



Hidden Risks of IT Staff Turnover

How to Safeguard Corporate Data as Job Roles Change

Summary

For one federal government agency, hiring contractors to handle IT administrative tasks was an expedient solution to soaring personnel costs. But then these IT contractors began walking out the door with full access to the agency's powerful privileged accounts. Without a way to audit and control this access, the agency risked having its sensitive data exposed.

This paper outlines the security risks that can arise when IT staff change job roles. It describes the steps that organizations can take to secure their privileged identities, and presents a study how the government agency mitigated the threats presented by IT staff turnover.

The Risks of IT Staff Turnover

When IT personnel change jobs they can take with them the password secrets that grant access to sensitive data, permission to execute programs, and the ability to and change configuration settings on virtually any piece of hardware or software. That's because IT staff have access to so-called super-user passwords they use to perform routine administrative duties and emergency, fire call repairs.

Privileged identities exist on virtually every server and desktop operating system, network device, security appliance, and program and service including databases, line-of-business applications, Web services, backup software, scheduled tasks, and others. Yet today's Identity Access Management (IAM) technologies don't detect or secure privileged identities, and can't change these passwords after IT personnel leave their jobs.

Recent events demonstrate how failure to safeguard privileged access during times of IT staff turnover can result in the loss of sensitive data and failures in business-critical services:

- A senior IT administrator at a large financial services company was accused of stealing and selling sensitive bank account and credit card information on 2.3 million customers.
- A pharmaceutical supplier discovered the presence of a logic bomb inserted by a administrator before company-wide layoffs; the malicious code was designed to wipe out the company's clinical trial data.
- A large US city was locked out of its network by an administrator who was arrested following an altercation on the job.

When a worker's employment ends, organizations commonly introduce physical barriers such as rescinded IDs and keycards to prevent further access. However, few organizations are able to block the so-called "super-user" access by former IT staff members because:

- Identity access management (IAM) frameworks from leading vendors like Microsoft, Oracle, IBM, Sun, and others don't control privileged identities.
- Organizations that lack automated processes to manage their privileged identities cannot maintain complete, authoritative lists of the systems, applications and services where these credentials reside and can't chart their interdependencies.
- Because privileged account interdependencies are rarely documented, changing a single privileged password has the potential to lock out other, dependent services that share the same credentials. The result can be cascading system failures and disruptions in critical business services.

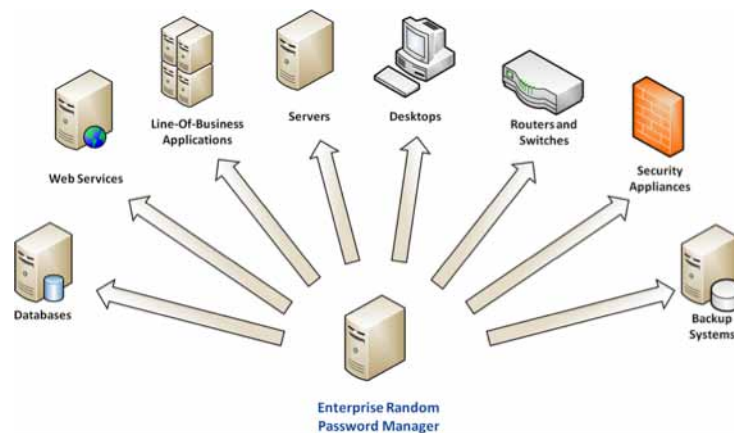
Regaining Control

A single server can have privileged identities present in local and domain accounts, in configured services and scheduled tasks, and in a wide range of applications including COM+ and DCOM applications, IIS websites, databases such as Oracle, SQL Server, and so on. Multiply these by the many servers and network appliances present in your organization to get an idea of the challenges involved in manually documenting each account and its interdependencies, and changing each account password frequently enough to comply with regulatory mandates.

Fortunately automated processes exist that can reliably help organizations regain control in a cost-effective manner. The processes can be described as four key steps that are abbreviated as *I.D.E.A.*:

- **Identify** and document all critical IT assets, their privileged accounts and interdependencies.
- **Delegate** access to credentials so that appropriate personnel, using least privilege required, with documented purpose, can login to IT assets in a timely manner at designated times.
- **Enforce** rules for password complexity, diversity and change frequency, synchronizing changes across all dependencies to prevent service disruptions.
- **Audit** and alert so that the requester, purpose, and duration of each privileged access request is documented and management is made aware of unusual events.

Privileged identity management software can automate the task to track an organization's privileged accounts, change privileged passwords according to the organization's policy, facilitate rapid password recovery so that IT staff can perform routine services and emergency repairs, and change each privileged password after check-out to prevent unaudited access.



Enterprise Random Password Manger (ERP) Identifies a Wide Range of Privileged Accounts and Interdependencies

Lieberman Software Solution

Enterprise Random Password Manager (ERPM) is software that discovers, updates, stores, and allows secure recovery of every local, domain, and process account in an organization. It detects and reports every location where privileged accounts are used – including local and domain accounts, configured services scheduled tasks, applications including COM+ and DCOM, IIS websites, databases such as Oracle, SQL Server, and so on – and then rapidly propagates password changes everywhere that each account is referenced in order to prevent account lockouts and service failures that can occur when manual processes create obsolete credentials. ERPM secures its passwords in an encrypted database that can be accessed from any web-enabled device. Users check out privileged account passwords through an automated processes that takes advantage an organization's existing identity access management framework to allow expedited, delegated access. Passwords are automatically re-randomized after check-in, and restricted recovery periods, forced check-ins, periodic verifications, web session timeouts, and phonetic spelling options are provided.

Customer Case Study

Lieberman Software was first contacted by a government agency when it faced security concerns over business practices that arose in response to budget cuts. At some of the agency's sites, new subcontractor agreements were being negotiated every six months in order to control personnel expenses. As a result, independent subcontractors were being discharged – and others taking their place – on a recurring basis.

When he contacted Lieberman Software, the agency's IT planning executive voiced anxiety over the privileged account password secrets that terminated subcontractors might be taking with them as they left their jobs. The executive said that the agency's priorities were to:

- Discover where privileged credentials were in use.
- Change all of these credentials frequently enough to avoid a data breach.
- Segregate existing privileged passwords to mitigate the threat of one compromised password exposing numerous systems to attack.
- Create a process so that privileged account passwords, once revealed to the agency's staff, would be quickly changed.
- Institute an auditing process so that each request for access would be known to management.

The agency first deployed Enterprise Random Password Manager at a single site to confirm that the product satisfied its goals. Because ERPM integrates directly with the organization's Identity Access Management (IAM) system, the executive said that the agency could prevent discharged employees from accessing IT resources the moment their credentials were revoked, and could also immediately give new IT staff the access needed to perform their duties.

The organization saw benefit that the product revoked all privileged passwords a short time after check-out and then immediately changed them. The executive also said that the product helped to significantly reduce the time it took his staff to configure new IT employees for privileged access to servers, workstations and applications.

Next Steps

Organizations that desire more insight into potential risks of the unsecured privileged accounts in their IT environments can contact Lieberman Software for an ERPM software trial. ERPM documents potential risks present in the infrastructure, enumerating privileged accounts by hardware platform, account and service type. It then continuously secures privileged accounts everywhere on your network and provides an audit trail of each access request. ERPM trial software is available at no cost to qualified organizations. For more information, email [**ERPM@Liebsoft.com**](mailto:ERPM@Liebsoft.com).

About Lieberman Software

Lieberman Software Corporation, established in 1978 as a software consultancy, has been a profitable, management-owned organization since its inception. Lieberman Software pioneered privileged account password management software, releasing its first product to this market in 1999. Since that time, the company has continuously updated and expanded its privileged password solutions while growing its customer base to include many of the world's most secure enterprises.

Lieberman Software is a Microsoft Gold Certified Partner and has technical partnerships with such other industry leaders as Cisco, Novell, Red Hat, Hewlett-Packard, IBM, RSA and Intel. The company is headquartered in Los Angeles, CA, and maintains a regional office in Austin, TX. All product development, testing, and support operations are based in the United States.

For more information, visit **www.liebsoft.com**
Call 800-829-6263 (USA and Canada) or 01-310-550-8575 (International)
Email **sales@liebsoft.com**



www.liebsoft.com | P 800.829.6263 (USA/Canada) P (01) 310.550.8575 (Worldwide) F (01) 310.550.1152
1900 Avenue of the Stars, Suite 425, Los Angeles, CA 90067
© 2011 Lieberman Software Corporation. Trademarks are the property of their respective owners.