From Chaos to Control - Managing Privileged Accounts

Angela J Carfrae, CPA, CISSP, CIPT
AJCarfrae Consulting

About Me

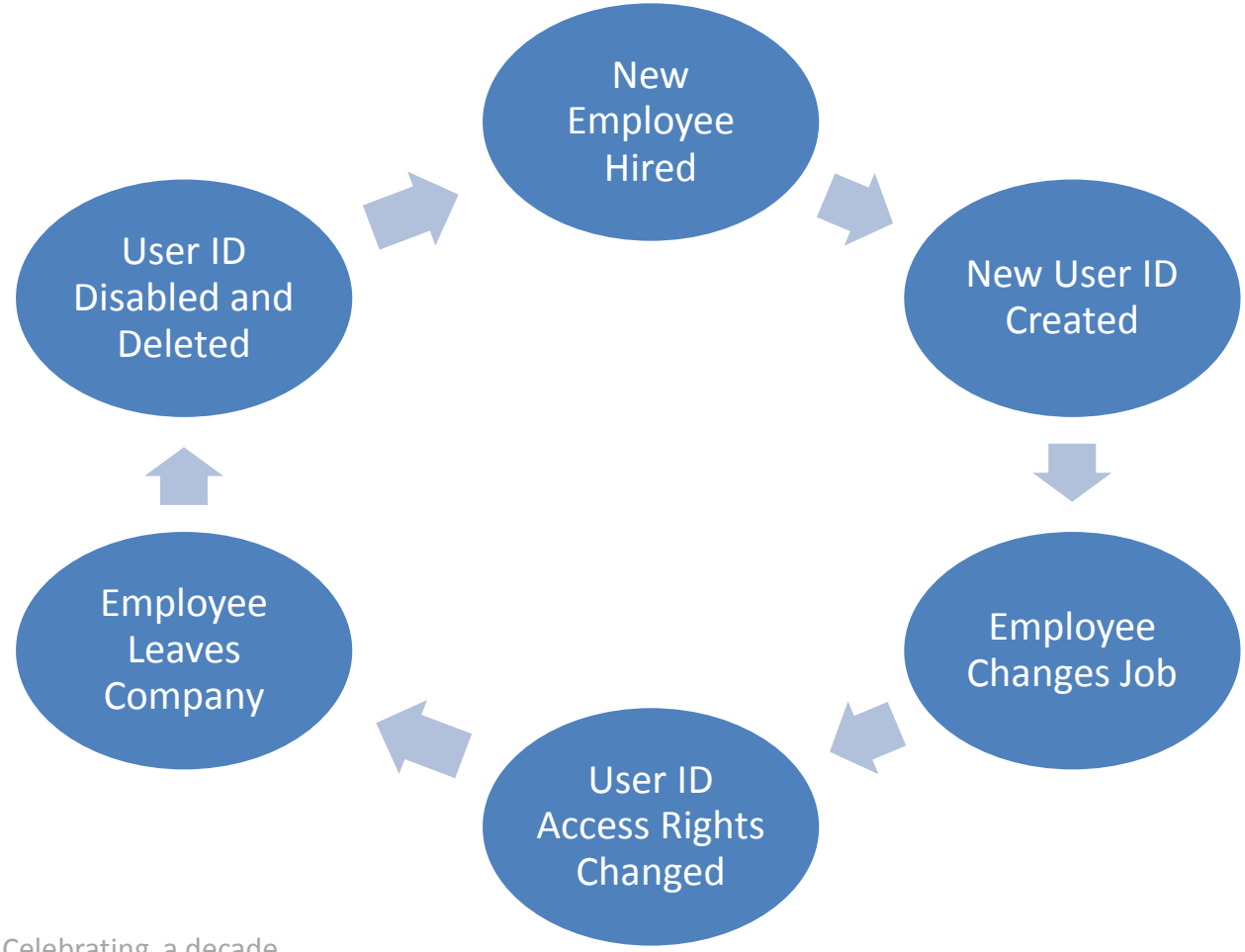
- CPA (CGA), CISSP, CIPT
- 27 years in the accounting and compliance arena
- As an employee
  - Internal controls (financial and IT), security, privacy, business continuity, internal controls
  - Familiar with regulatory requirements on both sides of the border including SOX, PIPEDA, HIPAA, OSFI, GLBA
- Consulting
  - Helping a client implement an automated Privileged Account Management solution

Agenda

- What is a privileged user and what's the big deal
- How do we take back "control"
  - Automation is the path forward
  - Benefits and Risks
- How to find the right automation solution
- Summary and wrap up

WHAT'S THE BIG DEAL

Access Control



But What about your Privileged Accounts?

How many Privileged accounts ?

A Company with 5000 employees....how many privileged accounts do they have?

1-250 ?

251-500 ?

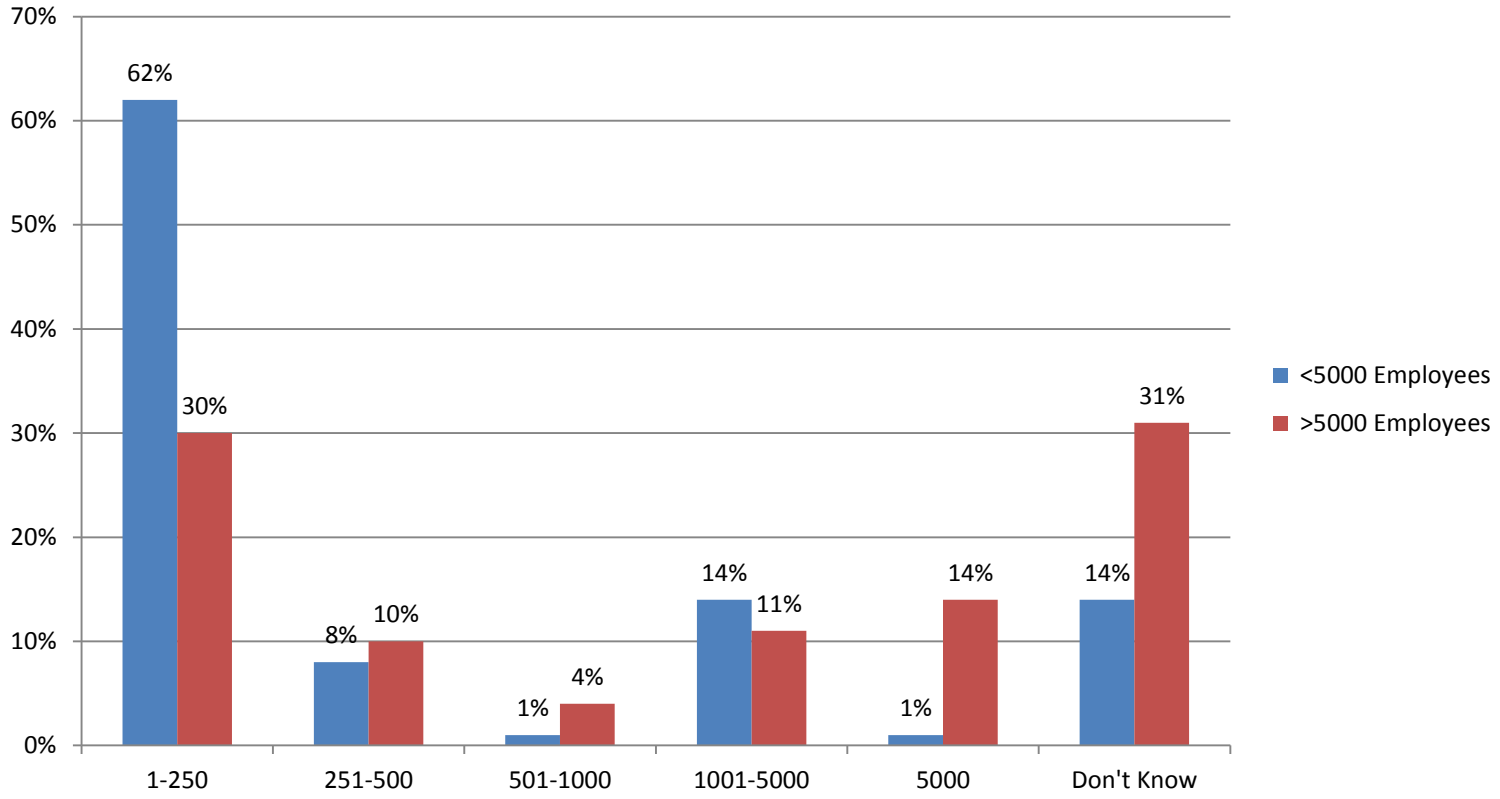
501- 1000?

1001 – 5000 ?

More than 5000?

Don’t know, don’t care – what’s for lunch ?

How many Privileged accounts ?



Source: Privileged Account Security and Compliance Survey Report, May 2013, CyberArk Software Inc.

What is a Privileged User?

Privileged user is a user or object that has elevated rights to do its / their job

Major Categories of Privileged Users

- Local Admin Accounts
- Domain Admin Accounts
- Service Accounts
- Application Accounts

Local Administrative Account

Local Admin Accounts is an account that provides admin access to the local device only. For example Windows administrator, UNIX root, and enable mode on certain routers.

Risks:

- Too complex to change
- Same password across a platform
- Often shared among IT personnel
- Often known by people who only need them once in awhile

Domain Administrative Account

Domain Admin Accounts have privileged access across all workstations and servers within a domain – this is often used by an IT Help Desk and Operations Departments

Risks:

- Compromise of credentials is a worse case scenario
- Lack of accountability
- Hard to change the password when someone leaves
- Lockout could be catastrophic

Service Accounts

- A non human account used to run services or automated tasks
- More of an issue in Windows environment
- May be local or domain depending on its use
- Risks
  - Password changes may need to be synchronized across many components
  - Potential operational failures
  - Admin personnel will know the passwords
  - “Password never expires” option often used

Application Accounts/Software Accounts

- Accounts created on remote systems for authentication by other services
- Passwords can be stronger because a human doesn't have to memorize them
- Risks
  - Usually aren't encrypted
  - Often are hardcoded into applications meaning applications have to be recompiled to change a password
  - If load balancing is used for the application, the id and password is on several servers
  - Often have access to data that resides in databases
  - The admin changing the passwords will know them

Application Accounts/Software Accounts

If you have 200 hosts

With
2 applications each

And
Each application has 5 scripts

Then:

You have 2000 embedded passwords that need to be managed

The Chaos

- Weak passwords or never changed
- Complexity
- Lack of auditing and accountability
- Risk of stopping services from running
- Embedded within applications – often in clear text

The keys to the kingdom – targeted by hackers

…and Don't Forget

- *Internal and external auditors*
- *OSFI*
  - *The FRFI tightly controls and manages the use of administrative privileges, on an enterprise wide basis*
- *PCI*
  - *Access to privileged user IDs is restricted as to least privileges necessary to perform job responsibilities and assigned only to roles that specifically require that privileged access*
- *HIPAA, GLBA, etc, etc.*

TAKING BACK CONTROL

Principles for the Solution

- Least Privilege Model
  - Use special account for admin tasks
  - Minimize number of passwords and shared privileged accounts
  - Limit the number of systems within the scope of each persons privileged accounts
- Policy Definition
  - Establish a process for managing accounts
  - Change passwords, use strong passwords
- Accountability and Audit
  - Password sharing eliminated
  - Use extra authentication for privileged accounts
  - Monitor and reconcile all privileged account activity
- Inventory

Stepping Towards Control

First Steps

- Policy
- Process
- Eliminate non-expiring passwords
- Secure Storage
- Accountability
- Inventory

Medium

- Change passwords
- Use one time passwords
- Eliminate human login
- Change hard coded and embedded passwords
- Implement auditing and monitor

TOWARDS AUTOMATION

Manual is Better than Nothing

- Auditing will be almost impossible especially to the degree required by regulatory bodies (SOX, HIPPA, PCI)
- Changing passwords on a manual basis will become overwhelming
- The admin who changes the passwords knows the passwords
- Tedious, time consuming and with significant overhead
- Doesn't work well is you are distributed geographically
- Doesn't scale well

Stepping Towards Control

First Steps

- Policy
- Process
- Eliminate non-expiring passwords
- Secure Storage
- Accountability
- Inventory

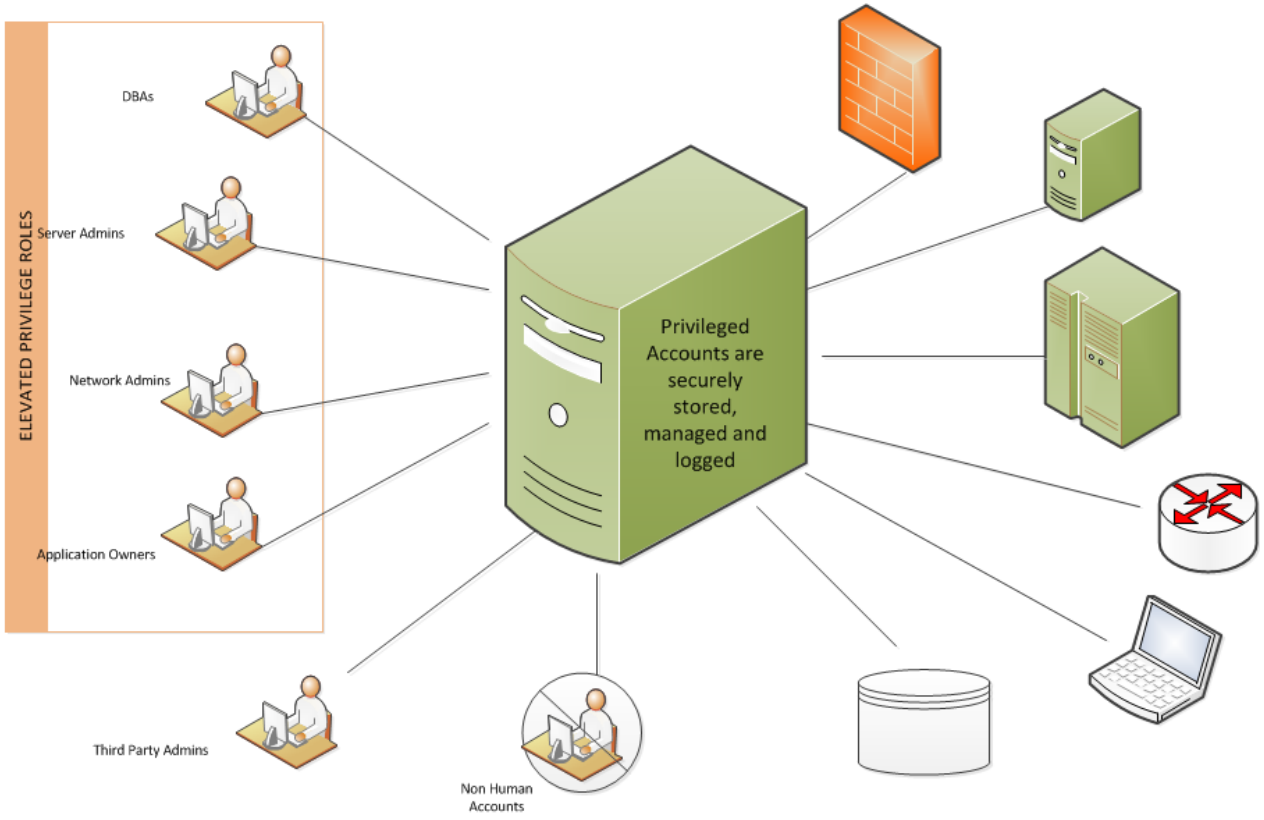
Medium

- Change passwords
- Use one time passwords
- Eliminate human login
- Change hard coded and embedded passwords
- Implement auditing and monitor

Managed

- Multifactor authentication
- Automated password change
- Workflows for access
- Session recording
- Automated disabling of inactive accounts
- Change hardcoded passwords within applications

A Privileged Access Management System



Benefits of Automation

- Enforcement of Password Policy
  - Centralized and automated management of passwords
  - Discovery of accounts on a variety of components
  - Password changes are synched with back end systems
- Audit and Accountability
  - Recording of privileged sessions
  - Filtering or controlling actions that a particular admin can take
  - Comprehensive view of privileged accounts and their use
  - Access to passwords can be in various forms –disclosure or direct connect
- Other
  - Can be integrated with ITSM and change management systems
  - Elimination of hard coded passwords in configuration files

Increased Market Interest

- Regulations and failed audits
- Risk of insider threats
- Existence of malware that targets privileged accounts
- Outsourcing of IT operations
- IT service providers (cloud solutions)

Source: Gartner: Market Guide for Privileged Account Management, June 2014

Risks of an Automated Solution

- Complex in its own right
  - Improper management
  - Rushed implementation
- Compromise would be catastrophic
- Operational disaster if fails
- Performance factors

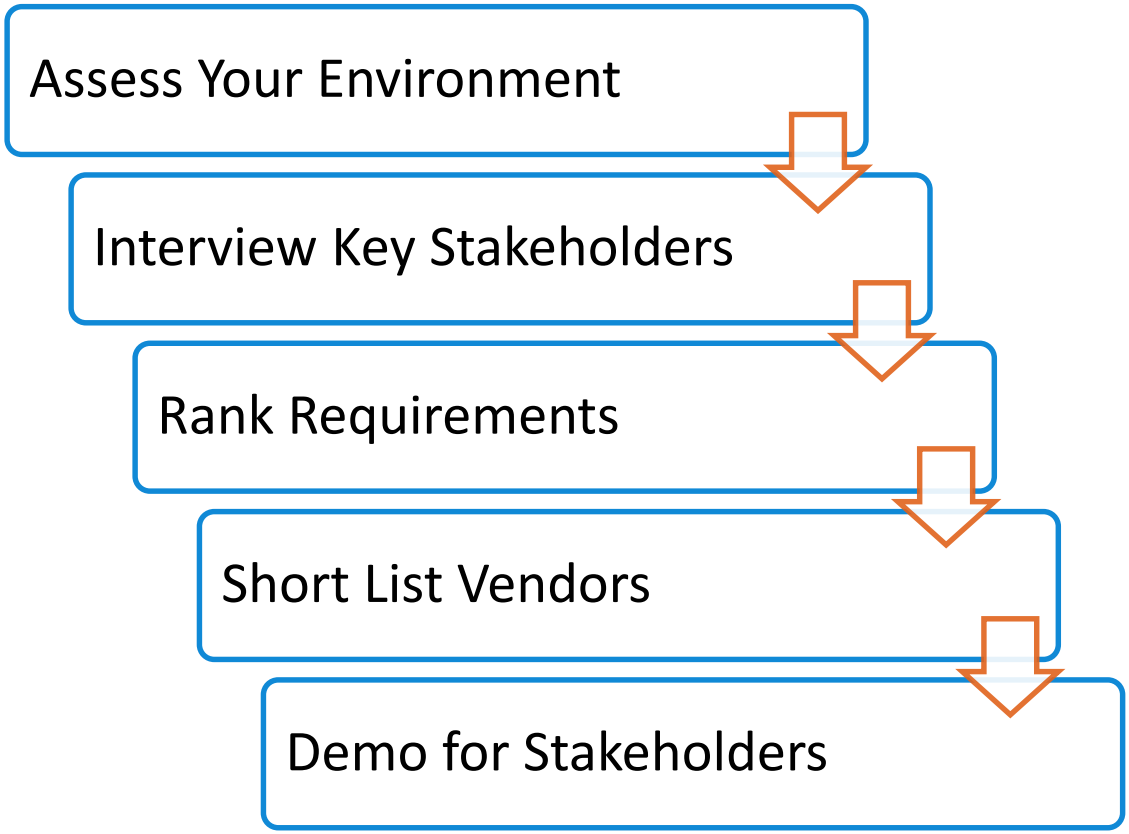
THE RIGHT SOLUTION FOR YOU

DIAMOND YEAR —2015—

Celebrating a decade of guiding security professionals.

SECURE360 conference

Choosing the Right Solution



Assess Your Environment

- Capacity and Performance
  - How many users will there be?
  - How many accounts will be managed?
  - Load balancing
- Access and Authentication
  - Do you want transparent user management
  - From where will the system be accessed
  - From where will the system be managed
- Architecture
  - Where will the PAM system be located? (secure network, DMZ?)
  - What is your DR model?
  - Impact on storage and management
  - Virtual versus physical servers
  - What devices are in your environment?

Assess Your Environment

- Roles and Responsibilities
  - Evangelist
  - System administrator
  - Policy administrator
- Ongoing Monitoring
  - Platform monitoring
  - Application monitoring
  - Security monitoring
- Ongoing Integrations
  - Enumerate qualifying IDs
  - How to keep systems current – accounting for new systems and accounting for retired systems

Interview Key Stakeholders

- What are your pain points?
- Do you just need somewhere to store passwords?
- Do you care about credential delivery?
- Do you want built in workflow?
- Do you want to tie into LDAP?
- Are you worried about hard coded applications?
- Are you worried about on line recording of admin activities?

Rank Requirements

- Using information gathered from interviews and assessment
- Rank based on Mandatory, Nice to Have, Don't Know or Don't Care

FINDINGS

Help with inventory
Help with management of Password Changes
Secure Storage of User IDs and Passwords
Segregation of Duties
Auditing and Monitoring
Highly Available
Storage of other files e.g. Certificates

Short List Vendors / Vendor Demos

Weight:		Score:	
3	Critical to Success	5	Out of the box, we don't have to do anything, this is exactly what we need
2	We could make use of	4	Included but we need to do some configuration or add agents to end points, pretty much meets our need and would satisfy our requirements
1	Cool, neat to have, but we could live without it	3	We can do it with training from the vendor or with some changes in our process to get what we need
		2	Vendor hands on required, included as part or support or installation. This requires a lot of work on our part.
		1	Consulting engagement with the vendor required - very complicated to implement, we might as well just to stick to our manual processes

Short List Vendors / Vendor Demos

		Weight	Vendor #1 Score	Vendor #2 Score
PRODUCT REQUIREMENTS:				
Safe or Vault	Does the product offer an encrypted password safe or vault for storing credentials?	3		
Ease of Use and Automation	How is the password change policy enforced ? Can we apply different rules for different groups or types of passwords? Can we apply different methods of enforcement for different groups? Does the tool look fairly easy to use or very complicated	3		
Implementation:				
Implementation model	How does the vendor suggest we implement the tool? "Big bang" versus install and integrate slowly. Can we add groups of accounts at a time? What kind of roadmap and implementation support does the vendor offer.	3		
Autodiscovery process	How easy is the auto discovery process – ease of use, does it run manually or automatically, do you require agents and how complicated is that to implement. How do you keep the inventory current? Is auto discovery available for a variety of environments – Windows, AIX, Unix, virtual, Sonic ESB, databases, network devices, etc.	2		

Short List Vendors / Vendor Demos

- Product Requirements
- Implementation
- Ongoing Use
- Other
  - Cost
  - Vendor Reputation / Track Record
  - Customer References

Summary

- Opportunities for improvement
  - Inventory of privileged accounts
  - Accountability of privileged account use
  - Automated password changes
  - Secure storage and use of passwords in services and scripts

Summary

- Chaos to Control One Step at a Time
  - Inventory (discovery) of privileged accounts
  - Build roadmap based on inventory
  - Start with low hanging fruit – usually Windows servers
  - Determine roles and responsibilities early
  - Add new accounts slowly
  - Turn on password change automation slowly

References and Resources

- Six Ways to Protect Privileged Accounts, Internal Auditor, www.theiia.org
- The Three Phases of Securing Privileged Accounts, www.cyberark.com
- Market Guide for Privileged Account Management, Gartner
- Adopt a Strategy to deal with Service and Software Account Passwords, Gartner
- Ten Best Practices for Managing Privileged Accounts, Gartner
- Best Practices for Securing Privileged Accounts, Hitachi ID Systems Inc.