One Identity Global Study: Assessment of Identity and Access Management

October 9, 2018

#GetIAMRight

Overview

To better understand the current state of best practices, challenges and technology deployments related to identity and access management (IAM) and privileged access management (PAM), One Identity commissioned Dimensional Research to survey IT security professionals from midsize to large enterprises around the world. A total of 1,005 individuals with responsibility for IT security as a major part of their job, and who are knowledgeable about IAM and PAM completed the online survey. The survey was conducted in August and September 2018. Respondents represented the United States, Canada, U.K., Germany, France, Australia, Singapore and Hong Kong.

Notable Findings

Privileged account practices are poor — and IT security teams know it.

- Nearly **one-third (31 percent) of businesses** use manual methods to manage privileged (or, administrative) accounts.
- **1 in 25 organizations** do not manage administrative accounts at all.
- **Two-thirds (66 percent) of respondents** grant privileged account access to third-party partners, contractors or vendors
- **75 percent** of IT security professionals admit to sharing privileged passwords with their peers at least sometimes, with 1 in 4 admitting this is usually or always the case.
- Only **13 percent of respondents** are completely confident in their PAM programs, while more than 1 in 5 (22 percent) are not confident at all.

31% of businesses use **manual methods** to manage privileged (or, administrative) accounts

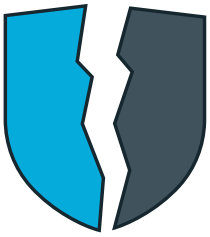
87% express a **lack of full confidence** in their PAM program

Organizations are letting basic access tasks and responsibilities slip — potentially impacting user productivity.

- **68 percent of IT security professionals** take five minutes or longer to unlock a user account or reset a user password.
- Nearly **1 in 10 (9 percent) respondents** admit a single password reset takes more than 30 minutes.
- **44 percent of organizations** take from several days to multiple weeks to provision a new user.
- Nearly **one-third (32 percent) of IT security professionals** take somewhere between several days to multiple weeks to deprovision former users.
- **1 in 20 respondents** having no way to know if users retain access to systems and data even after they've left the organization.
- Only **15 percent of security professionals** are completely confident that they will not be hacked due to an access control issue.

IT security professionals' top fear is disgruntled employees sharing sensitive data — but most admit it's easy to steal.

- When asked to share their worst IAM nightmare, respondents' most common answer (at 27 percent) was a disgruntled employee sharing sensitive information.
- **22 percent of IT security professionals'** worst nightmare is having their CIO interviewed on TV following an IAM-cause data breach, and 18 percent most fear usernames and passwords being posted to the dark web.
- Nearly **8 in 10 (77 percent) of the IT security professionals** polled admitted that it would be easy for them to steal sensitive information if they were to leave their organization.
- **12 percent of respondents** admit that they would steal data if they were mad or upset enough.



77%

of polled IT security professionals admitted that it would be **easy to steal** sensitive information if they were to **leave their organization**.

Summary

Effective IAM and PAM are critical to mitigating cyber risk and maintaining a firm security posture for any organization. These survey results reveal that many businesses across the globe are struggling to implement some of the most basic best practices across both IAM and PAM security disciplines, including but not limited to: resetting a privileged password after each time the account is accessed, and thereby restricting the sharing of administrative credentials; immediately deprovisioning former user accounts; quickly resetting user passwords to maintain user productivity; and monitoring and logging identity activity.

Adhering to these and other IAM and PAM best practices can greatly help organizations reduce the threat of security breaches and other risks due to inappropriate or unsanctioned user access. Conversely, the larger the volume of poorly managed user and administrative accounts available to bad actors, the more damage can be done, such as data breaches and leakage, compliance violations and fines, loss of customer trust, and a tarnished brand.

One Identity is committed to eliminating the IAM and PAM challenges business face today. Our comprehensive suite of access management, identity governance, privileged management and identity-as-a-service solutions and services—all from one source—help organizations Get IAM Right while enabling business agility and digital transformation. To learn more, visit: www.oneidentity.com.