Secure the Keys to Your Kingdom: How IT and Security Leaders Can Safeguard Their Admin Access

Todd Thiemann, Principal Analyst

Abstract: Privileged accounts are a crucial stage in modern attack chains. They offer elevated access to sensitive data and are often the keys that threat actors use to move laterally and exfiltrate sensitive or private information across fleets of endpoints or cloud environments. For the broad swath of businesses and organizations that are not billion-dollar enterprises, IT professionals and service desk leaders can provide a crucial layer of security to their clients. However, they face the difficult challenge of safeguarding their administrator privileges, as well as those across their customer base. They need a solution to support key identity security requirements around privileged access like password rotation, just-in-time access, and account discovery. This approach controls risk, improves efficiency, and facilitates business growth by cultivating a healthier IT-workforce relationship while facilitating additional IT service options.

Privileged Access: The Complexity Conundrum

IT and service desk leaders in small and medium-sized businesses (SMBs) as well as enterprise businesses must navigate an increasingly hostile threat environment where every step toward growth can increase risk and complexity and, thus, result in constant friction in their operations.

Workforces and the IT teams that support them frequently do not understand or appreciate the risk that identity-related threats and compromised privileged accounts can pose. There is a reason why privileged access management (PAM) and access controls are two key security controls that cyber insurers consider when evaluating company insurability.

When one considers the 2025 Change Healthcare attack (and its multi-billion dollar cost to the firm), the risk to IT providers and their end users becomes evident. After all, that incident originated with compromised credentials for a third-party service provider. And more recently, vulnerabilities within Microsoft Outlook and other Windows utilities allowed threat actors to access corporate mailboxes and make off with sensitive password hashes.

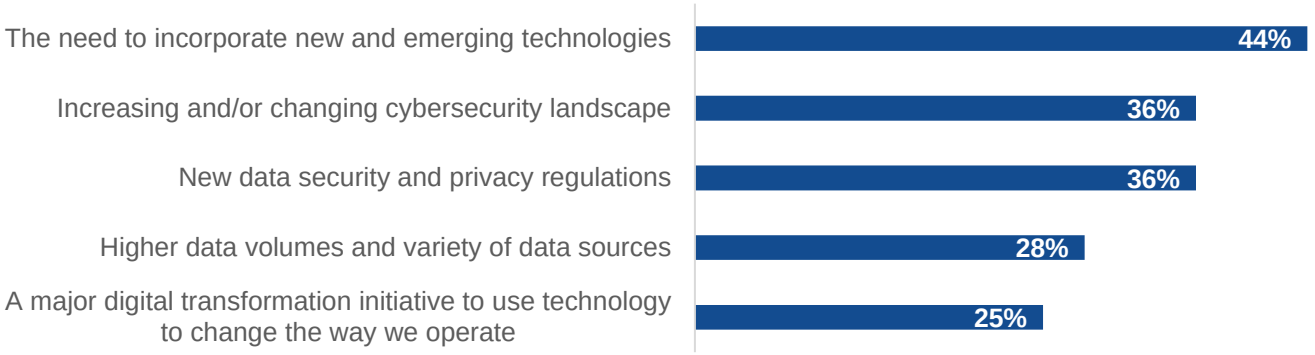
Part of this is due to how IT providers and the workforces they serve face increasing complexity as they conduct IT-driven activities from virtually everywhere and at any time.

Research from Enterprise Strategy Group showed that, for organizations with fewer than 100 employees, 44% believed their organization's IT environment had become more complex over the prior two years due to the need to deploy new and emerging technologies, while 36% of respondents attributed the increased complexity to the changing cybersecurity landscape (see Figure 1).[1]

[1] Source: Enterprise Strategy Group Research Report, *2025 Technology Spending Intentions Survey*, December 2024.

Figure 1. Increasing IT Complexity of SMB Environments

What do you believe are the biggest reasons your organization's IT environment has become more complex over the past two years? (Top five responses, percent of respondents, N=148, five responses accepted)



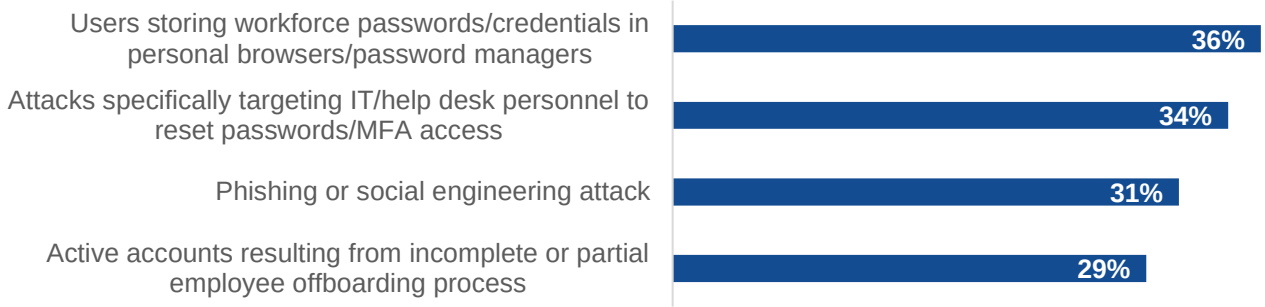
Source: Enterprise Strategy Group, now part of Omdia

For service desk leaders with mid-market customers and larger enterprises, this complexity is particularly acute in the realm of IT operations and PAM. PAM involves all IT businesses providing the least amount of privileged access for the least amount of time.

The security implications become clear when looking at the top factors that contributed to compromised workforce accounts (see Figure 2).[2] Inappropriate password practices topped the list, but of particular concern to IT professionals and service desk leaders is the potential for bad actors to socially engineer help desk staff into unknowingly contributing to a compromise.

Figure 2. Passwords and Social Engineering Continue to Pose Problems

Which of the following contributed to the compromise, or suspected compromise, of your organization's workforce accounts or credentials? (Top 4 responses, Percent of respondents, N=189, multiple responses accepted)



Source: Enterprise Strategy Group, now part of Omdia

[2] Source: Enterprise Strategy Group Research Report, *The State of Identity Security: Opening Doors for the Right Entities and Locking Out the Bad Actors*, July 2024.

Managing privileged admin credentials is a key element of PAM. However, many organizations typically don't have entry-level staff to handle the manual and repetitive work and lack the expertise to manage the access policies an organization needs to properly lock down their privileged access. IT professionals and service desk leaders can help their customers by implementing processes and technology to verify that inbound requests are legitimate and ensuring their own internal security aligns with best practices. Responsible service providers need to follow security best practices by deploying cybersecurity tools to discover anomalous or unseen administrator accounts, implementing just-in-time access for their technicians, and introducing automated password rotations for administrator accounts to reduce their attack surface.

This requires balancing security and convenience. IT professionals and service desk leaders need to ensure security for the workforce systems and data. However, they also need to ensure convenience and avoid imposing unnecessary security "friction" on their business customers.

In addition to the security and efficiency pieces of this puzzle, effectively managing privileged access risk affects other areas of the IT and SMB business.

For example, cyber insurance is a critical layer for protection that enables IT and security leaders to transfer or mitigate some of their financial risk associated with cyberthreats and incidents. Cyber insurance can be difficult to get, and cyber insurance premiums have risen significantly in recent years. A significant element of optimizing the ability to get insurance, also known as "cyber insurability," focuses on having key controls in place. Privileged access controls are typically one of the top controls that cyber insurers consider when evaluating the business.

To better service their workforces, IT professionals should consider investing in PAM solutions that deliver the following benefits:

- **Improved cybersecurity.** Security is integral to any business but is particularly important to IT professionals and service desk leaders. A breach can be immediately catastrophic to any business and cause ongoing harm as existing customers consider other, more secure options. Cyberthreats come in many forms, including insider threats and external adversaries trying to exfiltrate credentials. IT professionals and service desk leaders should be searching for solutions that improve identity security posture and minimize the risk posed by phishing and social engineering attacks.
- **Fulfilled compliance and contractual obligations.** Enterprise compliance requirements are ubiquitous for all businesses, from large enterprises to SMBs. Client compliance requirements flow downstream to vendors providing services to those organizations. The customers' compliance requirement is also the vendors' compliance requirement if the vendor wants to keep doing business with that customer. Compliance frameworks and regulatory regimes like NIST, CIS, CMMC, and HIPAA mandate for safeguards around procedures for creating, changing, and safeguarding passwords and managing privileged access. Contractual obligations, sometimes influenced by cyber insurability concerns, typically include requirements around PAM and password management.
- **Streamlined privileged access and password management operations to scale the business.** With 37% of organizations reporting that they have a problematic cybersecurity skills shortage,[3] IT professionals and service desk leaders need to automate operations to scale the abilities of their existing staff. Empowering customer users with a self-service management approach provides a way to streamline operations and reduce trouble tickets that arise with tasks like password resets.

Organizations that solve these challenges can improve their own operations by enabling their staff to solve privileged access issues more quickly, increase customer satisfaction by providing customers with an improved password operations process, and grow their businesses more quickly and profitably with healthier and "stickier" relationships.

[3] Source: Enterprise Strategy Group Complete Survey Results, *2025 Technology Spending Intentions Survey*, December 2024.

The CyberQP Approach to PAM

IT professionals and service desk leaders looking to better serve their SMB and midsize enterprise constituents' diverse and often-confusing environments need an easy-to-adopt, consistent, and powerful tool for PAM.

CyberQP delivers PAM and end-user access management (EUAM) that enable IT professionals and service desk leaders to protect customer admin accounts and secure their customers' identities and accounts.

The CyberQP portfolio solves key use cases, including:

- **A PAM solution** to accelerate service desk technician productivity. By automating password rotations, privileged account discovery, and documentation, service desks can use just-in-time account and passwordless multifactor authentication to control and limit who has privileged access for specified time periods.
- **Process-based privilege elevation.** This feature permits end users that require temporary admin privileges to install software or change settings on their workstations and avoid persistent local admin access that can expose organizations to excessive cyber-risks. The solution simplifies endpoint privilege management for service desks by empowering IT teams to automatically approve temporary process-based elevation for end-users based on pre-defined rules or on demand so that productivity remains high
- **Privileged account discovery.** Organizations can't control what they don't know about. CyberQP's solution enables organizations to locate and control privileged accounts in customer environments.
- **Control administrator access provisioning.** Tier-1 service desk teams and non-technical staff can complete simple tasks that disrupt technician workflows while minimizing privileged access to Active Directory, Entra ID, or local admin accounts.
- **Identity verification for help desk inquiries,** which enables IT teams and the workforces they serve to avoid impersonation attempts and phishing by providing end-user identity verification for credential resets and when accessing IT-controlled accounts.

Conclusion: Privileged Access Management and End-User Access Management Essential

Businesses of all sizes continue to struggle managing privileged access, credential management, and service desk identity verification processes as they grow rapidly. Organizations want a privileged access management and end-iser access management solution that delivers security while improving efficiency and productivity.

CyberQP is well-suited to solve privileged access and end-user access-related problems to mitigate risk, improve operational efficiency, and enable enhanced sales and margins.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com