ESG Brief

Advanced Cyber Threats Demand a New Privileged Account Security Model

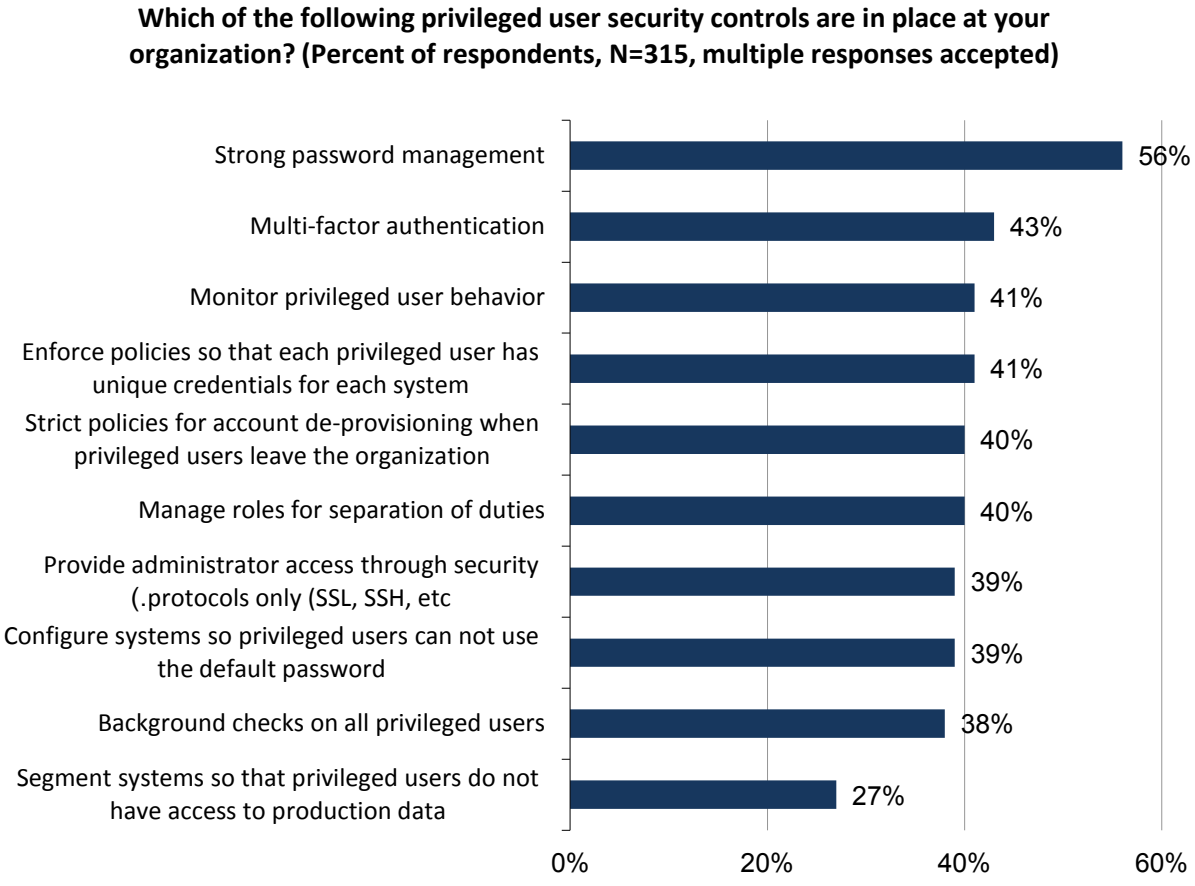
Date: June 2013 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: *In spite of marginal progress, privileged accounts remain vulnerable. Why? Sophisticated cyber attacks like APTs take advantage of informal processes, weak security controls, and monitoring limitations to target administrator accounts, compromise their systems, and gain access to valuable IT assets. Tactical changes don't go far enough. Rather, CISOs need to think in terms of a privileged account security architecture offering central control, management, monitoring, and oversight of privileged accounts for IT assets throughout the enterprise.*

Overview

Over the past few years, many organizations finally recognized the chaos associated with privileged account security and made a number of tactical changes. For example, ESG research indicates that more than half of organizations implement strong password management, 43% use multi-factor authentication, and 41% regularly monitor privileged user behavior (see Figure 1).[1]

Figure 1. Privileged User Security Control Usage



Source: Enterprise Strategy Group, 2013.

[1] Source: ESG Research Brief: *Deployment of Privileged User Access Controls at Enterprise Organizations*, September 2012.

To date, privileged account projects have focused on two primary issues:

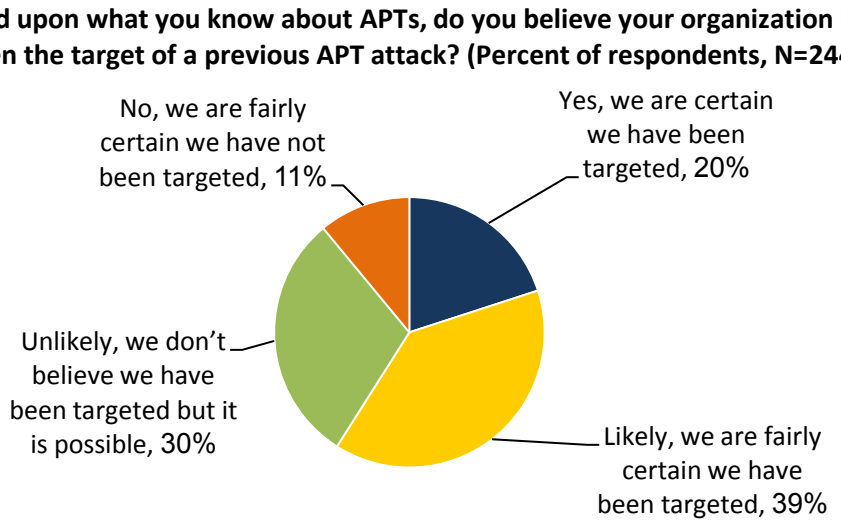
- **Compliance and audit requirements.** Industry and government regulators recognize the risk of a security breach associated with privileged users with access to sensitive systems and data. As a result, regulations such as FISMA, GLBA, NERC, HIPAA/HITECH, Basel II, and PCI demand privileged account security controls and auditing. Given the current state of cybersecurity, it is likely that subsequent regulations will stipulate further privileged account oversight. Smart security executives are anticipating these regulatory changes with incremental security controls and monitoring.
- **Visible insider attacks.** In 2008, a network administrator working for the City of San Francisco configured the network so that he and he alone had administrator rights to all Cisco switches and routers. Apparently, the administrator had an altercation with the city's new CIO, refused to divulge the passwords he had set up, and subsequently disappeared. He was later arrested but refused to divulge the password until he was persuaded to do so by the Mayor five days later. This and other incidents illustrate the magnitude of risk here. No organization wants a rogue IT administrator to disrupt business processes or leak sensitive data to WikiLeaks.

While these trends are driving more privileged account oversight, ESG believes it is time to recognize that a third and perhaps more dangerous threat also needs to be addressed.

Hackers Are Targeting Privileged Accounts

While organizations have made marginal adjustments to privileged account security over the past few years, they are likely missing a new type of dangerous threat. Historically, privileged account security was really set up as a countermeasure for a rogue employee like the San Francisco network administrator described above. Yes, this is a security best practice, but it ignores a new type of threat: Privileged accounts are used as part of sophisticated cyber attacks conducted by organized criminals, nation states, and hacktivists. Since the Advanced Persistent Threat (APT) attack on Google in 2010 (Aurora), many organizations have come face to face with this very type of situation. Just how widespread are APTs? ESG research indicates that 59% of enterprise organizations are certain or fairly certain they have been the target of an APT (see Figure 2).[2] It is worth noting that the APT threat is also exacerbated by IT trends such as SOA, mobile devices/BYOD, and cloud computing that open enterprise IT to additional threat vectors. This is likely to make enterprises even more vulnerable to attacks moving forward.

Figure 2. Enterprise Organizations Are Often the Target of APTs



Source: Enterprise Strategy Group, 2013.

[2] Source: ESG Research Report, *U.S. Advanced Persistent Threat Analysis*, November 2011.

So what's the connection between APTs and privileged accounts? APTs usually begin with a social engineering exploit like spear phishing to trick an insider into downloading a malicious executable. Once a single system is compromised, it is then used as a beachhead for network scanning, credentials harvesting, and account escalation. As the attack escalates, hackers actively seek out and compromise privileged accounts since they can open the door to critical systems and sensitive data for exfiltration.

Unfortunately, APTs have had a strong success record when it comes to compromising privileged accounts. Why? In spite of the basic security actions described above, privileged accounts remain extremely vulnerable because:

- **Password management remains marginal at best.** While many organizations take basic steps like disabling default passwords and requiring passwords of a certain length and format, these are baby steps toward strong authentication and privileged account security. Many privileged users depend upon the same password for a multitude of systems, so a password compromise could grant root access to many servers while that access remains anonymous since it is a shared privileged account. Privileged user provisioning can be difficult to track while accounts may become dormant and remain useable long after individual administrators move on. Finally, privileged account management is often anchored by manual, time-consuming tasks performed on an infrequent or as-needed basis—hardly a best practice for proactive monitoring or high security. In aggregate, it can be extremely difficult to look at any privileged account activity and determine whether it originated from a specific IT administrator or a command-and-control server in Odessa, Ukraine.
- **You probably have many more privileged accounts than you think.** Enterprise IT infrastructure is large, growing, and often distributed. Many organizations also have many administrative users (i.e., contractors, vendors, service providers) beyond their direct IT admin staff. This can add up to a very large number of visible and hidden privileged accounts—and significant risk.
- **Privileged accounts are spread and managed across the enterprise**. While some organizations use a central directory like Active Directory for account creation, privileged accounts tend to be spread across an army of networking equipment, servers, applications, storage devices, and security appliances distributed and managed across the enterprise. In many cases, there is no central control or secured storage of privileged accounts but rather a "best effort" to manage distributed chaos. Yes, privileged account security may leverage some IT infrastructure tools for help, but there is no central policy management, configuration management, or monitoring.
- **It is difficult, if not impossible, to detect anomalous behavior.** Many organizations log privileged account activity as part of overall system logging, but this information is buried in a sea of log data and doesn't provide the right level of detail or context. With multiple individual privileged users accessing servers and applications, it can be difficult to understand what constitutes "normal" or anomalous behavior—especially if log files are viewed independently or haphazardly integrated into a SIEM platform. When a security analyst does detect something fishy, it may be impossible to tell whether these activities indicate a rogue administrator or an APT. Finally, tampering with log files is a fairly routine aspect of an internal hack or advanced malware attack. Once an account is compromised, log data will likely indicate that all is well while cyber criminals are reconfiguring systems and exfiltrating valuable data.

Basic controls aside, privileged account security remains fraught with inefficiencies and vulnerabilities—especially at large organizations with a multitude of privileged users, privileged accounts, and IT assets. Meanwhile, CISOs have minimal oversight over day-to-day privileged user management and operations. These shortcomings make privileged accounts easy targets once cyber criminals establish themselves inside the network.

Privileged Account Security Must Address Advanced Malware Threats

New types of sophisticated threats mean that privileged account security must go beyond data center access and surveillance cameras. To address today's risks, CISOs need a comprehensive privileged account security solution in order to establish metrics and assess risk. To achieve this, privileged account management must include:

- **Account discovery.** As the old business saying goes, "you can't manage what you can't measure." Similarly, enterprises can only address privileged account security if they know the extent of the problem by answering questions such as: How many privileged accounts do we have? Do we have any active stale accounts? Who can and has recently accessed these accounts? Which passwords do not adhere to the enterprise security policies? To keep up with constant IT changes and evolving threats, CISOs need tools that can provide this information in an automated, continuous, and timely fashion.
- **A central control point.** Even organizations with ample resources and strong security skills have trouble maintaining security for thousands of privileged accounts on a potpourri of distributed IT assets. Rectifying this situation means centralizing privileged account security control functions like automatic account provisioning/de-provisioning, policy management and enforcement, and reporting. Armed with these capabilities, CISOs can systematically address the privileged account risks upon completion of the discovery phase so they can associate an individual identity with an individual user, delete all stale accounts, and maintain constant situational awareness to measure progress and address problems. Finally, they can apply central policies, such as preventing log tampering on all systems, which can lower overall risk.
- **An architecture built for separation of duties and isolation.** Separation of duties is a fundamental principle of information security and risk management. ESG believes that separation of duties can also be applied within the privileged account security architecture to achieve similar results. For example, privileged account credentials should be removed from individual IT assets and stored in a central repository built and operated for high security. Additionally, administrator access and communication can come through a secure control point that is isolated from target IT assets. This type of architecture effectively decreases the "attack surface" by preventing infected administrator workstations from spreading malware or tampering with applications, databases, and servers configuration settings.
- **Monitoring, analysis, and integration.** Privileged account security should centralize the collection, analysis, and storage of all log information related to administrator activity. Logs and context-based session recordings can then be used to trigger alerts, perform security analysis, or conduct forensic investigations. To enhance IT workflow and security analytics, leading privileged account security solutions will also integrate into help desk/ticketing systems, vulnerability scanners, LDAP directories/IAM systems, SIEM platforms, and big data security analytics platforms.

Privileged account management must also offer enterprise scalability by supporting the widest range of systems, applications, embedded systems, and other IT technologies.

Aside from improving protection and oversight, comprehensive privileged account security as described above can also help lower security and IT operations costs. How? By centralizing workflow, day-to-day activities, and troubleshooting. Improvements in these areas are sure to bolster efficiency.

Cyber-Ark Can Help Address APTs

Many CISOs have implemented network- or host-based controls as a countermeasure for APTs, but privileged accounts remain poorly managed and extremely vulnerable. Yes, security technologies can help, but most are delivered as tactical point tools rather than end-to-end solutions. One exception to this rule comes from Cyber-Ark, a company focused on providing comprehensive and integrated privileged/shared account protection, accountability, and intelligence solutions. Unlike point tools, Cyber-Ark provides an architectural solution for privileged account discovery, central control, separation of duties, and monitoring built with complete end-to-end security from the ground-up. In this way, Cyber-Ark can help organizations address the risk associated with external attacks and insider exploits, detect malicious behavior as it is happening, and accelerate incident response. Given its unique and wide-ranging privileged account

security coverage, CISOs would be wise to assess how Cyber-Ark can help them improve privileged account security and address advanced malware threats.

The Bigger Truth

Information security has changed quite a bit since the aforementioned Google Aurora attack in 2010. APTs clearly demonstrate that black hats are quite adept at circumventing existing security policies, controls, and monitoring tools. Privileged account security is a prime example of an area fraught with visibility gaps and vulnerabilities. Cyber criminals are launching sophisticated targeted attacks on privileged accounts while many enterprises continue to try to safeguard these accounts with minimal protection and sporadic incomplete monitoring. This is a recipe for failure.

There is simply too much focus on advanced malware as it relates to hosts and data, and not enough understanding of APT tactics and escalation. CISOs need to realize that privileged users have a bull's eye on their heads because they hold the "keys to the kingdom" for high-value IT assets like critical applications and sensitive data. Alarmingly, hackers get this situation while many CISOs don't.

It's time that CISOs take a comprehensive and systematic approach toward privileged account security. The only way to do this is to get their arms around their current status, centralize operations and monitoring, and minimize the "attack surface." This demands architectural solutions rather than tactical point tools. Yes, this means spending money and changing the status quo, but smart IT executives can justify these expenses by improving workflows, streamlining security and IT operations, and lowering the risk associated with an APT or insider attack.