SILA

Ponemon INSTITUTE

The 2019 Study on Privileged Access Security

Commissioned by Sila Solutions Group

The 2019 Study on Privileged Access Security

Independently conducted by Ponemon Institute LLC

October 2019

Contents

Part 1:
Executive Summary

“The status quo is not secure.”
- Dr. Larry Ponemon | Ponemon Institute

Executive Summary

Sila and Ponemon Institute Study Finds Substantial Lapses in Securing Sensitive Access

Privileged access security is essential: it restricts and protects access to the powerful administrative accounts that control organizations' critical servers, databases, and networks. *The 2019 Study on Privileged Access Security* by the Ponemon Institute and Sila Solutions Group surveyed 650+ North American IT and IT security professionals, including database administrators, network engineers, IT security practitioners, and cloud custodians. The survey both builds on historical trend data starting in 2011 and introduces new research questions reflecting recent developments in the privileged access management (PAM) space.

By the Numbers

The study found substantial lapses in securing privileged access including:

56% | of respondents said they expect the risk of privileged user abuse to increase over the next 12 to 24 months

52% | of respondents said their organizations do not have the capabilities to effectively monitor privileged access

62% | of respondents said it was likely that their organization assigns privileged access rights that go beyond an individual's role or responsibilities

70% | of respondents said it was likely that privileged users access sensitive information without a business need

According to study participants, the biggest challenges organizations face in granting and enforcing privileged user access rights are:

57%

Can't keep pace with the number of access change requests that come in on a regular basis

48%

Lack of a consistent approval process for access and a way to handle exceptions

43%

Burdensome process for business users requesting access

Experts Weigh In

“With organizations facing a multitude of threats on a daily basis and as the risks related to privileged access security continue getting worse, this year’s survey shows that overall progress toward effective implementation of privileged access management programs continues to stagnate in many areas. The status quo is not secure. Business and IT leaders need to look beyond simple tool integration and a “check the box” mentality solely driven by compliance demands. Organizations take a big risk by not properly investing in effective PAM strategies that not only promote security but propel business success.”

- Dr. Larry Ponemon | Chairman, Ponemon Institute

“The results of *The 2019 Study on Privileged Access Security* shed light on the fact that privileged access is more prevalent than people may realize. It touches every part of an organization and has far-reaching implications for an organization’s business objectives as well as its security. Leaders need to step back and ask why individuals have the access they do, and how that aligns with the mission of their business – unnecessary privileged access puts data, employees, customers, and the overall business at risk.”

- Tapan Shah | Managing Director, Sila

Key Findings

Key findings from the study include multi-year trends, differences in high- and low-performing organizations, and critical risks privileged access management (PAM) programs should address. This report covers these areas and more, grouped by the following themes:

Why privileged user abuse is increasing

The security risks created by not keeping up with the delivery and review of access rights

The need for new approaches to managing access rights

Part 2:
Introduction

56%

of respondents expect the risk of privileged user abuse to increase in the next 12-24 months

Introduction

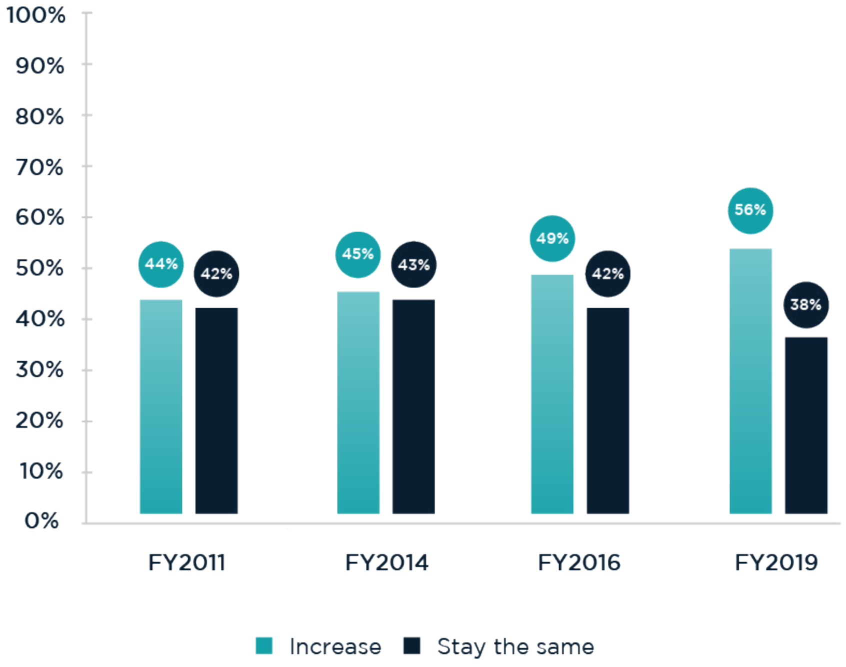
The ability to control access to critical information resources and mitigate data breach risks remains an elusive goal for many organizations. In *The 2019 Study on Privileged Access Security*, sponsored by Sila, Ponemon Institute presents four years of research findings on how elevated access to high-value information assets can be a serious risk to organizations when not properly secured.

For the purposes of this research, privileged users are defined as individuals assigned privileged access based on their roles and responsibilities. Such access can be defined as broad or elevated access rights to IT networks, enterprise systems, applications and/or information assets. However, according to the findings of this study, these individuals often use their rights inappropriately and put their organizations' sensitive information at risk. For example, the majority of respondents say privileged users feel empowered to access all the information they can view and although not necessary, will look at an organization's most confidential information out of curiosity.

The 659 respondents we surveyed self-reported that they have privileged access to IT resources. Seventy-seven percent of these respondents have access to at least three IT resources with 40 percent holding privileged access to six or more IT resources.

Figure 1

Do you expect the risk of privileged user abuse to increase or stay the same?



The expectation that the risk of privileged user abuse will increase has risen significantly since 2011.

As shown in Figure 1, 56 percent of respondents say they expect privileged user abuse to increase in the next 12 to 24 months, a significant increase from 44 percent of respondents in the 2011 research. Further, more than half of respondents (53 percent) say their organization experienced a data breach or other access-related security incident within the past three years.

The following are reasons new solutions and governance processes are needed to decrease the risk of privileged access abuse.

Even if an employee or contractor has appropriate access to high-value information assets, they put their organizations at risk by accessing sensitive or confidential data without a business need and sometimes share their access credentials with others in the organization.

The number of organizations that can't monitor privileged user activities has increased since last year; in a related access governance process problem, organizations don't have a unified view of privileged user access across the enterprise.

According to respondents, a lack of resources, in-house expertise, and in-house technologies are challenges to improving the efficiency and security of their access governance processes. Specifically, organizations are struggling to keep pace with the number of access change requests and to reduce burdensome processes for business users requesting access. Respondents also cite the lack of a consistent approval process for access and a way to handle exceptions as significant problems.

The increasing number of regulations is also contributing to the difficulty in managing access governance. It is also affected by the adoption of virtualization technologies or DevOps tooling.

Too much reliance on manual processes for granting privileged user access and reviewing and certifying privileged user access hinders organizations' abilities to meet growing requests for access changes.

To identify insider threats, organizations continue to rely upon monitoring and reviewing log files and using non-PAM security technologies. Fewer organizations are deploying PAM tooling capabilities like session monitoring, performing endpoint monitoring, and using big data analytics.

Part 3:
Key Findings

20%

of respondents who said they don't need privileged access to do their jobs but have it anyway say their organizations assigned it for no apparent reason.

Key Findings

The following is an analysis of the key findings. To understand trends in organizations' abilities to manage privileged user access, whenever possible we compare the findings from 2011, 2014, and 2016 to this year's research. The complete audited findings are presented in the appendix of this report.

Why privileged user abuse is increasing

The security risks created by not keeping up with the delivery and review of access rights

The need for new approaches to managing access rights

Why Privileged User Abuse is Increasing

According to 81 percent of respondents, privileged access rights are required to complete their current job assignments. However, 19 percent of respondents say they do not need privileged access to do their jobs but have it anyway. As shown in Figure 2, the two primary reasons are everyone at his or her level has privileged access even if it is not required to perform a job assignment (46 percent of respondents) and the organization failed to revoke these rights when they changed their role and no longer needed access privileges (30 percent of respondents). Since 2011, more respondents report that their organization assigned privileged access rights for no apparent reason.

Figure 2

Why do you still have privileged access rights?

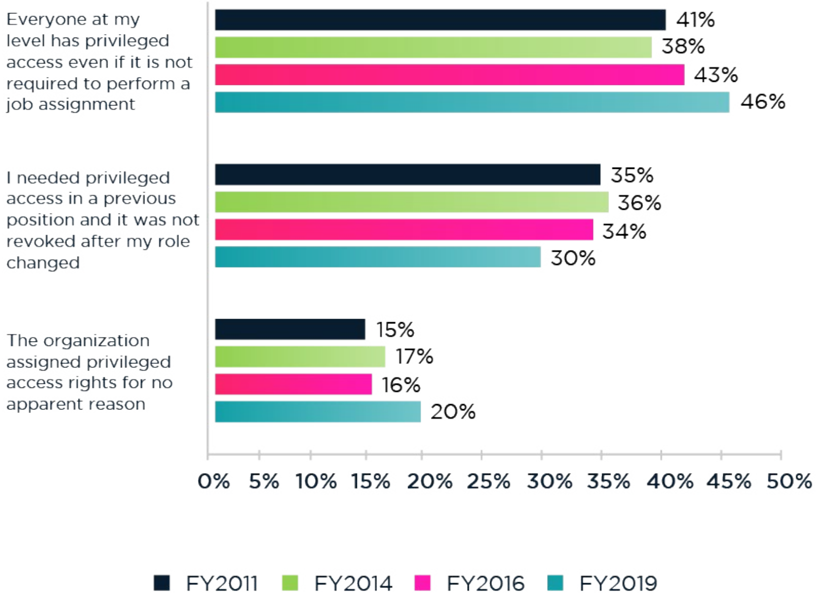
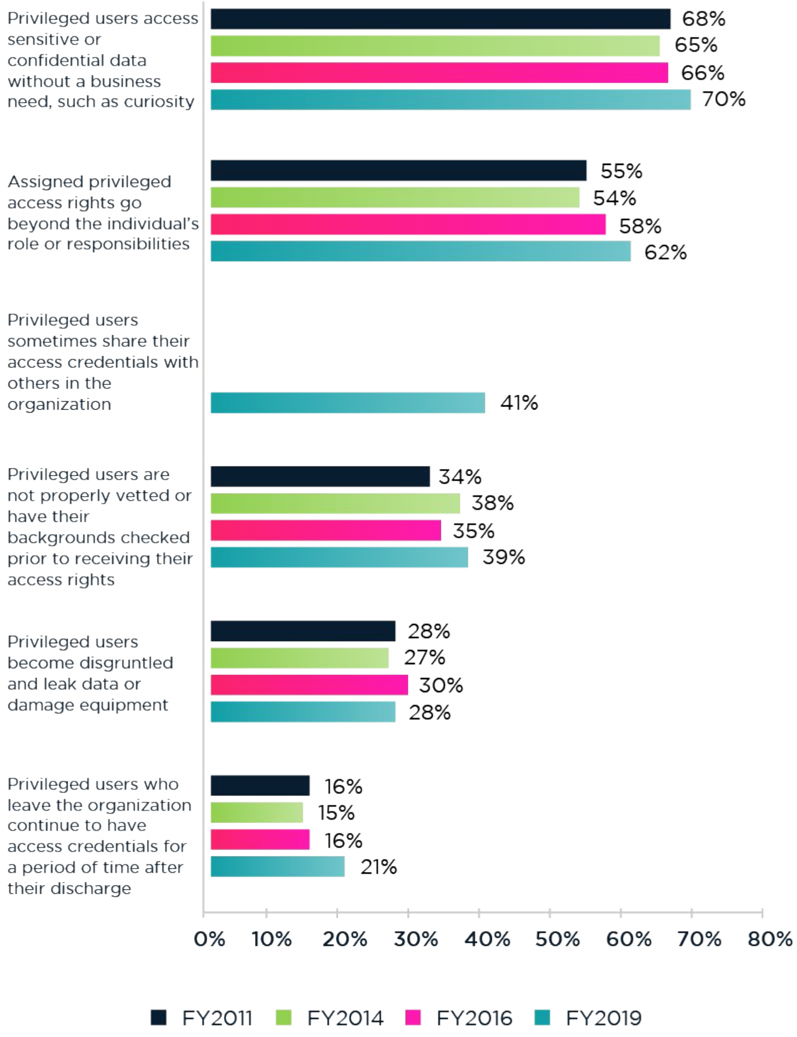


Figure 3

The likelihood of privileged access abuse

Very likely and Likely responses combined



Even if access rights are appropriate, privileged user abuse is prevalent.

According to Figure 3, 70 percent of respondents say it is very likely or likely privileged users access sensitive or confidential data without a business need, such as curiosity. Sixty-two percent of respondents say it is likely that their organization assigns privileged access rights that go beyond the individual's role and responsibilities, which indicates the difficulty organizations have in keeping up with access change requests and reviews of access rights. Many respondents (41 percent) say privileged users are sharing their access credentials with others in the organization.

The Security Risks Created by Not Keeping Pace with the Delivery and Review of Access Rights

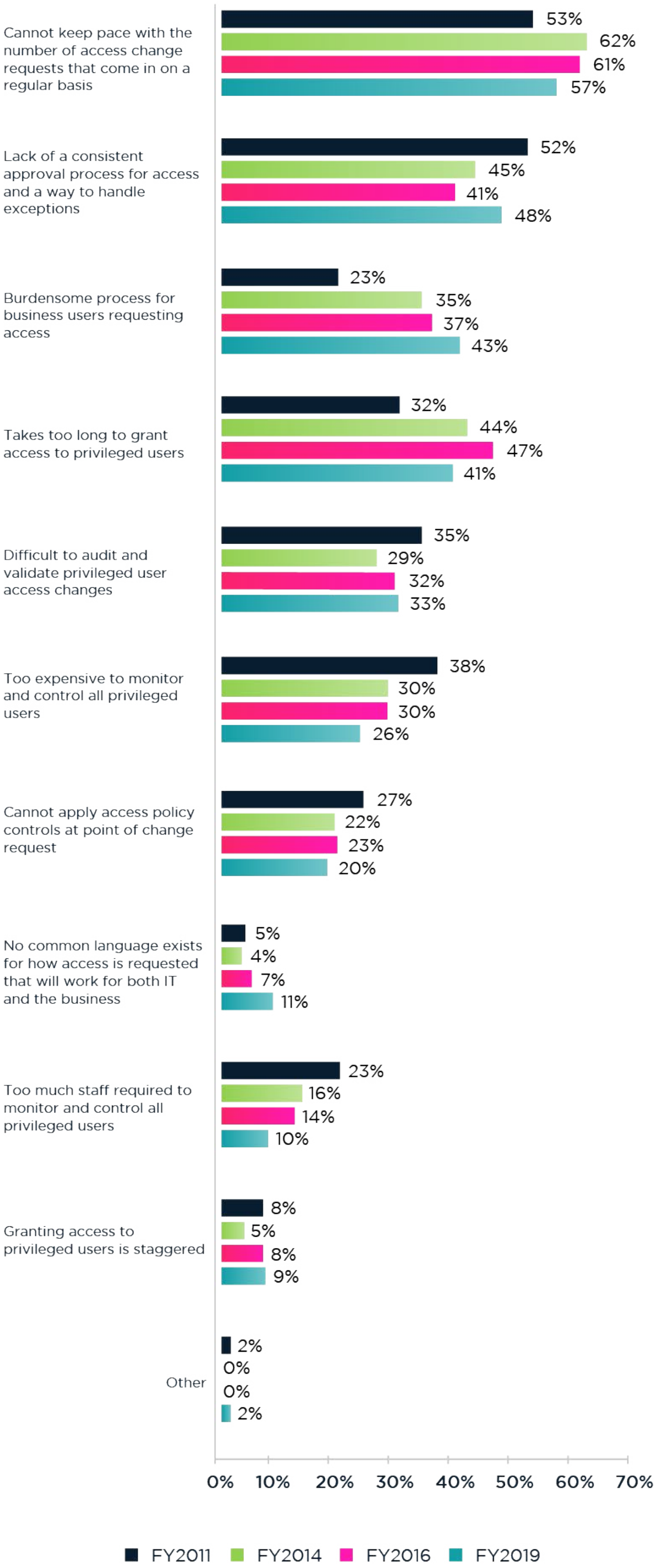
Organizations continue to struggle to keep pace with access change requests.

Figure 4 presents a list of reasons why organizations are at risk because of problems with delivering and enforcing privileged user access rights. As shown, companies still struggle to keep pace with the number of access change requests that come in on a regular basis (an increase from 53 percent in 2011 to 57 percent in 2019). Almost half of respondents (48 percent) say their organizations lack a consistent approval process for access and a way to handle exceptions.

Figure 4

The problems faced in delivering and enforcing privileged user access rights

Three choices permitted



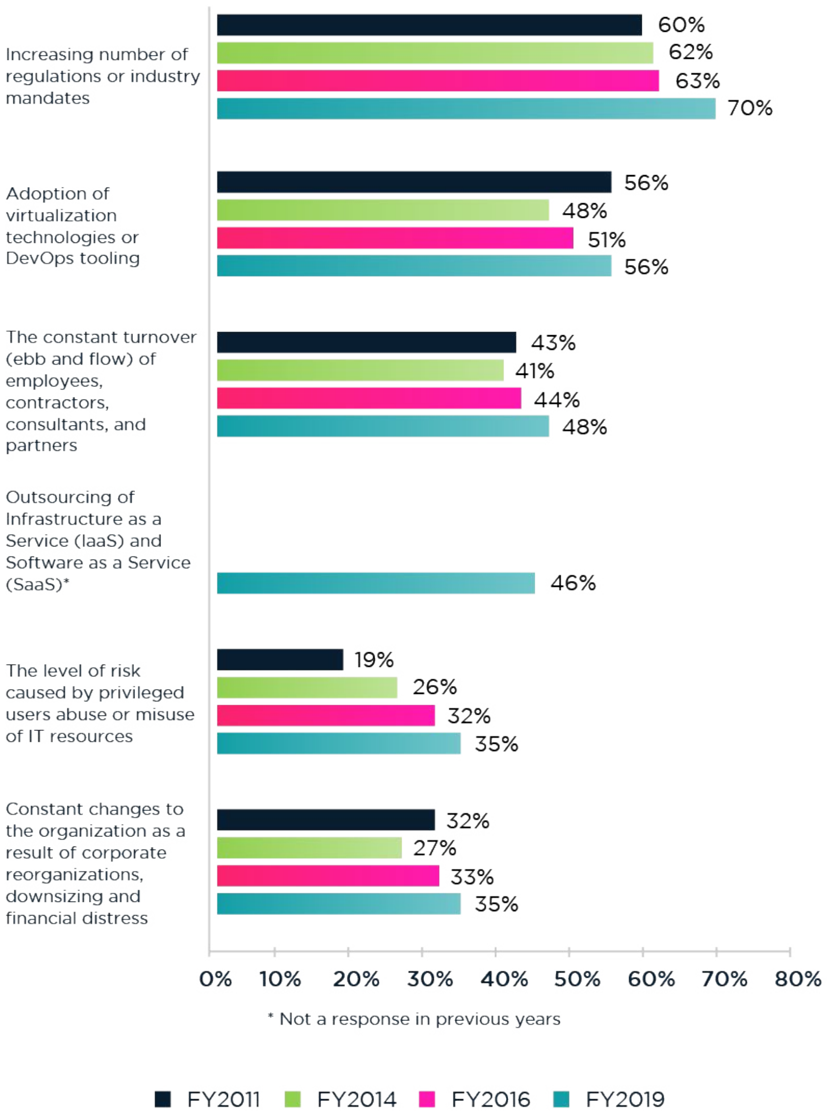
More regulations have the biggest impact on the governance of privileged access rights.

Figure 5 lists reasons for the difficulty in granting and enforcing privileged user access rights. Seventy percent say the increasing number of regulations or industry mandates will have the greatest impact on access governance processes followed by the adoption of virtualization technologies or DevOps tooling (56 percent). The impact of the risk caused by privileged user abuse or misuse of IT resources on access governance processes has increased significantly from 19 percent of respondents in 2011 to 35 percent of respondents in 2019.

Figure 5

Trends in factors that will affect access governance processes

Very significant and Significant repsponses combined

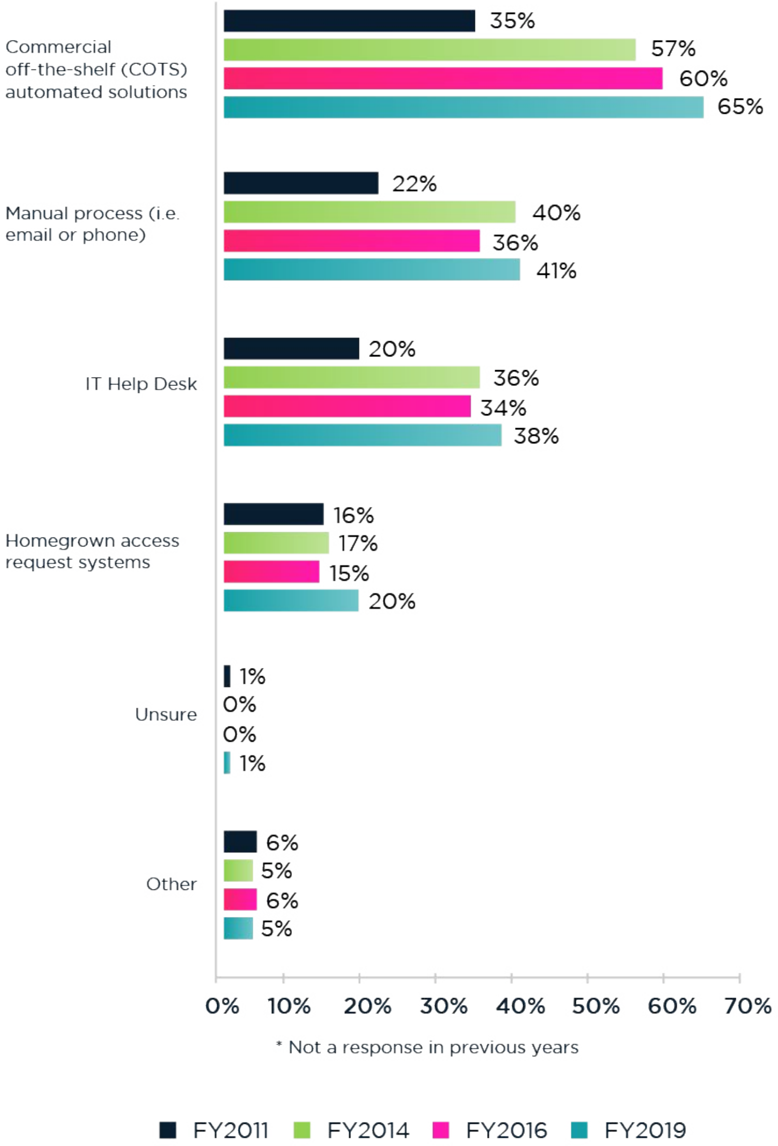


* Not a response in previous years

Figure 6

Processes used for granting privileged user access to IT resources

Two choices permitted



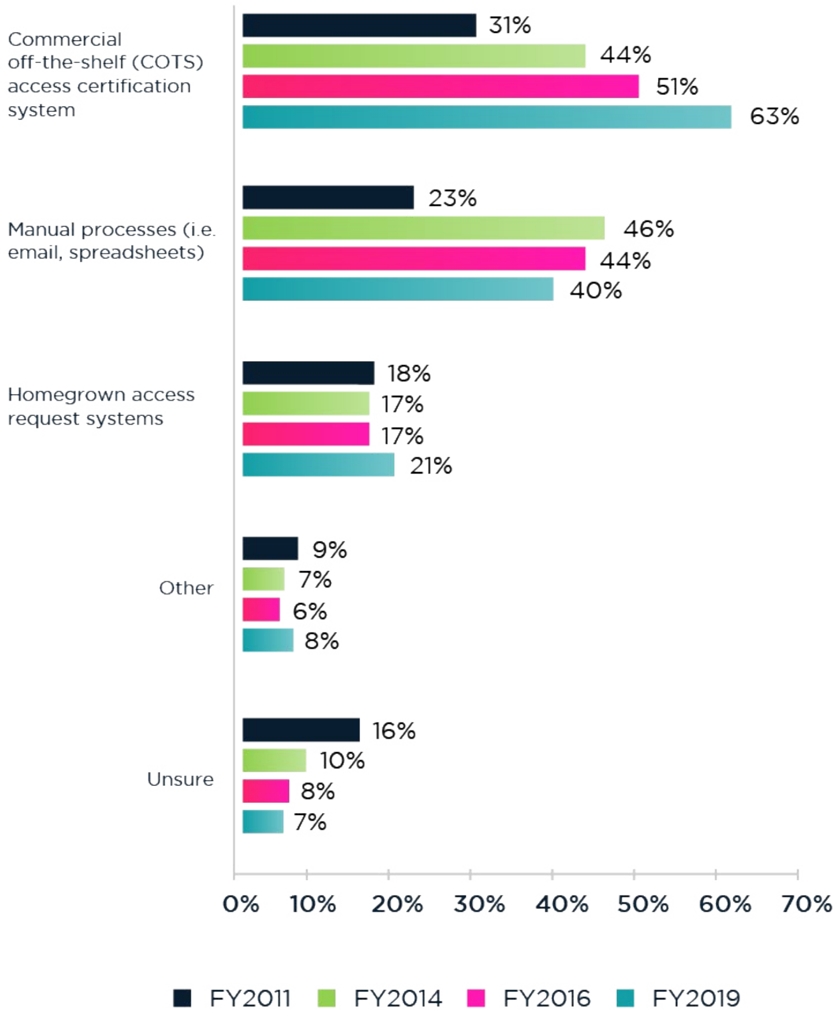
The use of commercial off-the-shelf automated solutions continues to dominate the process for granting privileged user access to IT resources.

There is a significant increase in the use of commercial off-the-shelf automated solutions from 35 percent of respondents in 2011 to 65 percent in 2019, as shown in Figure 6. The use of manual processes such as by phone or email increased from 22 percent of respondents in 2011 to 41 percent of respondents in 2019. The third most widely-used process is the IT help desk, which increased from 20 percent of respondents in 2011 to 38 percent of respondents in this year’s study.

Figure 7

Processes used to review and certify privileged user access

Two choices permitted



More organizations depend upon commercial off-the-shelf access certification systems to review and certify privileged user access, as shown in Figure 7. This is followed by the use of manual processes such as email and spreadsheets to review and certify privileged user access (an increase from 23 percent of respondents in 2011 to 40 percent of respondents in 2019).

The Need for New Approaches to Managing Access Rights

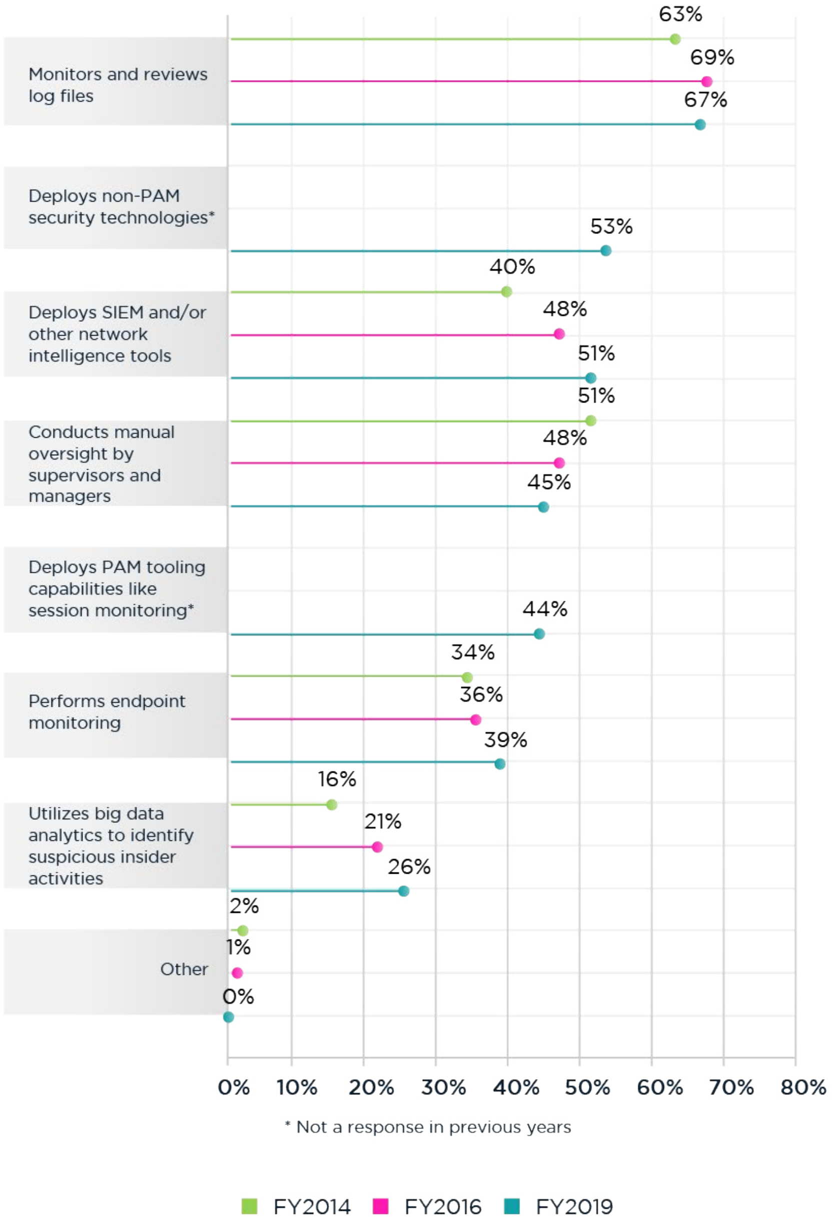
Organizations continue to rely upon monitoring and reviewing log files to identify insider threats.

According to Figure 8, 67 percent of respondents say their organizations monitor and review log files to determine if an action taken by an insider is truly a threat and 53 percent of respondents say they deploy non-PAM security technologies. Only 44 percent of respondents deploy PAM tooling capabilities like session monitoring. Since 2014 the use of endpoint monitoring and big data analytics has increased.

Figure 8

How does your organization determine if an action taken by an insider is truly a threat?

More than one response permitted



* Not a response in previous years

To prevent abuse, most organizations conduct privileged user training.

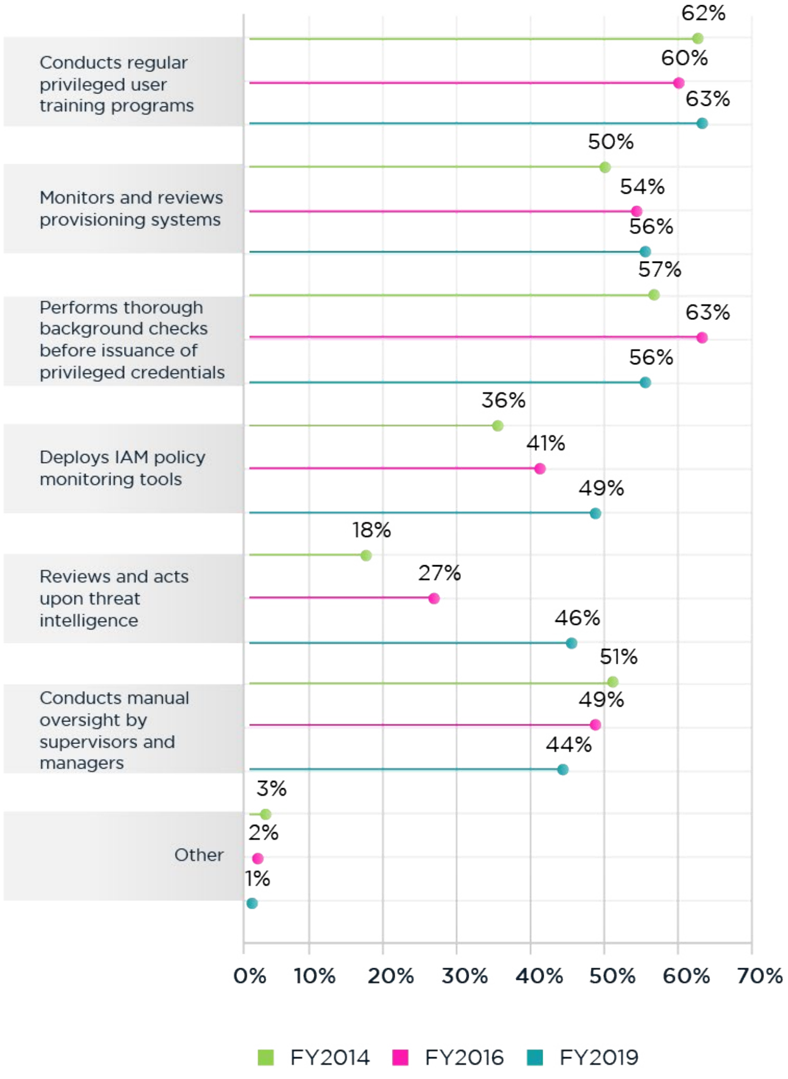
Most organizations represented in this research (63 percent of respondents) train privileged users, as shown in Figure 9. However, is such training effective? As discussed previously, the risk of abuse is increasing and many privileged users are not following their organizations' access governance policies. Fifty-six percent of respondents say they monitor and review provisioning systems.

The use of threat intelligence has increased significantly from 18 percent of respondents in 2014 to 46 percent of respondents in 2019 and the use of IAM policy monitoring tools has increased from 36 percent of respondents in 2014 to 49 percent of respondents in 2019.

Figure 9

How does your organization protect itself from privileged access abuse?

More than one response permitted

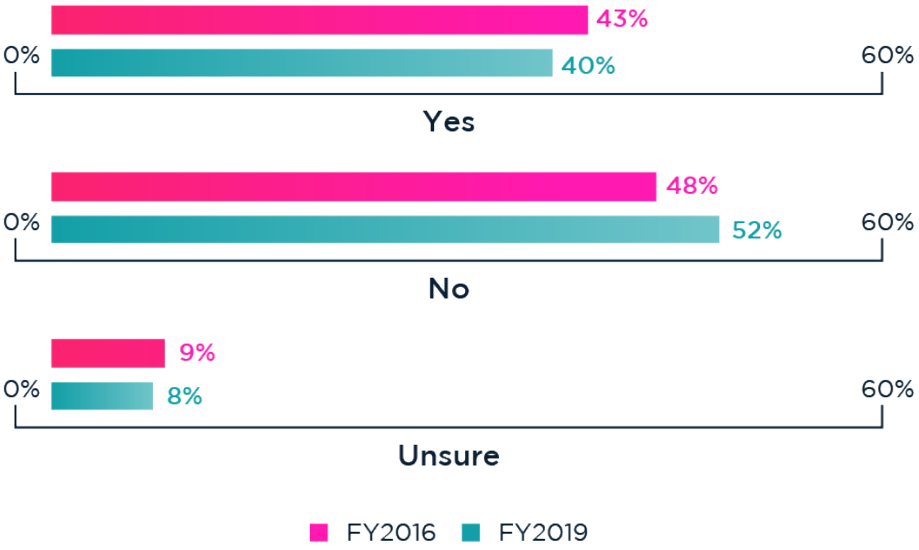


More organizations do not have the capability to effectively monitor privileged user activities and prevent abuse.

As shown in Figure 10, 60 percent of respondents say they do not have the capabilities (52 percent) or are unsure (8 percent) that they can effectively monitor privileged user activities. This is a slight increase from 2016.

Figure 10

Does your organization have the capabilities to effectively monitor privileged user activities?

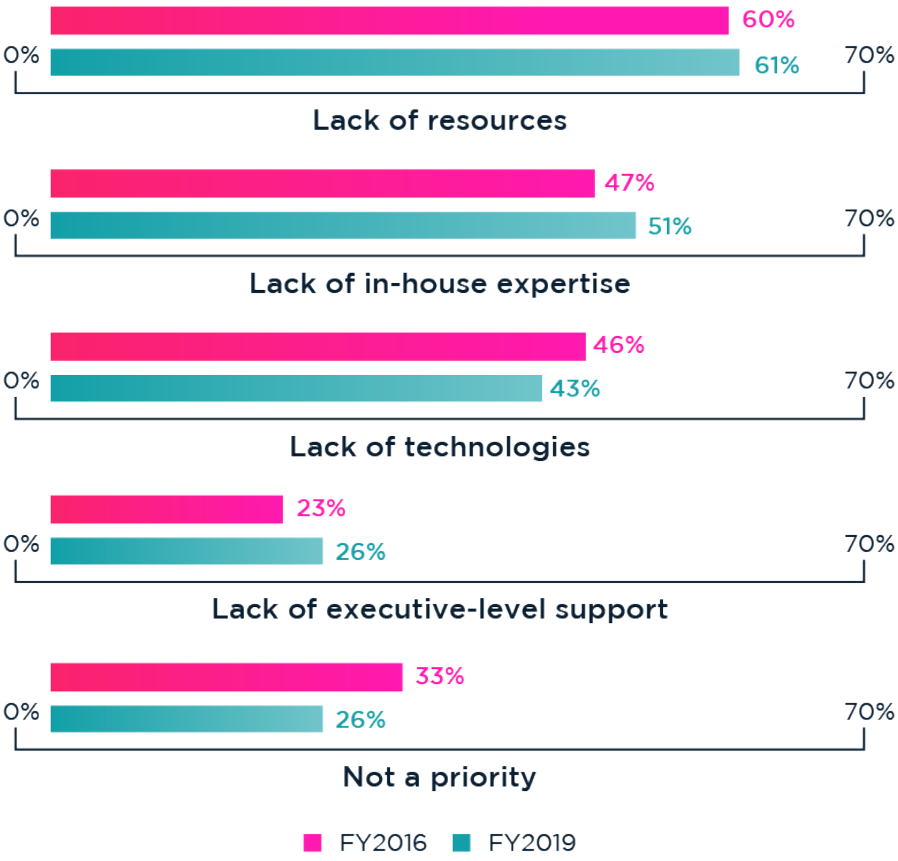


> A lack of resources, in-house expertise, and technologies are preventing companies from using correlation of trouble tickets and badge records to minimize the privileged user risk.

Figure 11

Reasons for not correlating activity from multiple sources

More than one response permitted



Most organizations are unable to effectively monitor privileged user activities.

As shown above, sixty percent of respondents say their organizations do not have the capabilities to effectively monitor privileged user activities or they are unsure. Furthermore, the majority of respondents (55 percent) are not correlating activity from multiple sources such as trouble tickets and badge records to determine risky privileged user behavior. The reasons for not correlating activity from multiple sources are shown in Figure 11.

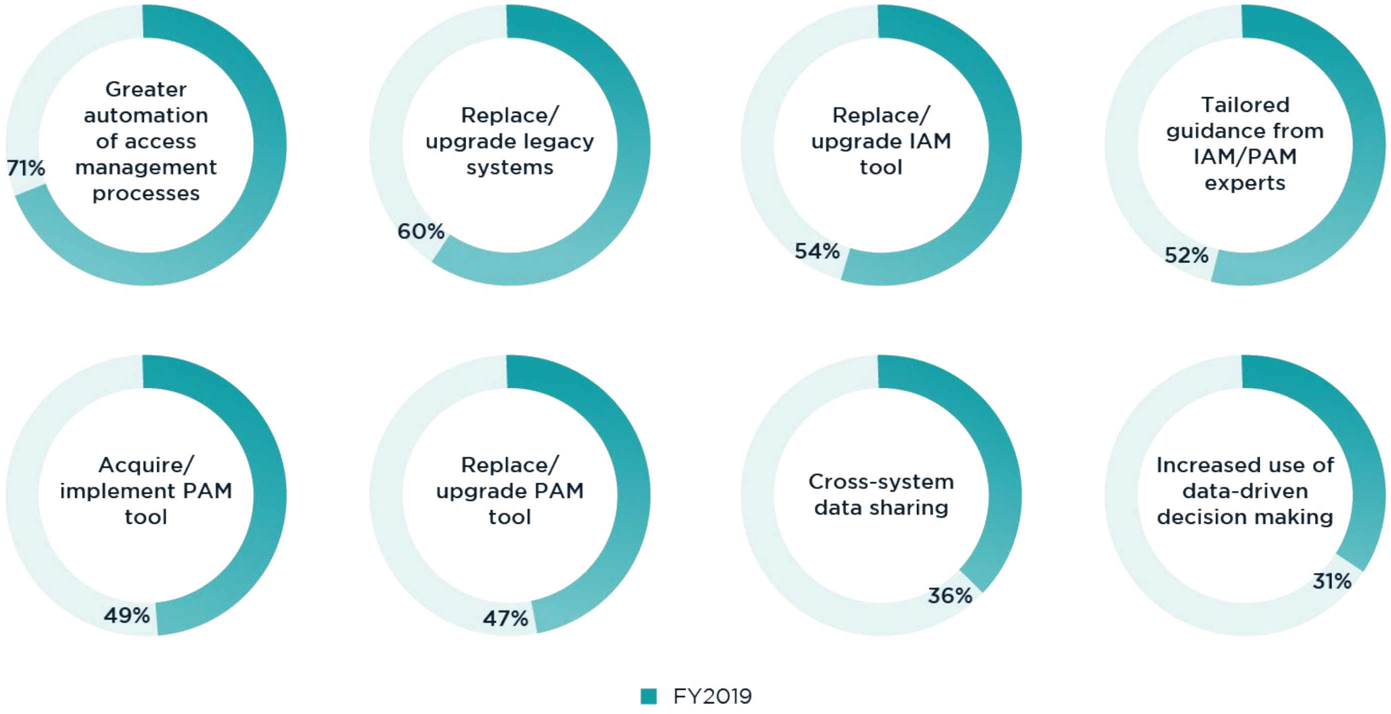
Automation of access management processes would improve organizations' IAM security posture.

According to Figure 12, 71 percent of respondents say more automation of access management processes would strengthen their organization's security posture followed by the replacement or upgrade of legacy systems.

Figure 12

What tools would most improve your organization's identity and access management security posture?

Four responses permitted

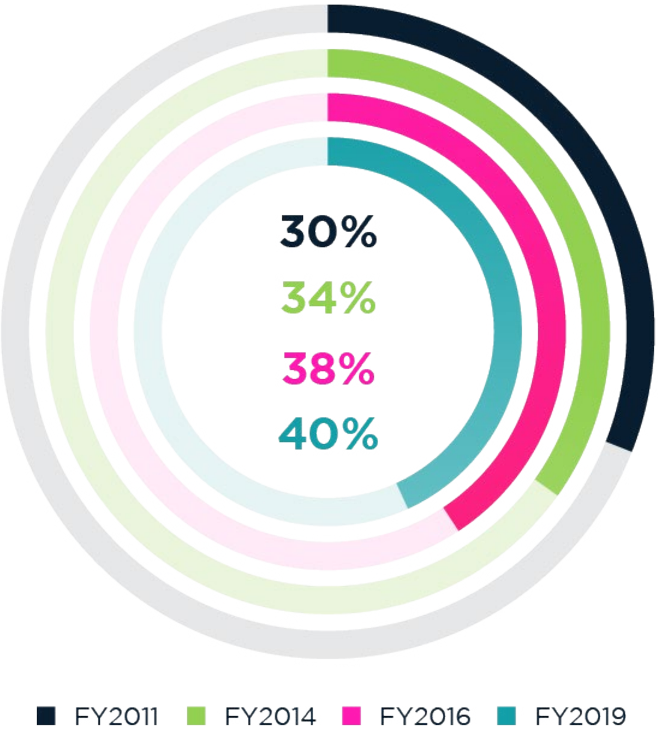


> "Unnecessary privileged access puts data, employees, customers, and the overall business at risk."
>
> – **Tapan Shah** | Sila

Figure 13

How confident are you that your organization has enterprise-wide visibility and can determine if privileged users are compliant with policies?

Combined responses of 7 to 10 on a scale of 1 = not confident to 10 = highly confident



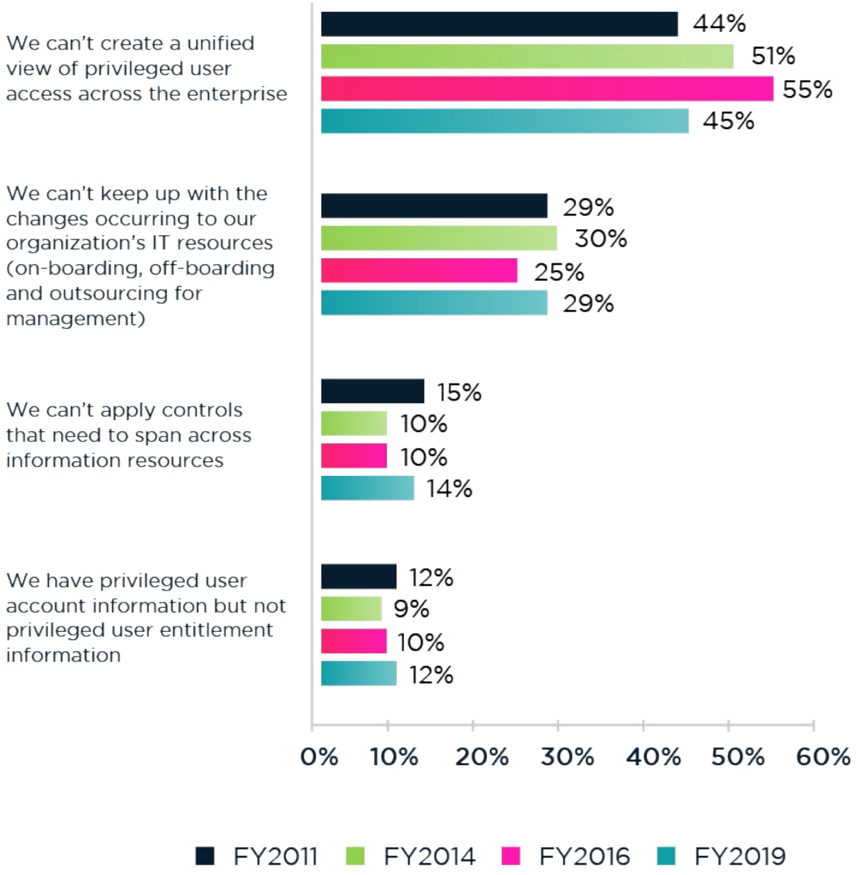
Lack of visbility continues to hinder the ability to determine if users are complying with policies.

When asked to rate their confidence in the ability to determine if privileged users are compliant with policies on a scale of 1 = not confident to 10 = highly confident, only 40 percent of respondents say they are confident that their organizations have enterprise-wide visibility of privileged user access and that they can determine if users are compliant with policies.

Forty-one percent of respondents rate their confidence as very low (responses 1 to 4 combined). The main reason for not being confident continues to be the inability to create a unified view of privileged user access across the enterprise. Another problem is keeping up with changes occurring in their organizations' IT resources (on-boarding, off-boarding, and outsourcing for management), according to 29 percent of respondents.

Figure 14

Main reasons for not being confident



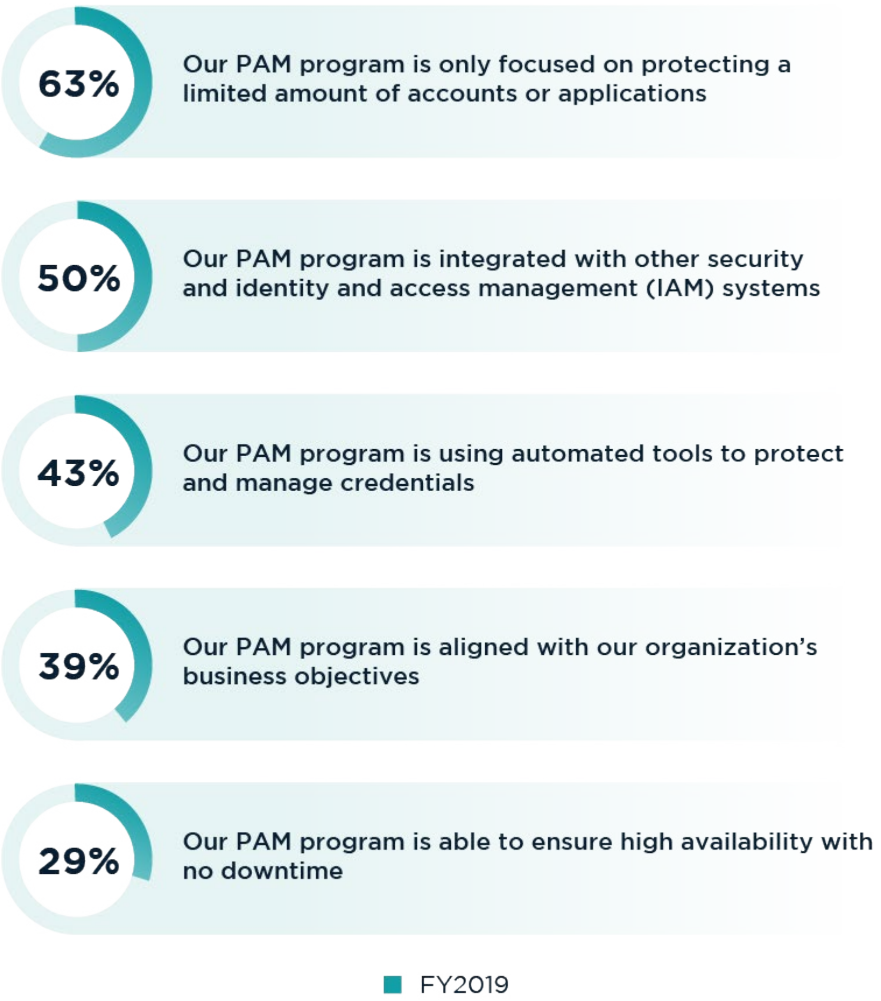
Are organizations maximizing the value of their dedicated Privileged Access Management (PAM) program?

A PAM program secures and manages an organization's privileged access to information resources. The goals of PAM are to protect critical data, ensure availability of essential business systems, reduce the likelihood that privileged credentials will be compromised or misused, reduce the impact if compromise or misuse does occur, and pinpoint which user is responsible for actions taken by a shared account.

Figure 15

Perceptions about organization’s PAM program

Strongly Agree and Agree responses combined

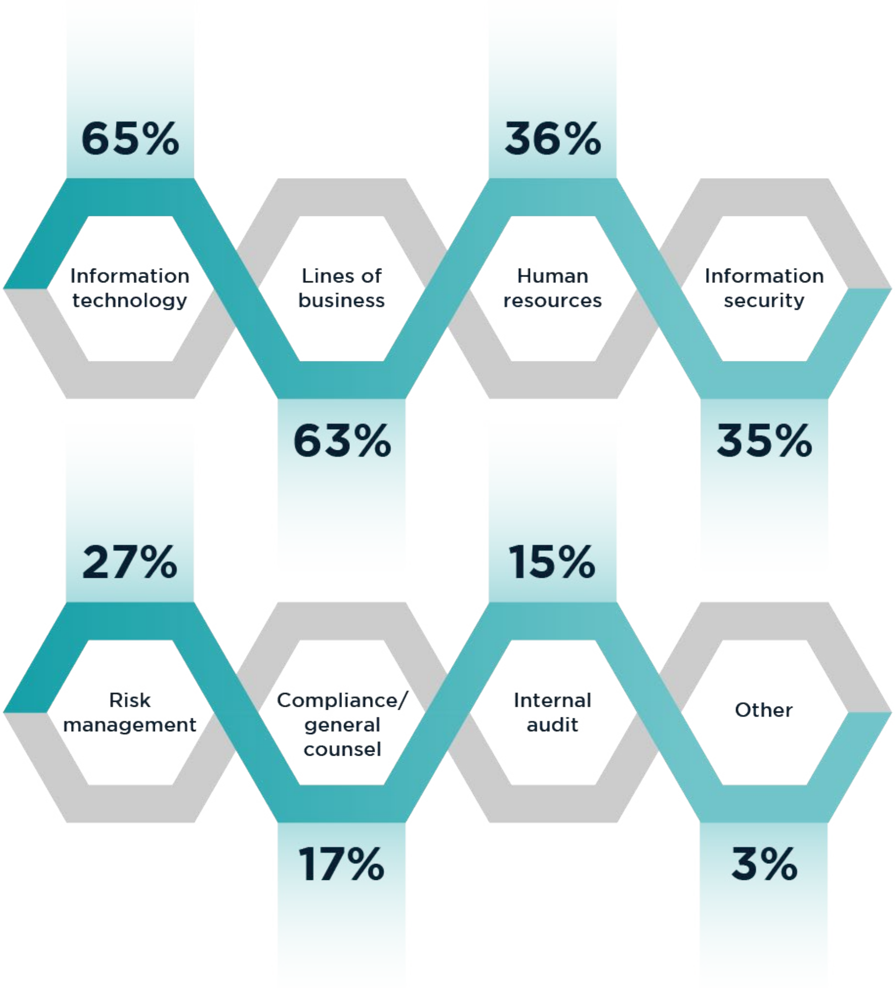


Forty-four percent of respondents say their organizations have a dedicated PAM program. However, only 37 percent of respondents say privileged users have increased mindfulness of their activities when they know the organization has PAM controls. As shown in Figure 15, 63 percent of respondents say their PAM program is only focused on protecting a limited amount of accounts or applications and only half of respondents say it is integrated with other security and IAM systems.

Figure 16

Which part of your organization is responsible for granting privileged access?

More than one response permitted



■ FY2019

Collaboration between business and IT is critical to reducing privileged user risk.

Responsibility for granting privileged access is dispersed throughout organizations. However, according to Figure 16, the functions most responsible for granting privileged access are IT and lines of business. As a solution to reducing the complexity of the access governance process and the difficulty in delivering and reviewing access rights, these two functions should collaborate to improve the process. Such collaboration could also result in more resources available to manage the process.

Complimentary Security

PAM programs are one part of an overarching IT security ecosystem that includes a number of complimentary areas, including cybersecurity risk and identity management.

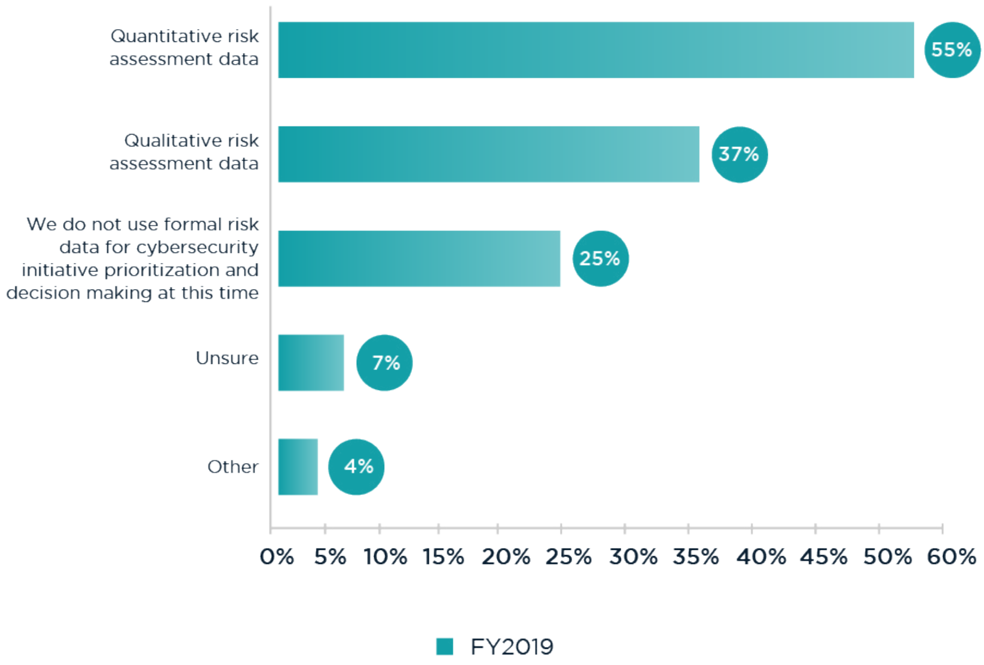
The majority of respondents say their organizations use quantitative risk assessment data.

According to Figure 17, 55 percent of respondents say their organizations are using quantitative risk assessment data followed by qualitative risk assessment data (37 percent of respondents).

Figure 17

What kind of risk data does your organization use for cybersecurity initiative prioritization and decision making?

More than one response permitted

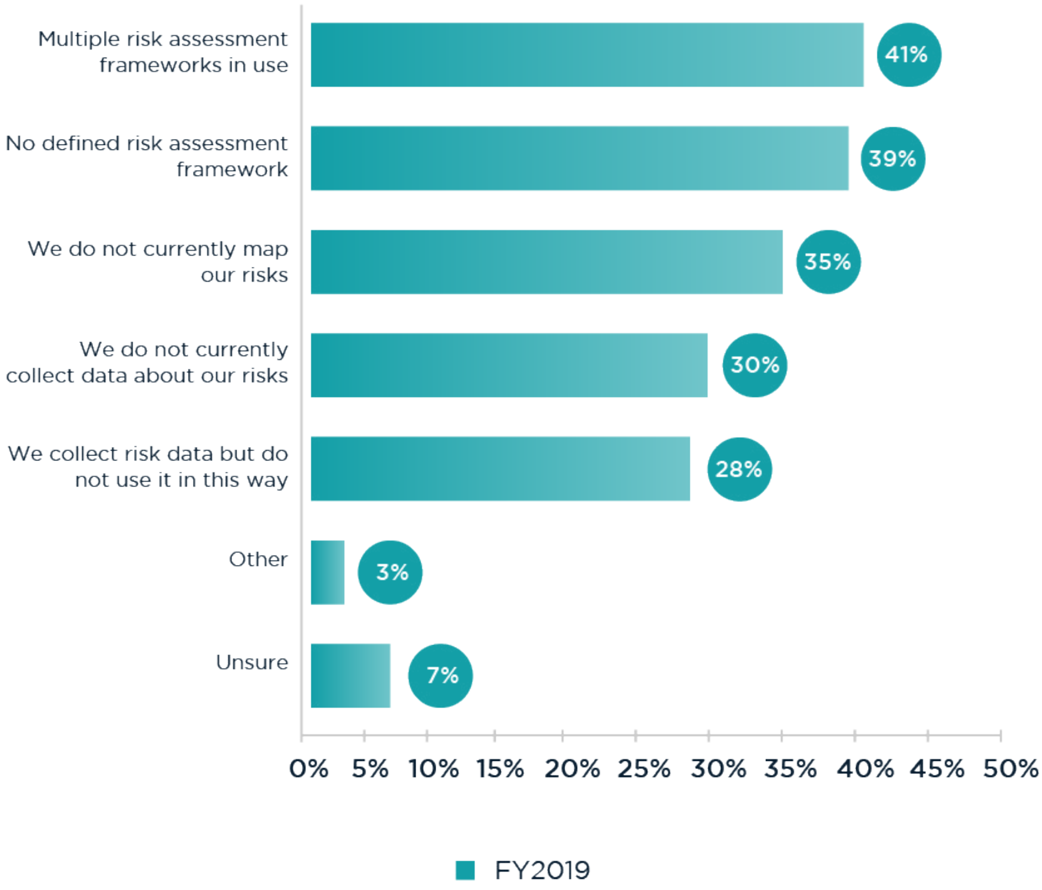


The use of multiple risk assessment frameworks is the primary challenge to the use of risk data for the prioritization of cybersecurity initiatives and decision making, as shown in Figure 18. However, 30 percent of respondents do not currently collect data about their risks.

Figure 18

What is the primary challenge your organization faces to using risk data to inform cybersecurity prioritization and decision making?

More than one response permitted



Part 4:
Research Methods

650+

North American respondents

Research Methods

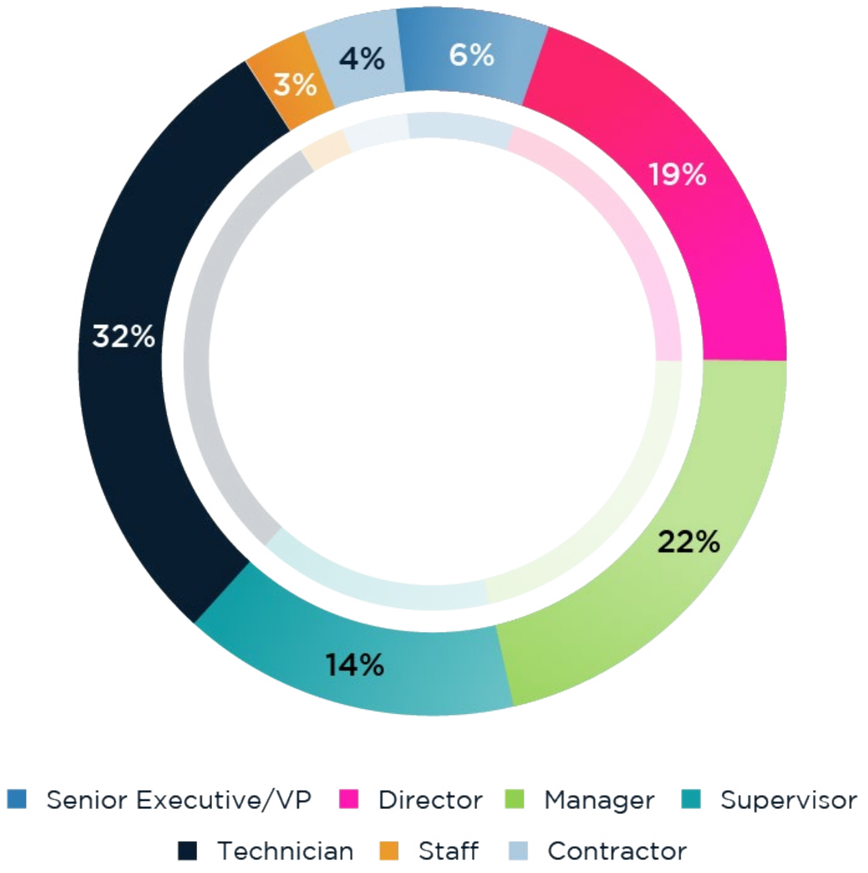
A random sampling frame of 16,075 privileged users, including database administrators, network engineers, IT security practitioners, and cloud custodians located in North America were selected as participants in this survey. As shown in Table 1, 701 respondents completed the survey. Screening and failed reliability checks removed 42 surveys. The final sample was 659 surveys (or a 4.1 percent response rate).

Table 1. Sample response	Frequency	Percentage%
Total sampling frame	16,075	100.0%
Total returns	701	4.4%
Rejected and screened surveys	42	0.3%
Final sample	659	4.1%

Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 61 percent of respondents are at or above the supervisory level.

Pie Chart 1

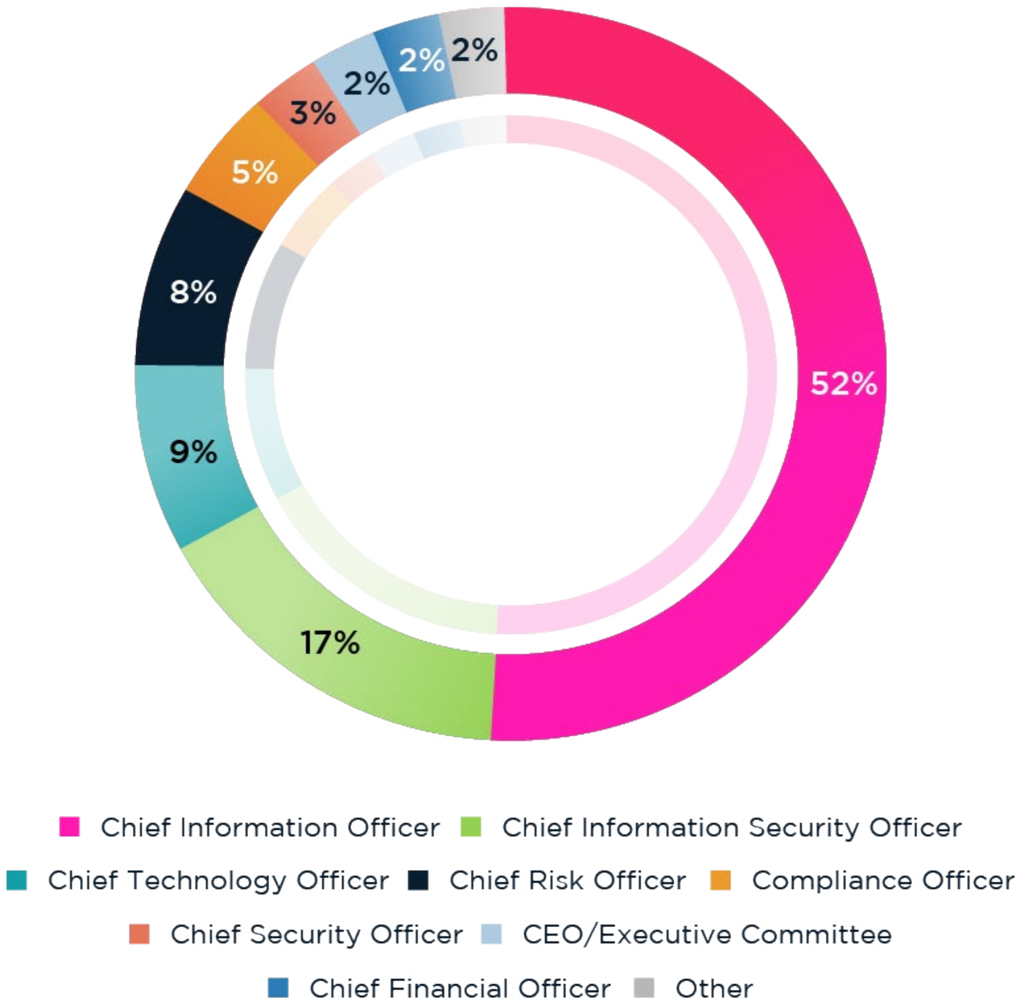
What organizational level best describes your current position?



Pie Chart 2 reports the respondents' direct reporting channels. Fifty-two percent of respondents report to the chief information officer, 17 percent of respondents report to the chief information security officer, and 9 percent of respondents report to the chief technology officer.

Pie Chart 2

Primary Person you or your IT security leader reports to within the organization

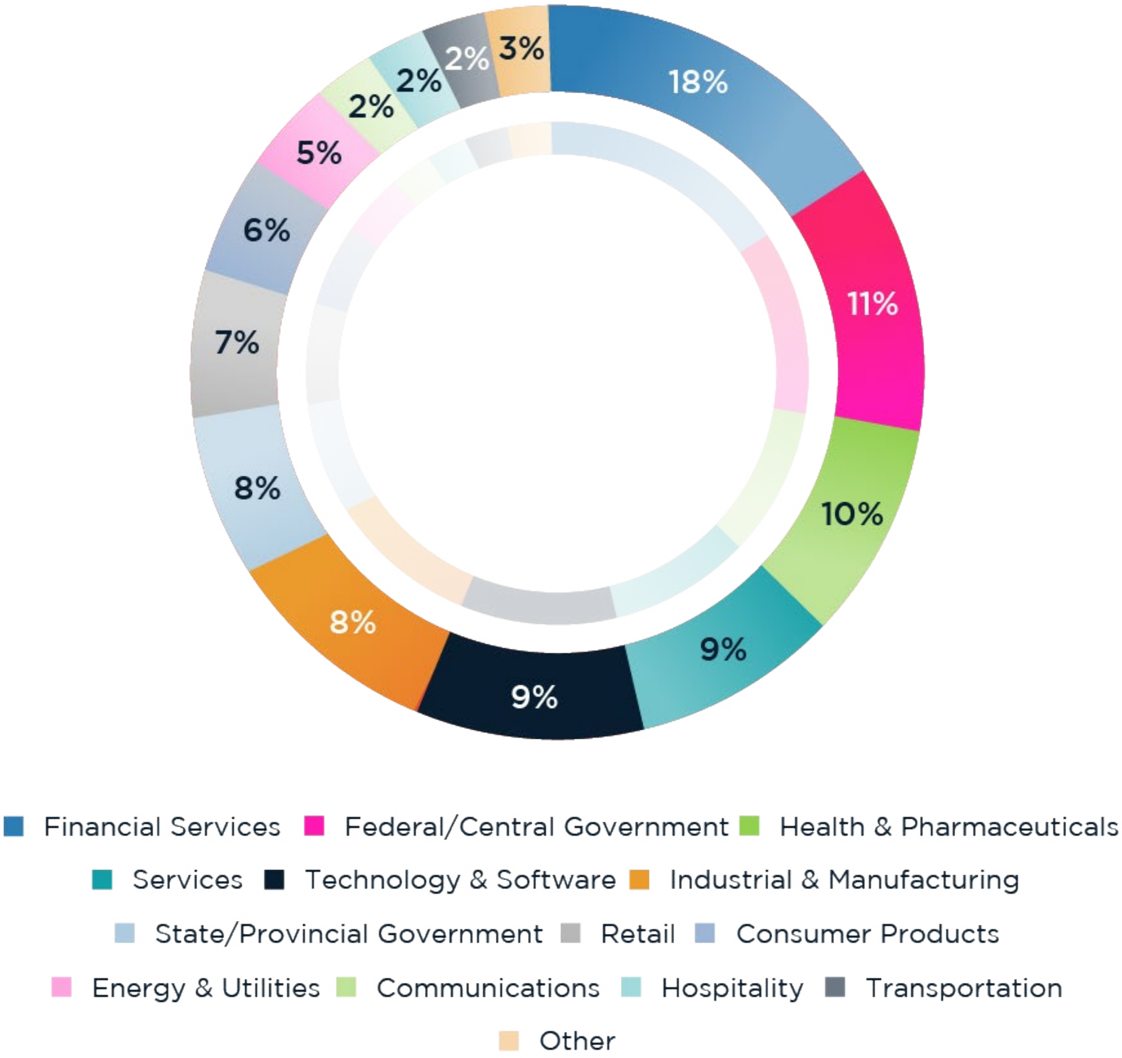


> "Business and IT leaders need to look beyond simple tool integration and a 'check the box' mentality"
>
> **– Dr. Larry Ponemon | Ponemon Institute**

Pie Chart 3 reports the industry focus of respondents' organizations. The largest industry classification is financial services (18 percent of respondents), which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by federal/central government (11 percent of respondents), health and pharmaceuticals (10 percent of respondents), services (9 percent of respondents), and technology and software (9 percent of respondents).

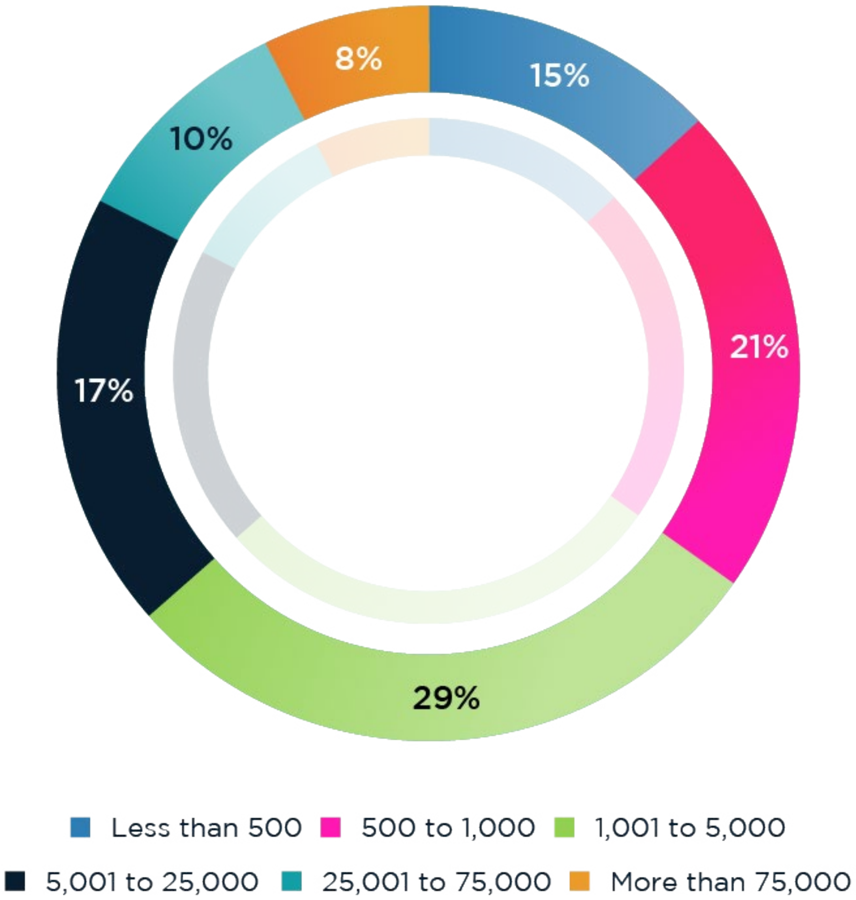
Pie Chart 3

Industry focus of respondents' organizations



Pie Chart 4

Worldwide headcount of respondents' organizations



As shown in Pie Chart 4, 64 percent of respondents are from organizations with a worldwide headcount of 1,000 or more employees, technology and software (9 percent of respondents).

Caveats

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.

Sampling-frame bias:

The accuracy is based on contact information and the degree to which the list is representative of individuals who are privileged users, database administrators, network engineers, IT security practitioners, or cloud custodians. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

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 a truthful response.

Part 5: **Appendix**

Privileged Access Management (PAM):

Securing and managing an organization’s privileged access to information resources.

Glossary

The following terms and definitions were used in the survey and were defined for the purposes of the survey.

Organization: Corporations or government agencies and departments

Information resources: Includes applications, databases, networks, servers, hosts, and file shares

Privileged access: Broad or elevated access rights to IT networks, enterprise systems, applications, and/or information resources

Privileged user: Any individual who is assigned privileged access based on their roles and responsibilities within the organization.

End user: Employees, temporary employees, contractors, consultants, and others who have limited or "ordinary" access rights to their organization's IT resources

Privileged Access Management (PAM): Securing and managing an organization's privileged access to information resources. The goals of PAM are to protect critical data and ensure availability of essential business systems, reduce the likelihood that privileged credentials will be compromised or misused, reduce the impact if compromise or misuse does occur, and pinpoint which user is responsible for actions taken by a shared account.

PAM program: An organization's overarching approach to PAM, including technology tools, business processes, and governance; not limited to PAM-focused technology tools alone.

Access governance: Ensuring that users of information resources have only the access rights that are appropriate for their business role(s) within the organization (no more and no less access than is necessary to do their job) while not violating any regulatory compliance mandates.

About Sila

Sila is a technology and management consulting firm that provides solutions in the areas of identity and access management, data analytics, cybersecurity and risk, software engineering and integration, strategy and transformation, and digital and creative services. Sila specializes in multifaceted engagements with Fortune 500 companies and Federal government agencies that are accomplished through active collaboration and strategic alignment. Deep technical acumen coupled with proven leadership capabilities enable Sila to develop solutions that result in long-term value, competitive advantages, and a positive impact to business and mission outcomes.

For more information visit **silasg.com**

About Ponemon Institute

Ponemon Institute conducts independent research on data protection and emerging information technologies. Our goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in regulations and the threat landscape that will affect the collection, management and safeguarding of information assets. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise.

Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured from July 24 to August 12, 2019.

Survey response	Freq	Pct%
Total sampling frame	16,075	100.0%
Total returns	701	4.4%
Rejected surveys	42	0.3%
Final sample, North America	659	4.1%
United States	558	
Canada	101	

Part 1. Screening Questions

S1. What best describes your level of access to your organization's IT networks, enterprise systems, applications and information resources? Please select only one choice.	FY2019
End user access rights to IT resources (Stop)	0%
Privileged access to a few (less than 3) IT resources	23%
Privileged access to some (3 to 5) IT resources	37%
Privileged access to numerous (6+) IT resources	40%
Total	100%

S2. Are you familiar with how privileged access is managed at your organization?	FY2019
Yes	100%
No (Stop)	0%
Total	100%

Part 2. Background

Q1. Does your organization have a dedicated PAM program?	FY2019
Yes, PAM is recognized as its own program	44%
No, privileged access is managed within another program such as an Identity and Access Management (IAM) program	50%
Unsure	6%
Total	100%

Q2a. Is privileged access required in order for you to complete your current job assignments or functions within the organization?	FY2019	FY2016
Yes	81%	79%
No	19%	21%
Total	100%	100%

Q2b. If you said no, what is the primary reason you still have privileged access rights? Please select only one choice.	FY2019	FY2016
I needed privileged access in a previous position and it was not revoked after my role changed	30%	34%
Everyone at my level has privileged access even if it is not required to perform a job assignment	46%	43%
The organization assigned privileged access rights for no apparent reason	20%	16%
Unsure	4%	7%
Total	100%	100%

Q3. How does your organization protect itself from privileged access abuse? Please select all that apply.	FY2019	FY2016
Performs thorough background checks before issuance of privileged credentials	56%	63%
Conducts manual oversight by supervisors and managers	44%	49%
Monitors and reviews provisioning systems	56%	54%
Reviews and acts upon threat intelligence	46%	27%
Deploys IAM policy monitoring tools	49%	41%
Conducts regular privileged user training programs	63%	60%
Other (please specify)	1%	2%
Total	315%	296%

Q4. Do you expect the risk of privileged user abuse to increase, decrease or stay at the same level over the next 12 to 24 months?	FY2019	FY2016
Increase	56%	49%
Stay the same	38%	42%
Decrease	6%	9%
Total	100%	100%

Q5. Has your organization experienced a data breach or other access-related security incident within the past 3 years?	FY2019
Yes	53%
No	42%
Unsure	5%
Total	100%

Q6. What best describes your role in your organization’s IT department or related functions? Please check all that apply.	FY2019
Chief Information Officer/Chief Information Security Officer	34%
Other C-Level Executive	15%
IT Security Director	31%
Other Director	7%
IT Security Manager	35%
Other Manager	6%
IT Security Architect	7%
Database Administrator	32%
Platform Administrator	23%
Application Administrator	17%
Application Developer	28%
IT Security Engineer	31%
IT Security Analyst	16%
Audit Practitioner	8%
Other Staff	12%
Contractor	9%
Other (please specify)	5%
Total	316%

Q7. How does your organization determine if an action taken by a privileged user is truly a threat? Select all that apply.	FY2019	FY2016
Monitors and reviews log files	67%	69%
Conducts manual oversight by supervisors and managers	45%	48%
Deploys SIEM and/or other network intelligence tools	51%	48%
Utilizes big data analytics to identify suspicious insider activities	26%	21%
Deploys PAM tooling capabilities like session monitoring	44%	
Deploys non-PAM security technologies	53%	
Performs endpoint monitoring	39%	36%
Other (please specify)	0%	1%
Total	325%	223%

Q8. Does your organization have the capabilities to effectively monitor privileged user activities?	FY2019	FY2016
Yes	40%	43%
No	52%	48%
Unsure	8%	9%
Total	100%	100%

Q9a. Does your organization correlate activity from multiple sources such as trouble tickets and badge records to determine risky privileged user activity?	FY2019	FY2016
Yes	45%	42%
No	48%	50%
Unsure	7%	8%
Total	100%	100%

Q9b. If your organization does not do this, why not? Please select all that apply.	FY2019	FY2016
Lack of technologies	43%	46%
Lack of resources	61%	60%
Lack of executive-level support	26%	23%
Lack of in-house expertise	51%	47%
Not a priority	26%	33%
Total	207%	209%

Q10a. Which part of your organization is responsible for granting privileged access? Please select all that apply.	FY2019
Information technology	65%
Information security	35%
Compliance/general counsel	17%
Internal audit	15%
Human resources	36%
Risk management	27%
Lines of business	63%
Other (please specify)	3%
Total	261%

Q10b. Has this ownership changed in the past five years?	FY2019
Yes	56%
No	44%
Total	100%

Q11. Using the following 10-point scale, please rate the ability of your controls to reduce the insider threat risk of privileged access abuse.	FY2019
1 or 2	15%
3 or 4	21%
5 or 6	22%
7 or 8	26%
9 of 10	16%
Total	100%
Extrapolated value	5.64

Q12a. Approximately, what is the dollar range that best describes your organization's IT security budget this year?	FY2019
Less than $5 million	15%
$5 to $10 million	43%
$11 to $50 million	24%
$51 to $100 million	13%
More than $100 million	5%
Total	100%
Extrapolated value (US$ Millions)	$ 26.55

Q12b. What percentage of your organization’s IT security budget is allocated to privileged access technology investments?	FY2019
Less than 5%	7%
5 to 10%	6%
11% to 15%	16%
16% to 20%	17%
21% to 30'%	21%
31% to 40%	15%
41% to 50%	12%
More than 50%	6%
Total	100%
Extrapolated value	25%

The following are statements about your organization’s PAM program. Only respondents in organizations with a PAM program were permitted to answer these questions. Please rate your organization’s perception about your PAM program using the scale provided below each statement. **Strongly Agree and Agree responses combined.**	FY2019
Q13. Our PAM program is aligned with our organization’s business objectives.	39%
Q14. Our PAM is using automated tools to protect and manage credentials.	43%
Q15. Our PAM is able to ensure high availability with no downtime.	29%
Q16. Our PAM program is integrated with other security and identity and access management (IAM) systems.	50%
Q17. Our PAM program is only focused on protecting a limited amount of accounts or applications.	63%

Part 2. Likelihood Scenarios:

How likely would it be for the following events to occur within your organization? **Very Likelihood and Likelihood responses combined.**	FY2019	FY2016
Q18. The organization assigns privileged access rights that go beyond the individual’s role or responsibilities.	62%	58%
Q19. Privileged users sometimes share their access credentials with others in the organization.	41%	
Q20. Privileged users are not properly vetted or have their backgrounds checked prior to receiving their access rights.	39%	35%
Q21. Privileged users become disgruntled and leak data or damage equipment.	28%	30%
Q22. Privileged users access sensitive or confidential data without a business need, such as curiosity.	70%	66%
Q23. Privileged users have increased mindfulness of their activities when they know the organization has PAM controls.	37%	
Q24. Privileged users who leave the organization continue to have access credentials for a period of time after their discharge.	21%	16%

Part 3. Privileged User Access Governance

Q25. What are the predominant processes used for granting users privileged access to IT resources? Please select no more than two choices.	FY2019	FY2016
Manual process (i.e. email or phone)	41%	36%
Homegrown access request systems	20%	15%
Commercial off- the-shelf (COTS) automated solutions	65%	60%
IT Help Desk	38%	34%
Unsure	1%	0%
Other (please specify)	5%	6%
Total	170%	151%

Q26. What are the predominant processes used to review and certify privileged access? Please select no more than two choices.	FY2019	FY2016
Manual process (i.e. email, spreadsheets)	40%	44%
Homegrown access certification system	21%	17%
Commercial off- the-shelf (COTS) access certification system	63%	51%
Unsure	7%	8%
Other (please specify)	8%	6%
Total	139%	126%

Q27. What controls does your organization use to grant runtime privileged access? Please select all that apply.	FY2019
Basic authentication	66%
Multifactor authentication (MFA)	69%
Vault check-in/checkout	47%
Automated session management with limited auditing	35%
Full session auditing	38%
Other (please specify)	3%
Total	258%

Q28a. How confident are you that your organization has enterprise-wide visibility for privileged user access and can determine if these users are compliant with policies? Please use the 10-point scale below, where 1 = low confidence to 10 = highly confident.	FY2019
1 or 2	17%
3 or 4	24%
5 or 6	19%
7 or 8	25%
9 of 10	15%
Total	100%
Extrapolated value	5.44

Q28b. If your confidence is low (responses 1 to 4), please select one main reason.	FY2019	FY2016
We can't create a unified view of privileged user access across the enterprise	45%	55%
We have privileged user account information but not privileged user entitlement information	12%	10%
We can't apply controls that need to span across information resources	14%	10%
We can't keep up with the changes occurring to our organization's IT resources (on-boarding, off- boarding and outsourcing for management)	29%	25%
Total	100%	100%

Q29. What are the main problems your organization faces in granting and enforcing privileged user access rights? Please select your top three choices.	FY2019	FY2016
Takes too long to grant access to privileged users (not meeting our SLAs with the business)	41%	47%
Too expensive to monitor and control all privileged users	26%	30%
Too much staff required to monitor and control all privileged users	10%	14%
Cannot apply access policy controls at point of change request	20%	23%
Granting access to privileged users is staggered (not granted at the same time)	9%	8%
Cannot keep pace with the number of access change requests that come in on a regular basis	57%	61%
Lack of a consistent approval process for access and a way to handle exceptions	48%	41%
Difficult to audit and validate privileged user access changes	33%	32%
Burdensome process for business users requesting access	43%	37%
No common language exists for how access is requested that will work for both IT and the business	11%	7%
Other (please specify)	2%	0%
Total	300%	300%

Part 4. Significance Scenarios. In your opinion, how will each of the following situations affect your organization's access governance process, especially concerning privileged users? Please use the scale from very significant impact to no affect. **Very Significant and Significant responses combined.**	FY2019	FY2016
Q30. Increasing number of regulations or industry mandates	70%	63%
Q31. Outsourcing of infrastructure as a service (IaaS) and Software as a Service (SaaS)	46%	
Q32. The constant turnover (ebb and flow) of employees, contractors, consultants and partners	48%	44%
Q33. Constant changes to the organization as a result of corporate reorganizations, downsizing and financial distress	35%	33%
Q34. Adoption of virtualization technologies or DevOps tooling	56%	51%
Q35. The level of risk caused by privileged users abuse or misuse of IT resources	35%	32%

Part 5. Complementary Security

PAM programs are one part of an overarching IT security ecosystem that includes a number of complimentary areas, including cybersecurity risk and identity management. The following questions pertain to complimentary security areas; please answer this section from the perspective of your overall organization, not just as applied to your PAM program.

Q36a. What kinds of risk data does your organization use for cybersecurity initiative prioritization and decision making? Please check all that apply.	FY2019
Quantitative risk assessment data	55%
Qualitative risk assessment data	37%
We do not use formal risk data for cybersecurity initiative prioritization and decision making at this time	25%
Other (please specify)	4%
Unsure	7%
Total	128%

Q36b. If your organization uses quantitative risk assessment data, what percentage of your organization's initiatives are evaluated via quantitative risk analysis?	FY2019
0 to 25%	15%
26 to 50%	35%
51 to 75%	32%
76 to 100%	18%
Total	100%
Extrapolated value	51%

Q37. What is the primary challenge your organization faces to using risk data to inform cybersecurity initiative prioritization and decision making? Please select all that apply.	FY2019
No defined risk assessment framework	39%
Multiple risk assessment frameworks in use	41%
We collect risk data but do not use it in this way	28%
We do not currently collect data about our risks	30%
We do not currently map our risks	35%
Other (please specify)	3%
Unsure	7%
Total	183%

Q38. Which of the following would most benefit your organization's identity and access management security posture? Please select your top four benefits.	FY2019
Replace/upgrade IAM tool	54%
Acquire/implement PAM tool	49%
Replace/upgrade PAM tool	47%
Replace/upgrade legacy systems	60%
Increased use of data-driven decision making	31%
Cross-system data sharing	36%
Greater automation of access management processes	71%
Tailored guidance from IAM/PAM experts	52%
Other (please specify)	0%
Total	400%

Q39. Please rate the ability of your organization to identify and mitigate risks posed by third-party access to your information resources from 1 = no ability to 10 = high ability.	FY2019
1 or 2	12%
3 or 4	16%
5 or 6	34%
7 or 8	25%
9 of 10	13%
Total	100%
Extrapolated value	5.72

Part 6. Market Study for internal purposes. Only respondents in organizations with a PAM program were permitted to answer these questions.

Q40a. Did/Do you use an implementation or system integration partner to implement, upgrade, or refine your PAM program?	FY2019
Yes	43%
No	51%
Unsure	6%
Total	100%

Q40b. If yes, what factors were most important when selecting a PAM partner? Please select the top three choices.	FY2019
Technical expertise	46%
Program/business process expertise	52%
Domain eminence and market reputation	33%
Trustworthiness	48%
Accelerated time to value	29%
Certified/recommended by PAM tool vendor	42%
Support provided is tailored to the organization's specific needs	50%
Other (please specify)	0%
Total	300%

Q41. What PAM tools does your organization use? Please select all that apply.	FY2019
BeyondTrust	12%
CA PAM	15%
CyberArk	12%
ForeScout	13%
Manual processes	35%
Palo Alto	16%
Thycotic	9%
Other (please specify)	45%
Total	157%

Q42. Is your organization interested in cloud-based, PAM as a Service?	FY2019
Yes	61%
No	38%
Unsure	1%
Total	100%

Part 7. Your role

D1. What organizational level best describes your current position?	FY2019	FY2016
Senior Executive /VP	6%	4%
Director	19%	18%
Manager	22%	21%
Supervisor	14%	15%
Technician	32%	34%
Staff	3%	5%
Contractor	4%	3%
Other (please specify)	0%	0%
Total	100%	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	FY2019	FY2016
CEO/Executive Committee	2%	0%
Chief Financial Officer	2%	3%
General Counsel	1%	0%
Chief Information Officer	52%	54%
Chief Technology Officer	9%	8%
Compliance Officer	5%	6%
Human Resources VP	0%	0%
Chief Security Officer	3%	2%
Chief Information Security Officer	17%	18%
Chief Risk Officer	8%	9%
Other (please specify)	1%	0%
Total	100%	100%

D3. What industry best describes your organization's industry focus?	FY2019	FY2016
Agriculture & food services	0%	1%
Communications	2%	3%
Consumer products	6%	5%
Defense & aerospace	0%	1%
Education & research	1%	2%
Energy & utilities	5%	5%
Entertainment & media	1%	2%
Federal/ central government	11%	10%
Financial services	18%	17%
Health & pharmaceuticals	10%	9%
Hospitality	2%	2%
Industrial & manufacturing	8%	7%
Retail	7%	6%
Services	9%	9%
State / provincial government	8%	10%
Technology & software	9%	9%
Transportation	2%	2%
Other (please specify)	1%	0%
Total	100%	100%

D4. What is the worldwide headcount of your organization?	FY2019	FY2016
Less than 500	15%	13%
500 to 1,000	21%	20%
1,001 to 5,000	29%	32%
5,001 to 25,000	17%	18%
25,001 to 75,000	10%	9%
More than 75,000	8%	8%
Total	100%	100%