2020

Cybersecurity
INSIDERS

Identity and Access Management Report

CORE
SECURITY
A HelpSystems Company

INTRODUCTION

The 2020 Identity and Access Management Report reveals the increasing importance of managing access as part of an organization's overall risk management and security posture. At the same time, a majority of organizations are, at best, only somewhat confident in the effectiveness of their identity and access management program.

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.

Key findings include:

- Nine out of ten organizations confirm that identity and access management is very to extremely important as part of their cybersecurity and risk management posture (90%). This is a 4 percentage point increase compared to last year's survey and confirms the rising importance of IAM.
- Organizations prioritize role-based access control as the most critical IAM capability (62%), followed by single sign-on (53%) and compliance/auditor reporting (51%).
- 75% of organizations have at least a few users with more access privileges than required. That is up by 5 percentage points compared to last year's survey.
- For 75% of organizations, utilizing identity and access management solutions has resulted in a reduction of unauthorized access incidents. Only a small fraction of 9% report no improvement.

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 Core Security, a HelpSystems Company, for supporting this important research project.

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

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

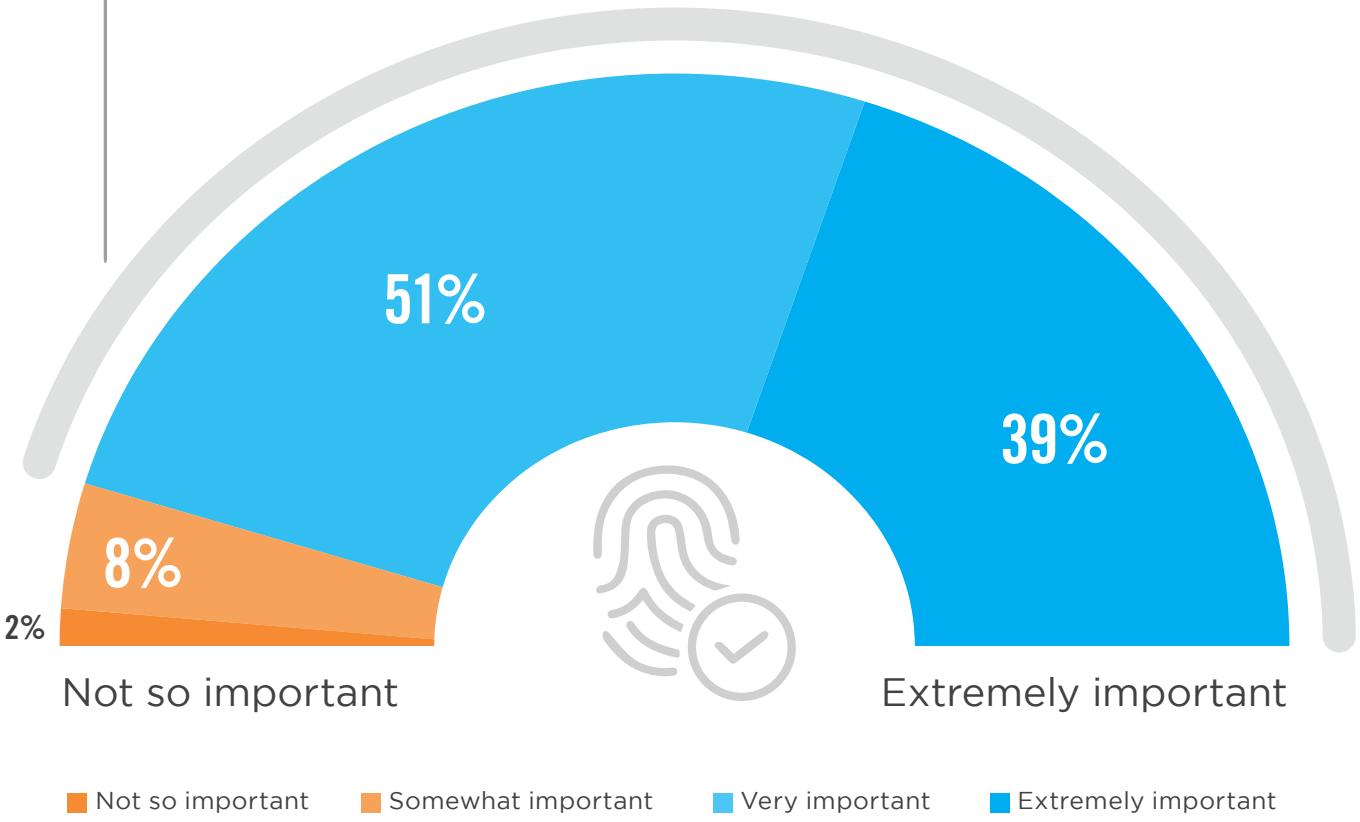
Cybersecurity
INSIDERS

IMPORTANCE OF IAM RISING

Nine out of ten organizations confirm that Identity and Access Management is very to extremely important as part of their cybersecurity and risk management posture. This is a four percentage point increase compared to last year's survey and confirms the rising importance of IAM.

How important is Identity and Access Management to your organization's overall risk management and security posture?

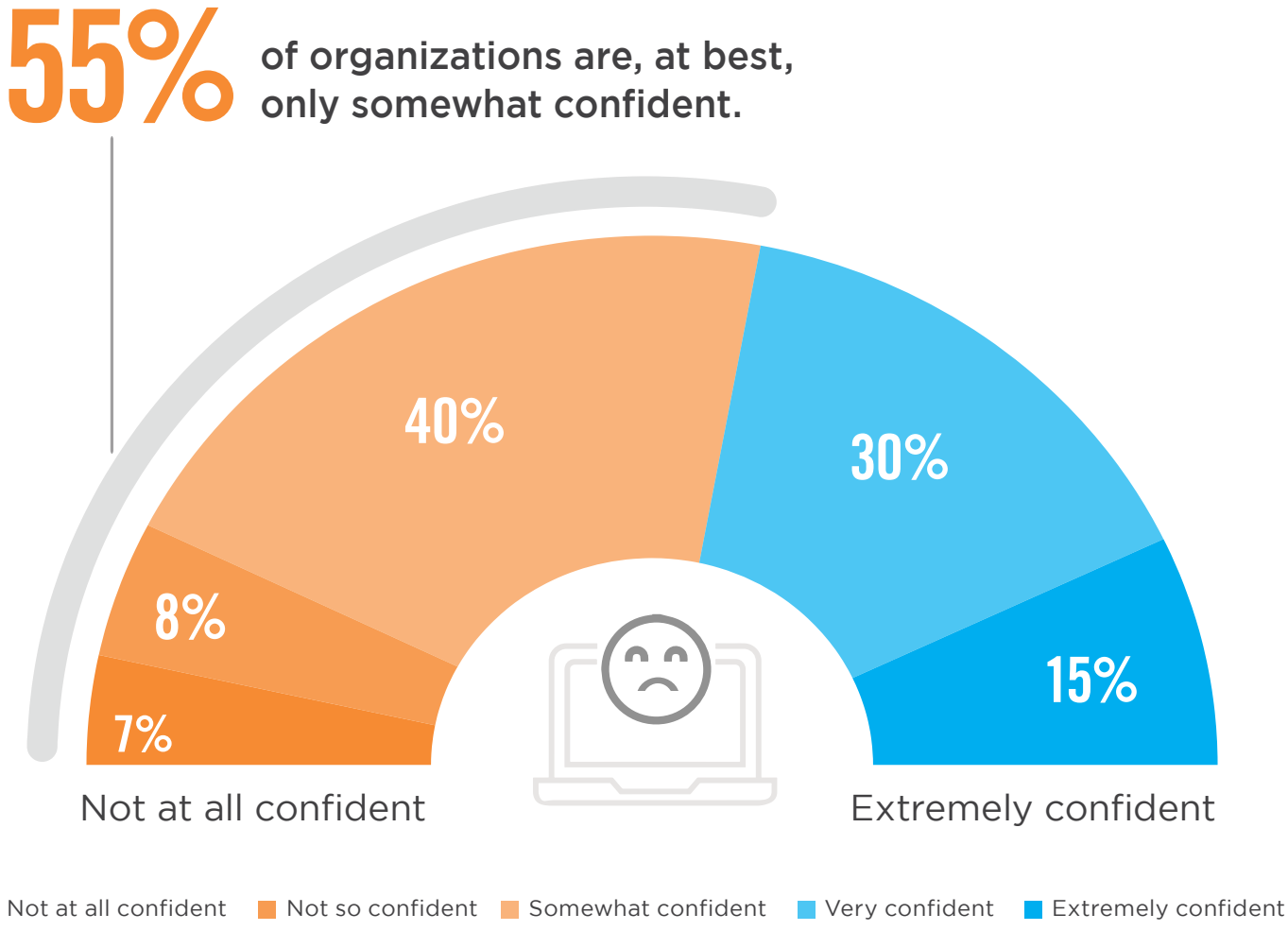
90% of organizations think IAM is very or extremely important (up four percentage points from last year).



IAM PROGRAM EFFECTIVENESS

Fifty-five percent are, at best, only 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.

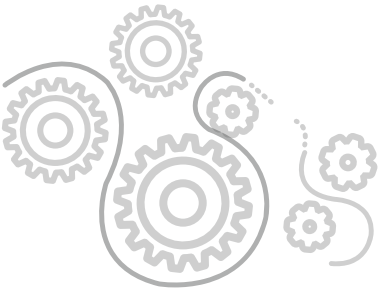
How confident are you in the effectiveness of your organization's Identity and Access Management program?



UNAUTHORIZED ACCESS

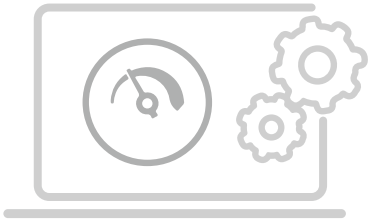
Organizations that experienced unauthorized access to sensitive systems and data reported they were most negatively impacted by disrupted business activities (23%). This is closely followed by system downtime (22%), reduced employee productivity (17%), and increased helpdesk load (tied at 17%).

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



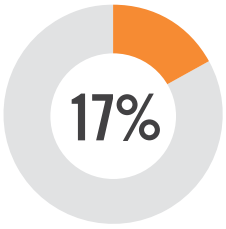
23%

Disrupted business activities

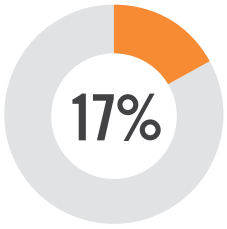


22%

System downtime

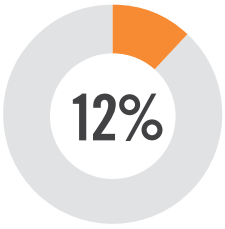


Reduced employee productivity



Increased helpdesk time

Deployment of IT resources to triage and remediate issue



Reduced revenue/lost business

Data loss 12% | Negative publicity/ reputational damage 10% | Loss/compromise of intellectual property 10% | None/no business impact due to unauthorized access 10% | Lawsuit/legal issues 7% | Customer loss 7% | Regulatory fines 2% | Other 2%

CRITICAL IAM CAPABILITIES

Organizations in our survey prioritize role-based access control as the most critical IAM capability (73%), up by five percentage points compared to last year's survey. This is followed by single sign-on capabilities (60%), and system and application access monitoring (53%).

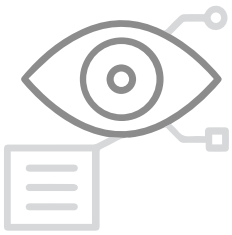
What IAM capabilities are deployed in your organization?

73%

Role-based access control

60%

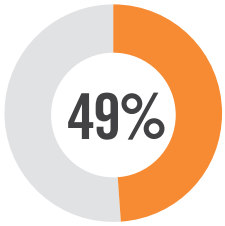
Single sign-on



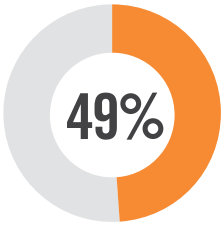
53%

System & application access monitoring

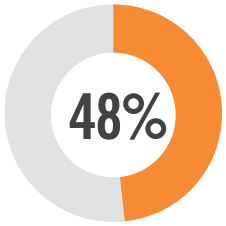
Password self-service



Automated user provisioning/ deprovisioning



Compliance or auditor reporting



Administrative reporting

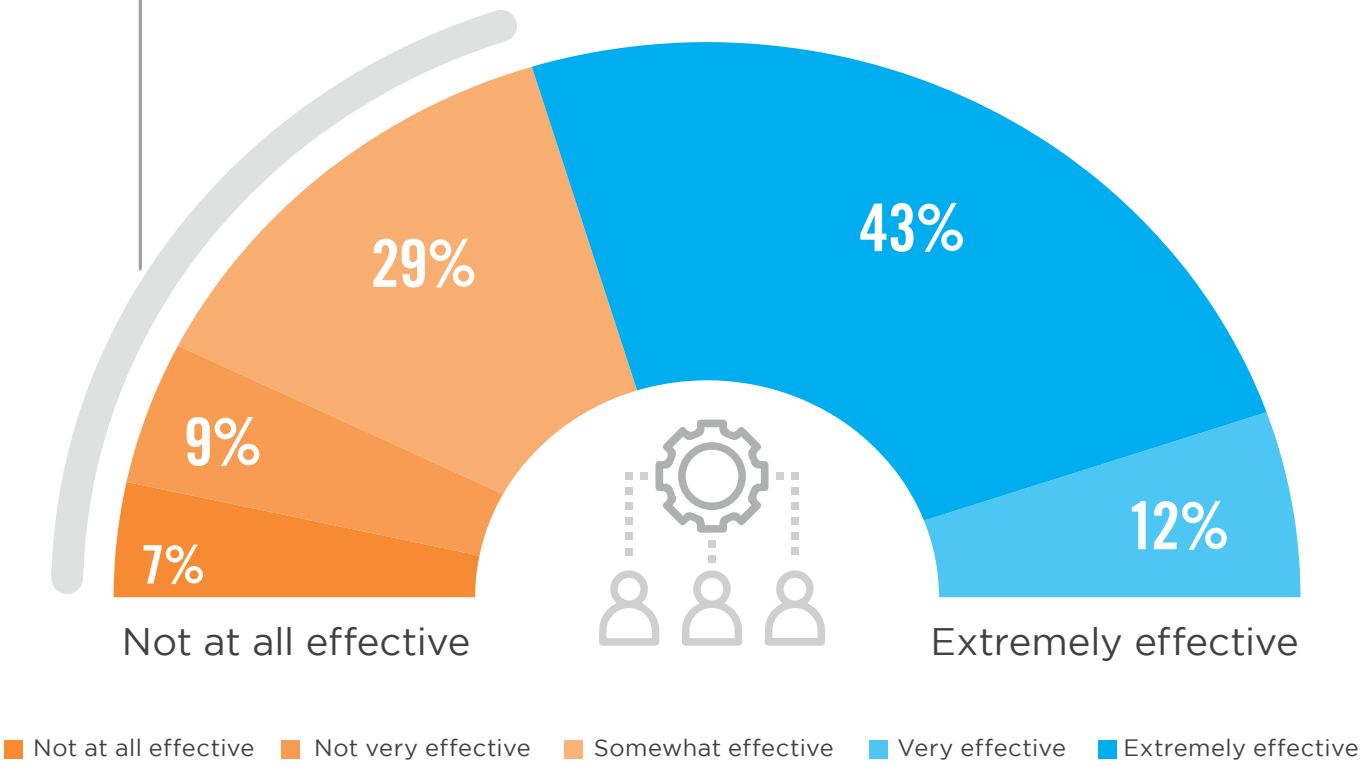
Considerations for contract or temporary staff 44% | User monitoring 44% | Integration with service desk/ITSM solutions 43% | Streamlined user certification/auditing 33% | Advanced analytics (e.g., as Artificial Intelligence (AI) or Machine Learning (ML)) 17% | Other 6%

DESIGNING ROLES

We asked organizations how effective they are in their ability to design roles as part of their identity and Access Management program. Role design enables organizations to focus on role definitions and assignments rather than individual accounts and entitlements. Only 45% are, at best, somewhat effective in their ability to design roles.

How effective is your organization's ability to design roles?

45% of organizations are, at best, only somewhat effective in their ability to design roles.

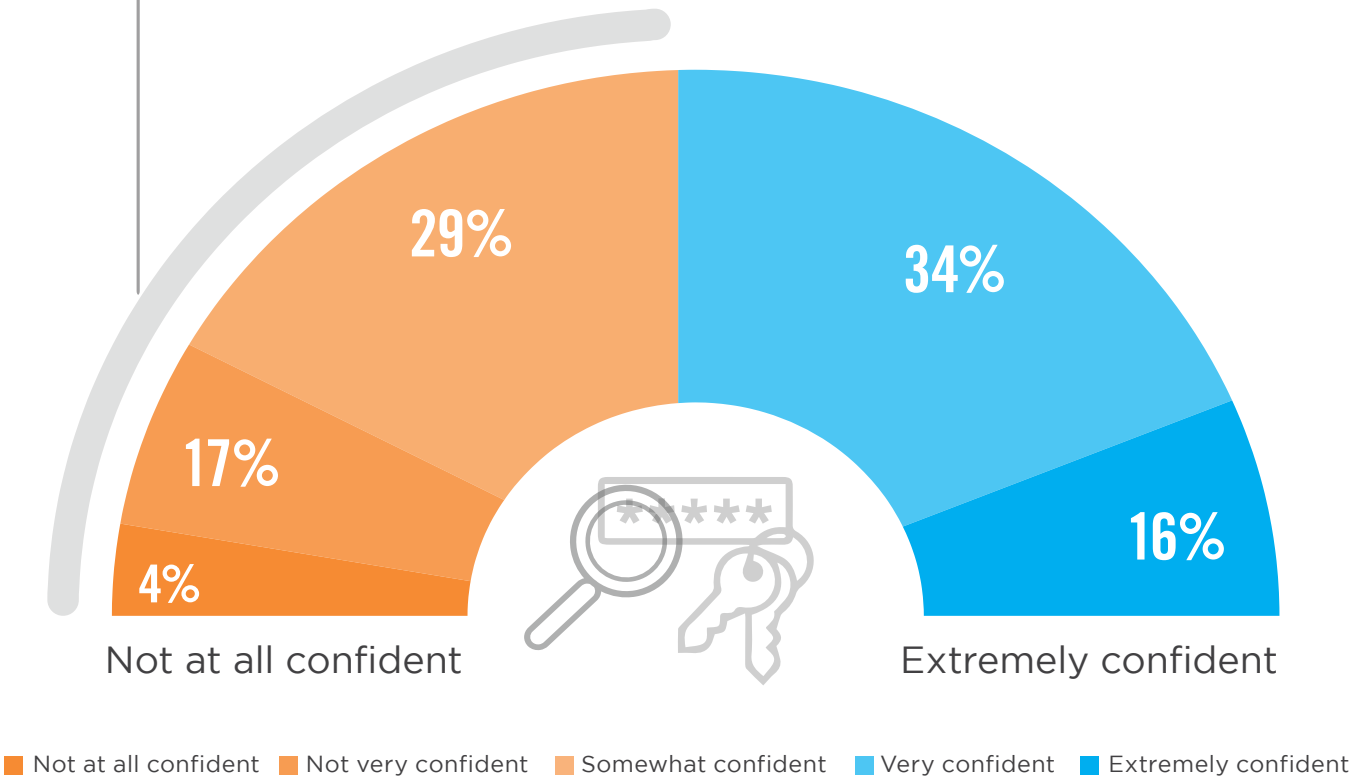


EXCESSIVE ACCESS PRIVILEGES VERIFICATION ABILITY

Fifty percent of organizations are, at best, only somewhat confident in their ability to verify that users don't have excessive access privileges.

How confident are you in your organization's ability to verify that users don't have excessive access privileges?

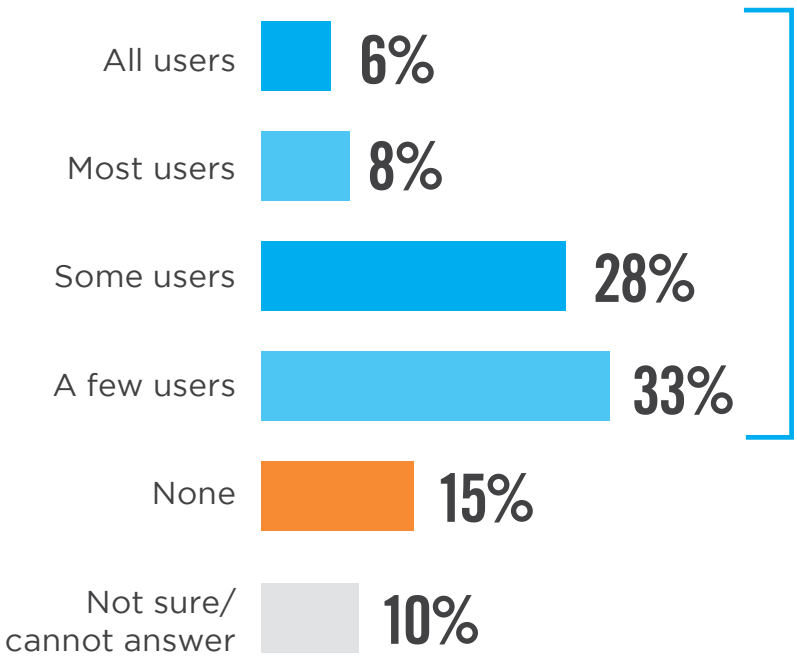
50% of organizations are, at best, only somewhat confident in their ability to verify users access privileges.



EXCESSIVE ACCESS PRIVILEGES

Seventy-five percent of organizations have at least a few users with more access privileges than required. This is an increase of five percentage points compared to last year.

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



75%

of organizations have at least a few users with more access privileges than required.

KEY DRIVERS FOR IAM

When asked about the key drivers for developing their IAM programs, organization's rank security as the biggest driver (76%), followed by operational efficiency (62%) and breach prevention (46%).

What were the key drivers for your organization's initial development of an Identity and Access Management program?

76%

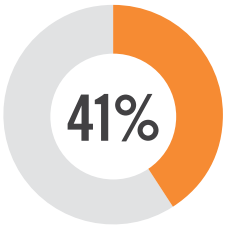
Security

62%

Operational efficiency

46%

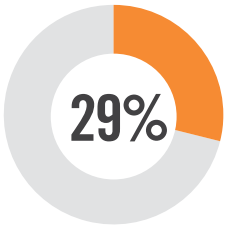
Breach prevention



Compliance with internal mandates

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

Insider threats



Response to a security incident or audit finding

Poor user experience 19% | Not applicable/We do not have an Identity and Access Management program 5% | Other 2%

IAM INVESTMENT PRIORITY

Over the next 12 months, organizations prioritize investment in privileged access management (57%), up five percentage points since last year to become the number one priority. This is followed by multi-factor authentication (49%), and identity management and governance (42%).

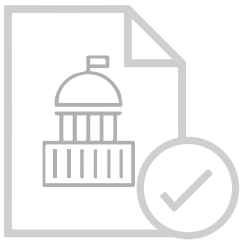
Which of the following areas is a priority for IAM investment in your organization in the next 12 months?

57%

Privileged access management

49%

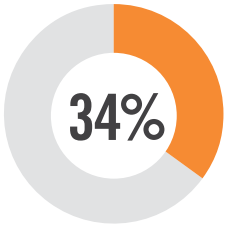
Multi-factor authentication



42%

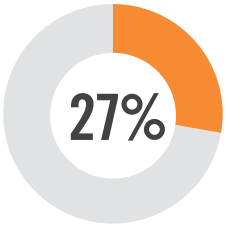
Identity management and governance

Single sign-on & federation



Network access control

Virtual Private Networks (VPN)



Cloud Access Security Broker (CASB)

Identity analytics 22% | Web application firewall 20% | Enterprise directory 18% | Software Defined Perimeter (SDP) 14% | Other 5%

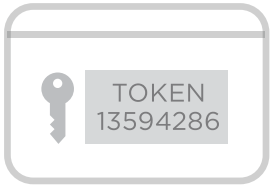
AUTHENTICATION METHODS

Not surprisingly, by far the most popular authentication method is username and password (88%), followed by software tokens (48%) and out-of-band authentication (41%) – a 21 percentage point jump compared to last year.

What authentication methods are used in your organization?

88%

Username and password



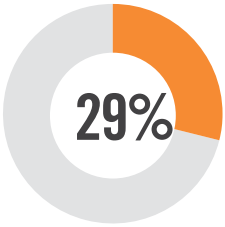
48%

Software tokens (e.g., One Time Password (OTP))

41%

Out-of-band authentication (e.g., Push, SMS, voice, etc.)

Hardware tokens (e.g., key fobs, USB tokens, smart cards)



Biometric authentication

Tokenless authentication (e.g., context-based authentication and pattern-based authentication)

Social identity credentials (e.g., using LinkedIn, Facebook, Twitter, etc.) 8% | Other 4%

CRITICAL CAPABILITIES

Organizations in our survey prioritize role-based access control as the most critical IAM capability (62%), followed by single sign-on (53%) and compliance/auditor reporting (51%).

What IAM capabilities are most important to you?

62%

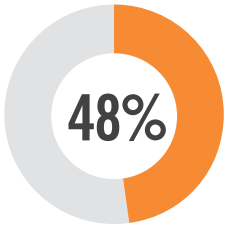
Role-based access control

53%

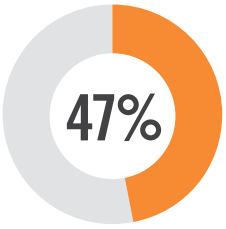
Single sign-on

51%

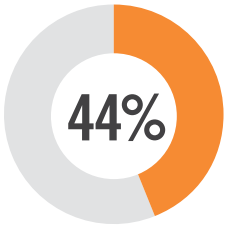
Compliance or auditor reporting



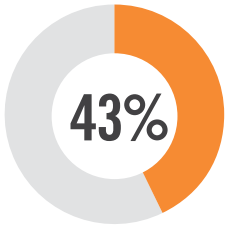
Automated user provisioning/ deprovisioning



System & application access monitoring



Support of compliance requirements



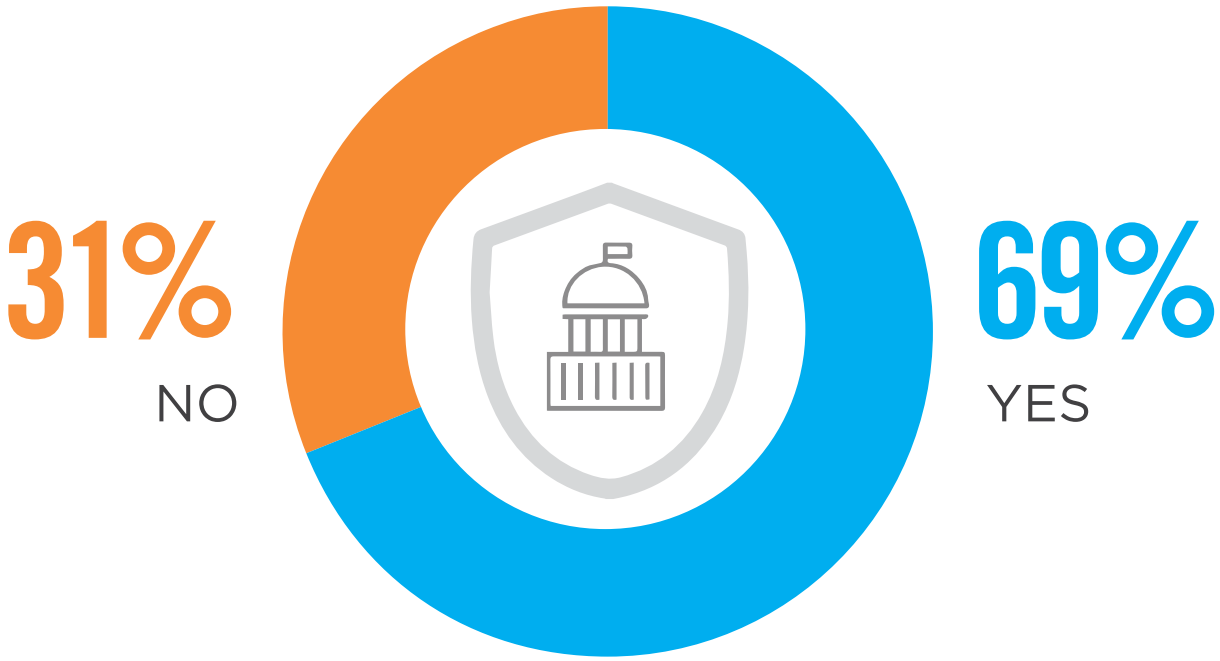
User monitoring

Password self-service 41% | Administrative reporting 39% | Workflow and case management 32% | Streamlined user certification/ auditing 30% | Considerations for contract or temporary staff 30% | Access request dashboards 27% | Ability to personalize platform 24% | Other 1%

IDENTITY GOVERNANCE

A majority of organizations (69%) are using solutions to address identity governance as part of their IAM strategy, a two percent increase from last year. Identity governance administration policies help define and standardize levels of access rights based on roles or job duties. Identity governance solutions can help streamline the provisioning process, adhere to relevant regulations, and provide actionable analytics.

Are you using solutions or tools to address identity governance as part of your IAM strategy?



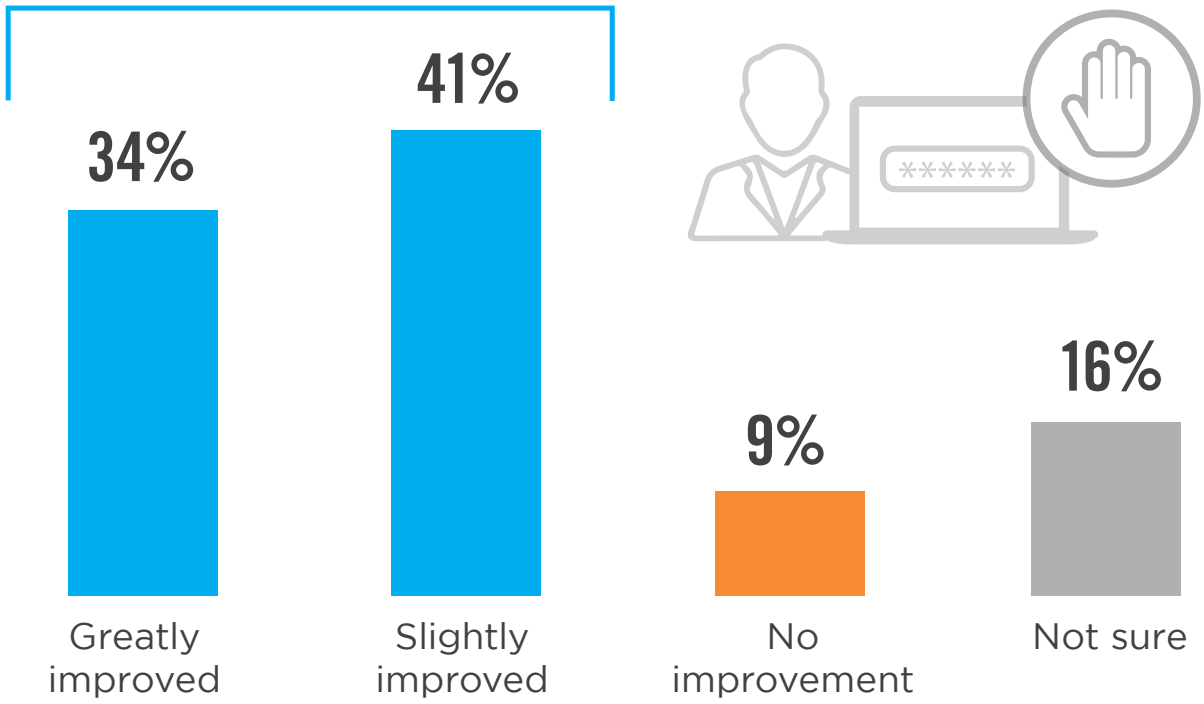
REDUCTION OF UNAUTHORIZED ACCESS

For 75% of organizations, utilizing Identity and Access Management solutions has resulted in a reduction of unauthorized access incidents. Only a small fraction of 9% report no improvement.

How has using IAM solutions changed the occurrence of unauthorized access in your organization?

75%

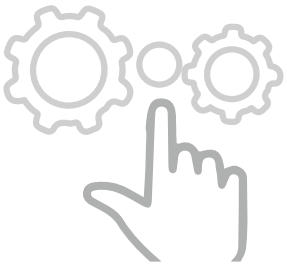
of organizations using IAM saw a reduction of unauthorized access incidents.



KEY CHALLENGES

Lack of automation and having to manually create and refine access rules and roles (38%) leads the list of key challenges for managing access. This is followed by lack of skilled staff (36%) and increasing use of mobile devices (32%).

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

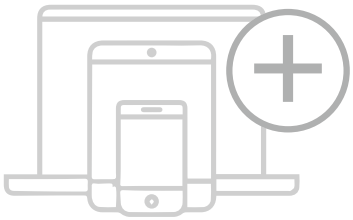


38%

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

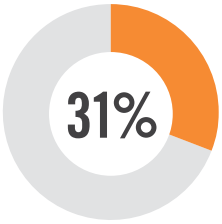
36%

Lack of skilled staff



32%

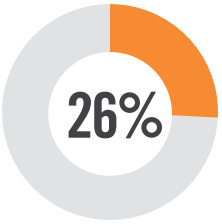
Increasing use of mobile devices



Difficulty implementing and deploying a solution

Not utilizing proper technologies

Lack of budget



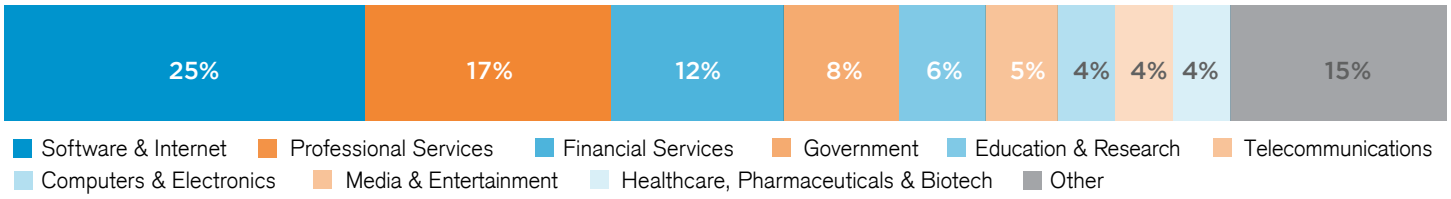
Detection and/or mitigation of insider threats (negligent, malicious, and compromised users)

Migration to the cloud 26% | Poor integration/interoperability between security solutions 25% | Increasing number of regulations and mandates 23% | Changes to the organization (due to re-organization, acquisition, etc.) 23% | Evolving threat landscape 22% User/staff turnover 21% | Poor vendor support 18% | Password management 17% | Application sprawl 16% | Lack of management support 14% | Lack of clearly defined access policies and procedures 13% | Reviewing and approving user roles 13% Lack of proper reporting tools 12% | Lack of effective IAM solutions available in the market 9% | Other 1%

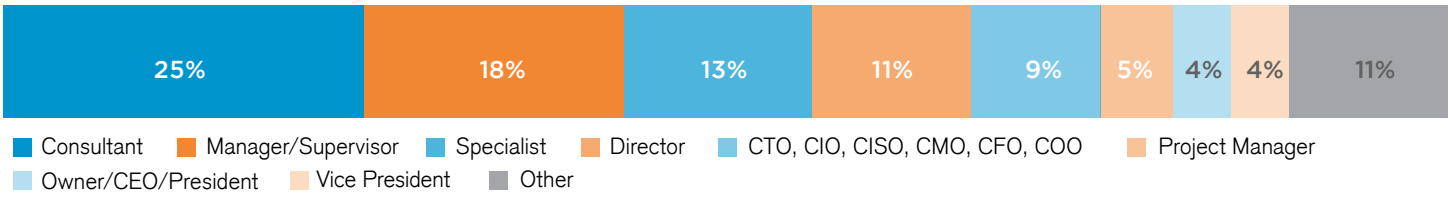
METHODOLOGY & DEMOGRAPHICS

The Identity and Access Management Report is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in May 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.

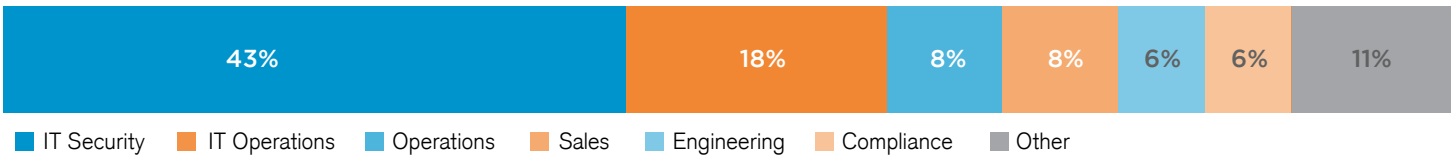
INDUSTRY



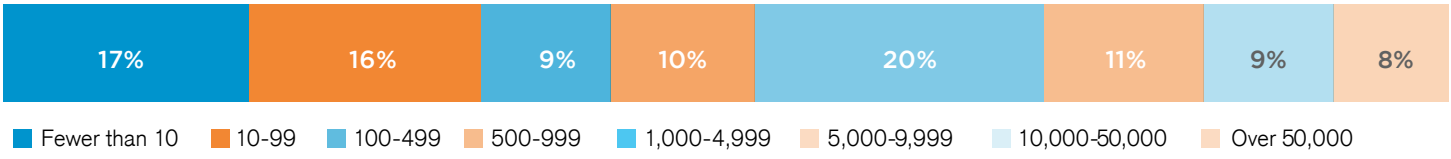
CAREER LEVEL



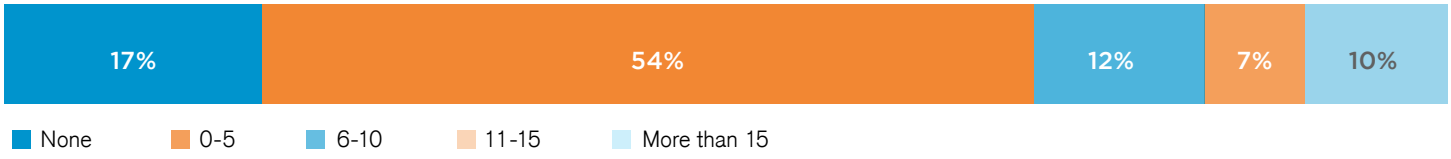
DEPARTMENT



COMPANY SIZE



STAFF DEDICATED TO IAM



Core Security provides leading-edge cyber threat prevention and identity governance solutions to help you prevent, detect, test, and monitor risk in your business.

www.coresecurity.com