2020

Cybersecurity INSIDERS

Identity and Access Management Report

simeio
Identity, intelligently managed.

INTRODUCTION

The 2020 Identity and Access Management Report reveals the increasing importance of managing access for a significant majority of organizations (89%) as part of their overall risk management and security posture. At the same time, a majority of organizations (56%) are, at best, only somewhat confident in the effectiveness of their identity and access management program.

In the context of this study, the purpose of Identity and Access Management is to grant access privileges for the right enterprise assets, to the right users, in the right context of their role and scope of responsibilities within an organization.

The 2020 Identity and Access Management Report highlights what is and what is not working for security operations teams in securing access to sensitive data, systems, and applications:

- 72% of organizations prioritize security over operational efficiency (52%) and breach prevention (47%) as the key drivers for developing an IAM program.
- Looking forward, organizations equally prioritize investment in multi-factor authentication (52%) and privileged access management (52%), followed by identity management and governance (49%).
- Role-based access control continues to be the most deployed IAM capability for 71% of organizations, followed by single sign-on (58%) and user monitoring (51%).
- Lack of automation (43%) and lack of skilled staff (41%) are the two biggest challenges regarding managing access in organizations, followed by not utilizing available technologies (33%).
- When selecting an IAM solution, 72% of organizations prioritize ease of integration above end user experience (62%) and product performance/effectiveness (61%).

To help shape, strategize, and execute IAM programs for enterprises, organizations should take ownership of their platforms so they can truly consume IAM-as-a-service whether it's deployed on-premise, the cloud, or a hybrid approach.

This 2020 Identity and Access Management Report has been produced by Cybersecurity Insiders, the 400,000 member information security community, to explore the latest trends, key challenges, gaps and solution preferences for Identity and Access Management (IAM).

Many thanks to Simeio Solutions for supporting this unique research study.

We hope you'll find this report informative and helpful as you continue your efforts in protecting your IT environments.

Thank you,

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

IAM BEST PRACTICES

1

INVESTMENT

What's the best investment you can make today with your limited cybersecurity dollars? Multi-Factor Authentication, or MFA for short. With credential stuffing attacks on the increase, and users still no better at maintaining secure passwords, an MFA solution provides every business with an additional layer of security beyond the simple password. With breaches as prevalent as ever, MFA protects both the business and the user from the loss of control over an account's password. If budgets are tight and timelines short, start with MFA for your privileged accounts first!

2

CAPABILITIES

Companies are still in the early stages of rolling out capabilities like role-based access control (RBAC), some because they have created roles so specific they've engineered themselves into having almost as many roles as employees! Access controls are an essential feature of IAM, but are roles still the best way to impose that control? No, they're not; it's far better to implement a risk-based access control model. That you happen to have a financial role at a company (even CFO) should not automatically grant you access to any and every financial data system at the company, especially if you're coming in from an unfamiliar IP address range, or at an unusual time of day, or attempting access to an unusual system, etc. The risk of granting you access needs to be considered beyond just your role, and the products that provide the capability of risk-based access control need to be considered first.

3

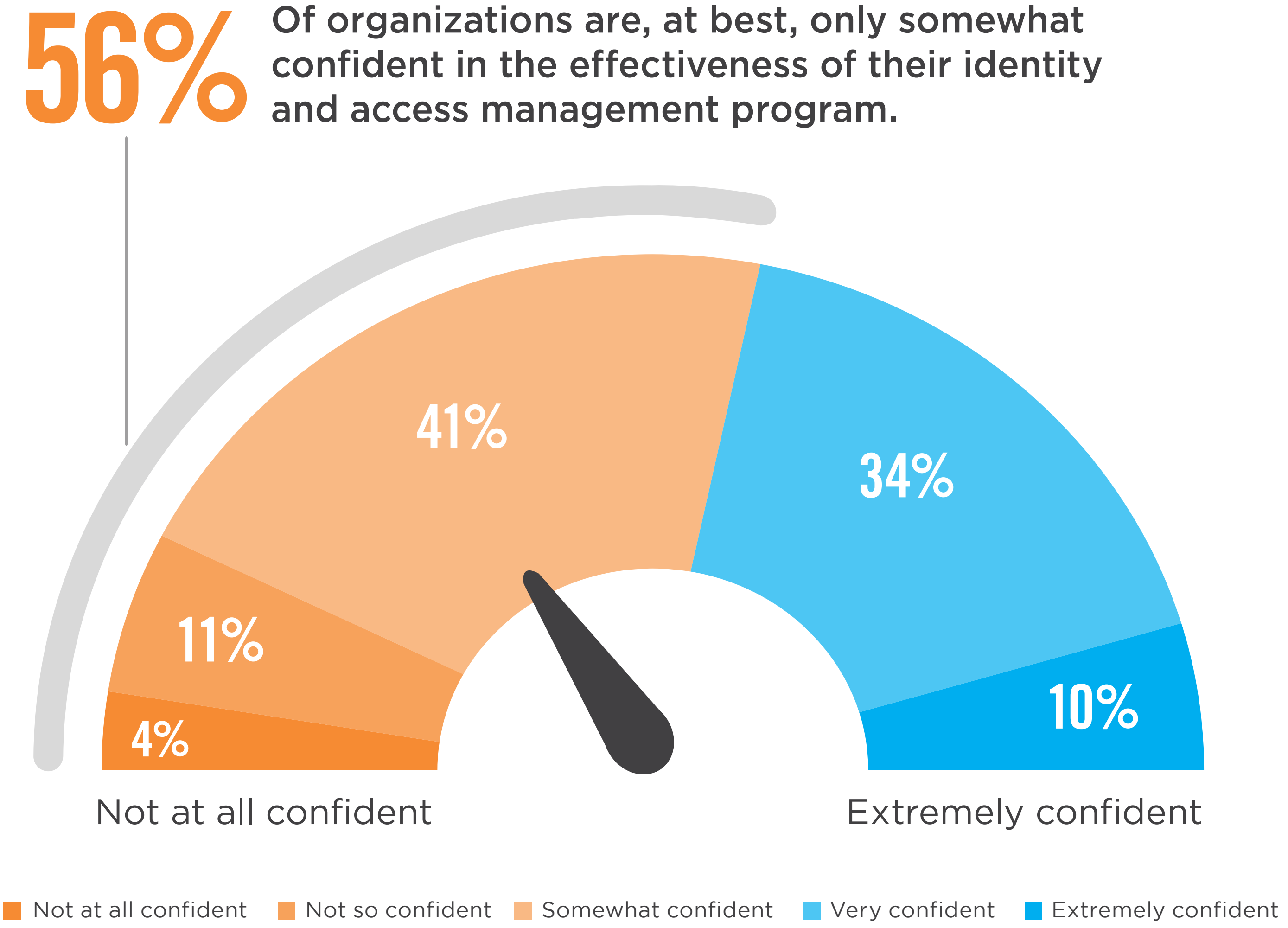
EVALUATING CRITERIA

It's no surprise that the most important criteria in evaluating IAM solutions happen to mirror each other – for IT, ease of integration, and for users, ease of use. Ease of integration means that you can get the IAM solutions up and running quickly in your unique environment, thus being able to demonstrate to your stakeholders the wisdom of their investment. For users, ease of use means that the IAM solution helps them work safer, with better risk mitigation, with greater speed of access to applications critical to their getting work done, and fewer passwords! And the best place to have IT and users meet and see those criteria in action is an IAM pilot in their own environment.

IAM PROGRAM EFFECTIVENESS

Fifty-six percent are, at best, somewhat confident in the effectiveness of their identity and access management program. This response represents a small decline in the share of organizations that expressed confidence in their IAM posture last year.

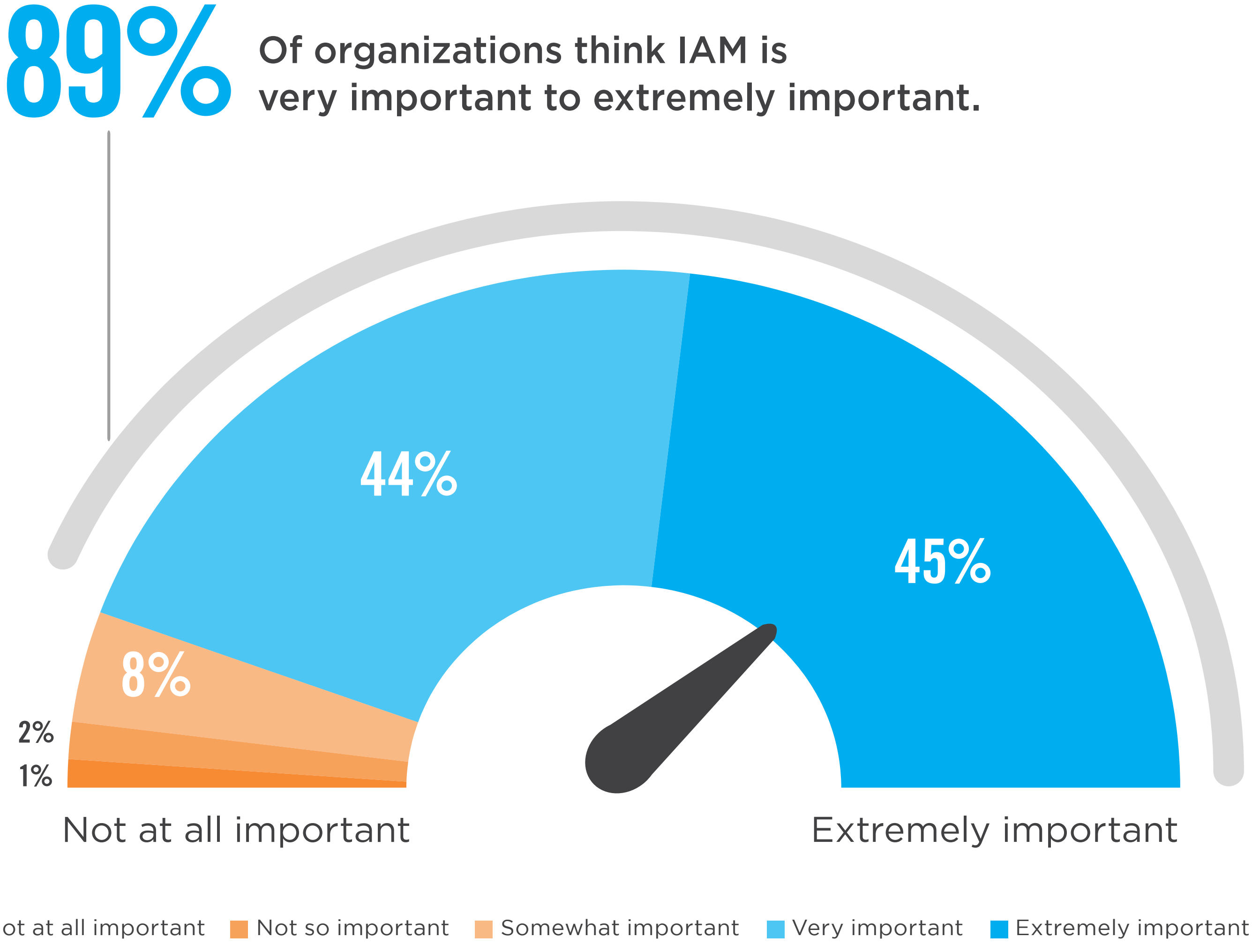
How confident are you in the effectiveness of your organization's Identity and Access Management program?



IMPORTANCE OF IAM RISING

About 9 out of 10 organizations confirm that identity and access management is very to extremely important as part of their cybersecurity and risk management posture (89%). This is a three percentage point increase compared to last year's survey.

How important is identity and access management to your organization's overall risk management and security posture?



KEY IAM CAPABILITIES

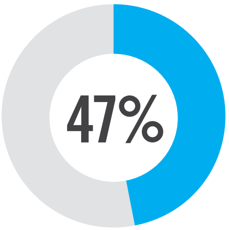
Role-based access control continues to be the most deployed IAM capability (71%), followed by single sign-on (58%) and user monitoring (51%) – up from the number five spot in last year's survey.

What IAM capabilities are deployed in your organization?

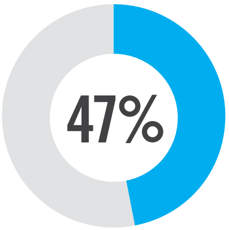
71%
Role-based access control

58%
Single sign-on

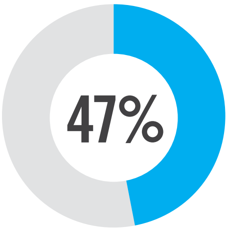
51%
User monitoring



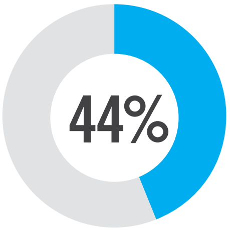
Compliance or auditor reporting



System & application access monitoring



Password self-service



Administrative reporting

Integration with service desk/ITSM solutions 42% | Automated user provisioning/de-provisioning 41% | Considerations for contract or temporary staff 35% | Streamlined user certification/auditing 27% | Advanced analytics (such as artificial intelligence (AI) or machine learning (ML)) 15% | Other 8%

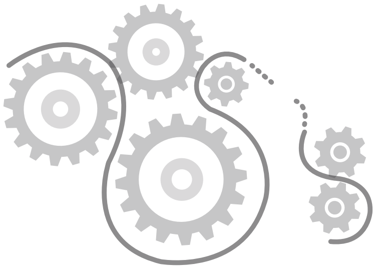
UNAUTHORIZED ACCESS

For organizations that experienced unauthorized access to sensitive systems and data, system downtime (23%) had the biggest business impact. This was closely followed by disrupted business activities (22%) and increased helpdesk load (21%).

▶ **What negative impact did your business experience from unauthorized access to sensitive data, applications or systems in the past 12 months?**

23%

System downtime

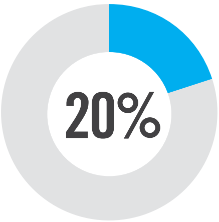


22%

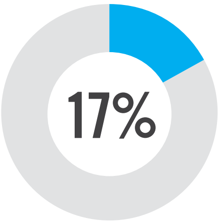
Disrupted business activities

21%

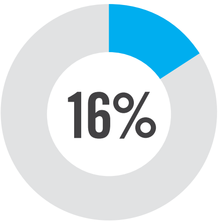
Increased helpdesk time



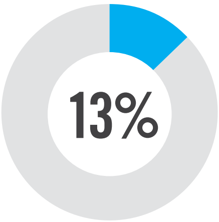
Reduced employee productivity



Data loss



Deployment of IT resources to triage and remediate issue



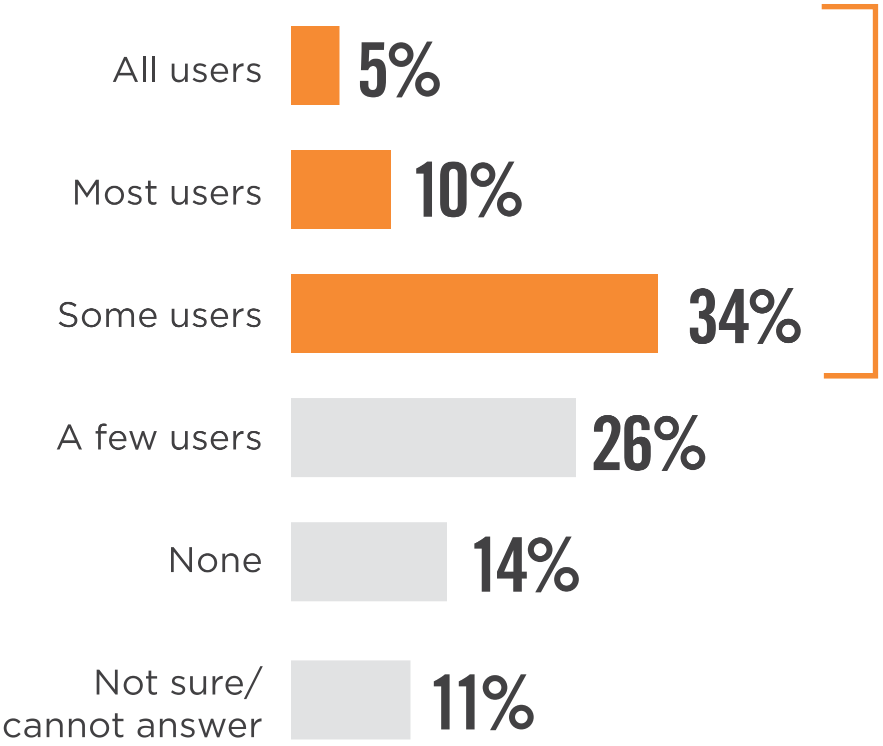
Negative publicity/ reputational damage

Reduced revenue/lost business 9% | Loss/compromise of intellectual property 9% | Lawsuit/legal issues 9% | Customer loss 6% Regulatory fines Other 1% | None/no business impact due to unauthorized access 34% | None/no unauthorized access was known to occur 26% | Other 4%

EXCESSIVE ACCESS PRIVILEGES

About half of organizations (49%) report that at least some users (34%), most users (10%) or all users (5%) have more access privileges than required for their job.

▶ **How many users in your organization might have more access privileges than required for their job?**



49%

Of users have at least some users with more access privileges than required for their job

KEY DRIVERS FOR IAM

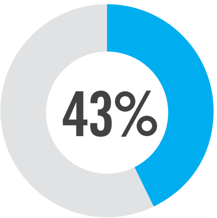
Organizations prioritize security (72%) over operational efficiency (52%) and breach prevention (47%) as the key drivers for developing an IAM program.

What were the key drivers for your organization's initial development of an identity and access management program?

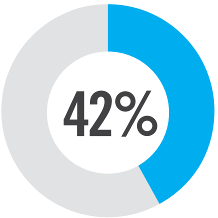
72%
Security

52%
Operational efficiency

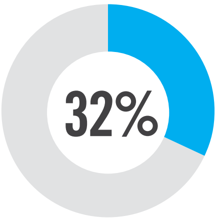
47%
Breach prevention



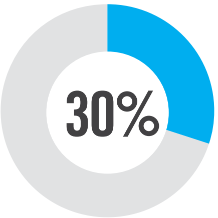
Response to regulation or industry standards (HIPAA, GDPR, etc.)



Compliance with internal mandates



Insider threats



Response to a security incident or audit finding

Poor user experience 17% | Not applicable/We do not have an Identity and Access Management program 4% | Other 6%

IAM INVESTMENT PRIORITY

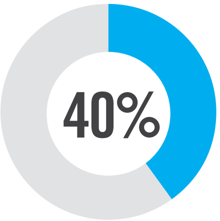
Over the next 12 months, organizations equally prioritize investment in multi-factor authentication (52%) and privileged access management (52%), followed by identity management and governance (49%).

Which of the following areas is a priority for IAM investment in your organization in the next 12 months?

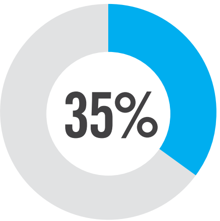
52%
Multi-factor authentication

52%
Privileged access management

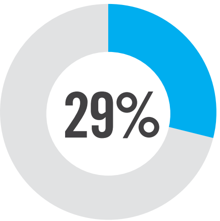
49%
Identity management and governance



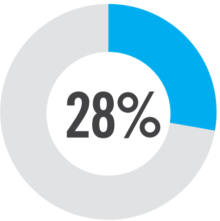
Single sign-on & federation



Network access control



Cloud Access Security Broker (CASB)



Virtual Private Networks (VPN)

Identity analytics 27% | Web application firewall 20% | Enterprise directory 18% | Software Defined Perimeter (SDP) 10% | Other 8%

CRITICAL IAM CAPABILITIES

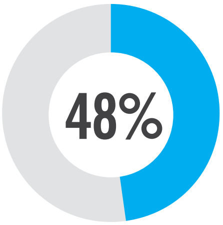
Organizations in our survey prioritize role-based access control as the most critical IAM capability (66%), followed by single sign-on (56%) and system and application access monitoring (51%).

What IAM capabilities are most important to you?

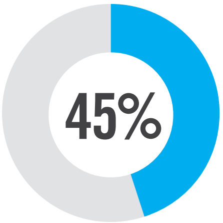
66%
Role-based access control

56%
Single sign-on

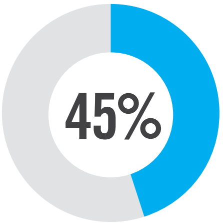
51%
System & application access monitoring



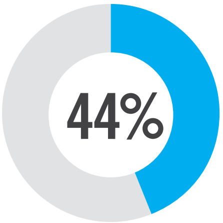
Compliance or auditor reporting



Automated user provisioning/ de-provisioning



Password self-service



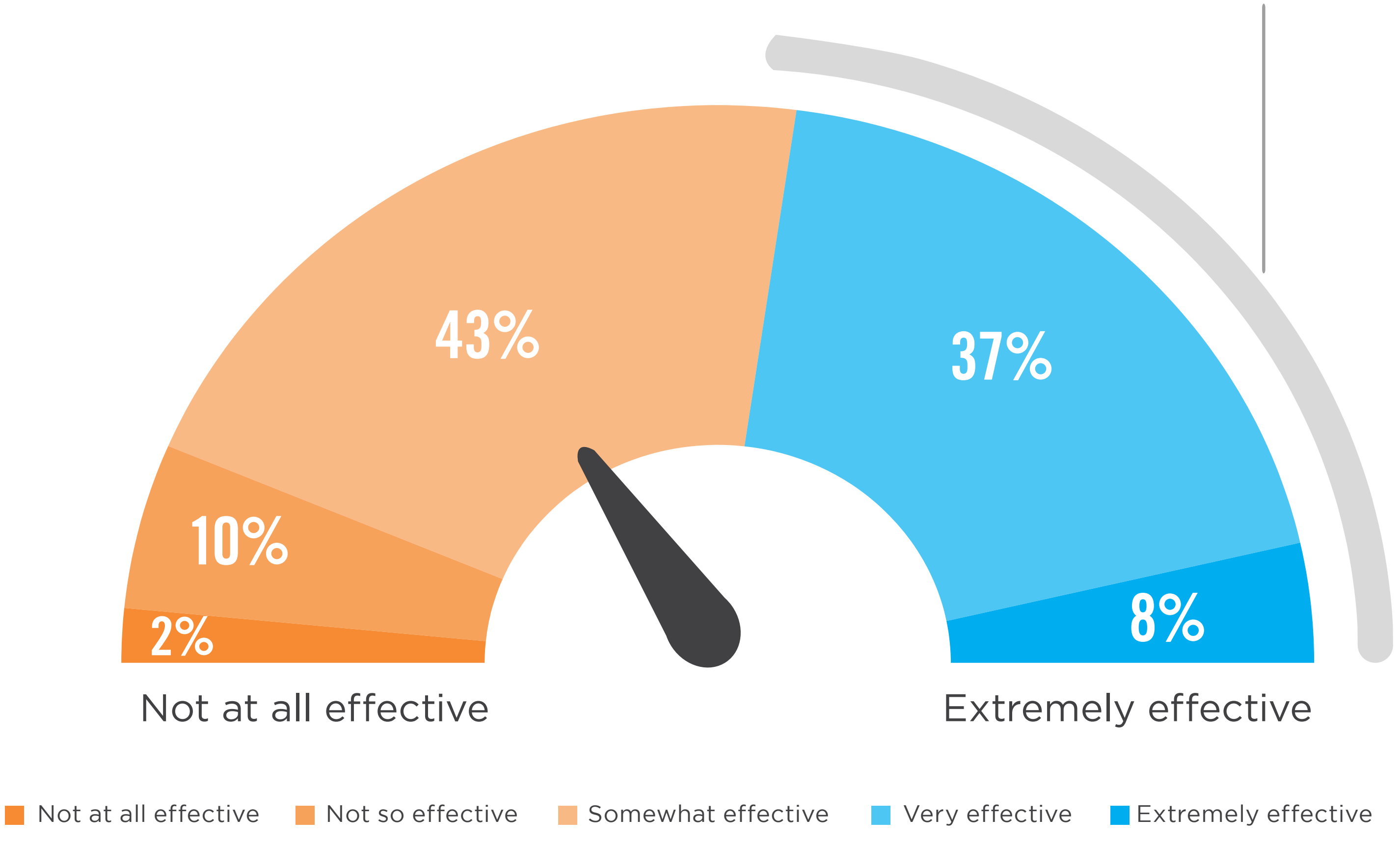
Support of compliance requirements

Administrative reporting 43% | User monitoring 40% | Workflow and case management 30% | Streamlined user certification/ auditing 29% | Considerations for contract or temporary staff 27% | Access request dashboards 26% | Advanced analytics (such as artificial intelligence (AI) or machine learning (ML)) 23% | Ability to personalize platform 21% | Other 2%

ACCESS MANAGEMENT EFFECTIVENESS

Only less than half of organizations (45%) rate themselves very effective or extremely effective in managing access to sensitive information, applications and systems.

How would you rate your organization's effectiveness in managing access to sensitive information, applications and systems?



Of organizations rate themselves very effective or extremely effective in managing access to sensitive information, applications and systems. **45%**

KEY CHALLENGES

Lack of automation (43%) and lack of skilled staff (41%) are the two biggest challenges regarding managing access in organizations, followed by not utilizing available technologies (33%).

What are the key challenges for managing access in your organization?

43%

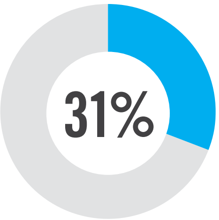
Lack of automation/ having to manually create and refine access rules and roles

41%

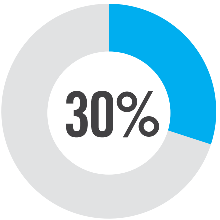
Lack of skilled staff

33%

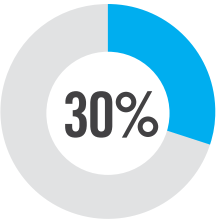
Not utilizing proper technologies



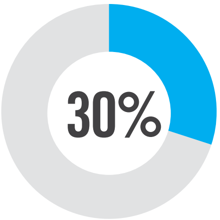
Password management and authentication



Detection and/or mitigation of insider threats (negligent, malicious, and compromised users)



Migration to the cloud



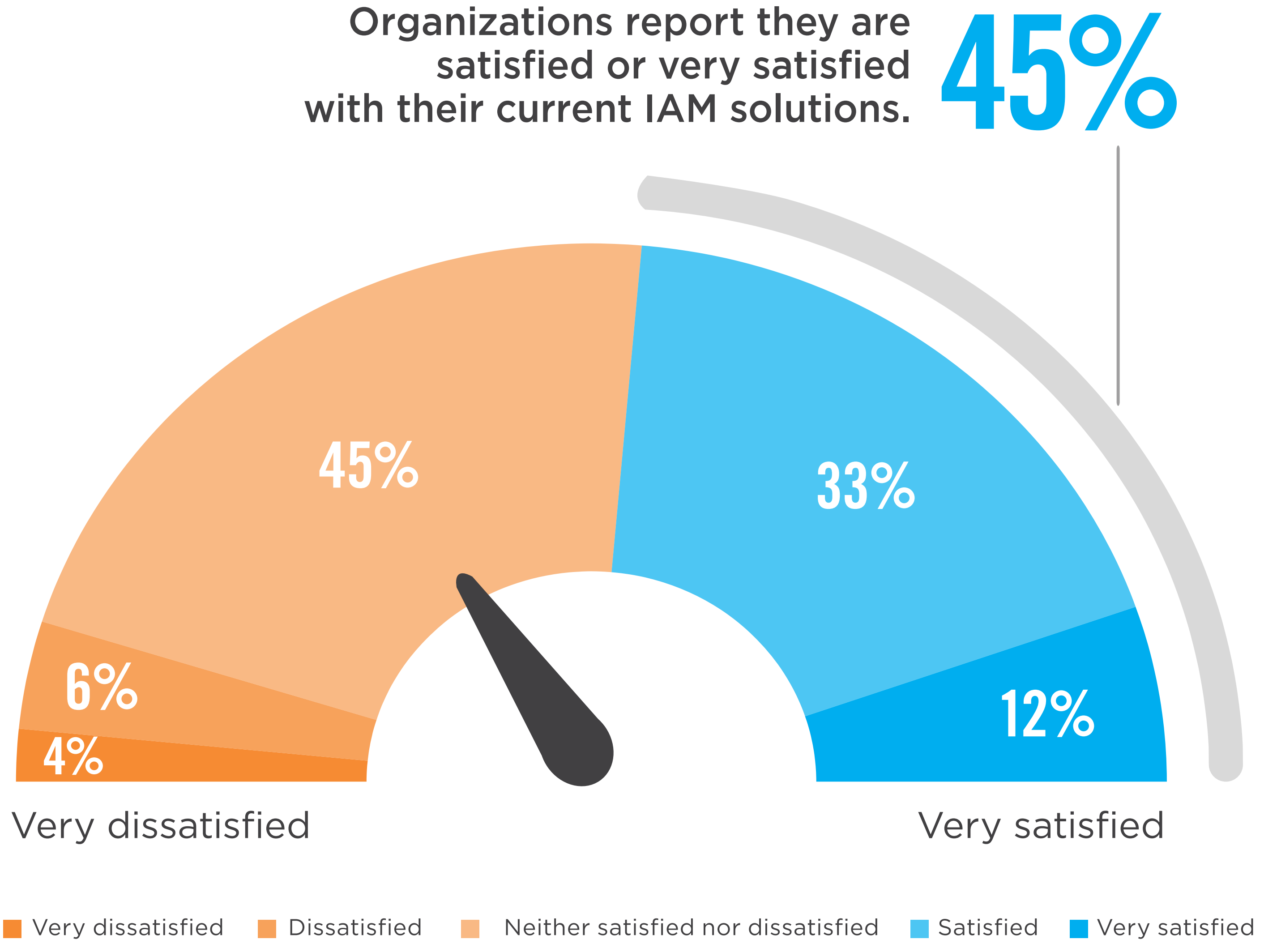
Increasing use of mobile devices

Lack of budget 30% | Difficulty implementing and deploying a solution 29% | User/staff turnover 27% | Increasing number of regulations and mandates 25% | Poor integration/interoperability between security solutions 25% | Lack of security awareness/ compliance among employees 23% | Lack of clearly defined access policies and procedures 20% | Evolving threat landscape Application sprawl 20% | Poor vendor support 18% | Changes to the organization (due to re-organization, acquisition, etc.) 18% Reviewing and approving user roles 16% | Lack of proper reporting tools 16% | Lack of management support 11% | Lack of effective IAM solutions available in the market 7% | Other 4%

IAM SATISFACTION

On balance, only 45% of organizations report they are satisfied or very satisfied with their current IAM solutions.

How satisfied are you with your current IAM solution(s)?



SWITCHING VENDORS

For companies considering switching to a new SIEM vendor, these factors play the biggest role: Solution complexity (41%), followed by license/subscription cost (43%) and lack of out-of-the-box integration with other security controls (33%).

What are the main reasons why you would consider switching to a new IAM vendor?

41%

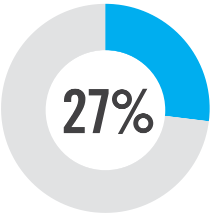
Solution complexity

43%

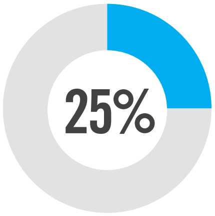
License/ subscription cost

33%

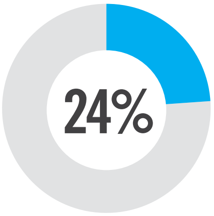
Lack of out-of-the-box integration with other security controls



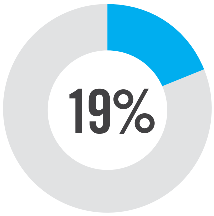
Lack of features/ functionality



Lack of ease of use



Support issues



Lack of ability to customize

Poor product performance 18% | Migrating to a Managed Service 14% | Not currently utilizing an IAM solution 12%
Other 10%

CRITERIA EVALUATING IAM SOLUTIONS

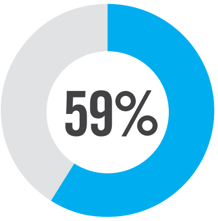
When selecting an IAM solution, organizations prioritize ease of integration (72%) before end user experience (62%), and product performance and effectiveness (61%).

What criteria do you consider most important when evaluating an IAM solution?

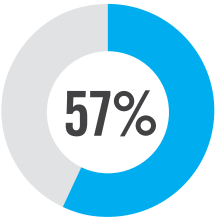
72%
Ease of integration

62%
End user experience/ ease of use

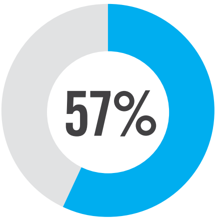
61%
Product performance and effectiveness



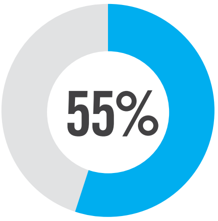
Ease of administration



Product features/ functionality



Cost

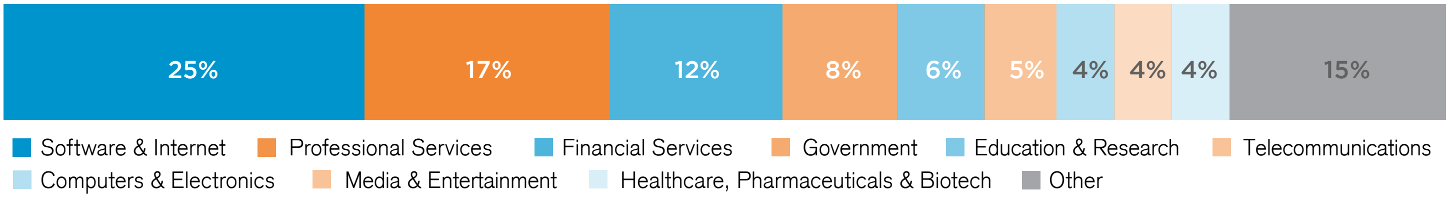


Vendor support

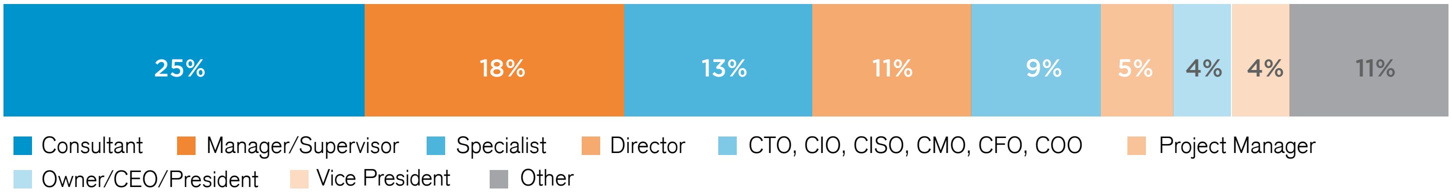
METHODOLOGY & DEMOGRAPHICS

The Identity and Access Management Report is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in January of 2020 to gain deep insight into the latest trends, key challenges and solutions for identity and access management. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

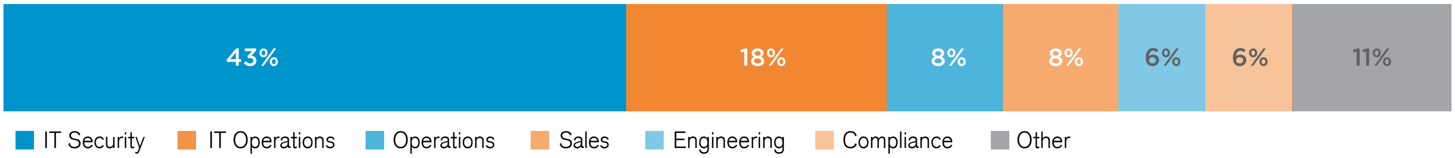
INDUSTRY



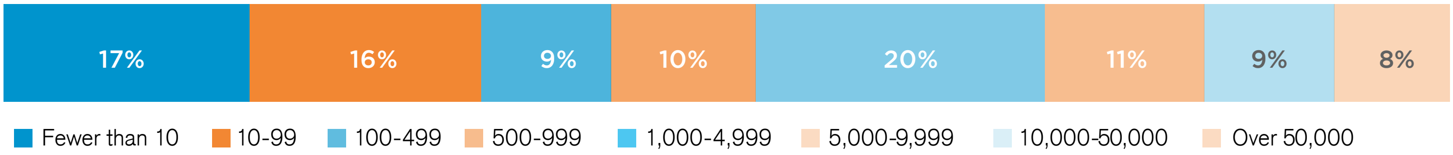
CAREER LEVEL



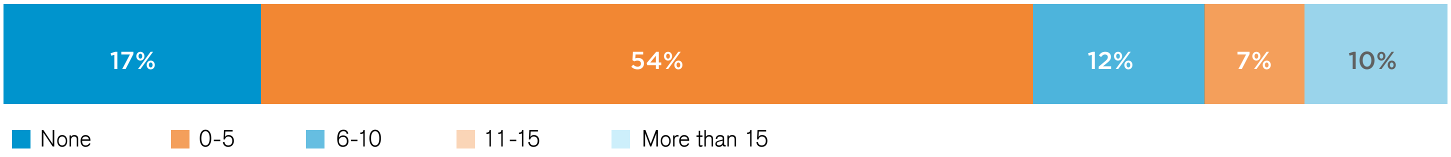
DEPARTMENT



COMPANY SIZE



STAFF DEDICATED TO IAM



simeio

Identity, intelligently managed.

Simeio provides the most complete Identity and Access Management (IAM) solution that engages securely with anyone, anywhere, anytime, with an unparalleled "service first" philosophy.

www.simeiosolutions.com