



# Take Control of Your Business with Privilege Centric Risk Assessment

Got Privilege? Controlling the power  
and bottom line of your business

April 16, 2010

# Take Control of Your Business with Privilege Centric Risk Assessment

Got Privilege? Controlling the power and bottom line of your business

## EXECUTIVE SUMMARY

The concept of privilege, as it impacts enterprise operations, is critical to assessing, prioritizing and mitigating business risk across the organization. It is broader than the proliferation and loss of control over privileged user accounts. Privileged Account Management, an issue long neglected, is now more or less generally recognized as a serious, albeit seemingly insuperable security issue and compliance challenge.

Taken narrowly, organizations treat privileged accounts—more specifically, privileged identity—as a check-box compliance matter and a break-fix security exposure. Understood holistically, privilege presents enterprises with an opportunity to effectively address a wide spectrum of risk throughout their business operations.

The key to understanding the potential business risk and potential business impact of privilege is that it is not only about accounts, but also about all the *contexts* in which we evaluate business accounts, information, applications and processes, and how they interact.

Understanding and managing privilege cuts across the organization and affects more than the data center. It affects the business in ways that improve efficiency and affect the bottom line.

## WHAT IS PRIVILEGE?

Privilege is not simply defined by a high-authorization user or account role, but by the interdependencies of accounts, activities, applications, data and policies. Understanding these relationships is the key to understanding how privilege translates to risk, not only to security and compliance but to the fabric of your business, including operations, efficiency and business resiliency.

If your business does not have control over their most privileged assets (users, data, applications, etc.) then you do not really have control of your business.

Taking a holistic, privilege-based perspective allows organizations to set and manage policies at a high level, rather than a piecemeal approach. This empowers enterprises to understand risk in its privilege context and prioritize activities to minimize and/or eliminate it.

Let's step back and examine the issue of managing, or, more to the point, not managing privileged accounts, and why they are not always a business priority. We can then see how they fit into a wider, more useful definition of privilege that can accurately reflect risk in terms of the business.

Not long ago, privileged account sprawl was the elephant in the room that organizations generally chose to ignore because it was perceived as simply too difficult, costly and disruptive to the business to remediate. Over time, even medium-sized organizations accumulate thousands of these system, database, application and network accounts.

These accounts and their credentials are shared by users, even those long gone from the company, and are embedded in hundreds or even thousands of applications across diverse platforms. Typically, organizations have long lost track of many of these accounts and who has access to them. They are, to put it mildly, reluctant to address the problem because they dare not risk bringing down or even breaking critical applications and systems.

These business risks generally trump the now generally well-understood security risks inherent in uncontrolled and undocumented user/account privilege, and make regulatory compliance with directives such as Sarbanes-Oxley extremely problematic.

But, privilege is a business matter and, business risk considerations, bound inextricably to security and compliance, must factor into the necessity to address privileged identity management. Consider how to 1) recognize privilege in terms of context, 2) assess risk and 3) prioritize remediation.

We define privilege in terms of high risk to the business and apply the litmus test of privilege in contexts, such as users, accounts, ID's, data and applications. It is not just about users with strong accounts, sensitive information or application IDs directing business processes. An account or process may or may not be privileged in of itself, but may rise to privileged status because of the relationships between them; think in terms of a "wheel of privilege" [see figure].

Viewed this way, privilege is not just about access and authorization. It is also about the process being executed and the fact that this is being viewed from a privileged perspective, and therefore, requires stronger security, closer management and tighter oversight.

Privilege can enter into the equation in one or multiple contexts—accounts, processes, assets, applications and so on. Consider some examples of how contexts help define privilege and the potential business risks:

- A point-of-sale system is not, in itself, privileged, even for the small amount of credit card or personally identifiable information (PII) it may be transmitting to back-end data stores at any given time. Neither the system, nor the process of scanning customer information, nor, particularly, the data is inherently high-risk and therefore privileged. However, an attacker might intercept the transmission from the POS device to the back end, and gain access to the database containing thousands of credit card numbers and PII records. It is that risk that elevates the POS systems and their processes to privileged status.
- A maintenance process for Active Directory groups is not privileged if the admin is managing groups to assign access to a local portal with discounts for employees. The admin is in what we have come to call a privileged account in a narrow sense, but if he is limited to tasks like this, the risk to the business is minimal. However, if an admin is exercising the same process, but this time for groups of admins with high privilege or groups that grant people access to financial systems, that same process becomes privileged.
- A backup process for Web applications may or may not be high risk, although the process is inherently innocuous. If it is an access, authorization and authentication application, the risk is high and it is therefore a privileged operation that requires tight security.
- Data analysts for an oil and gas company evaluate field data to determine the value of a potential drilling site. They are not, by traditional definitions, privileged users; the process and the applications they are using are not inherently high-risk, but the context in which they are working, that is, handling sensitive business data, is high risk. A rival company would love to get hold of this information. In this case, the context that creates privilege is the potential value of the data.
- Performing maintenance work on a database with credit card information carries a privilege context in the data at risk rather than in the maintenance process, and the level of admin authorization, if it exceeds that required to perform the task. The business risks created by poor access control are security (possible data breach), governance and compliance (unauthorized and probably undocumented access), and business interruption if an unqualified admin accidentally deletes production data or changes a configuration.
- A Web server managing a critical application is privileged and critical to the business if it goes down. Securing that server and protecting it from unauthorized access is a high priority.

## What is privilege?

Understanding and applying the concept privilege is to assess corporate risk and prioritize where you spend your money and commit resources on risk mitigation. Privilege is determined by *context*, which determines whether or not an account, application, process or data is privileged and therefore a potential risk to the business.

Business Scenario	What is Privileged?	Type of Risk
<b>Web server goes down because critical application was compromised</b>	Server Application	Business – bottom line impacted Security – server and application
<b>Admin performing maintenance work on credit card database has access to read and copy credit card information</b>	Database Maintenance Process Admin Account	Security – Database Business – potential data loss GRC – compliance
<b>Unsecured transfer of customer information from point-of-sale systems to back-end databases</b>	POS systems Transfer Process Back-end databases	Security – POS systems and data transfer process GRC – compliance
<b>Data analysts evaluating field data for oil and gas company</b>	Data Evaluation process	Business – potential loss of intellectual property Security – data
<b>Backup process for access, authorization and authentication Web app does not encrypt data</b>	Backup process Application	Security – application, data
<b>Maintenance for Active Directory includes groups of high-privilege admins</b>	AD maintenance process Admin maintenance account Admin groups	Security – access and authorization Business – key user functionality; misuse of highly privileged passwords to access mission critical systems; potential system downtime
<b>Grant employee access to CRM system</b>	CRM data	Security – sensitive data Business – potential theft of customer, pipeline, etc. information
<b>Archive old files on a file server</b>	Access File Data Archive process	Security – Potential data loss GRC – compliance
<b>Provision virtual desktop for new user</b>	Admin account Provisioning infrastructure	Security – access to all user workspaces Business – potential disruption of user functionality

In each of these examples, taking a holistic view of privilege gives the enterprise a clearer picture of the extent and nature of the business risk and where to prioritize remediation—decide where you should invest. Figure out what is most privileged in the organization and fix that first, rather than try to “boil the ocean.”

## BUSINESS RISKS: SECURITY IS JUST THE BEGINNING

If your business does not have control over their most privileged assets (users, data, applications, etc.) then you do not really have control of your business. Consider: the new CIO walks into a meeting with his security and IT

managers and asks for a list of everyone who has administrative access to corporate systems. Chances are better than excellent that no one knows everyone who has elevated access, and it follows that there is no list.

Now, extend that scenario to think in terms of not only privileged users but also privileged assets and processes. It is reasonable to assume that there is no list of everyone or every account that has high authorization to touch privileged corporate financial records, customer information, online transaction applications, manufacturing control systems, production data, etc.

The business implications of not addressing the risk from a privilege perspective are enormous.

In terms of business resiliency, it is impossible to determine who was responsible for a problem when a production system goes down, and to take steps to prevent it from recurring. It may not even be clear who is responsible for correcting the problem.

Shared administrative and embedded application accounts represent an enormous security risk. If everyone owns the account, no one owns it. This makes privileged assets, such as online retail applications, customer databases and corporate finance systems easy prey for external attacks. Malicious insiders can and do use these accounts to steal without leaving an auditable trail.

Recovery from a serious security compromise could be devastating to the business unless you left the compromised account(s) and credentials in place. For example, exploiting poorly managed accounts on privileged systems would have an impact on business operations far beyond a data breach. Mike Brannon, senior manager of information systems at North Carolina-based National Gypsum, a Cyber-Ark customer, used the results of pen tests against privileged accounts that are not associated with a person—"one of the killing fields of every IT shop" to help make the case for an automated privileged identity management tool.

"The only way to fix it would be to disrupt operation of all these systems almost as though we had a disaster without the building burning down," said Brannon. If key privileged accounts were disclosed, changing their passwords would break the systems where they are used. "If this ever happened in the real world (outside of an audit / penetration test), there's no way we could make this change without breaking production systems."

From an audit perspective, the trail grows cold when an organization is asked to demonstrate who *can* reconfigure a production server, change firewall rules, modify access control lists on routers that handle traffic containing credit card data, and add, modify or delete privileged information--let alone who *has* that level of privilege.

How can an organization enforce and audit change control workflows when multiple employees can make changes to high-value systems without following procedure? Change and configuration management policies and processes are

designed to support the business in terms of priority use of resources, efficiency, quality assurance and security.

Typically, employees are given a sledgehammer to drive in a half-inch nail. They get a level of privilege that they can either apply incorrectly and do some damage to the privileged system to which they have been given elevated rights, or gain access to confidential information.

Brannon says, "We have taken care at National Gypsum to ensure that people only have the level of access that is needed. This prevents users from unwittingly bringing down production systems because they have access to data and/or processes outside of their routine needs. We deny by default, then allow based on needs, granted by approval."

## PRIVILEGE MOVES OUT TO THE WORLD, INTO THE CLOUD

Evaluating risk in terms of privilege cannot be treated as a back-burner matter. The business environment that has allowed privilege account management to spiral out of control evolved rapidly over the last few years and will continue to do so.

The brick and mortar businesses have given way to Web-based and hybrid models. The closed, proprietary manufacturing systems and utilities, shut off from outside threat and all but the most heavy-handed sabotage from within, are giving way to IP networks with PC-based interfaces, supplier and partner extranets, and Internet-facing applications. Where there were relatively few Internet-facing applications just a few years ago, they are now ubiquitous. Applications built for contained environments with embedded account passwords and little or no concern for security is now accessible to the world.

Enterprises have to be concerned about privileged access for third parties, for example vendors who typically require high-level access and authorization to support installations, troubleshooting, etc. Organizations need to be concerned about limiting their exposure in terms of where third parties can go and when they can go there. Moreover, if privileged account passwords are not changed—perhaps cannot be changed—for employees, the issue grows more troubling if third party users retain that level of access after the need for it is gone. One cannot even be sure who is holding those credentials on the vendor side, or if that employee is still there.

That situation grows much more complex, as the trend towards outsourcing to hosted services and cloud computing brings a sense of urgency to controlling privileged accounts and access to privileged systems, process and data. You now have to be concerned with not only your own admins, but also the salesforce.com admins. You do not know where your data is, where your infrastructure is—"privilege" is everywhere. If you are not working towards prioritized risk based on privilege with systems, data, applications and activities under your control, how will you deal with this risk when one or more of these pieces are outside your direct control?

You cannot and should not assume that the hosting vendor is going to be better at managing privileged entities any better than your company is now, so you should be developing strategies and exploring supporting technologies to address privilege beyond the boundaries of the enterprise.

Virtualization compounds the problem by amplifying privilege. Administration has collapsed onto the "super admin," who can touch the entire applications stack, the entire infrastructure. The level of potential harm is much higher, and the challenge increases.

## AT THE PRIVILEGE CROSSROAD

An enterprise can either build on the shaky foundation of the past, adapting code with embedded accounts to new uses, expanding operations while doing business in the same old way, or take the lesson of privilege to heart and find a better way.

For example, National Gypsum leveraged its SAP deployment in an external data center to set up stronger system controls and appropriate levels of access. Some internal people said that approach would not work at the company and that NG did not have the staff, said Gypsum's Brannon.

"We knocked out the argument that all Windows environments require what we now regard as inappropriate access and privilege to operate efficiently," he said. "We built our new SAP applications with application roles and a Windows infrastructure that worked the right way - with limited privileges. We proved we can actually can set up systems that are very controlled, reliable, and that don't inexplicably get changed or go down unexpectedly."

New business initiatives, such as National Gypsum's SAP deployment, are challenging, but excellent opportunities to do things the right way.

Even a good faith effort to control access according to need and based on the privilege quotient for the applicable accounts, assets and processes are daunting, to say the least. Organizations will typically use spreadsheets or similar artifices to control and track privileged access, but find it is impossible to keep up with demands for access and quickly fall behind and lose track.

On the other hand, if an organization tries to play hardball and enforce proper controls without automated tools, the spreadsheet approach quickly becomes a bottleneck, an impediment to timely provisioning and an invitation to circumvent procedure. It becomes, once again, impossible to track who has and who needs privileged access and to what systems and applications.

The other major impediment is the fear of "breaking" critical systems and applications. In complex environments, the impact of attempt to change shared passwords to comply with best practice and regulatory requirements, or tampering with embedded application accounts and service accounts is never clear.

## MANAGING PRIVILEGE WITH CYBER-ARK

Cyber-Ark's insight into a concept of privilege, embodied in its "Got Privilege" initiative, extends beyond the notion that privilege is vested solely in role, such as systems administrator.

Management's understanding of and commitment to a privilege-centric risk management and mitigation course of action is essential to its success. Recognizing the business impact of privilege and the benefits of a program that assesses the level of risk, enterprises can prioritize its remediation and mitigation efficiently.

Cyber-Ark's Privileged Identity Management (PIM) suite provides the tools to translate a privilege-centric approach into a comprehensive, automated, transparent, auditable and secure process for prioritizing and managing risk associated with high-level accounts and passwords.

Built around its centerpiece, Enterprise Password Vault, the Cyber-Ark suite empowers enterprises to ensure secure access around privileged applications, systems, business processes and information. As the organization builds policy and establishes privilege-centric priorities based on potential impact to the business, Cyber-Ark supplies the necessary tools to build a sustainable program, overcoming the practical obstacles to success.

"We have thousands of privileged accounts managed by Cyber-Ark," said Brannon, who had been frustrated by the Excel approach to privilege management and had to deal head-on with the problem of embedded accounts when National Gypsum had to upgrade its SQL Server databases and a slew of dependent legacy apps as Microsoft wound down support for SQL Server 2000. "Never in our wildest dreams would we have attempted the application integration, as well as the Windows local systems administrators and some of the Windows services accounts that we're managing this way.

"The new approach really improves our ability to manage all access to privileged accounts."

The Cyber-Ark PIM suite tools, Enterprise Password Vault, Application Identity Manager and Privileged Session Manager, provide granular control over privileged business activity. All products in the suite are built upon the Digital Vault, a hardened and encrypted repository for managing highly sensitive data such as privileged access information.

The suite provides controlled access to privileged accounts, monitors and records privileged sessions, and manages application and service accounts. Organizations are finally able to protect their privileged business accounts, assets and processes, manage and enforce policy over privileged accounts, and comply with audit and regulatory requirements. The tools are secure, extensible and easy to use, enabling enterprises to quickly provision and de-provision privileged access based on need, maintaining detailed auditing for accountability and compliance.

Cyber-Ark Enterprise Password Vault (EPV), a secure for managing privileged access control—password management, privileged single sign-on, and long-term or temporary provisioning. One of the difficulties of temporary provisioning—such as a vendor, contractor or an internal user who needs elevated privilege to deal with an emergency—is revoking that privileged access when the need is gone. Cyber-Ark provisions privilege as needed, associates it with a particular individual, maintains an audit track and integrates with the enterprise’s ticketing system.

Application Identity Manager secures management of hard-coded, embedded application and script accounts, a persisting legacy of development that emphasized functionality at the expense of security. Application Identity Manager leverages Cyber-Arks Vault technology for central storage, security and management. This eliminates the risk of abuse by insiders, such as developers, or external attackers who can leverage embedded credentials to access privileged information.

Privileged Session Manager provides session-based secure remote access to managed devices, monitoring and recording all user activity for VCR-like playback and privileged single sign-on through the Privileged Identity Management portal. This secure session access is particularly valuable for third party access for vendors, contractors, service providers, etc.

As enterprises implement a privilege-centric approach, the Cyber-Ark PIM suite of tools gives them a practical, real-world, secure and auditable capability for implementing and managing privilege, mitigating risk as they identify it and establish priorities for action.

“Understanding privilege helps prioritize where organizations should be spending their current dollars,” said Adam Bosnian, Cyber-Ark vice president of products, strategy and sales. “Cyber-Ark can help you fix something that’s very high risk, in a very short time, all in all saving a lot of money and reputational damage.”

The information provided in this document is the sole property of Cyber-Ark® Software Ltd. No part of this document may be reproduced, stored or transmitted in any form or any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission from Cyber-Ark® Software Ltd.

Copyright © 2000-2010 by Cyber-Ark® Software Ltd. All rights reserved.