THE ROLE
OF PRIVILEGED ACCOUNTS
IN HIGH PROFILE BREACHES

How Privileged Account Security Can Significantly Reduce Risk, Stop Attackers & Prevent Data Exfiltration

By CyberSheath Services International, LLC
Commissioned by CyberArk
May 2014

www.cybersheath.com
# Table of Contents

Executive Summary ............................................................................................................. 3

A Case Study: The True Cost of a “Do-Nothing” Approach ............................................. 5

High Profile Attacks in 2013 Leveraged Privileged Accounts ......................................... 9

Strategic Take Aways For CISOs .................................................................................... 13

About CyberSheath ............................................................................................................ 14
As we examine a cross-section of recent high-profile, targeted, advanced cyber attacks, all indicators demonstrate that our patient and persistent adversaries have recycled many of the same tactics that they have successfully leveraged in years past. While new and sophisticated malware variants were continually developed to exploit systems in 2013, criminals, hacktivists and advanced attacks continued to do the most damage by exploiting privileged accounts to exfiltrate data.

Three themes related to privileged accounts emerged in 2013 as recurring security challenges for organizations of all sizes:

- Proliferation of local administrator accounts across the enterprise, often all sharing the same password
- Excessive use of privileged service accounts with passwords that never expire and the ability to log on interactively
- Lack of accountability around privileged account use

The methodology of advanced attacks is ultimately reliant on the exploitation of privileged accounts for groups to move throughout the network and exfiltrate data undetected. Organized or unorganized, political or state sponsored, these groups may have different motivations, tolerance for risk, and willingness to demonstrate persistence, but they all share the one common trait. Privileged accounts are on their critical path to success 100% of the time in every attack, regardless of the threat. Therefore, having increased visibility and actionable intelligence on privileged accounts within an organization’s IT environment greatly increases the ability to successfully detect and disrupt a compromise.

So what is a privileged account? Why aren’t organizations around the world making it a top priority to protect, manage and monitor them? The answer to the first question is relatively simple; the answer to the second question is complicated and ultimately disappointing.

So what is a privileged account? Privileged accounts represent a tremendous risk as they are routinely used to manage the infrastructure, as service accounts, or by applications to connect to one another. They are found in almost every instance of IT infrastructure, networked device, O/S and application in an organization. Privileged accounts are pervasive throughout an organization of any size because they are absolutely required for the IT department to maintain operations. They are also required by attackers and malicious insiders in order to successfully complete an attack without being stopped by security solutions. Our research shows that the exploitation of privileged accounts has a direct correlation with data loss in a cyber attack.

As for the second question; why aren’t organizations around the world making it a top priority to protect privileged accounts? For starters, there is a shared responsibility issue. In almost every IT organization CyberSheath works with, the authority and management of privileged accounts
rarely sits with the CISO. Instead the “owner of privileged account management” is the VP of IT Infrastructure or someone with a similar title. In this “Responsibility White Space” between security and IT infrastructure, lies the issue. In working towards a balance between ease of administration and protecting access to these accounts, doing nothing becomes the path of least resistance. What many organizations have yet to take advantage of is the maturity of solutions that both protect privileged accounts and facilitate ease of administration through workflow approvals, mobile access and direct connections to managed devices. Protecting, managing and monitoring privileged account access is a business enabler for the IT delivery organization in addition to a critical strategy in the protection against advanced and insider threats.

CISOs are often forced to cast a wide net, ineffectively doing a little bit of everything in an attempt to address the wide range of security threats facing their organization. Unfortunately, this approach breeds more failure than success, resulting in more tools purchased than could ever possibly be effectively deployed given the existing staff. Given that context, in 2013 we saw many CISOs prioritizing their resources by buying tools that were force multipliers rather than point solutions. We witnessed priority being given to products that integrated new security solutions with the existing security investments. Organizations are pushing the data they get from privileged session exploits into their security information and event management solutions for real time operational intelligence. Where previously you had to wait for forensics to be done to find out which privileged accounts had been compromised, now that information is available as it happens with privileged credential management solutions.

In this year’s research, we do a drill down using real, anonymized data from a global Fortune 500 company that deployed a privileged account security solution and realized a 100% decrease in successful attacks. Every year we compile this research based on our experience delivering IT security services for multi-billion dollar global businesses and Government Agencies. Every customer we work with has a privileged account management problem that stems from shared privileged account credentials (ex. local administrators), privileged service accounts or insufficient privileged account analytics to aid incident response. The data we are sharing in this year’s research is a visual illustration of how undeniably vital privileged account protection, management, monitoring and analytics is.

The customer study on the next page is representative of what we see every day: an organization that grew through merger and acquisition for many years and largely avoided any material investment in security generally, or privileged account security specifically. Mandated complex passwords and minimal monitoring of privileged accounts was considered the right balance between a need for security and the ability to do business. Consequently, the organization had been broadly and deeply compromised by an APT to the extent of which will never be completely understood beyond the known data exfiltration. This experience is not unique or in any way an outlier, it is the norm. What was unique, once the compromise was discovered, was the support of the executive board in addressing the problem and the strategic focus of the CISO in protecting, managing, monitoring and analyzing user activity on privileged accounts as a key element of his short- and long-term remediation plan.
A Case Study: The True Cost of a “Do-Nothing” Approach

As with any significant breach, given the nature and sensitivity of the information, confidentiality is paramount. While the customer will remain anonymous, it's useful to draw a profile of their business to set the context for the data we are going to share.

While this is an enormous organization, literally spanning the globe delivering products and services, privileged accounts represent a profound risk for organizations of all sizes.

This company has grown rapidly over several years, largely through acquisitions that were quickly assimilated from an IT perspective with a focus on minimizing disruption to the business. The tactical approach to dealing with privileged accounts was to broadly empower nearly every employee with administrative rights so they could “do their jobs”. This approach led to more than 100,000 privileged accounts in total of which 30,000 were traditional local administrator accounts sharing the same password.

Left unmonitored, the APT took full advantage of the unmonitored privileged accounts, selectively choosing less than 50 at the local and domain level throughout the sustained attack. This ratio is worth noting; 100,000 privileged accounts across the enterprise were available for compromise and ultimately less than 50 were actually used by the APT. The shared local administrator passwords and other privileged service accounts made it easy for the APT to find just a few privileged accounts to exploit. This is the scenario that leads to the “whack-a-mole” approach to incident response and an adversary’s ability to be persistent. No organization can afford the long-term risk exposure that unmanaged privileged accounts present.

When the compromise was first discovered, it was difficult if not impossible to determine the length of time the attackers had gone unnoticed. But given the breadth of the intrusion and value of the systems compromised, it appeared APT actors had been inside the network for at least three years. What can be said with 100% certainty is that exploiting valid credentials and privileged accounts
was a critical and routine tactic of the APT campaign. Given the proliferation of privileged accounts and lack of management or monitoring, the attacker was able to hide in plain sight for several years.

Besides the obvious impact of exfiltrated data and potential customer notifications, the effect of promiscuously granting privileged accounts to end-users was crippling to the IT organization when it came time to remediate the APT intrusion. Without the flexibility to manage password policy and allow users to perform daily tasks in a controlled and audited manner at the enterprise level, the company was forced to remove local administrator rights en masse and grant them back on a case by case basis, manually.

After removal of local administrator rights, call volumes to the help desk increased exponentially as did operational costs. The CIO had to bring in a small army of temporary staff just to deal with the increased call volume from users requesting access for a local admin account. Figure 1 below details the fallout.

![Daily Average Call Volumes and Wait Time for Help Desk](image)

**Figure 1: Daily Average Call Volumes and Wait Time**

The correlation between risk reduction and protecting, managing, and monitoring privileged accounts is undeniable. Post remediation our client was able to ensure server and local administrators worked in a least privileged environment. This also allowed for more granular privileged account policy at the business unit level and absolute accountability of privileged account use by leveraging a privileged account management solution.
In Figure 2 below the reduction in risk exposure was greater than 80% and the ability to better detect and disrupt attacks as a result of having fewer accounts to manage and monitor was an additional benefit of the effort. While reduction of the sheer number of privileged accounts is not an often stated benefit of privileged account security solutions, in our experience, it is always a tangible outcome.

![An 82% Reduction In Risk Exposure](image)

Figure 2: Privileged Accounts

The exploitation of privileged accounts in this case study directly led to more than 200 compromised machines, more than 10,000 man hours of overtime, and a total breach cost exceeding $3 million dollars in a six-month span. All of this could have been avoided with an enterprise privileged account security solution to address internal and external threats.

20/20 hindsight indicates that it would have been better to proactively manage the risk of privileged accounts which would have avoided the resource drain and data loss, but the most important things to do often don’t get done. **Don’t let that happen to you.** Take proactive charge of your privileged accounts and dramatically reduce your risk of data exfiltration and remediation. Every security organization aspires to be more proactive and less reactive, but it’s often an immeasurable goal. Unfortunately, in the domain of privileged account security, the cost of being reactive is easily measured once you realize that you have been breached. Despite volumes of best practice guides and expert recommendation to deal with privileged accounts as a first order of battle, many organizations are bearing the incredible cost of doing nothing until they have been compromised. Every organization has the opportunity to turn this high risk area of exposure into a measureable success story.
In this customer case study, a subsequent focus on privileged account management yielded measurable results in the fight against APTs. In sharing the data here, we hope that CIOs and CISOs will consider the far less painful proactive path by protecting, managing, monitoring, and analyzing user activity on privileged accounts. Map out a strategy for dealing with privileged accounts and then proactively implement that strategy, before the adversary uses them against you.
High Profile Attacks in 2013
Leveraged Privileged Accounts

2013 brought another year of high profile data breaches resulting in intellectual property and financial losses that rivaled previous years’ totals. Most of the breaches that you read about involved the exploitation of privileged accounts, despite a wide variety of targets and motives. Think about that for a second. In the criminal world, what other crime gets repeatedly committed using the same weapon, owned by the victim, regardless of target or motive?

There are not a lot of chances to gain ground previously lost in the domain of cybersecurity. The opportunity represented in protecting, managing, and monitoring privileged accounts is about CISOs taking inventory and accountability of the credentials in their environment. Each of the attacks we detail in this year’s research results from the failure to secure, manage or track the use of privileged credentials.

CyberSheath researched and analyzed 10 well-reported attacks over the last 12 months, all containing elements of privileged account exploitation. We examined how protecting, managing, and monitoring these accounts could have prevented these attacks. As you read through each of the attacks, learn from others’ mistakes rather than repeating them.

The first attack deals with one of, if not the most damaging acts of espionage in the history of the United States. At its core, the attack was carried out through the abuse of valid credentials and privileged accounts.

**EDWARD SNOWDEN AND THE NATIONAL SECURITY AGENCY**

In what was perhaps the best-known case of insider abuse of privileged credentials in 2013, Edward Snowden, a contractor working as a systems administrator for the NSA, convinced several of his co-workers to provide him with their system credentials, according to a report by Reuters. Snowden may have convinced up to 25 employees at the NSA to give him their usernames and passwords under the pretext that he needed them to do his job. Snowden allegedly exploited his elevated system administrator privileges to move laterally to other systems on the network and conduct unprecedented theft and disclosure of classified information.

*Privileged Account Security: Monitoring and analyzing the behavior of privileged account users and the intelligence gained as a result perhaps could have averted what Michael Hayden, former head of the National Security Agency and the CIA, referred to as “…the most serious hemorrhaging of American secrets in the history of American espionage.”*
BLACKPOS MALWARE BREACHES

Several large retailers suffered cyber attacks during the peak shopping season that may have exposed information from millions of credit and debit card records and millions more records containing information such as customer addresses and telephone numbers. Investigative research indicates that the attacks were facilitated using stolen credentials from a third party vendor.

Privileged Account Security: In an interconnected world the risk of breaches that leverage privileged credentials extends beyond the assets you own and manage. Solutions should be implemented to monitor and record the activity of third-party vendors accessing a network in order to terminate malicious activity and provide detailed information for forensics investigations.

COMPROMISE OF THE NEW YORK TIMES

Soon after publishing an article investigating the relatives of the Chinese prime minister, The New York Times found itself under attack. The security firm hired to investigate the incident found evidence that the attackers, after compromising the domain controller, cracked the hashed passwords and used them to gain privileged access to a number of Times systems. Having the keys to the kingdom allowed the attackers to install 45 pieces of custom malware throughout the environment.

Privileged Account Security: The reality is that protection of privileged accounts is a necessity not a luxury. The right set of privileged account credentials, when compromised, provides the attackers with full control of your network including solutions intended to protect the network from an attack.

MACRUMORS BREACHED BY HACKERS

In November of 2013 the MacRumors user forums reported that all 860,000 of its users’ passwords may have been compromised. It appears that the intruders tried to access the password database after compromising a moderator’s account and escalating their privileges.

Privileged Account Security: Having a system that manages password changes, enforces strict accountability and work flow approval for privileged account activity and the associated logging for after-the-fact analysis is the minimum standard of care for privileged accounts.
5 U.S. BANKING INSTITUTIONS
In 2013, a series of financially-driven criminal attacks targeted the “wire payment switch” at several U.S. banks to steal millions from specific accounts. Reports have speculated that the attackers might have targeted bank staff with phishing emails to lure bank employees into installing remote access trojans and keystroke loggers that stole their credentials. In similar incidents, attackers who gained the credentials of multiple employees were able to obtain privileged access rights and handle all aspects of a wire transaction, including the approval.

Privileged Account Security: Not all privileged accounts are created equal and implementing a policy of least privilege will reduce your risk. Define how far users can escalate with or without authorization before monitoring or technical controls halt their progress.

6 DEPARTMENT OF ENERGY
In July 2013, attackers hacked into the Department Of Energy (DOE) Employee Data Repository database by compromising database administration credentials. More than 104,000 records containing PII were compromised. The costs of the DOE breach was approximately $1.6 million for credit monitoring and an additional $2.1 million associated with the recovery and lost productivity.

Privileged Account Security: According to the 28-page investigation report released by the inspector general (IG) of the Department of Energy, the list of failures involved both technical and management issues. Due to the lack of urgency and awareness of information and cyber security matters, DOE continued to allow outdated, unpatched and unsecured systems to operate “even though they were known to have critical and/or high-risk security vulnerabilities.” Software vulnerabilities have dangerous repercussions if privilege accounts are not managed or privilege management best practices are not followed. Deploying privileged management software can greatly minimize the risk of privilege exploitations.

7 SOUTH KOREA DATA-WIPE MALWARE
On March 20, 2013 a synchronized malware attack paralyzed computer networks of at least 3 South Korean banks and 2 of the country’s largest TV broadcasters. Attackers obtained an administrator login to a security vendor’s patch management server and then used it to distribute the malware as a normal software update. Banking transactions were interrupted, ATMs were shut down and bank customers could not use their debit cards. South Korean stocks tumbled after the attacks with the Korea Stock Exchange KOSPI Index losing 1% of its value, according to Bloomberg.

Privileged Account Monitoring: Monitoring of privileged account activity provides the opportunity to stop in-progress attacks and mitigate potential impacts. Any privileged account that can access the network needs to be accounted for and monitored.
VODAFONE

Vodafone announced in September that an attacker, who allegedly worked for the company as a contractor, had gained access to the personal information of approximately two million customers. The incident highlights the fact that internal attacks by malicious users can often only be stopped through monitoring of privileged account use.

Privileged Account Monitoring: Monitoring the activity of privileged users isn’t limited to unauthorized users, but internal abuse and misuse as well. These users don’t have to bypass or hide from security; more often than not, their suspicious activities go unnoticed until it’s too late.

THE WASHINGTON POST

In December 2013 the Washington Post reported that their servers had been breached in what was at least the third intrusion in as many years. The compromise resulted in attackers ultimately accessing privileged credentials such as usernames and passwords. The intrusion was believed to have been discovered relatively quickly and Post spokeswoman Kris Coratti said, “This is an ongoing investigation, but we believe it was a few days at most.”

Privileged Account Security: Finding an intrusion that likely leveraged privileged accounts in a matter of days is a testament to an effective monitoring solution that likely includes the ability to leverage analytics related to privileged accounts. Previous intrusions at the Post had been ongoing for 2-3 years before being discovered. Considering that the Verizon 2013 Data Breach Investigations Report said 66% of breaches took months or more to discover, the Post appears to have made significant progress.

MANDIANT CONFIRMS IP THEFT FROM 140 ORGANIZATIONS

The widely covered APT1 report released in 2013 confirmed the systematic theft of intellectual property for more than 140 organizations across 20 major industries. Mandiant detailed tactics such as a spear phishing campaigns and targeting of privileged accounts such as domain administrators, service accounts and local administrator accounts that were ultimately used to exfiltrate massive amounts of data.

Privileged Account Security: The APT1 report clearly demonstrated the strategic value in protecting privileged accounts and valid credentials. The outcomes realized from failing to protect these accounts have cost more than 140 organizations countless gigabytes of data loss and competitive advantage. And that’s just what’s been documented in the APT1 report. The protection of privileged accounts and valid credentials is a fundamental part of any effective security program.
Strategic Take Aways For CISOs

1. The attacks that matter to your business, the ones that will have you briefing your board on data loss, all exploit privileged accounts 100% of the time.

2. Big company or small, you probably have more privileged accounts than you know about and the risk of exposure they represent makes them urgent priorities.

3. Protecting privileged accounts gives CIOs and CISOs an opportunity to quantify risk reduction and deliver results that can be measured.

4. Opportunities to make a business case for security, actually proving a return on investment and reduction in risk, are exceedingly rare. Privileged accounts are your chance to reduce risk and be a true business partner.

5. Protecting privileged accounts is an opportunity to become a challenging target and take back ground in the fight against APTs.

6. Ideally automated privileged account security solutions that reduce human error, overhead and operational costs are the way to take back ground previously thought lost to APTs.
About CyberSheath

Co-founded by a Chief Information Security Officer for a Global Fortune 500 company & Chief Executive Officer for an Inc. 500 company, CyberSheath applies business discipline to cyber security, enabling our customers to measure risk, meet compliance goals, prioritize investments, and improve overall security posture. We’ve built a global network of best-in-class partners that we leverage as a force multiplier to deliver pragmatic, end to end solutions for our customers. Having been in the trenches as security practitioners and business executives, CyberSheath goes beyond the WHAT (best practices) and delivers the HOW (measurable results).

CONTACT
CyberSheath Services International, LLC
942 Seneca Road
Great Falls, VA 22066
www.cybersheath.com
press@cybersheath.com
1-855-384-8070