

WHITE PAPER

Privileged Password Management: Combating the Insider Threat and Meeting Compliance Regulations for the Enterprise

Sponsored by: Cyber-Ark Software

Sally Hudson
January 2007

IDC OPINION

Reports of ID fraud, ID theft, and system sabotage are all too common in the news today. Living with the threat of these attacks has IT professionals on high alert. The ability to monitor who has access to which systems, when, and at what level of authorization is critical to establishing and maintaining security best practices. Much of this monitoring is accomplished with identity and access management (IAM) technologies. However, as organizations scramble to secure their perimeters and encrypt their data, who is guarding the guards — that is, the systems administrators and others with privileged access to system passwords from within?

With compliance regulators breathing down their necks, most IT organizations are understandably reluctant to discuss this real but ugly truth — insiders with privileged password access pose a significant threat. IDC believes that the risk of internal data misuse can be significantly mitigated by implementing policies that demand special treatment for privileged passwords. Such policies include:

- ☒ Privileged passwords must be "personalized" in order to meet compliance requirements. In other words, today's typically generic systems administrator users need to be resolved down to the *actual* user.
- ☒ Corporate policies must require that privileged passwords be changed/reset routinely and on a systemwide basis. Ideally (and pragmatically), this process should be automated.
- ☒ A secure, centralized management and storage capability must be available for privileged password accounts.
- ☒ Reporting and auditing capabilities must be available to underscore security measures and meet compliance regulations.

These types of actions constitute a best-practices approach to privileged password management (PPM), an important component of a sound overall IAM system implementation.

METHODOLOGY

IDC's industry analysts have been measuring and forecasting IT markets for more than 30 years. The actual strategy for doing so incorporates information from three different, but interrelated, sources:

- ☒ Product briefings, press releases, and other publicly available information (IDC's analysts meet with hundreds of vendors each year. These briefings provide an opportunity to review current and future product strategies, revenue, shipments, customer bases, target markets, and other key product information.)
- ☒ IDC demand-side research (This includes thousands of interviews annually and provides a powerful perspective for assessing competitive performance. IDC's user strategy databases offer a compelling and consistent time-series view of industry trends and developments.)
- ☒ Direct conversations with technology buyers (These conversations provide an invaluable complement to the broader survey-based results.)

IN THIS WHITE PAPER

In this white paper, IDC reiterates the severity of and threat to corporate IT posed by insider attacks, especially those insiders with privileged access rights. As systems become increasingly open and remote access is increasingly common, privileged users have more opportunities than ever before to exploit security and policy weaknesses as never before. This paper explores the concept of PPM and looks at a product from Cyber-Ark that is designed to provide a secure, automated, and integrated solution to this problem.

IDC research shows that government and industry compliance regulations are driving more than 70% of all IAM implementations within IT enterprises. The ability to provide secure and automated PPM is a technical cornerstone in achieving compliance for these organizations.

SITUATION OVERVIEW

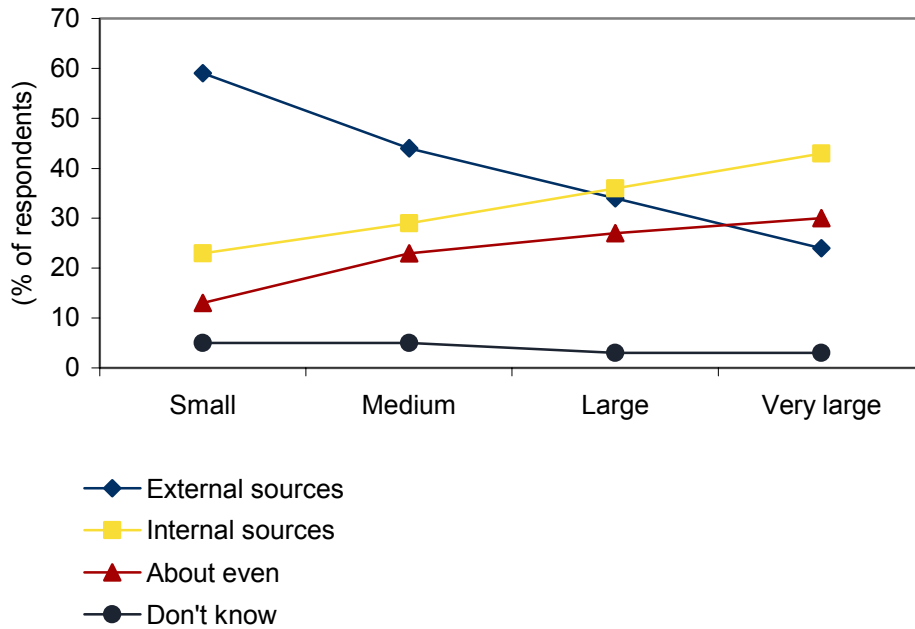
IDC research shows that spammers, hackers, and crackers are still top of mind for the majority of enterprise IT organizations. However, as companies move to secure their perimeters, there is an increasing, uneasy awareness of the inherent risk posed by those inside, not outside, the organization.

Figure 1 illustrates that while IT is taking appropriate measures to keep intruders out, there is growing concern for how to best thwart threats posed from employees within — especially those employees with system access to sensitive information. Systems administrators, high-level IT personnel, and developers have access to privileged passwords — the keys to the IT kingdom, as it were — and thus they possess the power to unleash havoc within a corporation if left unchecked.

FIGURE 1

Internal Versus External Security Threats to Enterprise IT Infrastructure by Company Size

Q. *Do you believe that the most serious threats to your company's enterprise IT infrastructure originate from internal or external sources?*



Source: IDC, 2007

Privileged user accounts have been aptly characterized as the most powerful accounts defined within an IT enterprise environment. Privileged passwords run on critical applications and servers, operating systems, and databases. Often generic in nature, they include, but are not limited to, generic accounts such as administrator on Wintel platforms, root on Unix systems, DBA passwords, and hard-coded passwords found in application scripts throughout an enterprise. If the password becomes known, multiple systems are at risk.

Today, in most organizations, we find that people use the same password value for many systems and devices. This reuse creates a common security hole that can be exploited by external hackers. System intruders use valid credentials to log in as a privileged user and a target system because the privileged password was either the default value provided by the manufacturer or was very weak, easy to guess, or simple enough that a password cracker program could be successfully deployed within a short period of time.

While all of the platforms accessed via a privileged password are critical and vulnerable, a particularly complex situation arises with embedded application passwords. When two unattended software applications connect, they require a powerful username and a powerful password, which are often stored in clear text or embedded in the application code, configuration file, or script. A recent Cyber-Ark

password survey revealed that 20% of enterprises have more than 1,000 applications and that 42% of enterprises reported that they never change these passwords. This situation poses serious security risks and an untold number of compliance violations as these powerful, embedded passwords are gradually distributed *undetected* throughout an organization.

Unfortunately for IT, the tasks of maintaining, storing, changing, and monitoring these passwords and their privileged users are expensive and daunting. There are often thousands of privileged passwords at all levels — devices, embedded, laptops, and so forth — and changing these passwords on a routine basis is impractical, if not impossible, to do manually in any time-effective manner.

It has been estimated that changing the systems administrator password on a *single* Microsoft Exchange Server takes approximately \$30 in man hours/labor. When this single instance is multiplied by the number of servers within an organization — and other devices, embedded applications, local administrative functions are added — the cost/time factor rapidly spirals upward. IDC estimates that the yearly cost that would be incurred for manually changing privileged passwords on a monthly basis would average more than \$500,000 for the typical Fortune 2000 company. Further complicating the issue is that many, if not most, privileged passwords are generic in nature and lack the personalization necessary for tracking and auditing purposes. No wonder so many organizations have let PPM slide to the bottom of the list of security tasks! To date there have not been many efficient or cost-effective methods for tackling this problem.

The recent uptake in computer-related ID theft and fraud, coupled with corresponding legislation demanding compliance for computer privacy and security, is forcing the issue of internal users and privileged access into the open. It has created a situation for corporations to deal with today or face legal penalties and stricter scrutiny in the future.

Fortunately, solutions are available that secure, automate, and audit privileged password accounts. We classify these offerings as PPM solutions. It is critical to both security and compliance to provide a strong and unique password for each target system being managed by a PPM solution.

Perception of IT Threat Source: Internal Versus External

According to the 2005 CSI/FBI Computer Crime and Security Survey, system security incidents were committed by insiders about as often as by outsiders. Organizations now realize that often the greater threat is posed by employees, both former and current. System attacks or sabotage by insiders is often orchestrated when employees know their termination is imminent, and in some cases, disgruntled employees have been able to gain access after being terminated.

A 2005 insider threat case study by CERT/SEI revealed the following:

- Most insiders had acted out in the workplace.
- The majority of insiders planned their activities in advance.
- Less than half of all insiders had authorized access at the time of the incident.

These statistics are sobering. The study also revealed that the majority of insiders compromised computer accounts, created unauthorized back-door accounts, or used shared accounts. It also showed that remote access was used to carry out the majority of the attacks and that the majority of the insider attacks were detected only after the damage was already done. It was determined that system logs were the most prevalent means by which the insiders were identified.

A significant potential threat of unauthorized use is when employees quit or are terminated and there is no coordination between the personnel department and the computer center. In some cases, employees still have system access and an email account after they have left an organization. This situation becomes even more grave when we consider the information outlined in the following section.

Regulatory Compliance and Auditing: Meeting These Demands Today

IDC research shows that increased compliance regulations and the enforcement of these regulations will continue to be the primary drivers of IAM security product sales and implementations in 2007 and 2008. This need will span a variety of industries and be felt on a worldwide basis. The sheer volume and demands of the regulations can seem overwhelming, and the penalties for failure to comply with these mandates can be very costly.

The regulations most often referred to include:

- ☒ **Basel II/CRD.** This is a round of deliberations by central bankers from around the world, under the auspices of the Basel Committee on Banking Supervision (BCBS) in Basel, Switzerland, aimed at producing uniformity in the way banks and banking regulators approach risk management across national borders. The European Parliament definitively signed the Capital Requirements Directive (CRD) in June 2006. The CRD adopts the regulatory requirements introduced by the Basel II agreement signed in 2004. The deadlines for European credit institutions and investment companies are the beginning of 2007 for the adoption of the basic or medium-level approaches of the Basel II agreement and 2008 for the adoption of the advanced approaches.
- ☒ **Sarbanes-Oxley Act of 2002.** In the wake of recent financial scandals, the Sarbanes-Oxley Act of 2002 requires public companies to validate the accuracy and integrity of their financial management. IDC believes this act will have long-term effects on federal securities regulation, corporate governance, and the regulation of auditors. Sarbanes-Oxley requires businesses not only to document and assess their internal controls but also to control access to financial systems. Section 404 covers internal control activities during the creation of financial reports and points to compliance risks that can be addressed by IAM solutions.
- ☒ **Gramm-Leach-Bliley Act.** The Gramm-Leach-Bliley Act mandates privacy and the protection of customer records maintained by financial institutions. These security requirements include access controls on customer information systems, encryption of electronic customer information, procedures to ensure that system modifications do not affect security, and monitoring systems to detect actual attacks or intrusions.

- ☒ **SB 1386.** California's Information Protection Act requires companies to report security breaches involving private consumer information. Personal information is defined as social security number, driver's license or California ID card number, account number, or credit or debit card number in combination with a required security code, access code, or password that permits access to an individual's financial account.

- ☒ **European Union (EU) Data Protection Directive.** Member countries are mandated to adopt standards for the collection, storage, and disclosure of personal data. This directive also outlines individuals' rights concerning their personal data. It is described as the most ambitious and stringent data privacy initiative, and the guidelines to ensure that data is transferred outside the EU only when it is adequately protected have extraterritorial implications on businesses. The U.S. Department of Commerce worked closely with the European Commission to develop a "safe harbor" framework to enable U.S. businesses to meet EU privacy regulations.

- ☒ **Payment Card Industry (PCI) Standard.** Regulated by an industry body that includes MasterCard, Visa, American Express and Discover Card, the PCI standard applies to any company that transmits or processes credit or debit card information. The standard establishes network security and business practice guidelines including deadlines, auditing requirements, and stiff penalties for noncompliance in order to protect cardholders' account and transaction information.

- ☒ **Homeland Security Presidential Directive/HSPD-12 (policy for a common identification standard for federal employees and contractors).** The primary objectives of HSPD-12 are the development and deployment of a federal government-wide common and reliable identification verification system that will be interoperative between all government agencies and serve as the basis for reciprocity between those agencies. In response to HSPD-12, the NIST Computer Security Division initiated the Personal Identity Verification (PIV) project and established the Federal Information Processing Standard (FIPS PUB 201).

Coupled with these compliance mandates, budgetary and staffing constraints will continue to drive organizations to look for better ways to cost-effectively manage their security infrastructures. It has become evident in the IT industry that IAM products are a key component of a compliance platform. To date, the internal controls and technical requirements for user access rights and controls for regulatory compliance have been largely vague.

IDC research suggests that the following are among the most common sources of compliance failures:

- ☒ Unresolved segregation of duties that inadvertently enables accounts with "superuser" access rights

- ☒ Failure to control the number of users with superuser access to files in production and in network share files

- ☒ Failure to adequately reference and secure data in custom applications
- ☒ Inability to properly document manual processes and reconcile these processes to the IT systems used
- ☒ Failure to manage and deprovision orphan accounts in a timely manner
- ☒ Inability to adequately secure access to operating systems and databases that support corporate financial applications and transactions

The ability to personalize privileged accounts will greatly reduce many of these issues for IT management. IDC advocates that IT managers and senior compliance officers follow a path of proactive prevention rather than reactive correction education in these matters in order to increase security while meeting and enforcing compliance mandates.

A Look Inside the Systems Administrator World: A Vast Topology

It is a little known and disturbing fact that most organizations have more privileged user passwords than personal passwords. Those with access to privileged passwords possess the power to change system data, user access, configuration, and so forth. They also have the power to easily sabotage the critical IT operations of any organization. On a nonmalicious scale, users often unknowingly place an organization in compliance violation by using the generic passwords for systems configuration and other activities. This is perhaps the greatest and most common threat today. Consider the following privileged account types commonly found in Fortune 2000 companies:

- ☒ **Administrative accounts.** These include shared predefined passwords, such as Unix root, DBA accounts, and Windows domain; shared passwords, such as those for help desk, fire call, developer accounts, and the like; and passwords owned by the system and not assigned to any single person or "identity." Privileged access means that the systems administrator could have full control of the configuration/setup of the target server as well as full access to all of the data on that machine. These passwords are extremely critical to overall system access and functionality, and in order to meet compliance regulations, organizations must address this issue.
- ☒ **Application accounts.** These are the hard-coded and embedded passwords for application IDs, testing scripts, and batch jobs. There are also Service Account passwords for Windows Service Accounts and Scheduled Tasks. This application-to-application process has transformed the way we do business and is growing exponentially with Internet enablement. The danger of these application-embedded passwords being misappropriated or mishandled is growing accordingly, and IDC advises organizations to take measures to account for and manage these passwords on a regular and timely basis.

☒ **Personal computer accounts.** These are most commonly associated with the Windows local administrator and include desktops and laptops — easily numbering into the thousands for many enterprise organizations. Given the sheer number and scope of the machines and devices associated with these privileged accounts, the risks of misuse and mismanagement are all too painfully obvious. These types, when taken in aggregate, push the sheer number of privileged passwords found within a typical Fortune 2000 company into the thousands. The chaos that could ensue from a renegade superuser account is almost too horrific for most of these organizations to contemplate.

The first logical step in helping to prevent this type of privileged user-initiated catastrophe (from an IT perspective) would be to utilize PPM capabilities to personalize the generic accounts; create a strong, unique password for each of these accounts; and then set up a system to regularly monitor access and use. A centralized form of management is ideal, and automated alerts and recommendations must be put into place for this approach to be effective. While all this would have been almost impossible in the past, due to complexity and time required, the implementation of a PPM system will go far in alleviating this situation by providing both the personalization and automation required in this instance.

It is often mandated that end users change their passwords routinely, perhaps monthly, quarterly, or annually. This security policy is not extended to the privileged password community because attempting such a task manually is extremely complicated and would entail hundreds of hours and dozens of employees often dispersed geographically around the world. Further complicating an already complex issue is the ability to provision/deprovision system access when employees are hired and terminated. While this is always important at any level of an organization, it is extremely critical when the former or soon-to-be former employee is a systems administrator or developer with access to privileged passwords.

Identity and Access Management as a Solution

There is a growing market for IT professionals to utilize IAM technologies to make their jobs easier. One of their most pressing problems is widespread access to root administration. Shared, generic passwords make users impossible to identify and therefore put the organization at huge risk of compliance violation. The ability to personalize account passwords or password names not only aids overall security but also allows the IT manager to track system server configuration processes for education and remediation purposes.

IAM is about the who, what, where, why, and when of system access. IDC defines the IAM market as a comprehensive set of solutions used to identify users in a system (e.g., employees, customers, contractors) and control their access to resources within that system by associating user rights and restrictions with the established identity. This is accomplished via implementation of some or a combination of the following technologies within an organization: Web single sign-on (SSO), host SSO, user provisioning, advanced authentication (which includes PKI), legacy authorization, and directory services. These technologies are all critical components of IAM.

IDC research shows that industries are looking to IAM technologies to solve the following issues:

- ☒ Compliance with both government and industry regulations
- ☒ Increased security, especially to prevent identity fraud and identity theft as well as to protect privacy and system integrity
- ☒ Auditability, which refers to who was accessing what information when within the system (Automated auditing and reporting capabilities have become part of the cost of doing business for the majority of organizations worldwide.)
- ☒ Accountability, which includes access and permission rights as well as who granted them and when and why they were granted (The granularity and flexibility required today go beyond simple directory management and are increasingly achieved via provisioning and other IAM products. They are becoming essential to managing and ensuring security in both large and medium-sized businesses.)

IAM technologies are now considered a critical component of IT infrastructure in thwarting insider, as well as outsider, threats and helping organizations meet governmental and industry regulatory mandates. A sometimes overlooked but critically important piece of a total IAM enterprise solution is the ability to adequately implement and enforce PPM policies.

Provisioning software, developed to manage identities and grant and restrict access privileges for employees and contractors within an organization, often drives the request for password changes. However, managing secure access to privileged accounts such as those previously described is typically outside the scope of today's provisioning software programs.

Ideally, PPM and provisioning should be integrated within the corporate environment. The ability to provide administrative self-service checkout for privileged passwords, combined with the capability of removing embedded privileged passwords from applications within an IAM infrastructure, can prove to be of significant value to organizations tasked with meeting ongoing compliance goals.

Getting Down to the Core PPM Problem: Secure, Automate, Personalize, Audit, and Simplify

To address the PPM problem that is so pervasive in enterprise IT today, one must first acknowledge its existence. As the world has evolved to open standards-based, wireless and distributed computing, security requirements have increased exponentially. Add to this the vast privileged password scenarios outlined above, and integrating a PPM solution into a large and already complex amorphous environment seems almost impossible. However, the ability to do so aids enormously in the compliance auditing, reporting, and tracking process.

The first step is to locate and label (or personalize) these passwords and then apply the appropriate security parameters for access, change, and control. Given the size and distribution of most enterprise organizations today, this task is, practically

speaking, insurmountable without the aid of automation. Ideally, there should be a centralized management function, or dashboard, available to make this monitoring process easier. All of this PPM activity must be audited regularly by appropriate internal systems management and external regulatory sources.

Fortunately, solutions are available to secure, automate, and audit privileged password accounts. We classify these offerings as PPM solutions. One of the vendors currently offering products in this category is Cyber-Ark Software, a privately held software security company based in Newton, Massachusetts.

Founded in 1999, Cyber-Ark offers corporations Enterprise Password Vault (EPV), a unique password management system that incorporates the company's Central Password Manager technology. Central Password Manager is designed to allow organizations to change privileged passwords automatically on remote machines, applications, and operating systems and store the new password securely in the Password Vault. These tasks can be accomplished without human intervention and can be completed rapidly and in accordance with corporate policy. Cyber-Ark EPV is used by Fortune 1000 customers, such as T. Rowe Price, ING, and KeyBank, as well as Global 2000 companies and government organizations throughout the world. Customers include government, financial, and pharmaceutical organizations.

The Enterprise Password Vault: A Complete PPM Solution

Cyber-Ark characterizes EPV as a "safe haven" within the enterprise where all privileged users' passwords can be securely archived, transferred, shared, and managed by authorized users, including individuals such as IT staff, on-call administrators, and local administrators in remote locations. This PPM solution features multiple security layers (including firewall, VPN, authentication, access control, dual control, encryption, and more) that make up the core of the Vault. They are assembled to offer organizations a comprehensive security platform for storing and sharing privileged passwords in an enterprise environment.

Inside the Vault are storage units called Safes, which are designed to give IT professionals flexibility and choice when organizing privileged passwords according to unique corporate requirements. Each Safe is configured with a specific list of users who have been granted authorized access — all others remain unaware of its existence. Within the Safe, additional security parameters enable the administrator to determine which activities each user can carry out on the passwords. For example, each privileged password that is stored in the Safe resides in a unique password object that consists of the password and its properties, which are the details required to log on with this password. Properties include the user name, the machine's address, the type of password, the database name (if appropriate), and so forth. All these properties are dynamic and can be specified and changed by authorized users.

Password policies define the type of password that is allowed and how frequently the password must be changed. The type of password indicates the rule that applies to the password, such as the minimum number of characters required for the password, the type of characters, and so forth. The frequency of the password change indicates whether the password must be changed at regular intervals or if it is a "one-time" password that must be changed after having been accessed.

This PPM solution is designed to support as many password policies as necessary to meet organizational requirements. A policy might apply to individual passwords or to a group of passwords. The password policies are stored in a different Safe from the passwords so that only users with authorization to enter the Safe can access the password policies.

Cyber-Ark's EPV is a plug-and-play PPM solution and reportedly is installed with minimal effort and time. It can be accessed and managed through a Windows Client, a Web interface, or a variety of APIs, making it easy to integrate with existing systems and software products. The latest version of the product provides out-of-the-box support for Windows, Unix, Linux, Solaris, AIX, z/OS, HP-UX, and IBM AS/400 operating environments. Additionally, credential storage support includes Microsoft Active Directory (AD), Unix Kerberos, and Unix NIS. All major databases are supported, including any ODBC-compliant database. The Vault supports leading network devices, such as Check Point FireWall-1 and Cisco routers. Other features include:

- Customizable user and administrator profiles
- Email notification
- Integration of verification and alerting system
- Central dashboard for displaying PPM data
- Bottom-up analysis and design around users and their usage of PPM

FUTURE OUTLOOK

IDC believes that organizations will increasingly step up controls and prevention measures to safeguard their systems from the threat of inside-the-walls attacks and to meet compliance regulations. To address this issue, corporate best-practices policy guidelines for preventing insider attacks should include the following suggestions:

- Establish clearly written and communicated security procedures and policies for all levels of the organization, and enforce the familiarity of these rules and policies for all employees. This would include everything from prohibiting passwords written on Post-its to enforcing random audits at the highest employee levels.
- Define and implement a strong provisioning program. This would include effective separation of duties based on the implementation of least privilege. Least privilege is authorization only for the resources required for a specific employee to successfully complete his or her job.
- Implement and enforce strict password and account management policies. Take measures to severely curtail insider opportunity to circumvent both manual and automated mechanisms that are in place to prevent such attacks.

- ☒ Continually monitor, audit, and report all online actions. This is critical to preventing ID theft and fraud, as well as key to meeting compliance requirements at both the government and industry-specific levels. The ability to monitor and audit employee system behavior allows organizations to uncover suspect insider actions and prevent serious system damage.
- ☒ Establish rigorous standards and policies specifically for systems administrators and other privileged password users.
- ☒ Implement a comprehensive and easily integrated provisioning system to ensure that employee access is immediately terminated to all systems upon employee termination.
- ☒ Ensure that secure backup and recovery processes are in place in the event of system disruption or failure.
- ☒ Never underestimate the human factor. Be aware of suspicious behavior and listen when employees become angry or disgruntled. Don't minimize or trivialize; acknowledge that when something doesn't seem quite right, it probably isn't.

IDC's *Worldwide Identity and Access Management Forecast, 2006–2010*, published in August 2006, anticipates that organizations will spend more than \$5 billion on IAM technologies by 2010. We anticipate that PPM technology purchases will be included on those shopping lists as corporations realize that "guarding the guards" is a core component of their IAM strategies for achieving compliance and systems security.

CHALLENGES/OPPORTUNITIES

Perhaps the biggest challenge faced by Cyber-Ark today is the reluctance of corporate IT to openly recognize that opportunists may exist among their own ranks. As data such as that provided by the 2005 CSI/FBI Computer Crime and Security Survey continues to surface, IDC believes that corporations are now more willing to face the more unpleasant facts of life and deal head on with the situation. Further complicating this scenario is that historically there have been no easy solutions to the privileged password problem — as illustrated in this paper, a regularly implemented manual solution would require too much time and too much money to be effective in a large organization. Couple this with difficulty in effectively integrating PPM with existing directories or provisioning solutions for monitoring and enforcement, and it is understandable why many corporations are slow to tackle this issue.

The largest opportunity for Cyber-Ark is that comprehensive, automated, and easily integrated enterprise-class PPM systems are few and far between these days. If Cyber-Ark can continue to reassure buyers and prospects that its EPV solution is a cost-effective way of solving a critical problem while also helping to meet compliance goals, we believe the company is well-placed for success in the coming months and years.

CONCLUSION

Insider sabotage and data theft are becoming increasing problems within enterprises worldwide. These issues are being seen across many industries today, including finance, retail, travel, government, and education.

IDC believes that the risk of internal data misuse can be significantly mitigated by implementing policies that demand special treatment for privileged passwords. They include the ability to disable an employee's system access promptly upon employee termination; enforcing a companywide password change on a regular basis; and implementing reliable auditing and reporting systems.

There should be corporate mandates that privileged passwords be changed/reset routinely and on a systemwide basis; ideally (and pragmatically), this process should be automated. Additionally, centralized management and storage capability for privileged password accounts is optimal from a security perspective. These types of actions constitute a best-practices approach to PPM, an important component of a sound overall IAM system implementation.

Companies such as Cyber-Ark that offer a PPM solution are well-positioned to assist organizations in preventing unwanted insider attacks.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.