



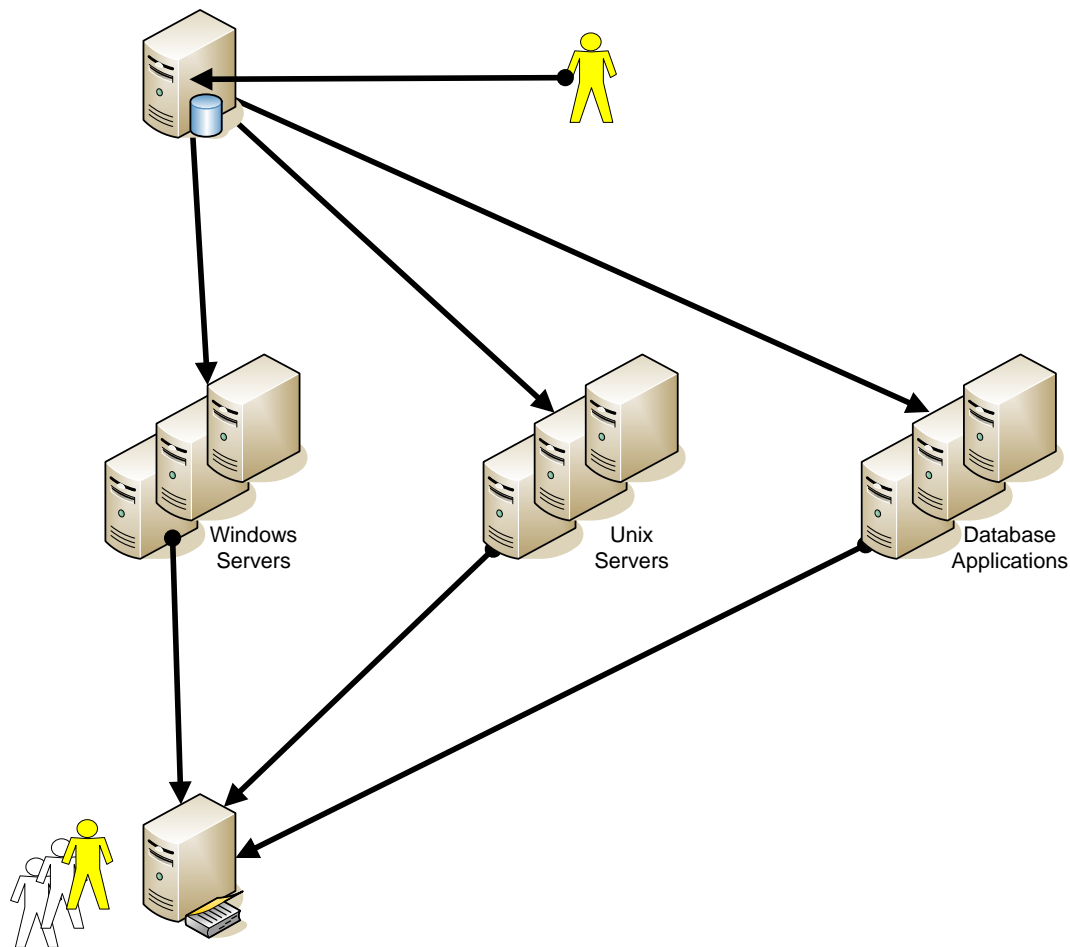
Privileged Password Management Enterprise Password Vault

Privileged Password Management – Agenda



- Privileged Users 101
 - What are privileged Users
- The Challenge
- Common Practices and the Risks Involved
- Drivers: Regulations and Internal Breaches
- Business and Technical Requirements
- Cyber-Ark Enterprise Password Vault
 - Technology
 - Architecture
 - Benefits
 - Demonstration
- Q&A

Identity Management – Individual Users Component - Directories



What Are Privileged Accounts?



Administrative Accounts

Shared Predefined:

- UNIX root
- Cisco enable
- DBA accounts
- Windows domain
- Etc.

Shared:

- Help Desk
- Fire-call
- Operations
- Emergency
- Legacy applications
- Developer accounts

Owned by the system:

- Not owned by any person or "identity"

Application Accounts

Hard-coded, embedded:

- Resource (DB) IDs
- Generic IDs
- Batch jobs
- Testing Scripts
- Application IDs

Service Accounts:

- Windows Service Accounts
- Scheduled Tasks

Personal Computer Accounts

Windows Local administrator:

- Desktops
- Laptops

Privileged Accounts Today



- **Common practices:**
 - **Storage:** Excel spreadsheets, physical safes, sticky notes, locked drawers, memorizing, hard coded in applications and services
 - **Resets:** Handled by a designated IT members, call centers, mostly manual
 - **Known to:** IT staff, network operations, help desk, desktop support, developers
- **Common problems:**
 - Widely known, no accountability
 - Unchanged passwords
 - Lost passwords
 - Same password across multiple systems
 - Simplistic passwords – easy to remember
 - Passwords not available when needed

Jerry, we are on schedule for
the security audit next week.



Yes, we are prepared.



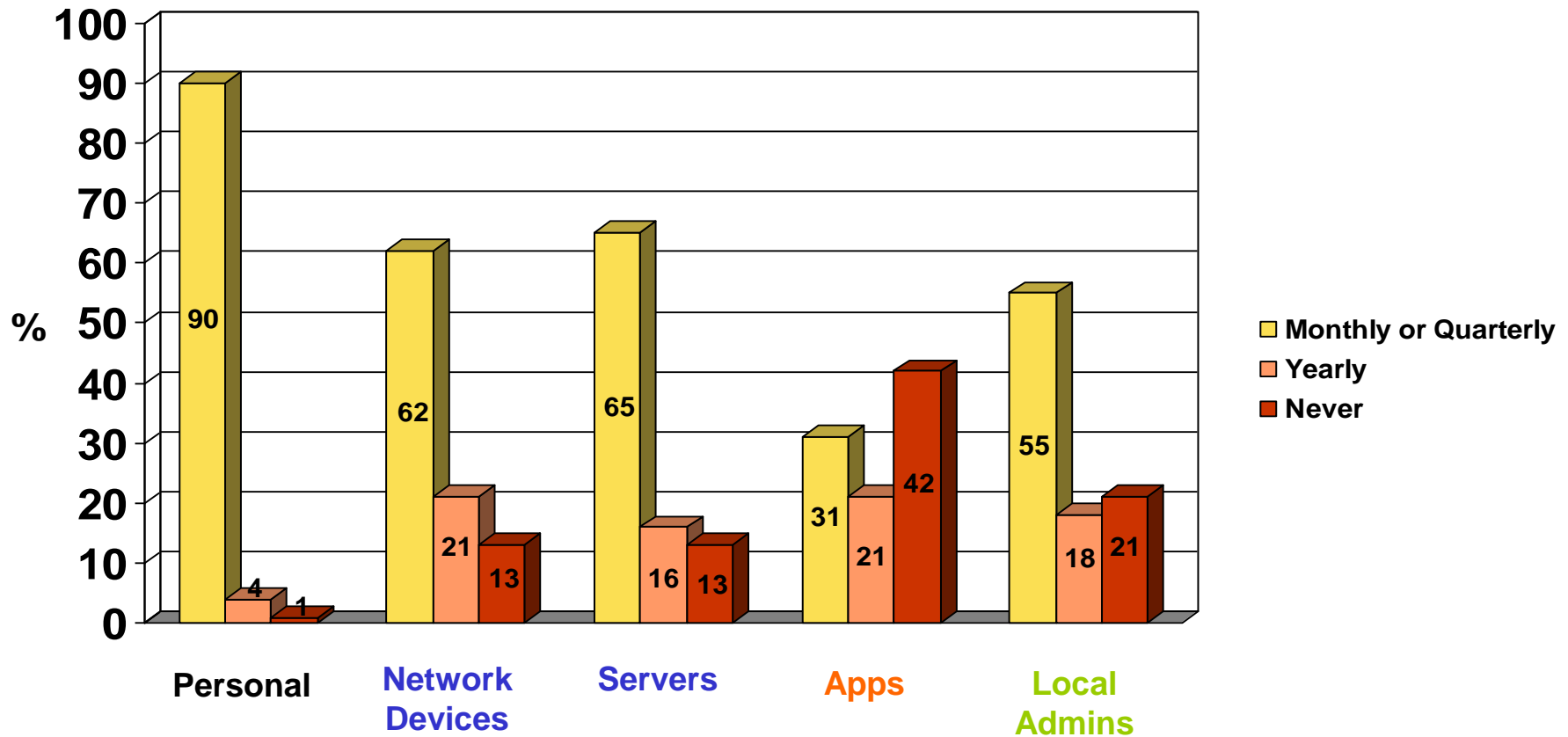
I can't see any reason
we will fail.



Which Doors Are Being Locked?



Password reset frequency



Policies for *regular* accounts are not implemented for *privileged* accounts

Key Business Drivers



- Proactive Improvement of Information Security Practices
 - Lost and Risk prevention
 - Return on Investment
 - Administrative Password Management
- Internal Breach
- Return On Investment
 - Efficiency and Productivity
- Regulatory Compliance (Sarbanes Oxley, PCI, BS7799 etc.)
 - Auditing and Reporting
 - Control
 - Segregation of Duties

Requirements for Privileged Accounts Management Solution

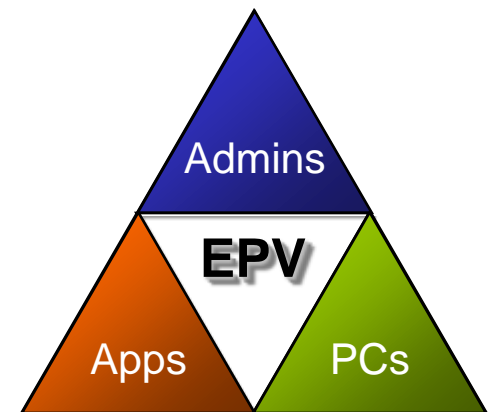


- ✓ Exceptionally secure solution for the keys of the kingdom
- ✓ Supreme performance, availability and disaster recovery due to its mission-critical nature
- ✓ Flexible distributed architecture to fit the enterprise complex network topology
- ✓ Single standard solution for a multi-facet problem
- ✓ Intuitive and robust interfaces

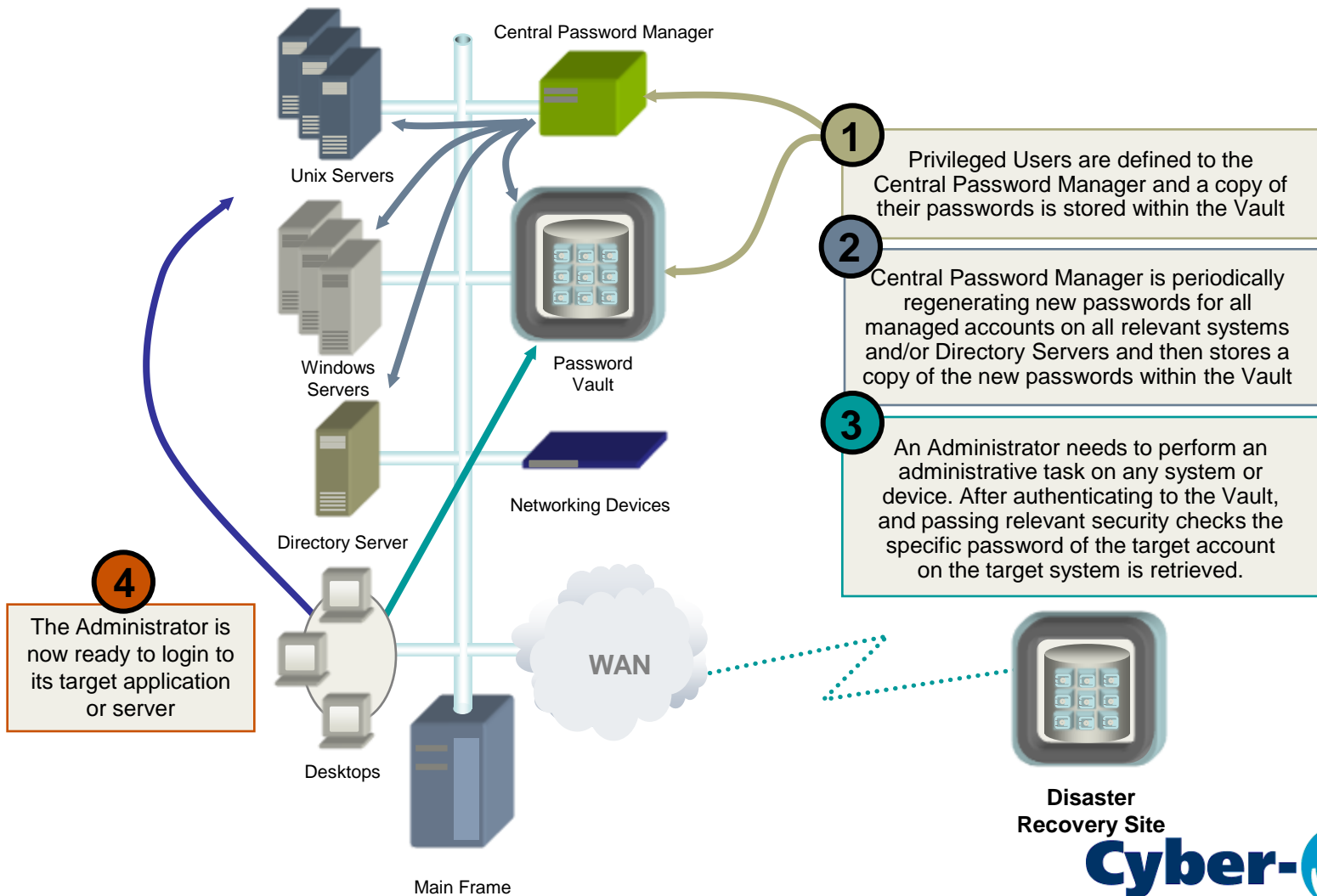
Cyber-Ark Enterprise Password Vault



- Cyber-Ark Enterprise Password Vault:
 - Provides manageability, control and audit of privileged accounts
 - Reduces cost and resources associated with privileged accounts
 - Enhances security and reduces risk related to privileged accounts
- Covers all three aspect of privileged accounts:
 - Administrative Accounts
 - Applications Accounts
 - Personal Computer (Local admins)
- Integrates with and complements Identity Management solutions



Password Vault Architecture



Application Password Management



Before:

- \$ IF P1.EQS. "TEST" THEN PW = **"TEST"**
- \$ IF P1.EQS. "PPRD" THEN PW = **"PPRD"**
- \$ IF P1.EQS. "QUAL" THEN PW = **"QUAL"**
- \$ CSTRING := "FIMSUSR/"PW"
- \$ SQLPLUS 'CSTRING @FIN\$PLUS:FORAPPL.SQL 'P1

After:

- \$ IF P1.EQS. "TEST" THEN PW = **getPassword("TestPass")**
- \$ IF P1.EQS. "PPRD" THEN PW = **getPassword("PprdPass")**
- \$ IF P1.EQS. "QUAL" THEN PW = **getPassword("QualPass")**
- \$ CSTRING := "FIMSUSR/"PW"
- \$ SQLPLUS 'CSTRING @FIN\$PLUS:FORAPPL.SQL 'P1



Thank You

David Adamczyk

Channel Sales Manager

Cyber-Ark Software

david.adamczyk@cyber-ark.com

