


Unprepared & Vulnerable:

*The Urgency in Reinforcing IAM Protocols
to Prevent Data Breaches*



This report is to understand how organizations are approaching Identity and Access Management (IAM), to what extent they are adopting leading security practices, and how well they are mitigating identity security threats. Sponsored by Converge Technology Solutions, Ponemon Institute surveyed 571 IT and IT security practitioners in the US to hear what they are currently practicing in IAM.

Introduction

Keeping enterprise and customer data secure, private, and uncorrupted has never been more important to running a business. Data is the great asset in our information-driven world and keeping it secure can allow your organization to maintain a healthy operation and reduce operational, financial, legal, and reputational risk.

Keeping information safe has gotten more complex as technology has advanced, the number of users has grown, and the devices and access points they use have proliferated beyond the walls of the enterprise. Attackers see their opportunities everywhere.

Threat actors have also changed. It's no longer the "lone wolf" hacker that is the threat, but now organized criminal organizations and bad-actor nation states are a constant threat to our data security. They have more sophisticated tools, expanding compute power, and AI. They've also had decades to hone their methods and are innovating daily.

Not a week goes by without a new data breach hitting the news cycle. A single successful attack can be painfully expensive. In the United States the average cost per data breach was \$9.48 million in 2023 . And this is just the financial impact which may not include reputational harm, loss of customers and other hidden costs.

Surprisingly, stolen or compromised credentials are still the most common cause of a data breach. While there is an entire industry devoted to identifying and remediating breaches as or after they happen, the best defense is to prevent credential theft in the first place.

At the heart of prevention are the practices of **Identity and Access Management** or **IAM**. IAM ensures that only trusted users are accessing sensitive data, that usernames and passwords aren't leaked or breached, and that the enterprise knows precisely who, where and when their systems are being accessed. Keeping the bad guys from stealing credentials severely limits their ability to cause harm. Good IAM and awareness training does that.

The State of the Art of IAM

Like all technology practices, IAM has evolved over the years to become more sophisticated and robust as new techniques have been developed in keeping data and systems secure. Organizational adoption and enforcement vary greatly.

While some advanced businesses are already using endpoint privileged management and biometrics, there are still organizations with policies loose enough that using a pet's name with a rotating digit as a password is still possible or credentials are on sticky notes stuck to employee monitors.

This report is to understand how organizations are approaching **Identity and Access Management (IAM)**, to what extent they are adopting leading security practices, and how well they are mitigating identity security threats. Sponsored by Converge Technology Solutions, Ponemon Institute surveyed 571 IT and IT security practitioners in the US to hear what they are currently practicing in IAM.

PART 1 | INTRODUCTION

For most companies, it all begins with the basics of **authentication**. If you're only using username and password, it is no longer enough authentication for your "primary" login for mission-critical systems. In legacy systems, where sophistication beyond usernames and passwords are not available, best practices must be taught and enforced rigorously. Practices such as very long passwords or passphrases and checking passwords against a blacklist must be put in place. These password basics are a starting point that many users still don't universally adhere to.

The next critical step is adding **Multi-Factor Authentication (MFA)**. Many cyberattacks are initiated by phishing where credentials and personal information are obtained from susceptible users. Others are brute force attacks where the password is eventually guessed. Using MFA introduces a second level of authentication that isn't password-based to thwart attackers who may have discovered the right password. If your organization hasn't yet implemented MFA, it is past time to act. This additional layer of security can dramatically reduce the risk of credential compromise.

If you've already deployed basic MFA, the next logical steps include **Adaptive Authentication** or **Risk Based Authentication**. This technique adds intelligence to

the authentication flow to provide strong security but reduces a bit of the friction by creating authentication requirements based on the risk and sensitivity of each specific request rather than using the same MFA prompt every time. This reduces MFA response fatigue for end users.

On the leading edge, organizations may choose to forgo using passwords altogether and go **passwordless** to nearly eliminate the risk of phishing attacks. This method uses passkeys that may leverage biometrics (e.g., fingerprint, retina scan), hardware devices or PINs with cryptographic key pairs assigned and integrated into the access devices themselves.

A layer on top of these methods is **Identity Threat Detection and Response (ITDR)**. This technology gathers signals across the ecosystem to automatically deal with a credential breach (or risk of one) as they happen to limit lateral movement. ITDR uses analytics and AI to monitor access points and authentication and identify anomalies that may represent possible attacks to force re-authentication or terminate sessions before further damage can be done. These systems have sophisticated reporting and analytics to identify areas of risk across the environment.

Regulatory Compliance: Identity Governance and Administration (IGA)

Regulatory non-compliance is another risk of failed IAM. Since regulations such as GDPR (General Data Protection Regulation), SOX (Sarbanes-Oxley), and HIPAA (Health Insurance Portability and Accountability Act) all set standards for data privacy, it is imperative that organizations identify, approve, and monitor access to critical data and systems.

The authoritative source of identity information for most organizations should be their HR system(s). A properly configured IGA solution utilizes this authoritative source as the starting point for determining access to an organization's critical systems based upon the person's role.

Beyond providing access, a viable IGA solution should also allow you catalog and attest to user entitlements associated with mission critical systems and systems

with regulated data to create an audit trail. Periodic reviews of access (e.g., quarterly, annually) in addition to Separation of Duty (SoD) policies and event driven micro-reviews should be part of an IGA solution to ensure that compliance requirements are continually met.

Another avenue that is often exploited is over-privileged user accounts, where a user has access to data or systems that they don't need, creating unneeded risks. User accounts can gain too much privilege in many ways, such as the retention of past privileges as individuals' roles within the organization change. By managing lifecycle events with an IGA solution, organizations can minimize the risks of overprivileged accounts being compromised.

IGA solutions can enforce a policy of "least privileged access" where users are only assigned the necessary privileges to perform the duties required of them. This

PART 1 | INTRODUCTION

approach combined with SoD policy enforcement can help to greatly reduce your data security risk profile.

Similarly, **Role Based Access Control (RBAC)** can be a valuable methodology for managing the evolving access requirements of an organization. RBAC associates the required access based on the role an employee plays within the organization instead of using mirrored account privileges, thereby limiting the scope of what they can access to what is necessary. RBAC can greatly reduce the timeline necessary to roll-out large changes to systems and data thus allowing your organization to adapt quickly to the market and new requirements.

Privileged Access Management (PAM): The Rise of Enterprise Password Vaults

PAM systems control access and passwords to highly sensitive data and systems, such as those controlled by IT to access root systems, administrator access, command-line access on vital servers, machine user IDs or other applications where a breach could put the entire IT footprint in jeopardy. The key component of a PAM system is an enterprise password vault that monitors access activity on highly sensitive accounts.

The password vault does more than just safely store passwords. It updates them, rotates them, disposes of them, tracks their usage and more. Users “borrow” privileged accounts temporarily for time-bound sessions, creating an abstraction between the person’s typical user account and the privileged account, minimizing the potential for privileged account credential compromise. Once a vault is established, the next level is to automatically rotate the passwords after they are borrowed. This ensures that nobody but the current user knows the password for a temporary timeframe.

Adoption and Use are Key to IAM

IAM best practices and new technologies don’t work if they are not fully implemented to understand the current prevalence, adoption and impact of IAM practices, Converge Technology Solutions sponsored the Ponemon Institute to study and understand organizations’ approach to IAM and how they are working to mitigate security threats targeting their user credentials, sensitive information, and confidential data.

In addition to improving security, an IGA solution should also make life easier for users and administrators. An integrated IGA solution can take time- and labor-intensive manual provisioning operations and move them to automated request and fulfillment processes. The IGA solution not only performs the actions faster than manual provisioning activities, but it also ensures that the right resource is granted to the right person with the right approvals at the right time.

For highly regulated systems with extremely sensitive data, like found in healthcare and finance, security can go one step further and automatically proxy the privileged session so that even the admin doesn’t even know the username and password to use it. These sessions can also be recorded for forensic evidence of the work performed under privilege to provide auditability.

Privileged Identity Management (PIM) is another approach based upon the concept of zero standing privileges that can work in conjunction with traditional PAM. This is a “just-in-time” temporary enrollment into privileged access and their subsequent removal after use. In PIM, each session is provisioned, subject to approval, based on the requester’s justification for needing access. Sessions are time-bound and an audit history is recorded. This ensures that the most sensitive systems are extremely difficult to hack.

Ponemon Institute surveyed 571 IT and IT security practitioners in the US who are involved their organizations’ IAM program. The top three areas of respondents’ involvement are evaluating IAM effectiveness (51 percent of respondents), mitigating IAM security risk (46 percent of respondents) and selecting IAM vendors and contractors (46 percent of respondents).

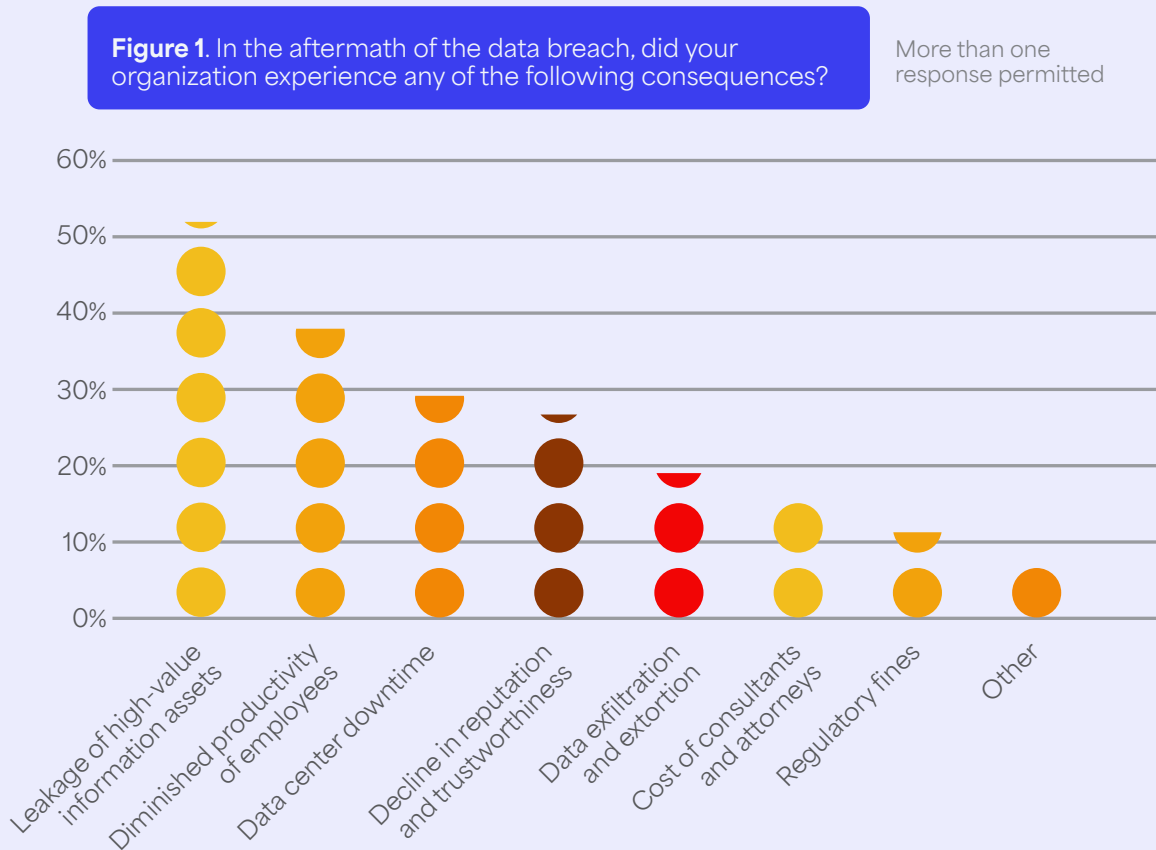
PART 1 | INTRODUCTION

The key takeaway from this research is how vulnerable organizations' identities are to attacks. While organizations seem to know they need to improve the security posture of their IAM practices, they are not moving at the necessary speed to thwart the attackers. According to the research, organizations are slow to adopt processes and technologies that could strengthen the security posture of IAM programs.

Only 20 percent of respondents say their organizations have fully adopted zero trust. Only 24 percent of respondents say their organizations have fully implemented passwordless authentication, which uses more secure alternatives like possession factors, one-time passwords, register smartphones, or biometrics.

Data breaches due to leaked, compromised, or stolen credentials are affecting the majority of organizations.

Fifty-four percent of respondents say their organizations had at least one data breach in the past 24 months due to leaked, compromised, or stolen credentials. Forty-seven percent of these respondents say they have had four to five incidents (29 percent) or more than five (18 percent). As shown in [Figure 1](#), the consequences from the data breach research experienced were severe. More than half of respondents (51 percent) say high-value information assets were leaked, which can result in serious financial losses and reputation damage. Thirty-seven percent of respondents say it affected employees' productivity and 29 percent had data center downtime.



FOLLOWING ARE RESEARCH FINDINGS THAT REVEAL THE STATE OF IAM INSECURITY.

Less than half of organizations represented in this research are prepared to protect identities and prevent unauthorized access. Only 45 percent of respondents say their organizations are prepared to protect identities when attackers have AI capabilities. Less than half (49 percent) use risk-based authentication to prevent unauthorized access and only 37 percent of respondents say their organizations use AI security technology to continuously monitor authenticated user sessions to prevent unauthorized access.

PART 1 | INTRODUCTION

Organizations lack the ability to respond quickly to next generation attacks. Forty-six percent of respondents say if a threat actor used a stolen credential to login to their organization, it could take 1 day to 1 week (18 percent), more than 1 week (28 percent) to detect the incident. Eight percent of respondents say they would not be able to detect the incident.

IAM security is not a priority. As evidence, only 45 percent of respondents say their organizations have an established or formal IAM program, steering committee and/or internally defined strategy and only 46 percent of respondents say IAM programs compared to other security initiatives are a high or very high priority.

IAM platforms are not viewed by many organizations as effective. Only 46 percent of respondents say their IAM platform(s) are very or highly effective for user access provisioning, lifecycle and termination. Only 44 percent of respondents rate their IAM platform(s) for authentication and authorization as very or highly effective. Similarly, only 45 percent of organizations that have a dedicated PAM platform say it is very or highly effective.

More organizations need to implement MFA as part of their IAM strategy. Thirty percent of respondents say their organizations have not implemented MFA. Only 25 percent of respondents say their organizations have applied MFA to both customer and workforce accounts.

Few organizations have fully integrated IAM with other technologies such as SIEM. Only 30 percent of respondents say IAM is fully integrated with other technologies and another 30 percent of respondents say IAM is not integrated with other technologies. Only 20 percent of respondents say practices to prevent unauthorized usage are integrated with the IAM identity governance platform.

As evidence that IAM security is not a priority for many organizations, many practices to prevent unauthorized usage are ad hoc and not integrated with the IAM platform. To perform periodic access review/attestation/certification of user accounts and entitlements, 31 percent of respondents say they use custom in-house built workflows, 23 percent say the process is manual using spreadsheets, and 20 percent of respondents say it is executed through IAM identity governance platform. Twenty-six percent of respondents say no access/review/attestation/certification performed.

Organizations favor investing in improving end user experience. Improved user experience (48 percent of respondents) is the number one driver for IAM investment. Forty percent of respondents say the constant changes to the organization due to corporate reorganizations, downsizing and financial distress is a reason to invest.



Key Findings

In this section, we present an analysis of the research findings. The complete findings are presented in the [Appendix](#) of this report.

Risks & threats to the security of IAM

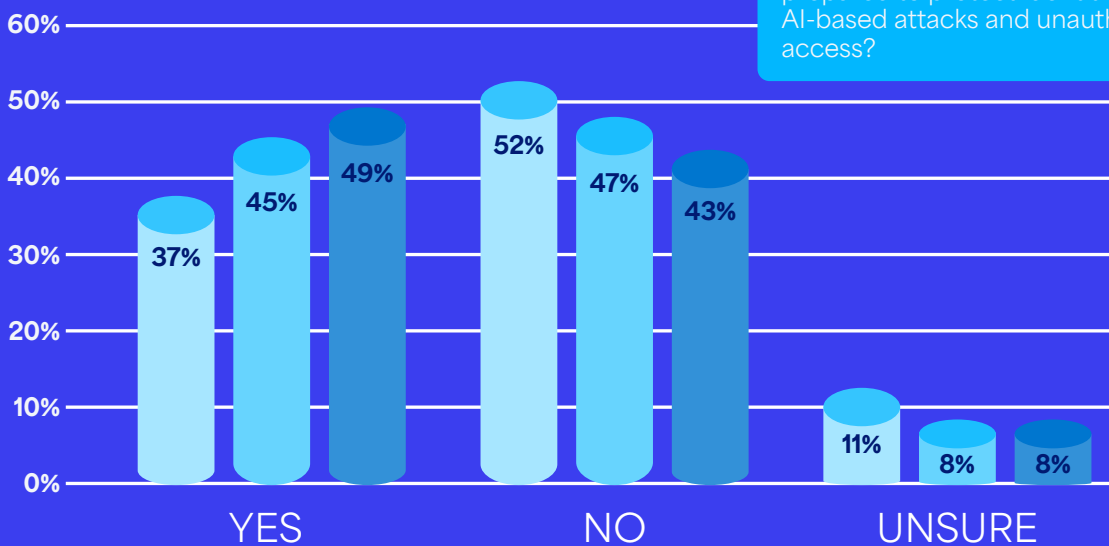
The effectiveness of organizations' IAM practices

How organizations are investing in & staffing IAM

Risks and threats to the security of IAM

AI in the hands of cyber criminals is a serious threat to the protection of identities. As shown in *Figure 2*, only 45 percent of respondents say their organizations are prepared to protect identities when attackers have AI capabilities. Less than half (49 percent) use risk-based authentication to prevent unauthorized access and only 37 percent of respondents say their organizations use AI security technology to continuously monitor authenticated user sessions to prevent unauthorized access.

Figure 2. Are organizations prepared to protect identities from AI-based attacks and unauthorized access?



● AI security technology is used to continuously monitor authenticated user sessions to prevent unauthorized access

● The organization is prepared to protect identities when attackers have AI capabilities

● Risk-based authentication (e.g. adaptive authentication) is used to prevent unauthorized access

PART 2 | KEY FINDINGS

Organizations are not ready for next generation attacks. Forty-six percent of respondents say if a threat actor used a stolen credential to login to their organization, it could take 1 day to 1 week (18 percent), more than 1 week (28 percent) and 8 percent of respondents say they would not be able to detect the incident.

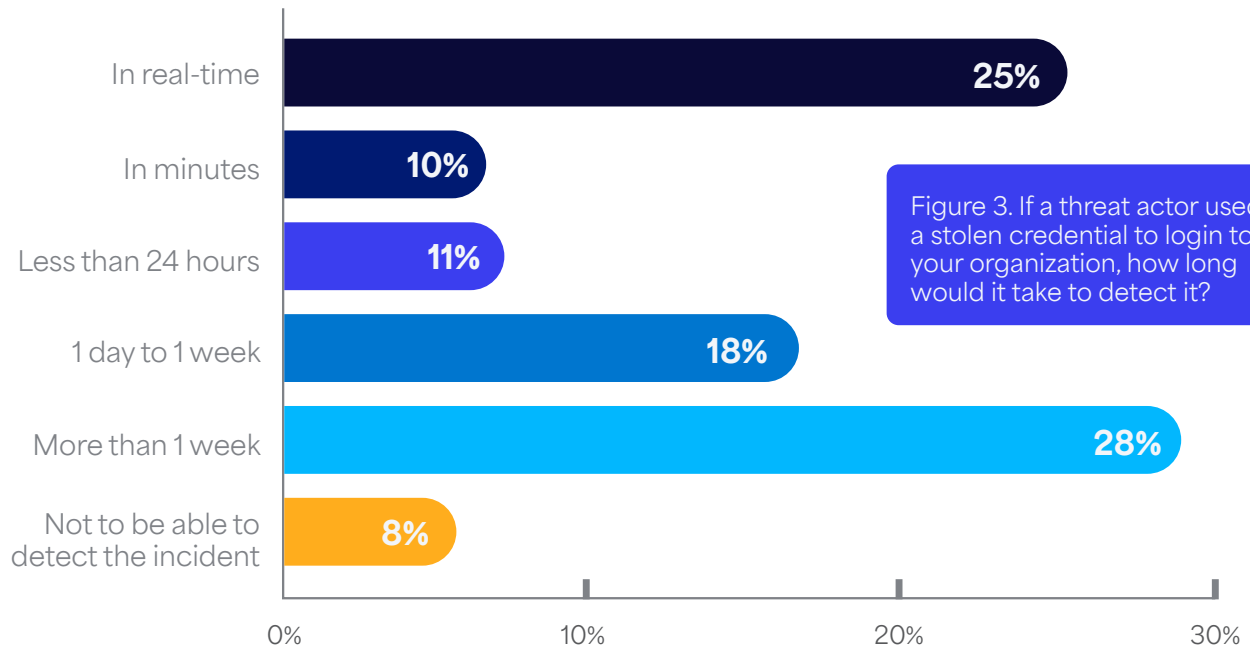


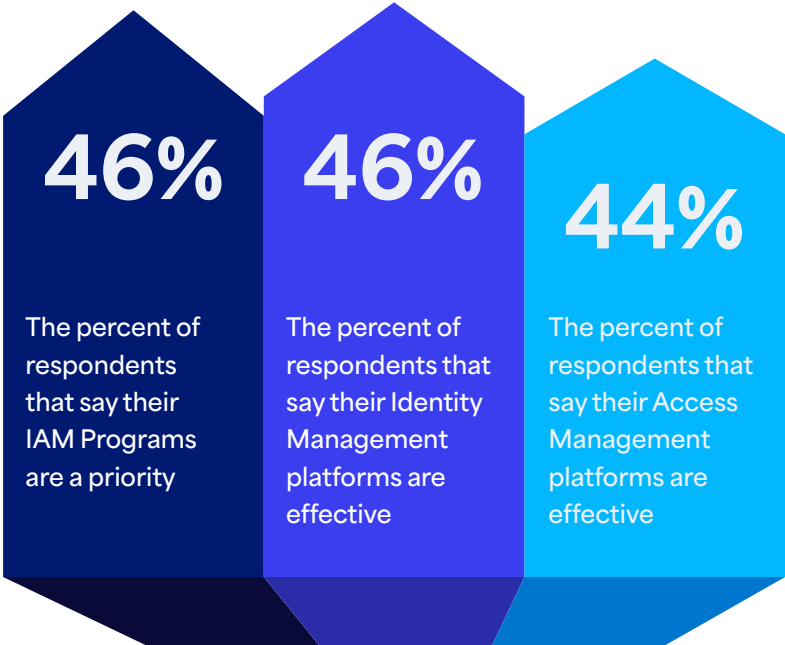
Figure 3. If a threat actor used a stolen credential to login to your organization, how long would it take to detect it?

IAM security is not a priority. Only 45 percent of organizations in this research have an established/formal IAM program, steering committee, and/or internally defined strategy. Respondents were asked to rate the priority of IAM security from 1 = not a priority to 10 = very high priority. **Figure 4** shows the 7+ responses (a high or very high priority). Only 46 percent of respondents say IAM programs compared to other security initiatives are a high or very high priority.

Respondents were also asked to rate the effectiveness of their IAM platforms from 1 = not effective to 10 = highly effective. Less than half of respondents (46 percent) say their organizations' IAM platform(s) are very or highly effective for user access provisioning, lifecycle, and termination. Only 44 percent of respondents rate their IAM platform(s) for authentication and authorization as very or highly effective.

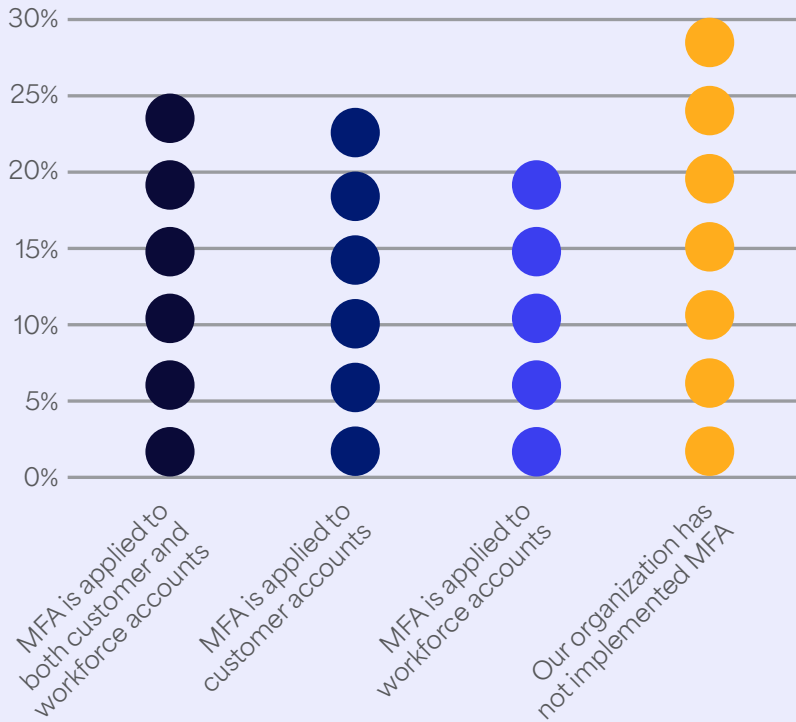
Figure 4. The priority of IAM security and the effectiveness of IAM platforms and programs

On a scale from 1 = not a priority to 10 = very high priority
1 = not effective to 10 = highly effective
7+ responses presented



Organizations need to implement MFA as part of their IAM strategy. As shown in *Figure 5*, 30 percent of respondents say their organizations have not implemented MFA. Only 25 percent of respondents have applied MFA to both customer and workforce accounts (25 percent).

Figure 5. Has your organization implemented multifactor authentication (MFA)?



Organizations are slowly adopting zero trust. According to NIST, zero-trust architecture is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership.

As shown in Figure 6, only 20 percent of respondents have fully adopted zero trust and only 13 percent say implementation and testing is in process. Forty-four percent of respondents say they will adopt zero trust within one year (23%), between one to two years (12%), or more than two years (9%).

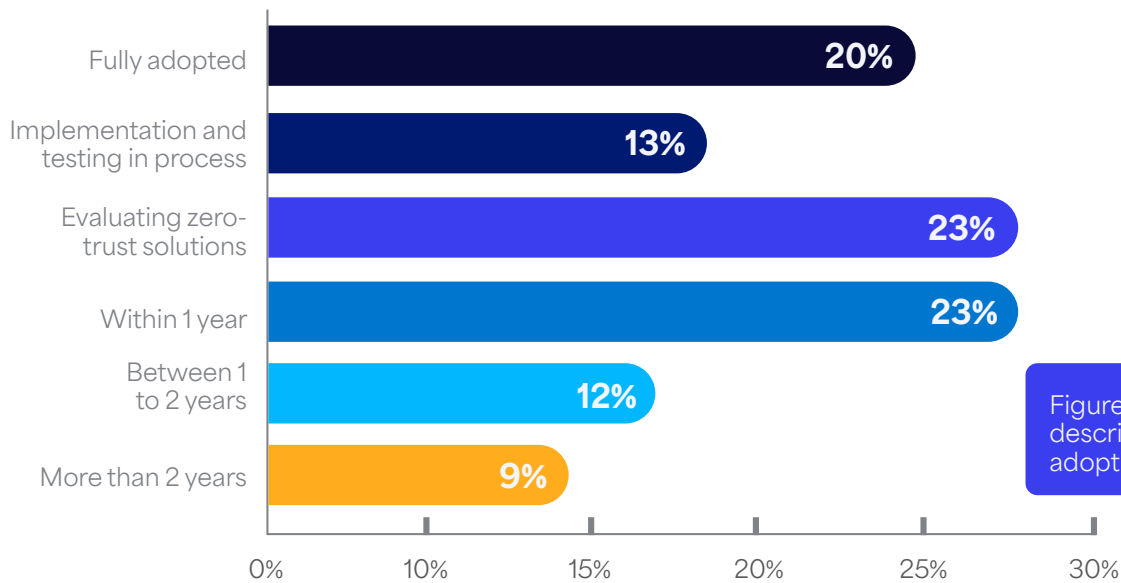


Figure 6. What best describes your organization's adoption of zero trust?

The effectiveness of organizations' IAM practices

Organizations lag in integrating IAM with other technologies, including SIEM. As shown in *Figure 7*, only 30 percent say IAM is fully integrated with other technologies, 23 percent say IAM is partially integrated with other technologies, and 17 percent say IAM is in the process of being integrated.

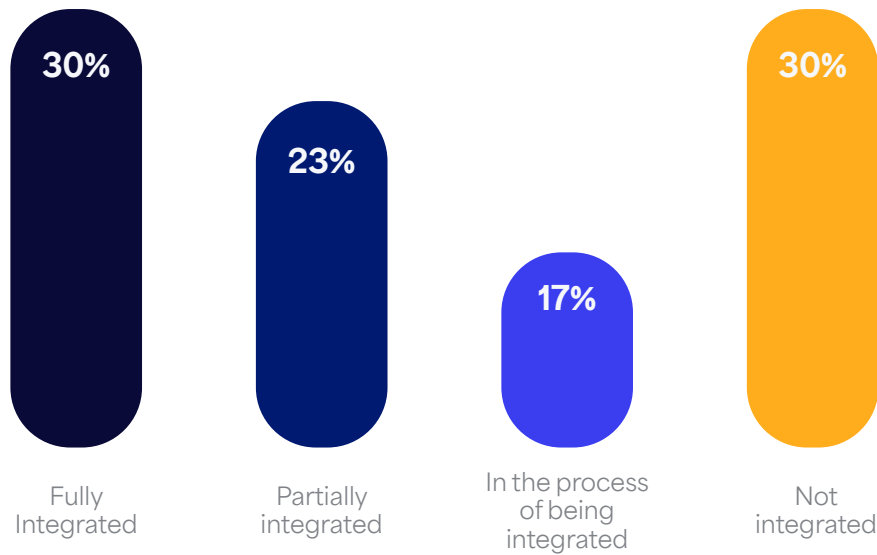


Figure 7. To what degree is IAM integrated with other technologies, including SIEM

Policies and processes used to manage machine, service, and other non-human identities and to perform periodic access review/attestation/certification of user accounts and entitlements are not integrated into the IAM platform. As shown in *Figure 8*, to manage machine, service,

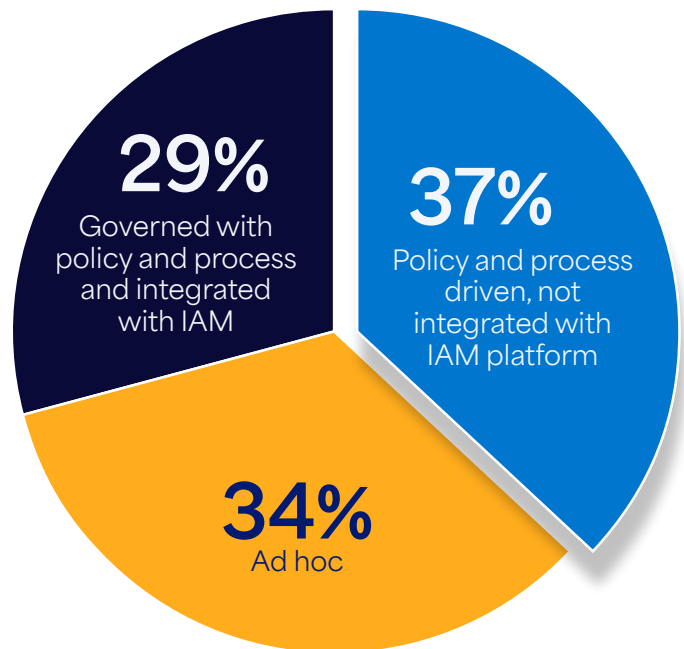
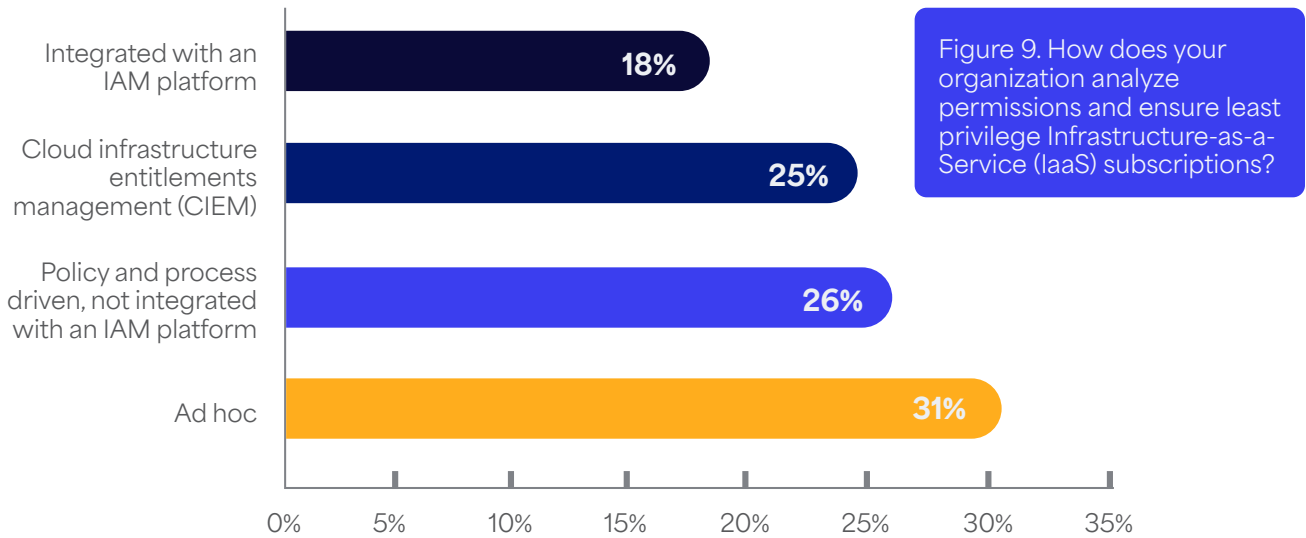


Figure 8. How does your organization use its IAM platform and/or processes to manage machine, service, and other non-human accounts or identities?

PART 2 | KEY FINDINGS

and other non-human identities, 37 percent of respondents say it is policy and process driven, not integrated with the IAM platform, and 34 percent of respondents say it is ad hoc. Only 29 percent of respondents say it is governed with policy and process and integrated with the IAM platform.



Only 18 percent of respondents say their process to analyze permissions and ensure least privilege IaaS subscriptions is integrated within an IAM platform. As shown in *Figure 9*, most processes are ad hoc according to 31 percent of respondents.

As evidence that IAM security is not a priority for many organizations, many practices to prevent unauthorized usage are ad hoc and not integrated with the IAM platform. To perform periodic access review/attestation/certification of user accounts and entitlements, 31 percent of respondents say they use custom workflows built in-house, 23 percent say the process is manual using spreadsheets and 20 percent of respondents say it is executed through IAM identity governance platform. Twenty-six percent of respondents say no access/review/attestation/certification is performed, as shown in *Figure 10*.

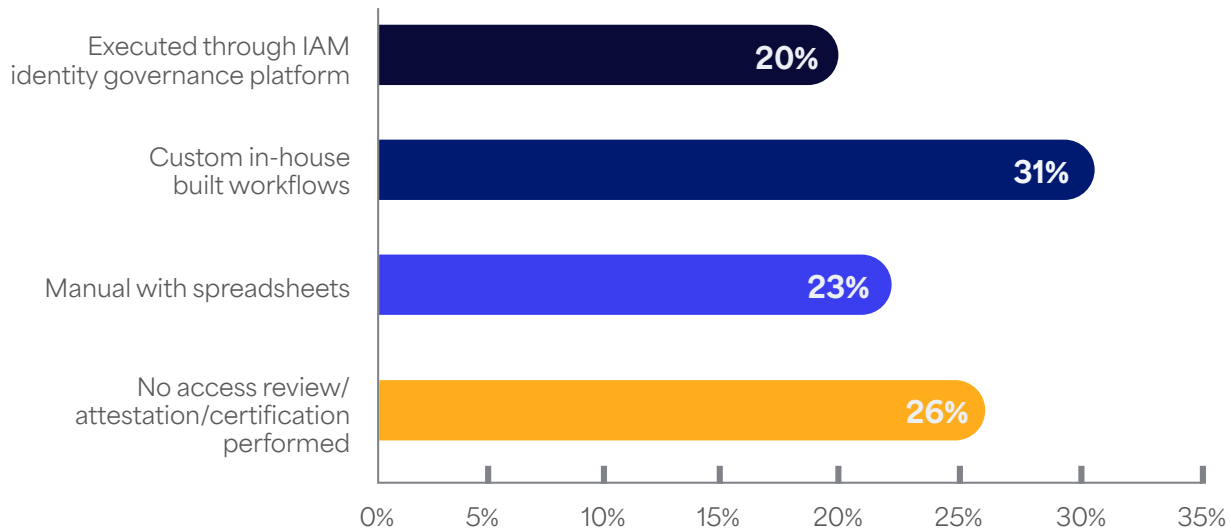


Figure 10. How does your organization use its IAM platform and/or processes to perform periodic access review/attestation/certification of user accounts and entitlements?

PART 2 | KEY FINDINGS

Active Directory (AD) is Microsoft’s proprietary directory service. It runs on Windows Server and enables administrators to manage permissions and access to network resources. AD stores data as objects. An object is a single element, such as a user, group, application, or device, such as a printer. Objects are normally defined as either resources—such as printers or computers—or security principals, such as users or groups. AD categorizes directory objects by name and attributes. For example, the name of a user might include the name string, along with information associated with the user, such as passwords. Source: Tech Target

The use of AD forest and domains is mostly ad hoc or only somewhat organized and managed. As shown in *Figure 11*, 30 percent of respondents say it is ad hoc, 27 percent of respondents say it is somewhat organized and managed, and only 18 percent of respondents say it is well organized and managed.

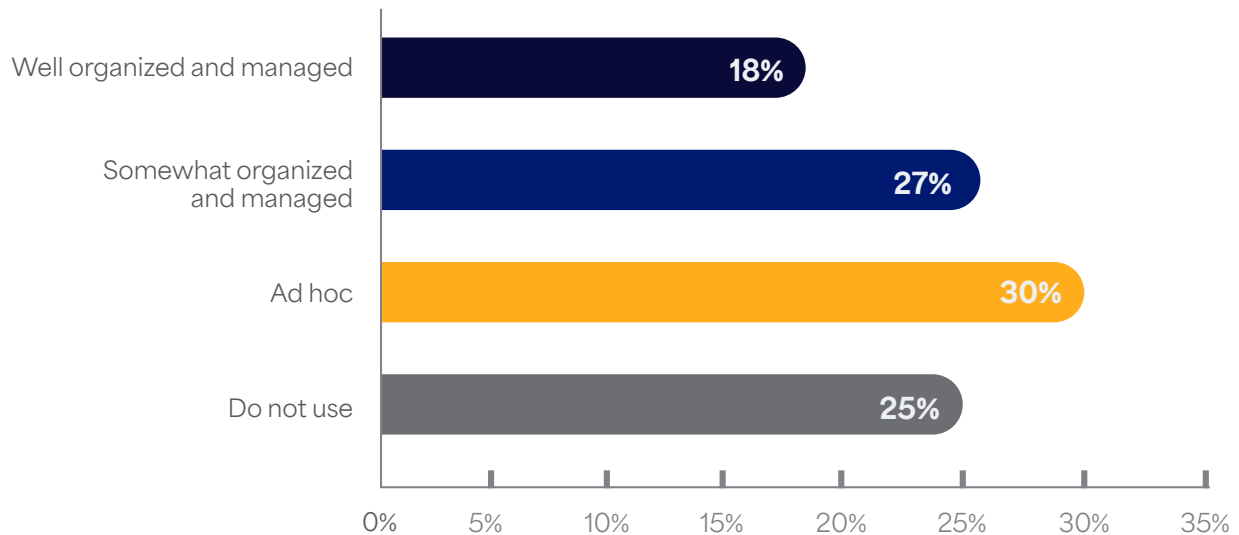


Figure 11. What is the state of your organization’s Active Directory (AD) forest and domains?

Only one choice permitted

Role-based access control (RBAC) restricts network access based on a person’s role within an organization and has become one of the main methods for advanced access control.

The roles in RBAC refer to the levels of access that employees have to the network. According to *Figure 12*, 65 percent of respondents use RBAC to simplify IAM processes but only 37 percent say it is advanced and 28 percent say it is basic.

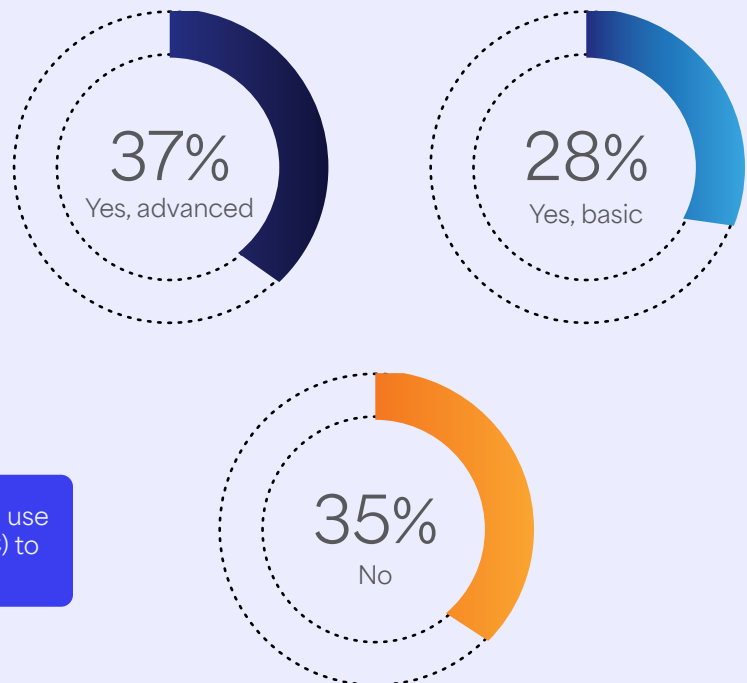


Figure 12. Does your organization use role-based access control (RBAC) to simplify IAM processes?

Forty-two percent of respondents say their organizations have a dedicated privileged access management (PAM) platform. As shown in *Figure 13*, 42 percent of respondents say PAM is running on a dedicated platform and 35 percent of respondents say privileged access is integrated with other IAM systems. The 42 percent of respondents with a dedicated platform were asked to rate its effectiveness on a scale from 1 = not effective to 10 = highly effective. Only 45 percent of these respondents say the IAM platform(s) for PAM are very or highly effective.

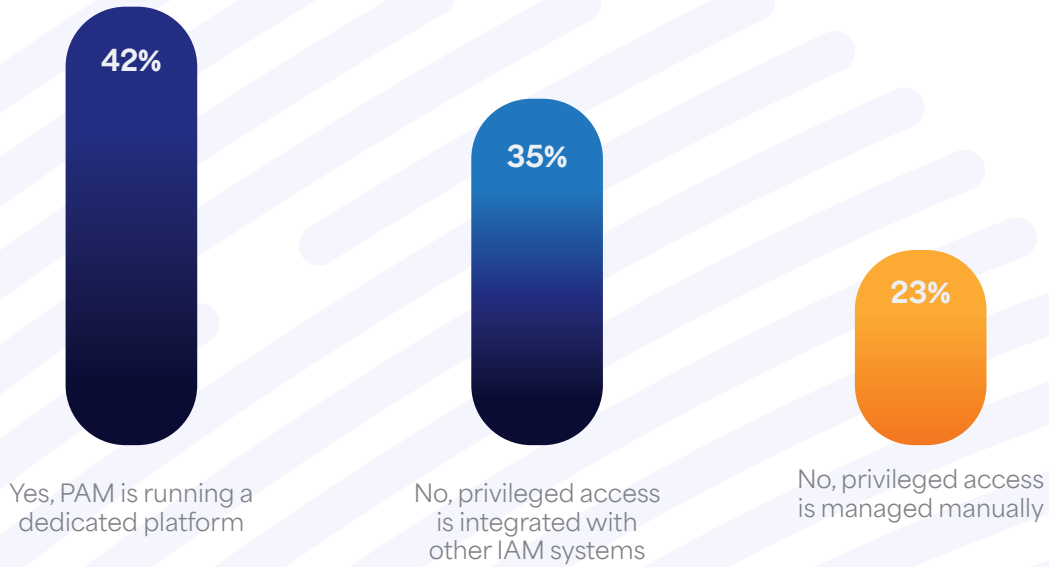


Figure 13. Does your organization have a dedicated PAM platform?

Of the 42 percent of respondents with a dedicated PAM platform, as shown in *Figure 14*, privileged access is permanently assigned to a primary account (40 percent of respondents). Thirty-three percent of respondents say a manual or scripted process exists to temporarily assign privilege account access, and 27 percent of respondents say privileged access is permanently assigned through a secondary account.

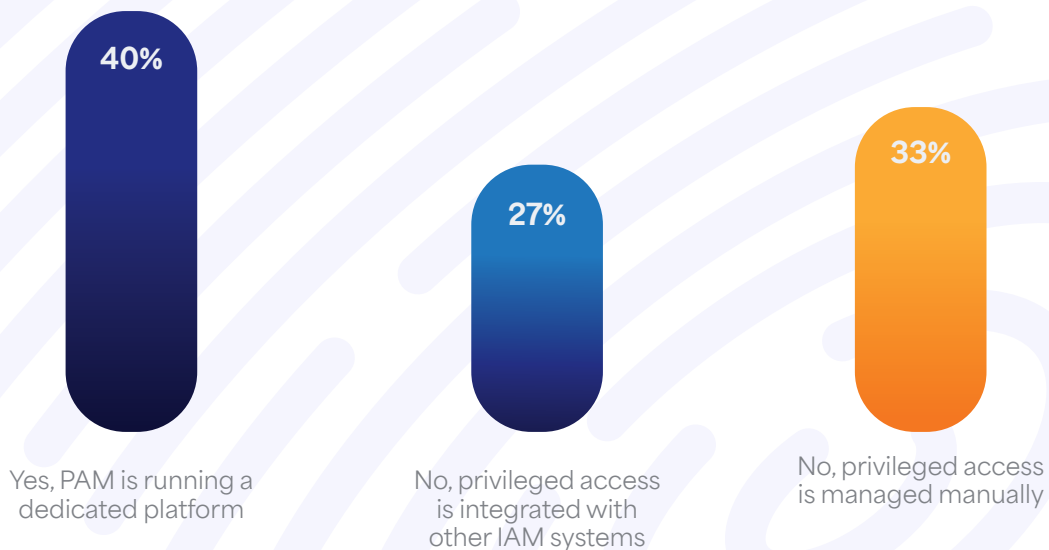


Figure 14. How does your organization assign privileged access?

If managing privileged access passwords and verifying if privileged access is required, 41 percent of respondents say passwords are assigned and managed by the account owner, 40 percent of respondents say passwords are regularly rotated by a process or system, and 19 percent of respondents say passwords are static, as shown in *Figure 15*.

To verify if privileged access is required, 41 percent of respondents say privileged access is periodically reviewed and certified, 30 percent of respondents say cybersecurity/IT security approval is required to obtain access, and 29 percent of respondents say privileged access is tracked in a sheet, table, or custom database, as shown in *Figure 16*.

Sixty-six percent of respondents create an automated report of privileged access and who is responsible for determining privileged access (36%) or use a manual report. Thirty-four percent say their organization is not able to create a report, as shown in *Figure 17*.

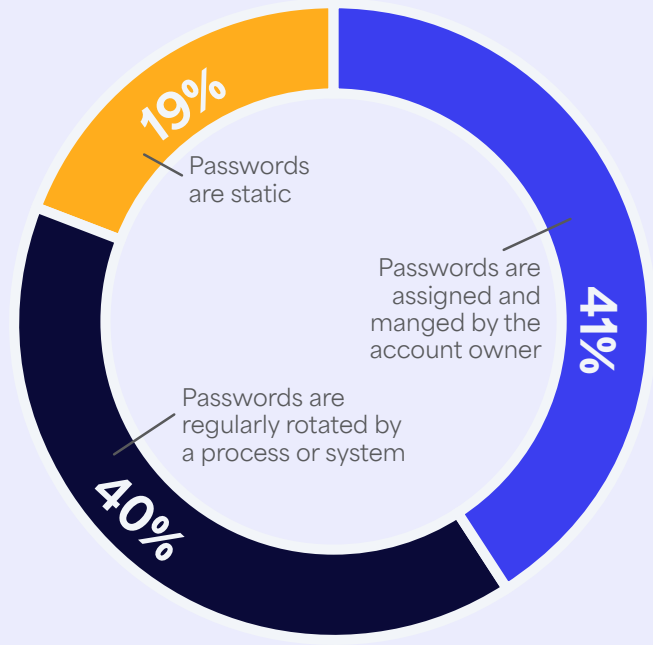


Figure 15. How does your organization manage privileged access passwords, including privileged access assigned to service accounts?

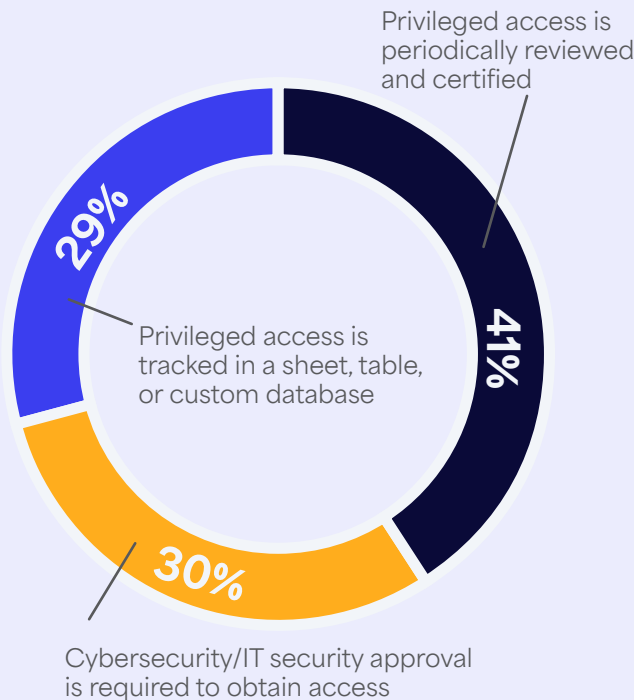


Figure 16. How does your organization's verification process determine if privileged access is required?

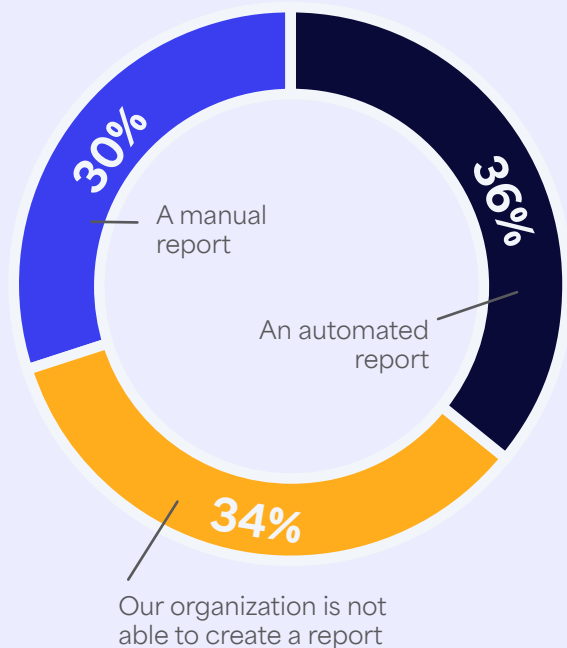


Figure 17. Does your organization create a report of privileged access and who is responsible for determining privileged access?

PART 2 | KEY FINDINGS

As shown in *Figure 18*, only 29 percent of respondents have an automated mechanism to check for compromised passwords for both customer and workforce accounts.

Organizations are slow to adopt passwordless authentication. Passwordless authentication is a means to verify a user's identity without using a password and can significantly improve the security of identities. Passwordless uses more secure alternatives, like possession factors, one-time passwords (OTP), registered (smartphones), or biometrics (fingerprint, retina scans). As shown in *Figure 19*, only 24 percent have fully implemented passwordless authentication and 35 percent say they plan to adopt within one year (15%) or between one to two years (20%).



Figure 18. Does your organization have an automated mechanism in place to check for compromised passwords?

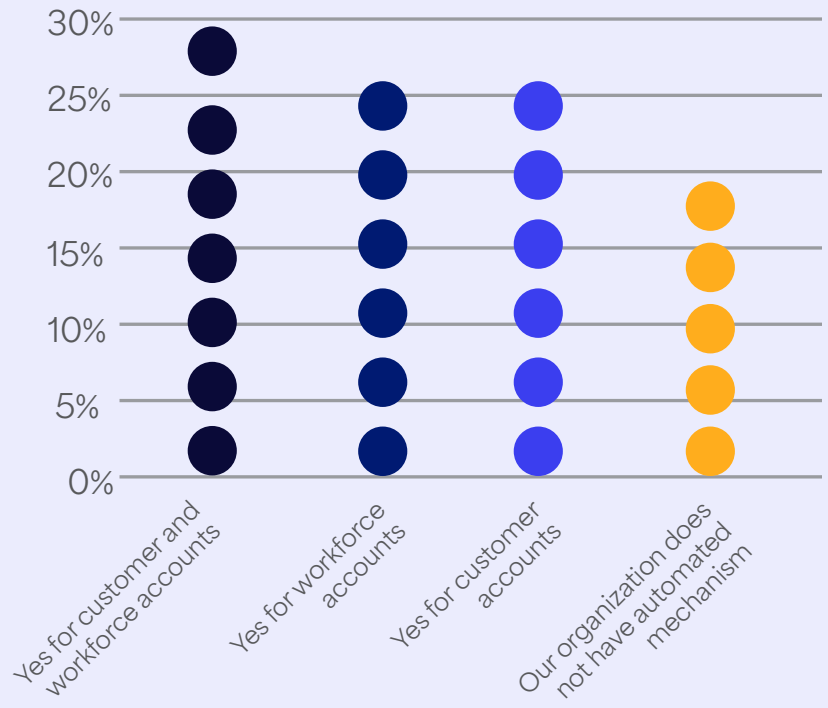


Figure 19. What describes your organization's adoption or plan to adopt passwordless authentication?

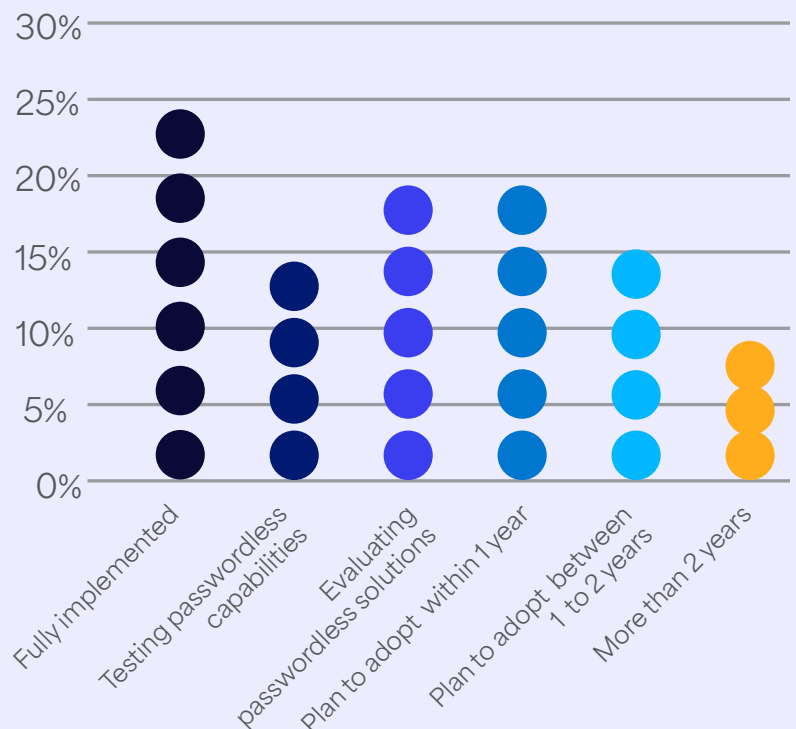
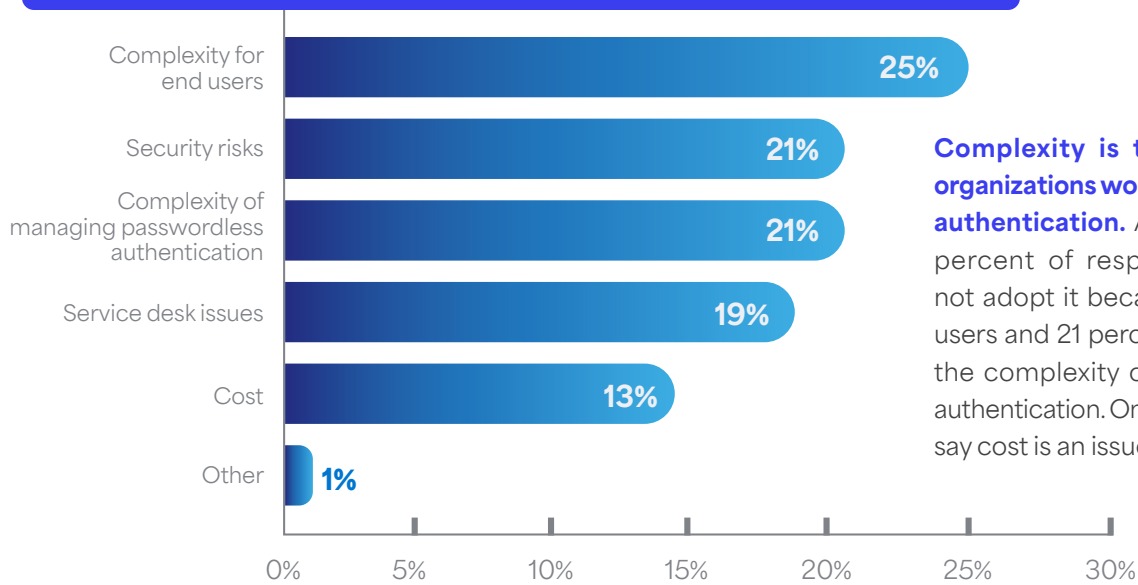


Figure 20. Why would your organization not adopt passwordless authentication?



Complexity is the primary reason why organizations would not adopt passwordless authentication. As shown in *Figure 20*, 25 percent of respondents say they would not adopt it because of complexity for end users and 21 percent of respondents say it is the complexity of managing passwordless authentication. Only 13 percent of respondents say cost is an issue.

Cloud infrastructure adoption varies among organizations represented in this research. Fifty-two percent of respondents say they are leveraging their organizations' cloud infrastructure heavily (21%), for limited, low-risk workloads (19%), or for some business-critical workloads (12%), as shown in *Figure 21*.

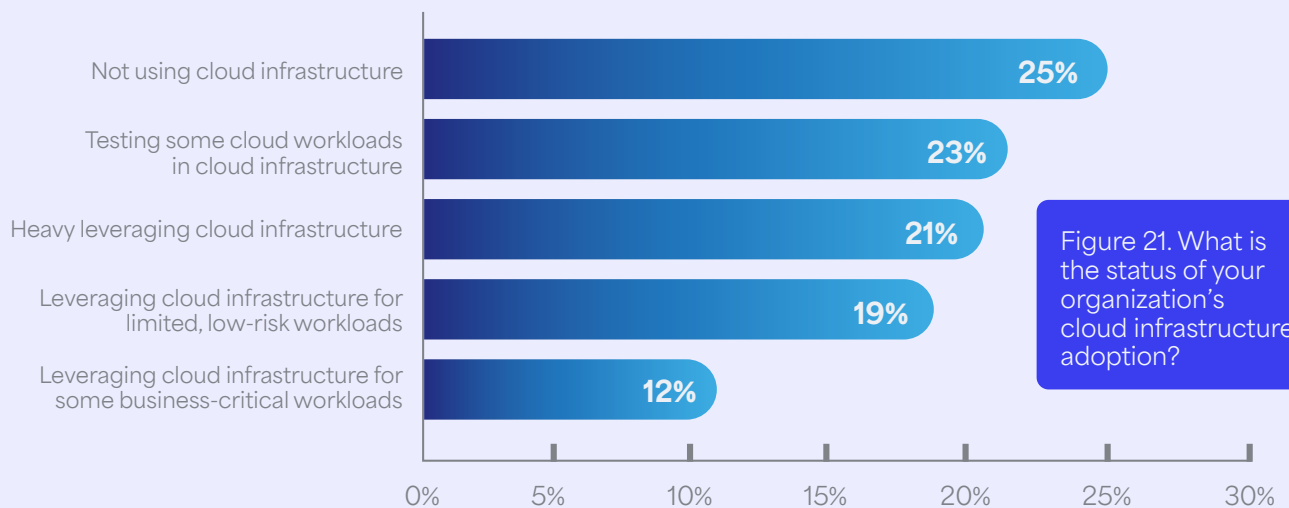


Figure 21. What is the status of your organization's cloud infrastructure adoption?

Of these 52 percent of respondents, 48 percent say their organizations' IAM is already SaaS cloud-delivered. Of the 52 percent of respondents that do not have SaaS, 91 percent say their organizations are considering a refresh to a cloud or SaaS-delivered IAM platform for user access provisioning, lifecycle, and termination, as shown in *Figure 22*.

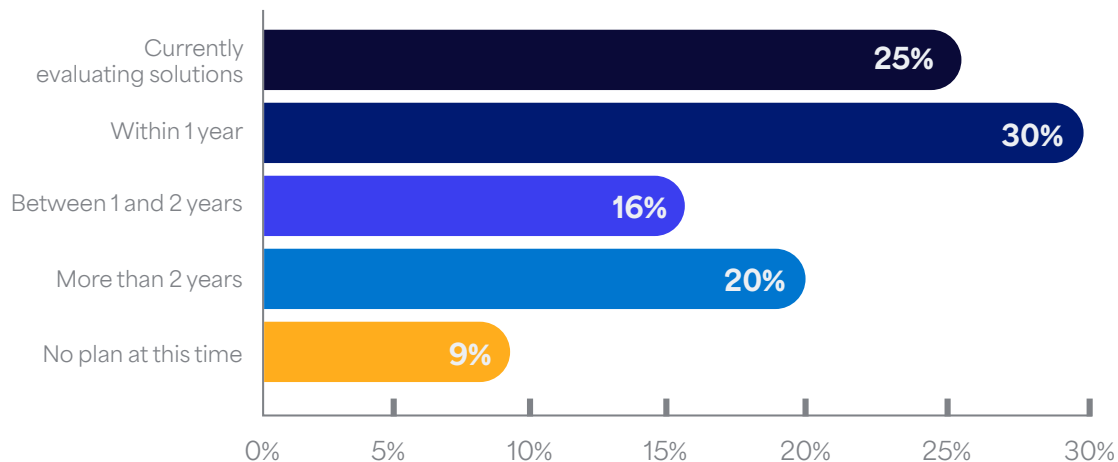


Figure 22. Is your organization considering a refresh to a cloud or a SaaS-delivered IAM platform for user access provisioning, lifecycle, and termination?

How organizations are investing in and staffing IAM

Organizations favor investing in improving user experience. According to *Figure 23*, the number one reason to invest in IAM is to improve user experience (48 percent of respondents). Forty percent of respondents say the constant changes to the organization due to corporate reorganizations, downsizing, and financial distress is a reason to invest in IAM.

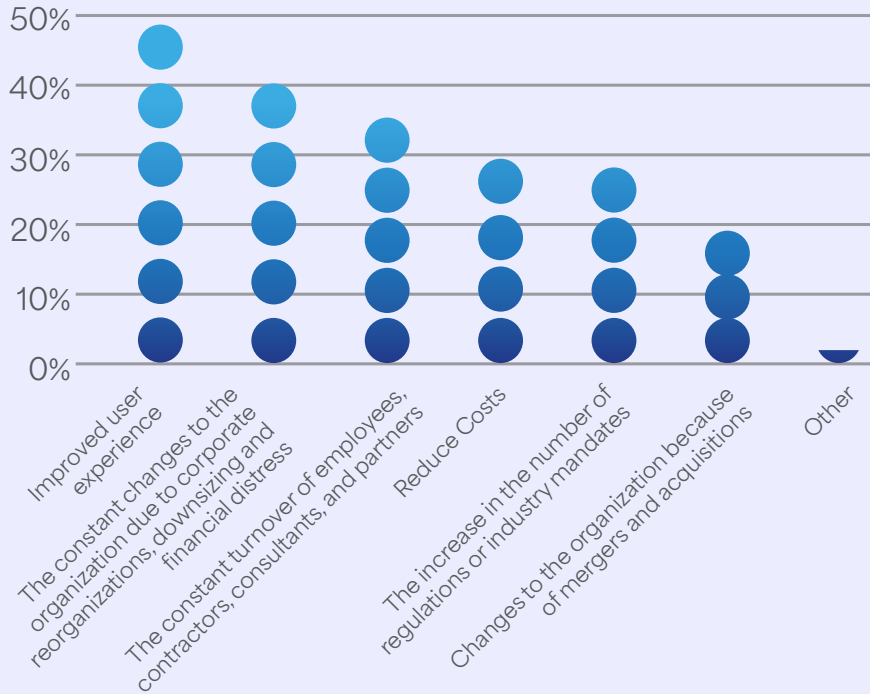


Figure 23. What are the important drivers for investing in IAM?

Two responses permitted

Organizations are moving slowly to invest in technologies that could improve the security of IAM. As shown in *Figure 24*, only 21 percent of respondents say their organization are currently evaluating AI-driven threat technology for IAM, 19 percent of respondents are currently evaluating an IAM platform that automates user access provisioning, lifecycle, and termination, and only 21 percent of respondents say they are evaluating an IAM platform to automate access review/attestation/certification of user accounts and entitlements.

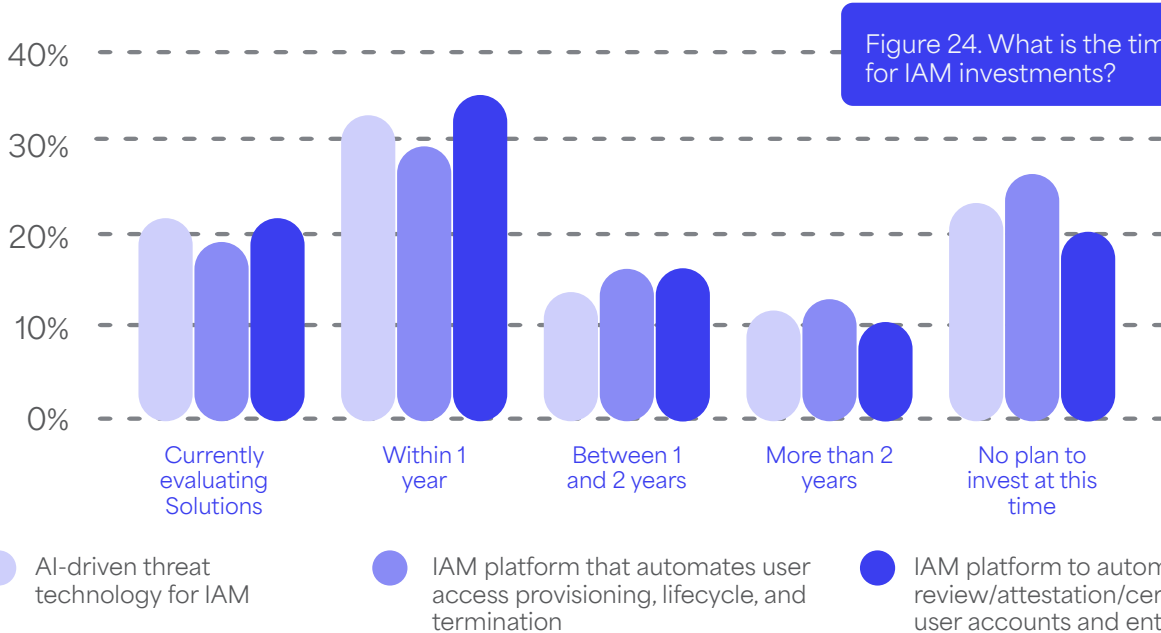


Figure 24. What is the timeframe for IAM investments?

PART 2 | KEY FINDINGS

The IT infrastructure/operations staff is most likely to manage and respond to most identity-related tasks and activities in their organizations. Various functions are involved in managing or responding to identity-related tasks and activities. According to *Figure 25*, 50 percent of respondents say that IT infrastructure/operations staff manage these activities, followed by service desk/help desk (41 percent of respondents).

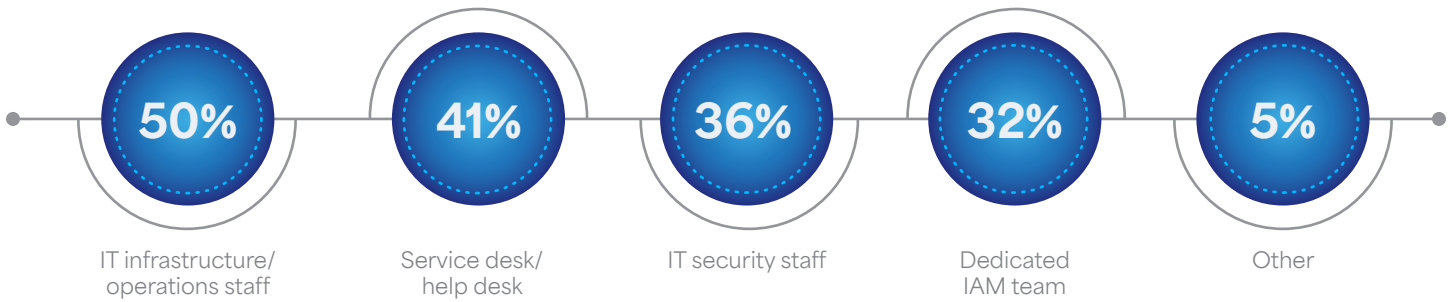


Figure 25. Which team manages or responds to most identity-related tasks and activities in your organization?

More than one response permitted

IAM technology delivery teams are most likely to report to lines of business and IT or IT infrastructure. As shown in *Figure 26*, 22 percent of respondents say their teams report to lines of business and 21 percent of respondents say it is IT or IT infrastructure. On average, there are eight staff on the IAM team.

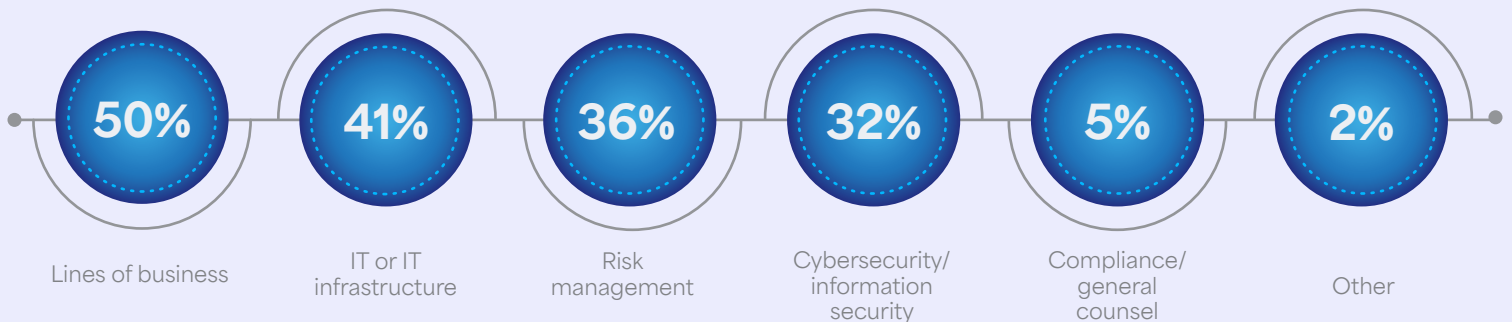


Figure 26. Which function does the IAM technology delivery team/service report to?

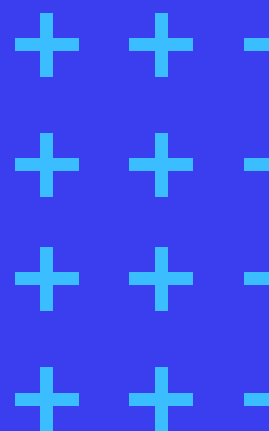
Conclusion



Enterprise and customer information is growing and is more critical than ever. As attackers become more sophisticated and empowered, IAM practices will need to continue to evolve to keep threats at bay. But many enterprises aren't even keeping up with yesterday's IAM practices much less the cutting edge. With less than half of organizations stating that they have an established or formal IAM program, **the opportunity is big: big for hackers to continue their expensive mayhem and destruction!** But the opportunity is also big for smart organizations looking to protect themselves. Long before specific IAM tactics are adopted, organizations need to understand the threats that are out there, what IAM strategies and technologies are the best fit, and how to plan and deploy them.

Based on this research, here are the top 5 immediate actions recommended by Converge to strengthen IAM and prevent credential breaches, reducing the risk of costly and reputational impacts:

- 1. Implement MFA:** MFA is essential as it mitigates security breaches caused by compromised credentials by requiring multiple forms of verification before granting access. If your organization has not implemented MFA for internal workers, the risk is amplified, and immediate action is needed.
- 2. Deploy PAM:** Attackers target privileged accounts above all. Without a PAM solution, these accounts are vulnerable to attacks, risking data breaches, system takeovers, and non-compliance with regulatory requirements. If your organization lacks a PAM solution, a critical layer of defense is missing, and it's time to act.
- 3. Integrate IAM Signaling Data to Detect Anomalies:** Integrating SIEM with IAM and implementing ITDR are crucial technology layers to detect and thwart attackers, minimizing lateral movement in case of a breach. These technologies reduce the impact of a breach regardless of your organization's IAM maturity.
- 4. Align IAM with Cybersecurity:** IAM teams should collaborate closely with cybersecurity teams to ensure risk mitigation and appropriate controls, as stolen or compromised credentials remain the most common cause of data breaches.
- 5. Establish an IAM Program:** IAM governance requires executive-level attention and focus. If your organization does not have a formal IAM program, it's essential to act now to minimize the cost of breaches, ensure compliance, and garner support for necessary investments.



Methodology

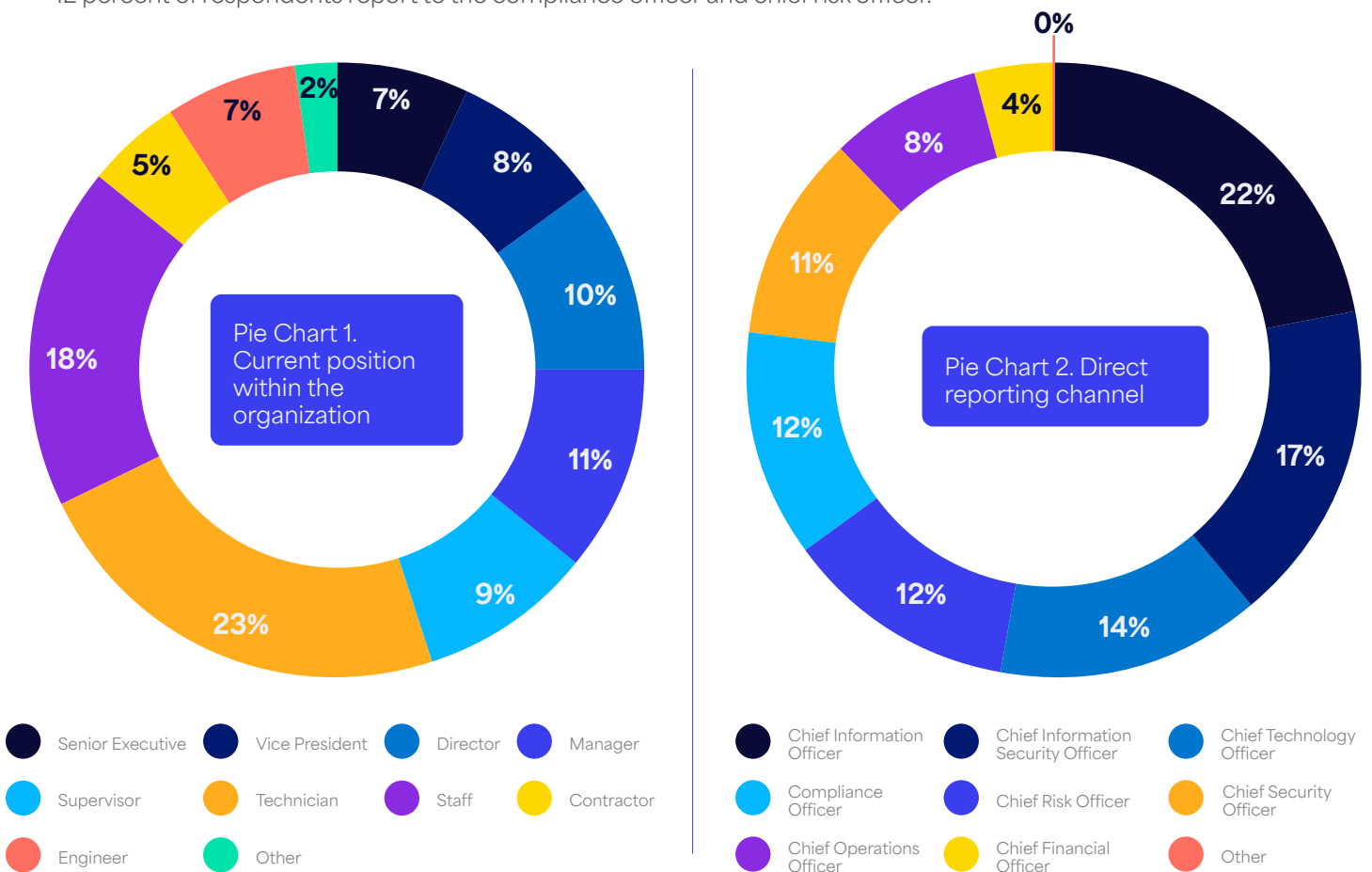
A sampling frame of 15,052 IT and IT security practitioners in the US who are involved their organizations' IAM program were selected as participants to this survey. [Table 1](#) shows 656 total returns. Screening and reliability checks required the removal of 85 surveys. Our final sample consisted of 571 surveys or a 3.8 percent response rate.

TABLE 1. SAMPLE RESPONSE

	FREQ	PCT%
Sampling frame	15,052	100.0%
Total returns	656	4.4%
Rejected or screened surveys	85	0.6%
Final sample	571	3.8%

Pie Chart 1 reports the respondent's organizational level within participating organizations. Forty-five percent of respondents are at or above the supervisory levels. The largest category, at 23 percent of respondents, is technician.

As shown in *Pie Chart 2*, 22 percent of respondents report to the chief information officer, 17 percent of respondents report to the chief information security officer, 14 percent of respondents report to the chief technology officer, and 12 percent of respondents report to the compliance officer and chief risk officer.



Caveats to this Study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-Response Bias

The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable, returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sample-Frame Bias

The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT and IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-Reported Results

The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix

With Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to survey questions. All survey responses were captured in April 2024.

SURVEY RESPONSE	FREQ
Total sampling frame	15,052
Total survey returns	656
Rejected surveys	85
Final sample	571
Response rate	3.8%

PART 1 SCREENING	PCT%
S1. Which best describes your role and involvement in your organization's IAM program. Please select all that apply.	
Setting IAM program priorities	31%
Managing budget	37%
Selecting IAM vendors and contractors	42%
Determining IAM strategy	26%
Evaluating IAM effectiveness	51%
Mitigating IAM security risk	46%
IAM engineering or support	29%
Managing IAM personnel, teams, and projects	36%
No involvement in the IAM program (Stop)	0%
Total	298%
S2. What is the headcount of your organization?	
Less than 500 (Stop)	0%
500 to 2,000	20%
2,001 to 10,000	34%
10,001 to 25,000	18%
25,001 to 75,000	13%
More than 75,000	15%
Total	100%
Extrapolated Value	21,170

PART 2 BACKGROUND ON IAM PRACTICES		PCT%
Q1. Which team(s) manages or responds to most identity related tasks and activities in your organization? Please select all that apply.		
Service desk/help desk		41%
IT infrastructure/operations staff		50%
IT security staff		36%
Dedicated IAM team		32%
Other (please specify)		5%
Total		164%
Q2. How large is your organization's IAM team?		
1 to 3		27%
4 to 5		30%
6 to 10		16%
11 to 20		18%
More than 20		9%
Total		100%
Extrapolated Value		7.9
Q3. Which function does the IAM technology delivery team/service report to? Please select one choice only.		
Cybersecurity/information security		19%
IT or IT infrastructure		21%
Compliance/general counsel		17%
Risk management		19%
Lines of business		22%
Other (please specify)		2%
Total		100%
Q4. What are the most important drivers for investing in IAM? Please select the top two choices.		
The increase in the number of regulations or industry mandates		27%
The constant turnover of employees, contractors, consultants, and partners		35%
Improved user experience		48%
Reduce costs		29%
The constant changes to the organization due to corporate reorganizations, downsizing, and financial distress		40%
Changes to the organization because of mergers and acquisitions		19%
Other (please specify)		2%
Total		200%

Q5a. Has your organization been involved in a merger or acquisition in the past 5 years?

Yes	64%
No (please skip to Q6)	36%

Total 100%

Q5b. If yes, using the following 10-point scale, please rate how effective your organization was in integrating identity and access practices following the merger and acquisition from 1 = not effective to 10 = highly effective.

1 to 2	8%
3 to 4	21%
5 to 6	23%
7 to 8	27%
9 to 10	21%

Total 100%

Q5c. If very or highly effective (7+ responses), how long did the integration take?

Less than 1 year	19%
1 to 2 years	31%
2 to 3 years	29%
More than 3 years	21%

Total 100%

Q6. Does your organization have an established/formal IAM program, steering committee, and/or internally defined strategy?

Yes	45%
No	45%
Unsure	10%

Total 100%

Q7. Using the following 10-point scale, please rate the effectiveness of your organization’s IAM platform(s) for user access provisioning, lifecycle, and termination from 1 = not effective to 10 = highly effective.

1 to 2	15%
3 to 4	21%
5 to 6	18%
7 to 8	25%
9 to 10	21%

Total 100%

Q8. Using the following 10-point scale, please rate the effectiveness of your organization’s IAM platform(s) for authentication and authorization from 1 = not effective to 10 = highly effective.

1 to 2	9%
3 to 4	23%
5 to 6	24%
7 to 8	21%
9 to 10	23%
Total	100%

Q9. Using the following 10-point scale, please rate the priority of your organization’s IAM program compared to other security initiatives from 1 = not a priority to 10 = high priority.

1 to 2	10%
3 to 4	19%
5 to 6	25%
7 to 8	25%
9 to 10	21%
Total	100%

Q9. Using the following 10-point scale, please rate the priority of your organization’s IAM program compared to other security initiatives from 1 = not a priority to 10 = high priority.

1 to 2	10%
3 to 4	19%
5 to 6	25%
7 to 8	25%
9 to 10	21%
Total	100%

Q10. Has your organization implemented multifactor authentication (MFA)? Please select one choice only.

Yes, MFA is applied to customer accounts	24%
Yes, MFA is applied to workforce accounts	21%
MFA is applied to both customer and workforce accounts	25%
Our organization has not implemented MFA	30%
Total	100%

Q11a. Has your organization adopted or plan to adopt zero trust as part of your organization’s IAM approach?

Yes	65%
No	35%
Total	100%

Q11b. If yes, what best describes your organization’s adoption of zero trust?

Implementation and testing in process	13%
Evaluating zero-trust solutions	23%
Fully adopted	20%
Within 1 year	23%
Between 1 to 2 years	12%
More than 2 years	9%

Total 100%

Q12. To what degree is IAM integrated with other technologies, including SIEM?

Fully integrated	30%
Partially integrated	23%
In the process of being integrated	17%
Not integrated	30%

Total 100%

Q13. How does your organization use its IAM platform and/or processes to manage machine, service, and other non-human accounts or identities? Please select one choice only.

Ad hoc	34%
Policy and process driven, not integrated with IAM platform	37%
Governed with policy and process and integrated with IAM platform	29%

Total 100%

Q14. How does your organization use its IAM platform and/or processes to perform periodic access review/attestation/certification of user accounts and entitlements? Please select one choice only.

	Pct%
Manual with spreadsheets	23%
Custom in-house built workflows	31%
Executed through IAM identity governance platform	20%
No access review/attestation/certification performed	26%

Total 100%

Q15. Does your organization use role-based access control (RBAC) to simplify IAM processes?

Yes, basic	28%
Yes, advanced	37%
No	35%

Total 100%

Q16. What is the state of your organization's Active Directory (AD) forest and domains?

Well-organized and managed	18%
Somewhat organized and managed	27%
Ad hoc	30%
Do not use	25%

Total 100%

PART 3 IAM SECURITY RISKS**PCT%****Q17a. In the past 24 months, did your organization have a data breach due to leaked, compromised, or stolen credentials?**

Yes	54%
No	46%
Unsure (please skip to Q18)	0%

Total 100%

Q17b. If yes, how frequently did these incidents occur in the past 12 months?

Only once	21%
2 to 3 times	32%
4 to 5 times	29%
More than 5 times	18%

Total 100%

Q17c. Following the data breach, did your organization experience any of the following?

Leakage of high-value information assets	51%
Data center downtime	29%
Data exfiltration and extortion	18%
Diminished productivity of employees	37%
Cost of consultants and attorneys	16%
Decline in reputation and trustworthiness	26%
Regulatory fines	11%
Other (please specify)	5%

Total 193%

Q18. If a threat actor used a stolen credential to login to your organization, how long would it take to detect it.

In real time	25%
In minutes	10%
Less than 24 hours	11%
1 day to 1 week	18%
More than 1 week	28%
We would not be able to detect the incident	8%

Total 100%

Q19. Is your organization prepared to protect identities when attackers have AI capabilities?

Yes	45%
No	47%
Unsure	8%

Total 100%

Q20. Does your organization use risk-based authentication (e.g. adaptive authentication) to prevent unauthorized access?

Yes	49%
No	43%
Unsure	8%

Total 100%

Q21. Does your organization use AI security technology to continuously monitor authenticated user sessions to prevent unauthorized access?

Yes	37%
No	52%
Unsure	11%

Total 100%

PART 4 IAM INVESTMENTS**PCT%****Q22. Would your organization invest in AI-driven threat technology for IAM?**

Currently evaluating solutions	21%
Within 1 year	32%
Between 1 and 2 years	13%
More than 2 years	11%
No plan to invest at this time	23%

Total 100%

Q23. Does your organization currently have an IAM tool or platform that automates identity management (user access provisioning, lifecycle, and termination)?

Yes, on premises (please skip to Q25)	33%
Yes, cloud-delivered (please skip to Q25)	39%
No	28%

Total 100%

Q24. If no, would your organization invest in an IAM platform that automates user access provisioning, lifecycle, and termination?

Currently evaluating solutions	19%
Within 1 year	29%
Between 1 and 2 years	15%
More than 2 years	12%
No plan to invest at this time	25%

Total 100%

Q25. Would your organization invest in an IAM platform to automate access review/attestation/certification of user accounts and entitlements?

Currently evaluating solutions	21%
Within 1 year	34%
Between 1 and 2 years	15%
More than 2 years	10%
No plan to invest at this time	20%

Total 100%

Q26. Does your organization currently have an IAM tool or platform that provides authentication, authorization, and single sign-on (SSO)?

Yes, on premises (please skip to Q28)	32%
Yes, cloud delivered (please skip to Q28)	39%
No	29%

Total 100%

Q27. If no, would your organization invest in an IAM platform that provides authentication, authorization, and single-sign-on?

Currently evaluating solutions	23%
Within 1 year	29%
Between 1 and 2 years	18%
More than 2 years	10%
No plan to invest at this time	20%

Total 100%

PART 5 IAM IN THE CLOUD	PCT%
Q28. What is the status of your organization's cloud infrastructure adoption?	
Heavy leveraging cloud infrastructure	21%
Leveraging cloud infrastructure for limited, low-risk workloads	19%
Leveraging cloud infrastructure for some business-critical workloads	12%
Testing some cloud workloads in cloud infrastructure (please skip to Q31)	23%
Not using cloud infrastructure (please skip to Q31)	25%
Total	100%
Q29a. Is your organization's IAM already SaaS cloud-delivered?	
Yes (please skip to Q30a)	48%
No	52%
Total	100%
Q29b. If no, is your organization considering a refresh to a cloud- or SaaS-delivered IAM platform for user access provisioning, lifecycle, and termination?	
Currently evaluating solutions	25%
Within 1 year	30%
Between 1 and 2 years	16%
More than 2 years	20%
No plan at this time	9%
Total	100%
Q30a. Does your organization analyze permissions and ensure least privilege in Infrastructure-as-a-Service (IaaS) subscriptions?	
Yes	49%
No (please skip to Q31)	37%
Unsure (please skip to Q31)	14%
Total	100%
Q30b. If yes, how does your organization analyze permissions and ensure least privilege in Infrastructure-as-a-Service (IaaS) subscriptions? Please select one choice only.	
Ad hoc	31%
Policy and process driven, not integrated with an IAM platform	26%
Integrated with an IAM platform	18%
Cloud infrastructure entitlements management (CIEM)	25%
Total	100%

PART 6 PRIVILEGED ACCESS MANAGEMENT (PAM)		PCT%
Q31. Does your organization have a dedicated PAM platform?		
Yes, PAM is running a dedicated platform		42%
No, privileged access is integrated with other IAM systems (please skip to Q37)		35%
No, privileged access is managed manually (please skip to Q37)		23%
Total		100%
Q32. How does your organization assign privileged access? Please select one choice only.		
Privileged access is permanently assigned to primary account		40%
Privileged access is permanently assigned through a secondary account		27%
Manual or scripted process exists to temporarily assign privileged account		33%
Total		100%
Q33. How does your organization manage privileged access passwords, including privileged access assigned to service accounts? Please select one choice only.		
Passwords are assigned and managed by the account owner		41%
Passwords are regularly rotated by a process or system		40%
Passwords are static		19%
Total		100%
Q34. How does your organization's verification process determine if privileged access is required? Please select all that apply.		
Cybersecurity/IT security approval is required to obtain access		30%
Privileged access is tracked in a sheet, table or custom database		29%
Privileged access is periodically reviewed and certified		41%
Total		100%
Q35. Does your organization create a report of privileged access and who is responsible for determining privileged access? Please select one choice only.		
An automated report		36%
A manual report		30%
Our organization is not able to create a report		34%
Total		100%
Q36. Using the following 10-point scale, please rate the effectiveness of your organization's IAM platform(s) for PAM from 1 = not effective to 10 = highly effective.		
1 or 2		16%
3 or 4		18%
5 or 6		21%
7 or 8		20%
9 or 10		25%
Total		100%

PART 7 PASSWORDLESS AUTHENTICATION PCT%

Q37. Does your organization have an automated mechanism in place to check for compromised passwords? Please select one choice only.

Yes, an automated mechanism for customer accounts	26%
Yes, an automated mechanism for workforce accounts	26%
Yes, an automated mechanism for customer and workforce accounts	29%
Our organization does not have an automated mechanism	19%

Total **100%**

Q38. Has your organization adopted or plan to adopt passwordless authentication?

Yes	49%
No plans to adopt (please skip to Q40)	51%

Total **100%**

Q39. If yes, what describes your organization's adoption or plan to adopt passwordless authentication? Please select only one choice.

Fully implemented	24%
Testing passwordless capabilities	14%
Evaluating passwordless solutions	19%
Plan to adopt within 1 year	15%
Plan to adopt between 1 to 2 years	20%
More than 2 years	8%

Total **100%**

Q40. Why would your organization not adopt passwordless authentication? Please select only one choice.

Cost	13%
Complexity of managing passwordless authentication	21%
Complexity for end users	25%
Service desk issues	19%
Security risks	21%
Other (please specify)	1%

Total **100%**

PART 8 ROLES AND DEMOGRAPHICS **PCT%**

D1. What organizational level best describes your current position?

Senior Executive	7%
Vice President	8%
Director	10%
Manager	11%
Supervisor	9%
Technician	23%
Staff	18%
Contractor	5%
Engineer	7%
Other	2%

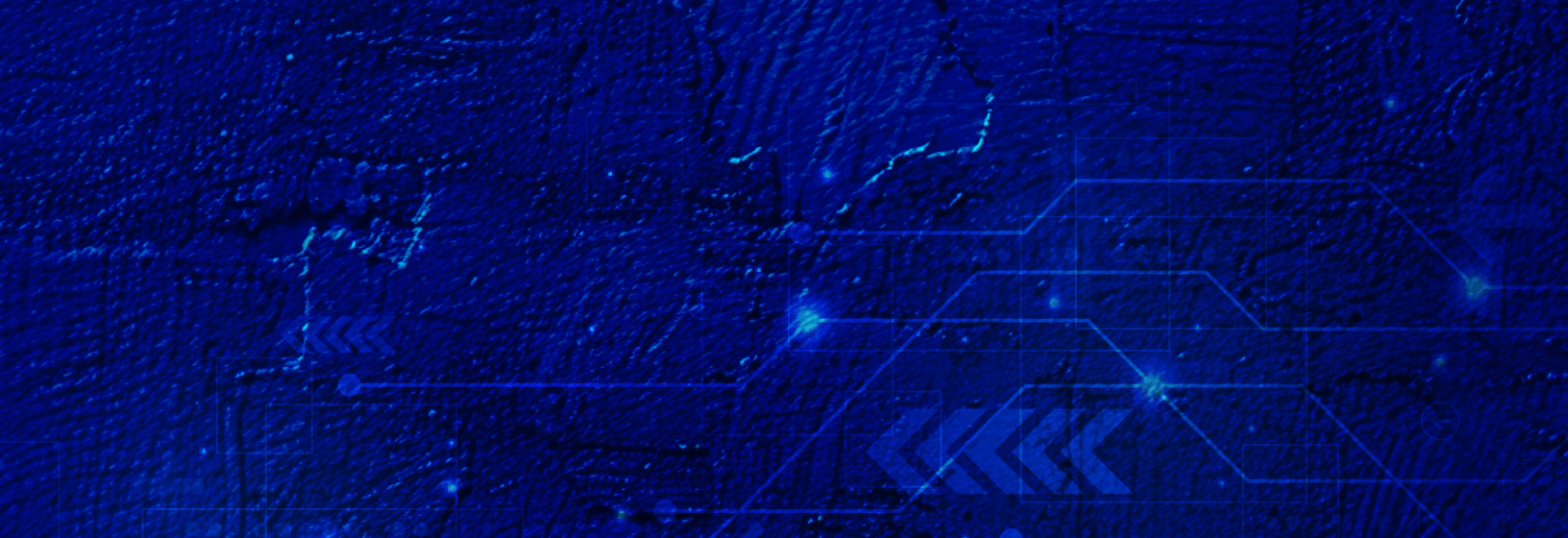
Total **100%**

D2. Check the primary person you report to within the organization.

Chief Financial Officer	4%
Chief Operations Officer	8%
General Counsel	0%
Chief Information Officer	21%
Chief Technology Officer	13%
Chief Information Security Officer	16%
Chief Security Officer	11%
Compliance Officer	12%
Chief Risk Officer	12%
Other	3%

Total **100%**





For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at **1.800.887.3118**.



Ponemon Institute Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.