2019
MID-YEAR

Cybersecurity
INSIDERS

Identity and Access Management Report

CORE SECURITY
A HelpSystems Company

INTRODUCTION

The 2019 Identity and Access Management Report reveals the increasing importance of managing access for a significant majority of organizations (86%) as part of their overall risk management and security posture. At the same time, a majority of organizations (53%) are, at best, only somewhat confident in the effectiveness of their identity and access management program.

In the context of this survey report, 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 or scope of responsibilities within an organization.

The 2019 Identity and Access Management Report highlights what is and what is not working for security operations teams in securing access to their sensitive data, systems, and applications:

- 70% of organizations have at least a few users with more access privileges than required for their job.
- 66% view role-based access control as most important to them.
- 75% of organizations using IAM saw a reduction of unauthorized access incidents.
- 49% deem identity management and governance, multi-factor authentication, and privileged access management as a priority for IAM investment in the next 12 months.

This 2019 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'll 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

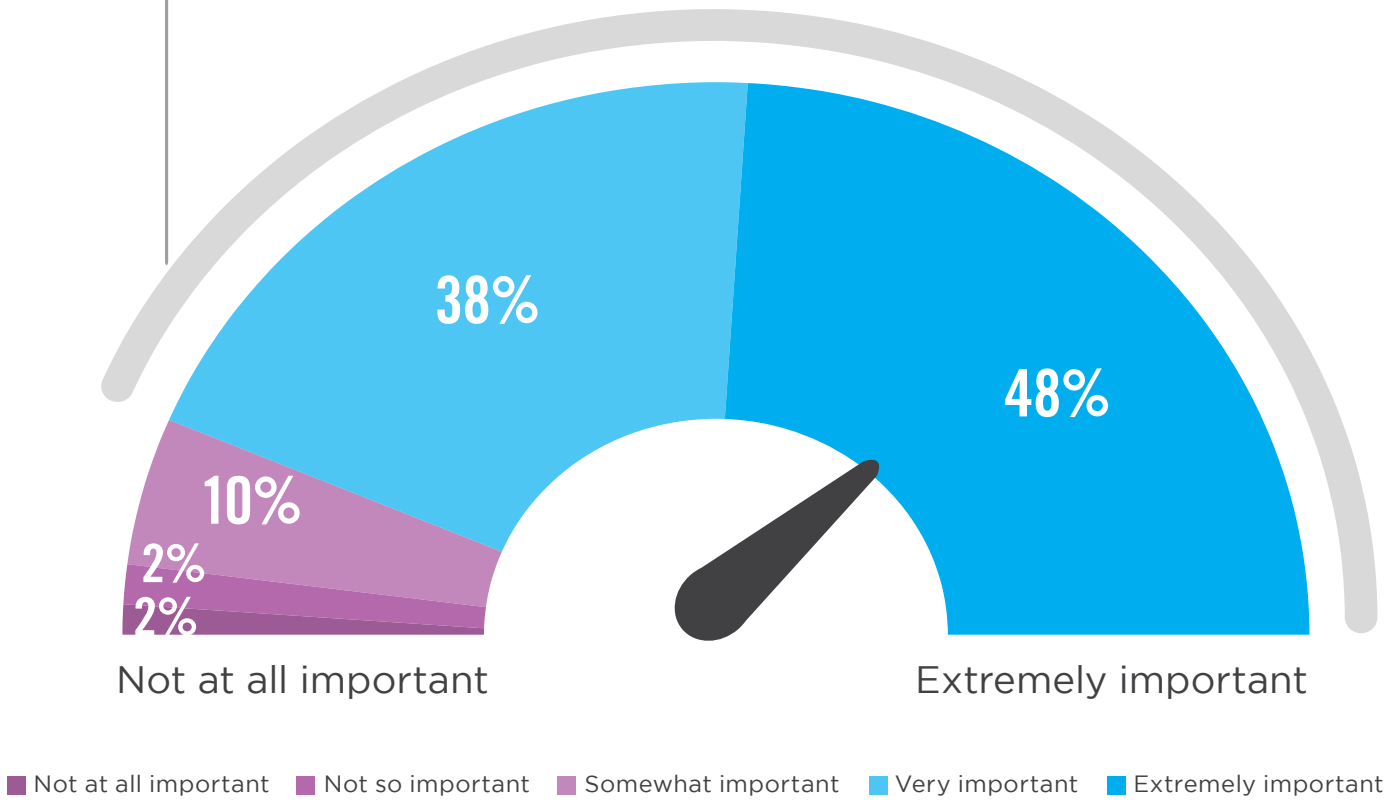
Cybersecurity
INSIDERS

IMPORTANCE OF IAM

Identity and access management is very important to extremely important to a significant majority of organizations (86%) as part of their overall risk management and security posture.

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

86% of organizations think IAM is very important to extremely important.

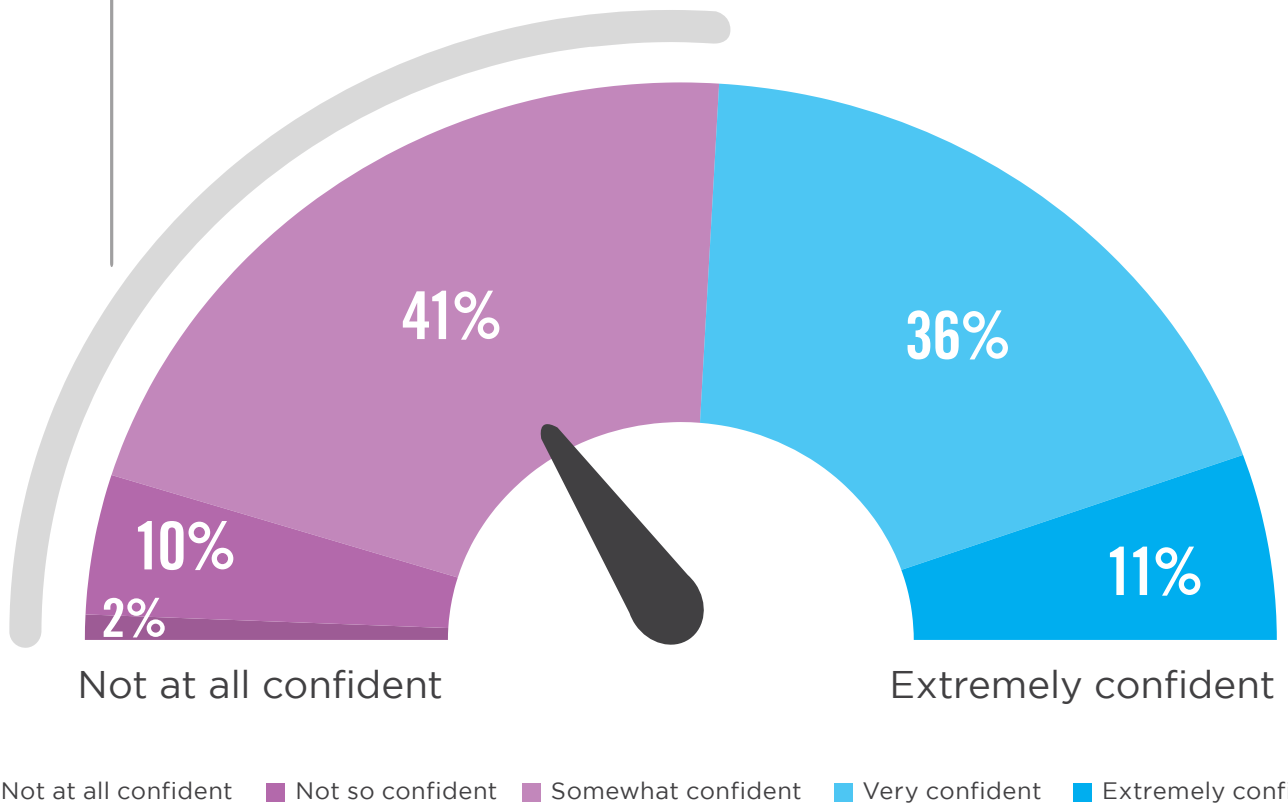


IAM PROGRAM EFFECTIVENESS

A majority of organizations (53%) are, at best, only somewhat confident in the effectiveness of their identity and access management program. Forty-seven percent are very confident to extremely confident.

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

53% of organizations are, at best, only somewhat confident in the effectiveness of their identity and access management program.



IAM CAPABILITIES

The most frequently deployed IAM capabilities include role-based access control (68%), followed by single sign-on (57%) and self-service password management (50%).

What IAM capabilities are deployed in your organization?

68%

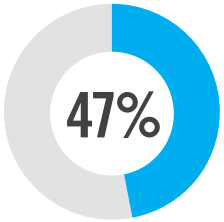
Role-based access control

57%

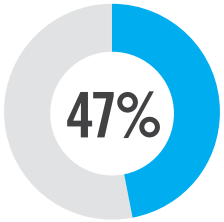
Single sign-on

50%

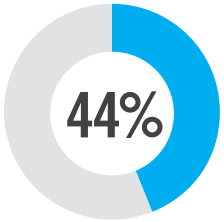
Password self-service



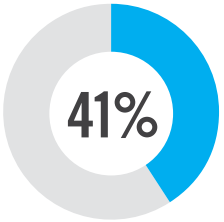
Compliance or auditor reporting



User monitoring



Administrative reporting



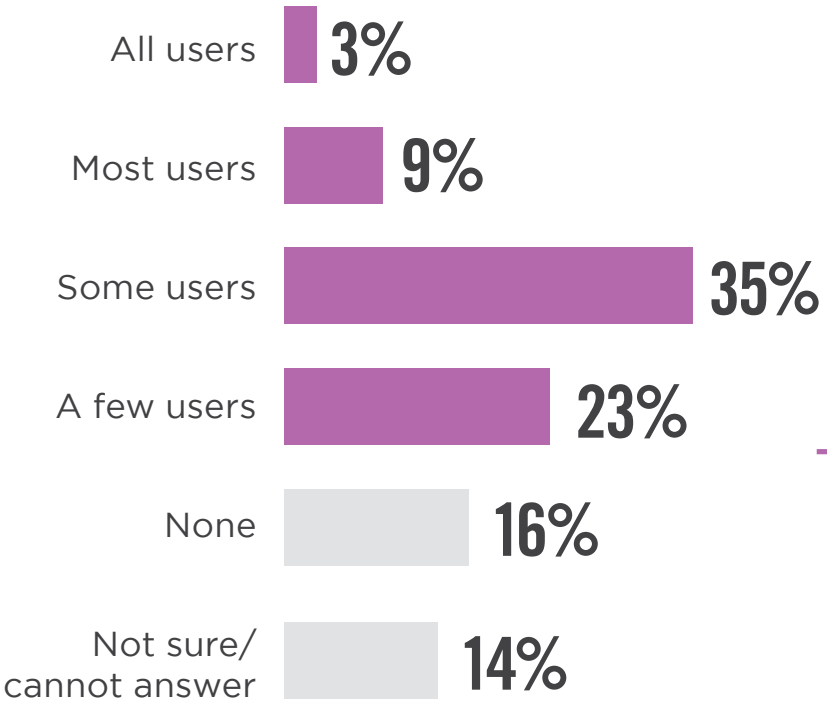
System & application access monitoring

Automated user provisioning/de-provisioning 38% | Integration with service desk/ITSM solutions 36% | Considerations for contract or temporary staff 31% | Streamlined user certification/auditing 26% | Advanced analytics (such as artificial intelligence (AI) or machine learning (ML)) 12% | Other 7%

EXCESSIVE ACCESS PRIVILEGES

Bulk approvals of access requests, departmental/role changes, and not reviewing user access periodically often leads to excessive access privileges. A large majority of organizations (70%) report at least a few users with more access privileges than required for their job.

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



70%

of users have at least a few users with more access privileges than required for their job.

KEY DRIVERS FOR IAM

Organizations prioritize security (68%) over operational efficiency (49%) and breach prevention (45%) 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?

68%

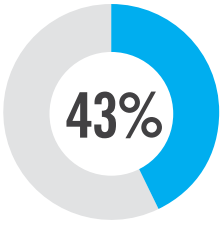
Security

49%

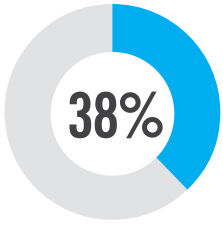
Operational efficiency

45%

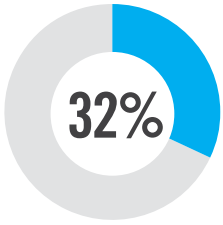
Breach prevention



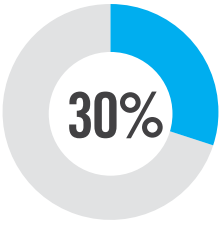
Compliance with internal mandates



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



Response to a security incident or audit finding



Insider threats

Poor user experience 17% | Not applicable/We do not have an Identity and Access Management program 5% | Other 8%

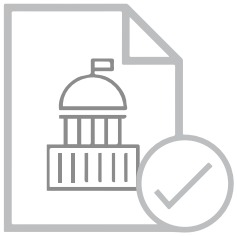
IAM INVESTMENT PRIORITY

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

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

49%

Multi-factor authentication

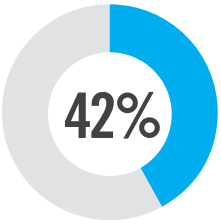


49%

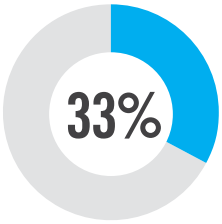
Identity management and governance

49%

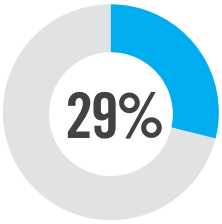
Privileged access management



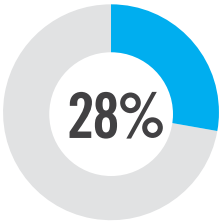
Single sign-on & federation



Network access control



Virtual Private Networks (VPN)



Cloud Access Security Broker (CASB)

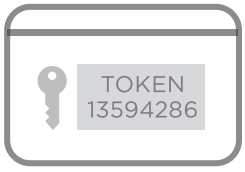
Identity analytics 27% | Web application firewall 19% | Enterprise directory 16% | Software defined perimeter (SDP) 9% | Other 9%

AUTHENTICATION METHODS

Not surprisingly, by far the most popular authentication method is username and password (86%), followed by software tokens (43%) and hardware tokens (38%).

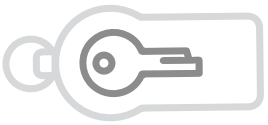
What authentication methods are used in your organization?

86% Username and password



43%

Software tokens
(e.g. one time password (OTP))

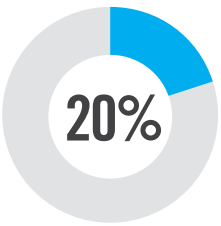


38%

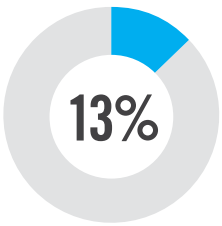
Hardware tokens
(e.g. key fobs, USB tokens, smart cards)

25%

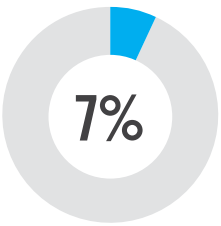
Biometric authentication



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



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



Social identity credentials (e.g. using LinkedIn, Facebook, Twitter, etc.)

Other 3%

CRITICAL CAPABILITIES

Organizations in our survey prioritize role-based access control as the most critical IAM capability (66%), followed by single sign-on (59%) and system and application access monitoring (50%).

What IAM capabilities are most important to you?

66%

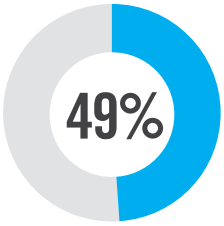
Role-based access control

59%

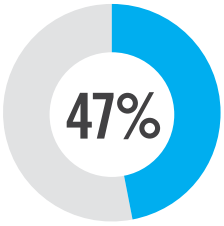
Single sign-on

50%

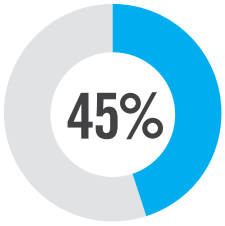
System & application access monitoring



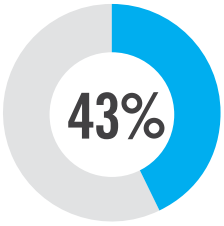
Compliance or auditor reporting



Automated user provisioning/ de-provisioning



Password self-service



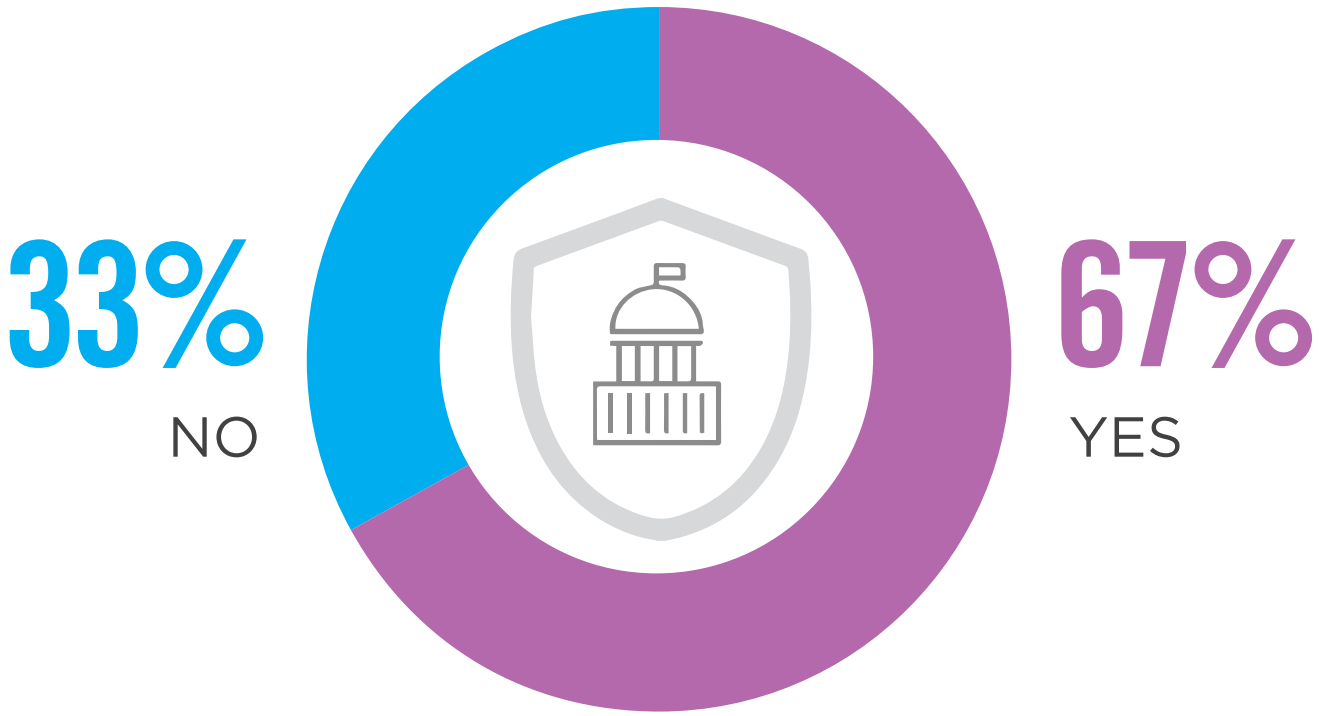
Administrative reporting

Support of compliance requirements 42% | User monitoring 36% | Streamlined user certification/auditing 33% | Workflow and case management 30% | Access request dashboards 23% | Considerations for contract or temporary staff 23% | Advanced analytics (such as artificial intelligence (AI) or machine learning (ML)) 22% | Ability to personalize platform 20% | Other 3%

IDENTITY GOVERNANCE

A majority of organizations surveyed (67%) are using identity governance solutions as part of their IAM strategy. 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?

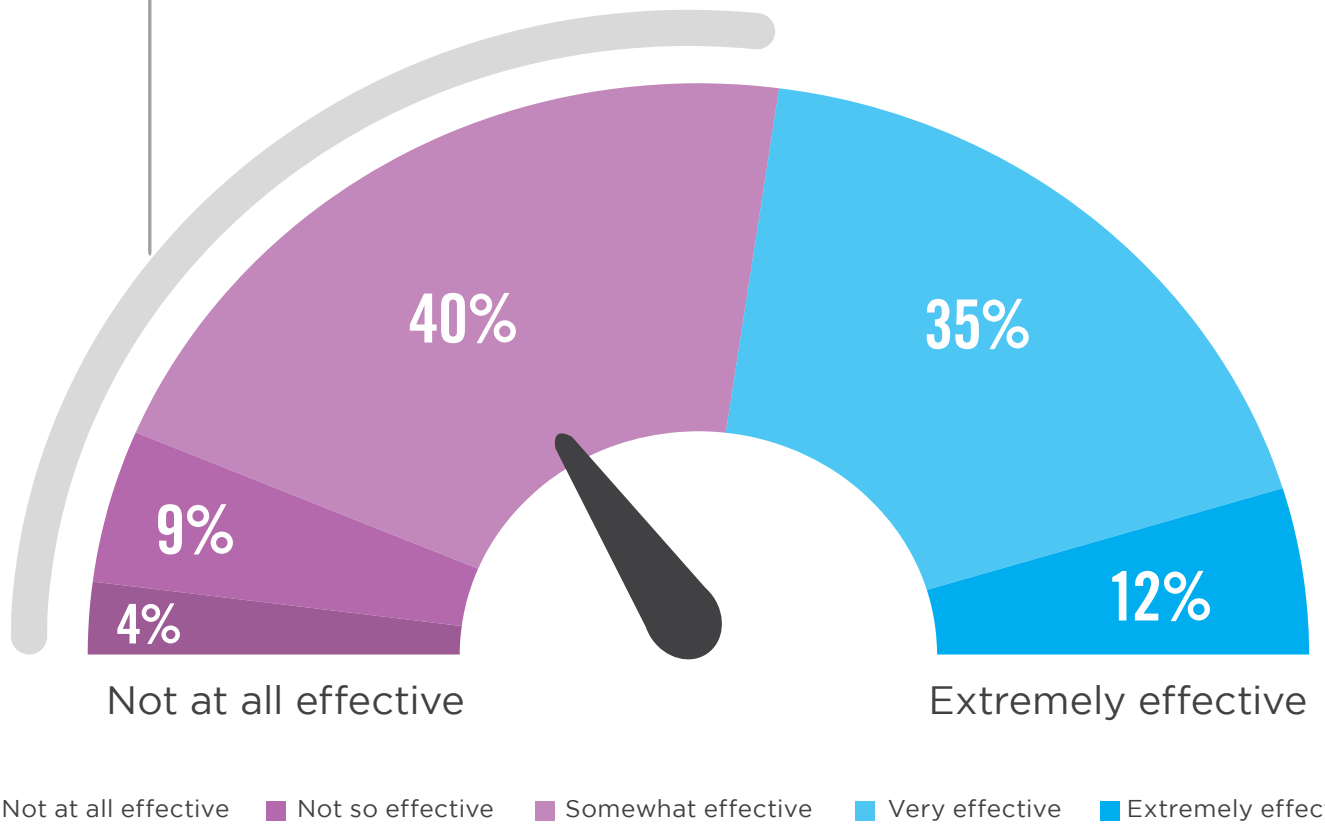


ACCESS MANAGEMENT EFFECTIVENESS

A majority (53%) of organizations rate themselves, at best, somewhat 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?

53% of organizations rate themselves, at best, somewhat effective in managing access to sensitive information, applications and systems.



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 6% 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

Those not using Identity Governance and Administration (IGA) solutions or tools report a lack of skilled staff, automation, and proper reporting tools in addition to poor integration/interoperability between security solutions as key challenges in their organization more frequently than those using IGA solutions.

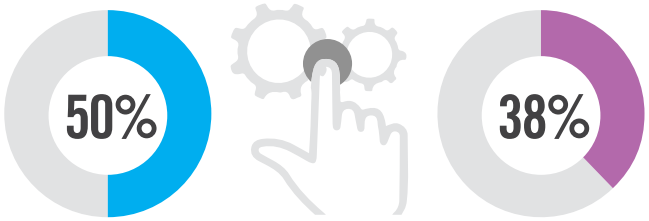
What are the key challenges for managing access in your organization?

Those who are not using IGA solutions or tools

Those using IGA solutions or tools

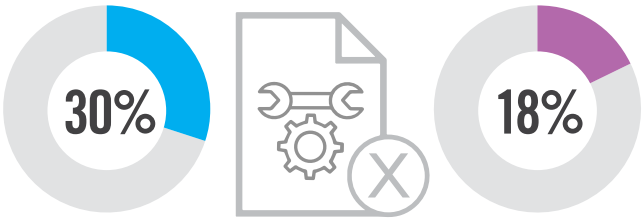
Lack of skilled staff

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



Poor integration/interoperability between security solutions

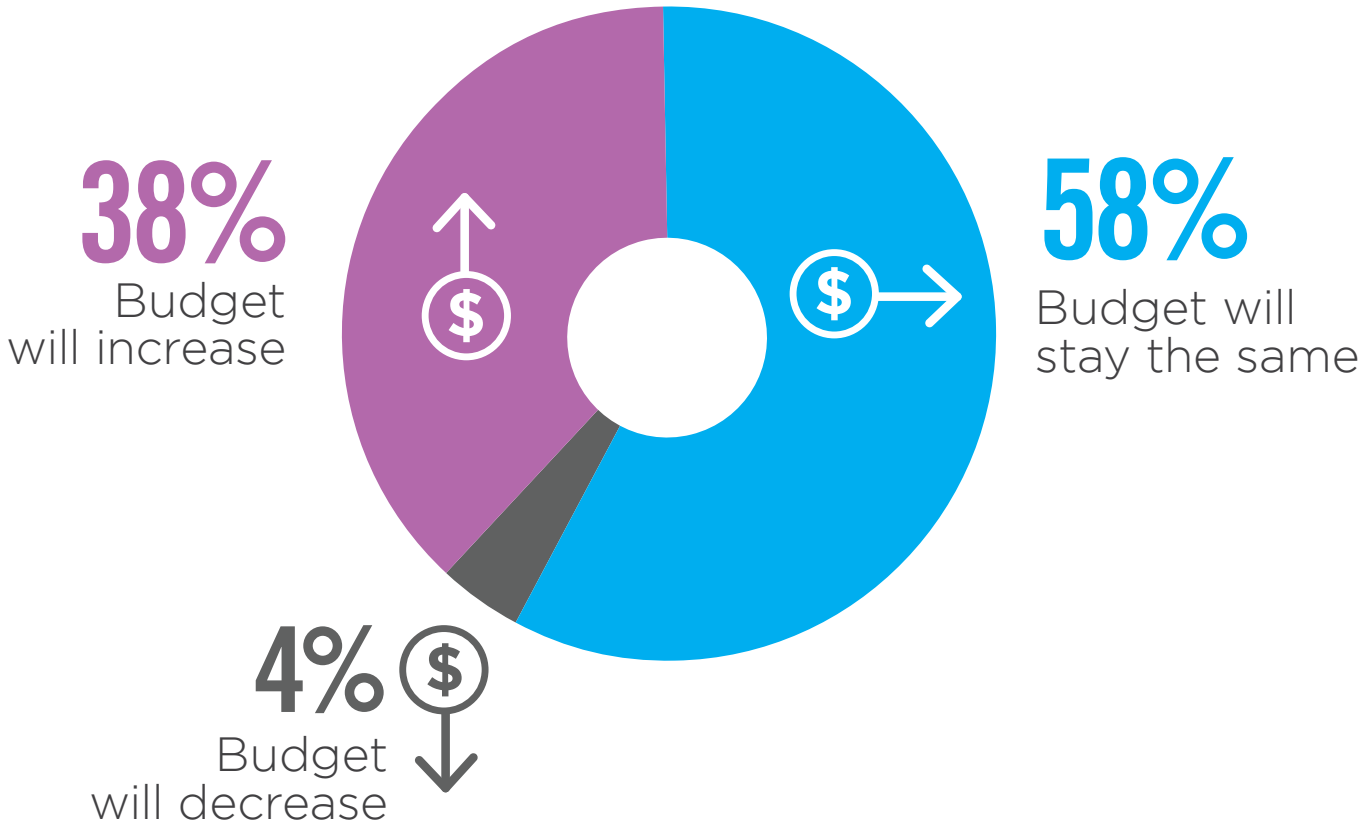
Lack of proper reporting tools



BUDGET TREND

On balance, IAM budget will increase for 38% of organizations that participated in the survey. Only 4% report a planned budget reduction over the next 12 months.

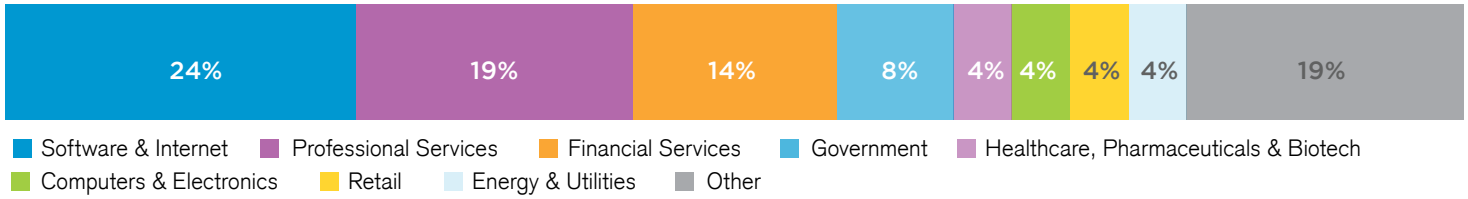
How do you expect your organization's access management related budget to change over the next 12 months?



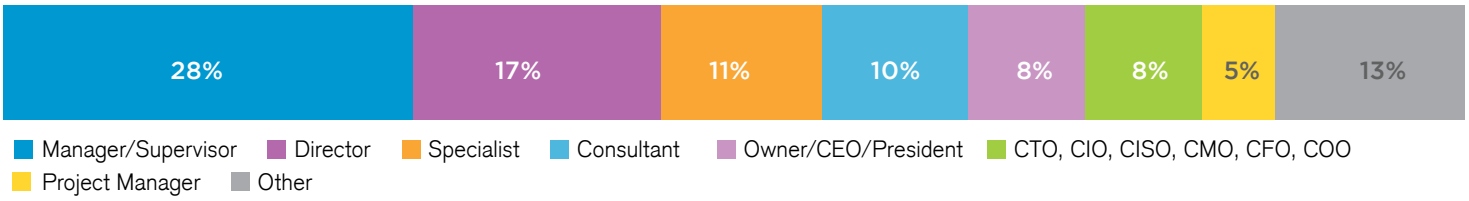
METHODOLOGY & DEMOGRAPHICS

This Identity and Access Management is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in June of 2019 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.

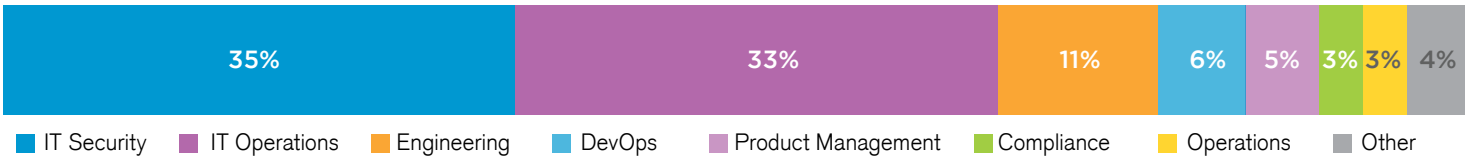
INDUSTRY



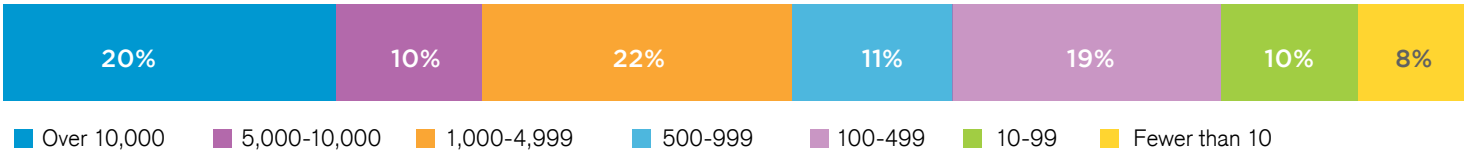
CAREER LEVEL



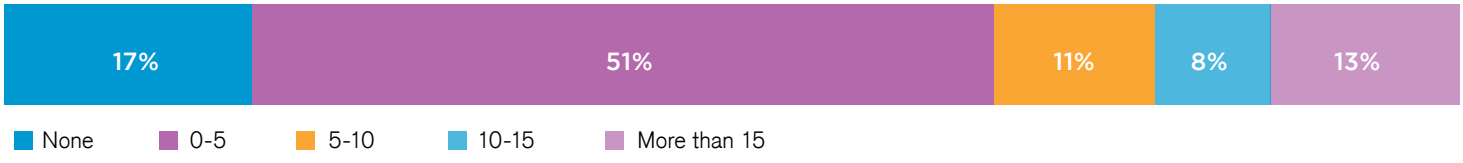
DEPARTMENT



COMPANY SIZE



STAFF DEDICATED TO IAM



Core Security provides organizations with critical, actionable insight and context about who, how, and what is vulnerable in their IT environment. Streamline security and safeguard critical data and assets with access management and vulnerability identification.

www.coresecurity.com