Respondents whose organizations are considering IAM, have developed an IAM strategy, or implementing IAM (n=189).
Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.

Survey respondents offered some advice and best practices for those planning an IAM program.

Q: Based on your own experience with IAM, what advice or lessons learned can you share with other organizations that are considering or planning an IAM program for the near future?


Build a Roadmap

"You need to build out a roadmap of the most important to least important. There is a lot that goes into the planning, and you can't do everything at once. But I would start with user provisioning and user removal when they leave the company."




Automate and Integrate

"The most important advice that I have learned through experience with IAM is that AI/ML, automation and integration are the most important elements to be included in planning an IAM in the future."




Understand the True Costs

"Ensure that if the plan is to implement in stages, the true cost of full implementation is understood. We have found as we want to add on additional features, there are certain services that must be purchased for them to work correctly. These, of course, come at an additional cost."




Get Management Buy-in

"It's important to think about management's perspective when planning for IAM solutions. Often times, management may not be as security focused so it's critical to help them understand the risks associated with any decisions you're intending on making for IAM so that they can support your program."




Outline Roles and Permissions

"Outline roles/permissions each dept/group needs prior to implementation. Easier to do it right from the beginning then to clean-up/fix it after everyone is in the system."




Identify Requirements

"Identify requirements, scope accordingly in line with business and industry requirements. Scope a deployment after sufficient testing."



Educate End Users

"It may seem difficult up front and your users are going to complain about a change coming, but you have to educate them on the why's. Why it is so important for organizations to use this technology and how it can and will help to secure the data that you are trying to protect. I don't care what you want to change, people do not like change, so come up with a plan and just do it. They will adapt!"



3

IAM CHALLENGES

Costs, staffing, user acceptance, and technical challenges hinder IAM adoption

We wish achieving IAM mastery were as easy as flipping a switch. Unfortunately, many organizations find their ambitions grounded by economic and staffing realities.

Approximately half say IAM's hefty price tag is a progress killer. Nearly as many struggle to reconcile what users will tolerate with the security requirements that IAM necessitates. At least a third have experienced the nightmare of integrating IAM policies or tools with existing IT infrastructure. Getting IAM right means answering a lot of questions, questions that many can't identify in the first place.

"We don't have enough staff members and outside consultants to assist us with IAM at this time," says one respondent. "We are trying to get more help for future implementations this year."

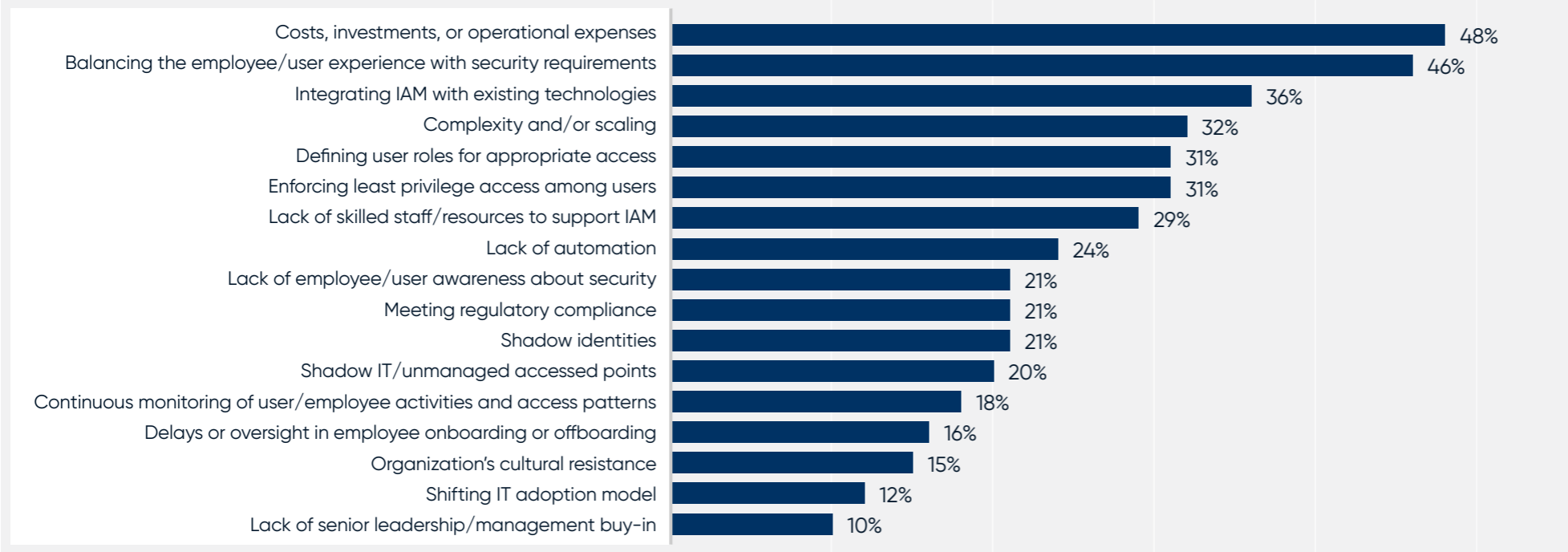
"Integrating IAM with existing systems and equipment running on legacy software and hardware presents us with continuous issues," says another respondent.

46%

say balancing the employee experience with security requirements is a top IAM challenge

Costs/expenses and balancing user experience with security requirements are the most commonly encountered challenges of IAM.

Q: What are your organization's challenges or expected challenges in implementing or planning for IAM?



Note: Respondents were asked to select up to 5 choices.
 Base: Respondents whose organizations are considering IAM, have developed an IAM strategy, or implementing IAM (n=189).
 Source: CyberRisk Alliance Business Intelligence (CRA BI), IAM Survey, January 2024.


“A clear strategy is critical [and] the distinction between employee, partner, and customer identities is important to implement and scale the right identity solutions.”

– SURVEY RESPONDENT




Survey respondents described their primary issues and challenges implementing and planning for IAM.

Q: Please describe your primary issues or challenges in implementing or planning for IAM.

 **Financial**


"Costs of implementing IAM (often multi-year, multi-million-dollar projects)."

26%

 **Employees/Users**


"Users only seem to know what they know from experience. They are resistant to change and work outside their existing cubbyholes."

21%

 **Least Privilege Access**

"We have many staff members who shouldn't need all the access rights they have. Some users do not understand the security implications of allowing them to have more access than they need."

19%

 **Integration**

"Integrating IAM with existing systems and equipment running on legacy software and hardware presents continuous issues."

15%

CONTINUED

Survey respondents described their primary issues and challenges implementing and planning for IAM.

Q: Please describe your primary issues or challenges in implementing or planning for IAM.



Software/Solutions

"Not able to find the matured OTS [Commercial Off-the-Shelf] product that fits in the requirements of my company."

13%



Skilled Staff

"We don't have enough staff members and outside consultants to assist us with IAM at this time. We are trying to get more help for future implementations this year."

12%



Security

"Keeping balance between work efficiency and security."

11%



Leadership Buy-in

"Stakeholder buy-in across the organization is challenging as well, especially with the 'we've always done it this way' attitudes."

8%

Survey methodology

The data and insights in this report are based on an online survey conducted in January 2024 among 202 security and IT leaders and executives, practitioners, administrators, and compliance professionals in North America from CRA's Business Intelligence research panel.

The objective of this study was to explore various issues and topics related to organizations' IAM strategy, efforts, challenges, and related opinions.

Notes:

Some figures may not add up to 100% as a result of rounded percentages.

The respondent profile is as follows:

IT or IT Security Roles/Titles:

- CISOs/CROs/CIOs/CTOs (10%)
- VPs/SVPs/EVPs (8%)
- Directors (31%)
- Managers (29%)
- IT/security admins (18%)
- Analysts/consultants (4%)

Organization sizes:

- Small (1 to 99 employees) (11%)
- Medium (100 to 999 employees) (24%)
- Large (1,000 to 9,999) (42%)
- Enterprise (10,000 or more) (23%)

Top Industries:

- High-tech, IT software, or telecom (19%)
- Education (17%)
- Manufacturing (14%)
- Healthcare (11%)
- Financial services (9%)
- Professional services (consulting, legal, etc.) (6%)
- Retail, trade, or eCommerce (5%)

Other CRA Business Intelligence reports

2024

1. [Threat Intelligence: Organizations seek expertise and guidance to help build their threat intelligence programs](#) (February 2024)
2. [The zero-trust dilemma: Ensuring a positive user experience and getting leadership buy-in](#) (January 2024)

2023

1. [Tough on Ransomware: Organizations fighting ransomware with continuous monitoring, IR playbooks, backups, and user education](#) (November 2023)
2. [Cloud security: Gaps in skillsets and lack of visibility leaves many organizations flying blind](#) (October 2023)
3. [Easy Prey: The Danger of Vulnerable Endpoint and Devices](#) (September 2023)
4. [Threat Intelligence: Eyes on the Enemy](#) (August 2023)
5. [Vulnerability Management: A Maelstrom of Moving Targets](#) (June 2023)
6. [Controlling the Chaos: The Key to Effective Incident Response](#) (May 2023)
7. [Identity and Access Management: Can Security go hand-in-hand with User Experience?](#) (April 2023)
8. [Finding the Way to Zero Trust](#) (March 2023)
9. [Wanted: A Few Good Threat Hunters](#) (February 2023)
10. [Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations](#) (January 2023)

2022

1. [Threat Intelligence: Critical in the Fight Against Cyber Attacks, But Tough to Master](#) (December 2022)
2. [Ransomware Ready: Organizations Fight Back with More Aggressive Strategies and Technology](#) (November 2022)
3. [Harsh Realities of Cloud Security: Misconfiguration, Lack of Oversight and Little Visibility](#) (October 2022)
4. [Zero Trust Adoption Faces Ongoing Headwinds](#) (October 2022)
5. [Endpoint Security: Security Pros Concerned About the Proliferation of Non-Traditional Devices and Endpoints](#) (September 2022)
6. [Organizations Adopt Aggressive, More Proactive Vulnerability Management Strategies in 2022](#) (August 2022)
7. [Threat Intelligence: The Lifeblood of Threat Prevention](#) (July 2022)
8. [CRA Study: Attackers on High Ground as Organizations Struggle with Email Security](#) (July 2022)
9. [Security Teams Struggle Amid Rapid Shift to Cloud-Based Operations](#) (June 2022)
10. [CRA Study: XDR Poised to Become a Force Multiplier for Threat Detection](#) (May 2022)
11. [CRA Study: Zero Trust Interest Surges, But Adoption Lags as Organizations Struggle with Concepts](#) (April 2022)
12. [CRA Study: Managing Third-Party Risk in the Era of Zero Trust](#) (March 2022)
13. [CRA Ransomware Study: Invest Now or Pay Later](#) (February 2022)
14. [CRA Research: A Turbulent Outlook on Third-Party Risk](#) (January 2022)

CRA Business Intelligence contacts

Bill Brenner
SVP of Audience Content Strategy
bill.brenner@cyberriskalliance.com

Dana Jackson
VP of Research
dana.jackson@cyberriskalliance.com

Daniel Thomas
Custom Content Producer
daniel.thomas@cyberriskalliance.com

About CyberRisk Alliance

CyberRisk Alliance provides business intelligence that helps the cybersecurity ecosystem connect, share knowledge, accelerate careers, and make smarter and faster decisions. Through our trusted information brands, network of experts, and innovative events we provide cybersecurity professionals with actionable insights and act as a powerful extension of cybersecurity marketing teams. Our brands include SC Media, the Official Cybersecurity Summits, TechExpo Top Secret, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, Cybersecurity Collaborative, Security Weekly, ChannelE2E, MSSP Alert, and LaunchTech Communications. Learn more at www.cyberriskalliance.com.



About Savvy

Savvy's SaaS Security platform provides organizations with unparalleled visibility into SaaS risks. Its just-in-time security guardrails automate security workflows to prevent potential incidents before they take place and provide suggestive guidance that empowers users to make smarter decisions. Savvy provides customizable security automation playbooks that empower security teams to automate responses to various user actions, engage users at critical decision points to prevent incidents, reduce event overload, and improve security outcomes. For more information, visit www.savvy.security.



Identity-First Security for SaaS

Automatically discover and remediate the most toxic combinations of SaaS identity risk. Guide users at scale towards proper security hygiene using just-in-time security guardrails.

[Learn more](#)

