

RISK Factor

Volume 3, Issue 1

April 2007

Protecting Privileged Passwords

By Adam Bosnian

As auditors become savvier about investigating companies' security practices, more businesses are being put on notice that existing safeguards are not up to snuff. Many public companies have received a wake up call to this reality in the form of a poor performance on an internal audit or even a bad 404 report from SOX auditors. As we enter the second year of SOX regulations, and as companies continue to face increasingly stringent regulatory mandates from the Food and Drug Administration (FDA), the Federal Reserve and other agencies, it will be vital for organizations to proactively be aware of and address these shortcomings before they become a vulnerability identified on an audit result.

These regulations send the same warning about data security—that most organizations allow too many people to have unfettered access to sensitive information, leaving them vulnerable to costly data and identity theft. Companies suffered \$250 billion in intellectual property theft in 2004 alone. According to a study by the FBI, an estimated 70 percent of these network breaches originate from within. With more than 90 identity theft incidents last year and more than 51 million identities stolen, companies are under pressure to enact measures to avoid information leaks that could mar their financial status and business reputation.

Security concerns are similar, regardless of what information you're looking to protect. Are you changing passwords on a regular basis? What measures are in place to shield high-level passwords? Do you securely store and transmit sensitive data? How do you prevent misuse of information, internally and externally?

According to Gartner analyst Rich Mogull, "perimeter security alone doesn't guard against all the threats enterprises face, such as malicious internal staff, [or] physical theft of machines... Enterprises must also protect content and data with internal security controls, including appropriate use of encryption, vulnerability management, identify management, and activity monitoring."

Flexible digital vaults are an emerging technology that addresses this concern. While most security solutions offer a point solution approach at the network level, digital vaults form a barrier around the company's most critical information. Much like a physical vault, this technology creates a safe haven for protecting vital records, with distinct areas for storing, protecting and sharing this data. Sensitive information resides on a dedicated server with multiple layers of security, including session encryption for protecting the information both in storage and in transit. Granular access control is provided through the application layer.

Overlooked Security Concern

It's often necessary for system administrators to give out *super user* passwords to numerous internal parties, such as technicians troubleshooting an issue or developers maintaining their own applications. Yet this is like giving away the keys to the kingdom. These privileged user passwords are extremely powerful if they fall into the wrong hands. Users with these passwords can wreak havoc on internal systems, or bypass firewalls to gain access to confidential information residing in databases and servers across the organization.

Administrators often assign simple, easy-to-guess passwords or even give out the system's default password—a highly risky endeavor since it's likely the first password someone would try when looking to infiltrate the system. Others choose to assign complex passwords and require users to change these on a regular basis. Unfortunately this often results in users jotting the password down, and leaving them in unsecured locations, or worse, writing them down on a sticky note next to the computer. In large organizations they may not know how many people have administrative accounts on the system.

Unmanaged administrative ID's and passwords have begun to be an issue that is highlighted by both internal audit and 404 report results. Whether it is due to uncontrolled access to an organization's production network, or unmanaged access to key applications and databases, or even just a poorly documented and executed firecall process, the need to improve administrative ID management has been identified and heightened via regulatory drivers. To avoid such perils, companies need to:

- Securely store and manage administrative IDs/passwords
- Implement strong controls over usage of administrative IDs/passwords
- Automatically change administrative IDs/passwords on target systems and applications based on policy or regulations definitions
- Define reliable processes for accessing and using administrative passwords in emergency/firecall situations

Controlling Access Privileges

Digital vaults provide an effective way to safeguard super user passwords. This technology encompasses a very secure repository for passwords and password objects, as well as the ability to centrally manage passwords, forcing users to comply with corporate password policies. Instead of the system administrator manually assigning passwords and

tracking these in a spreadsheet, these password management capabilities generate a password that automatically changes or expires. For example, a developer may be given a password authorizing him to access the server for 60 minutes, or for one-time use. Passwords on target systems are changed on a predefined basis. This is ideal for users who may need to get to the server for a specific purpose but should not be given permanent access.

An ideal vault solution includes the ability to automatically update passwords based on predefined criteria, control usage of those passwords, and track usage for auditing purposes.

The Business Driver

Compliance managers have been aware of these password problems for years, but until recently they had a difficult time gaining funding and internal buy-in. SOX and other regulatory pressures have changed all that. Public companies must attest to having strong measures in place to protect critical data. This requires technology that controls all access rights to this information, and provides audit reports to track system access activities.

A chief compliance officer at a major financial institution reported that a bad 404 report was the catalyst for looking into digital vaults. The company traditionally provided access to their production network to the developers who created the business applications. When the auditor highlighted that this policy had created an environment where developers had unfettered access to their critical systems, the company was driven to look for a solution that could better rein in and manage these security rights.

With an automated administrative ID management solution in place, developers will now be given one-time-use passwords to target systems on an as needed basis. The passwords automatically expire after a given time instead of providing the ongoing access rights that left the system vulnerable.

When a developer requires access to the system for maintenance they submit a request through the vault, which assigns, tracks, and logs password activities. To access the server, the developer enters credentials to access the server password via the vault. They also benefit from greater granularity of access control. Typical role-based passwords don't do a sufficient job of segregating duties at the super user level. Thus, a technician would have different access than a database administrator.

Key criteria for Digital Vaults:

- *Prevention and detection of unauthorized attempts at modification and deletion of financial information.* An essential component of anti-theft technical controls is the ability to immediately alert the responsible individual when suspicious activity is detected. In addition, the system should detect changes as part of an auditable paper trail. This is particularly important when multiple individuals are modifying the same financial records.
- *Multi-layered security.* Using multiple security technologies will prevent single points of failure that can hinder internal controls. This may include a combination of session encryption, firewall, access control, file encryption, strong authentication, secure backup, and version control. This end-to-end layered approach is essential for protecting sensitive data throughout the information lifecycle.
- *Dual control.* This added security measure requires two individuals to give consent before allowing access to confidential records. Much like requiring two keys to open a safe deposit box, dual confirmation involves dual permissions as a pre-requisite to viewing Vault-protected information. When dual control is configured, any attempt to access Vault-protected information will trigger a request for clearance to the pre-defined secondary person.
- *Configurable time delays.* Security systems should allow for passwords to be issued for specific time frames, such as during working hours, or for one-time use. Passwords can also limit access based on user location. For example, confidential records might only be accessible from certain rooms or buildings.

No longer is it sufficient to simply guard the perimeter of the enterprise. Regulatory mandates require businesses to do whatever possible to prevent malicious use of information by internal and external sources.

To offer the best protection against data theft, digital vaults should be deployed. Ultimately, digital vaults offer protection against internal and external threats, securing information both while in storage and during transmission. This not only aids businesses in complying with regulatory measures but protects the interests of company executives and stockholders.

Adam Bosnian is Vice President of Sales & Strategy, Cyber-Ark Software. Please visit www.cyber-ark.com.