

Safeguarding Information Assets *From Doors to Desktops*



Step 1 of 3: Recognize Screen
To learn the screen, please use your mouse to drag the magnifier and drop it on the screen of this application.
Learn Screen



Server information

OneSign Server process running
Number of requests handled by OneSign Server since start
Average Server response time

David Ting
Founder and CTO
Imprivata, Inc.
dting@imprivata.com



What's Happening Out There?



Step 1 of 3: Recognize Screen
To learn the screen, please use your mouse to drag the magnifier and drop it on the screen of this application.



Server information

OneSign Server process running
Number of requests handled by OneSign Server since start
Average Server response time

Data Protection Regs/Mandates

... Y2K without an end date!

Canada

- The Privacy Act 1983
- PIPEDA 2001

Scandinavia

- Finland - FPDA 1995/1999
- Denmark - DPRA 1978, APPD 1995/2000
- Sweden - PDPA 1995/1998

United States

- FCRA 1970
- PA 1974/1975
- RFPA 1978
- CTVPA 1984
- ECPA 1986
- VPPA 1988
- HIPAA 1996/2002
- COPPA 1998/2000
- DMPEA 1999/2000
- FSMA/GLBA 1999/2001
- Sarbanes-Oxley 2002
- PCI 2004

UK/Ireland

- Ireland - DP(A)A 1995/2003
- UK - DPA 1995/2000

Europe

- Belgium - LPPLRPPD 1992, DPA 1995/2001
- Germany - FDPA 1995/2001
- Austria - DPA 1995/2000
- Luxembourg - "EUD" 1995/2002
- Netherlands - PDPA 1995/2001
- France - ADPDFIL 1978, "EUD" 1995/Pending
- Spain - DPA 1995/2000
- Italy - DPA 1995/1997
- Portugal - PDPA 1995/1998
- Greece - PIPPD 1995/1997
- Eastern Europe - Estonia (96), Poland (98), Slovak (98), Slovenia (99), Hungary (99), Czech (00), Latvia (00), Lithuania (00)

Mexico

- eCommerce Act 2000

South America

- Chile - APPD 1998
- Argentina - PDPA 2000

Asia Pacific

- Australia - PA/PA(PS)A 1988/2000 2001
- New Zealand - Privacy Act 1993
- Hong Kong - Personal Data 1996
- Taiwan - CPPDP Law 1995
- South Korea - eCommerce Act 1999
- Japan - J-SOX 2006

Source: CSC and IDC, 2006

Look Familiar?



RCMP asked to probe Club Monaco security breach

Updated Fri, Jan. 26 2007 11:07 PM ET

CTV.ca News Staff

Club Monaco has asked the RCMP to investigate a possible privacy breach involving the credit card numbers of some of its shoppers.

December 14, 2006

Thief jets with Boeing staff data

Filed under: [Privacy](#)

Kaiser Permanente Laptop Stolen

Personal Data on 38,000 Members Missing

Nationwide Insurance data stolen

Records of 28,279 health insurance customers contained claim information

Johns Hopkins Loses Data On 130,000 Patients, Employees

By [Sharon Gaudin](#), *InformationWeek*

Fri, Feb. 09, 2007

Johns Hopkins disclosed this week that it has lost the personal data on roughly 52,000 employees and 83,000 patients.

The New York Times

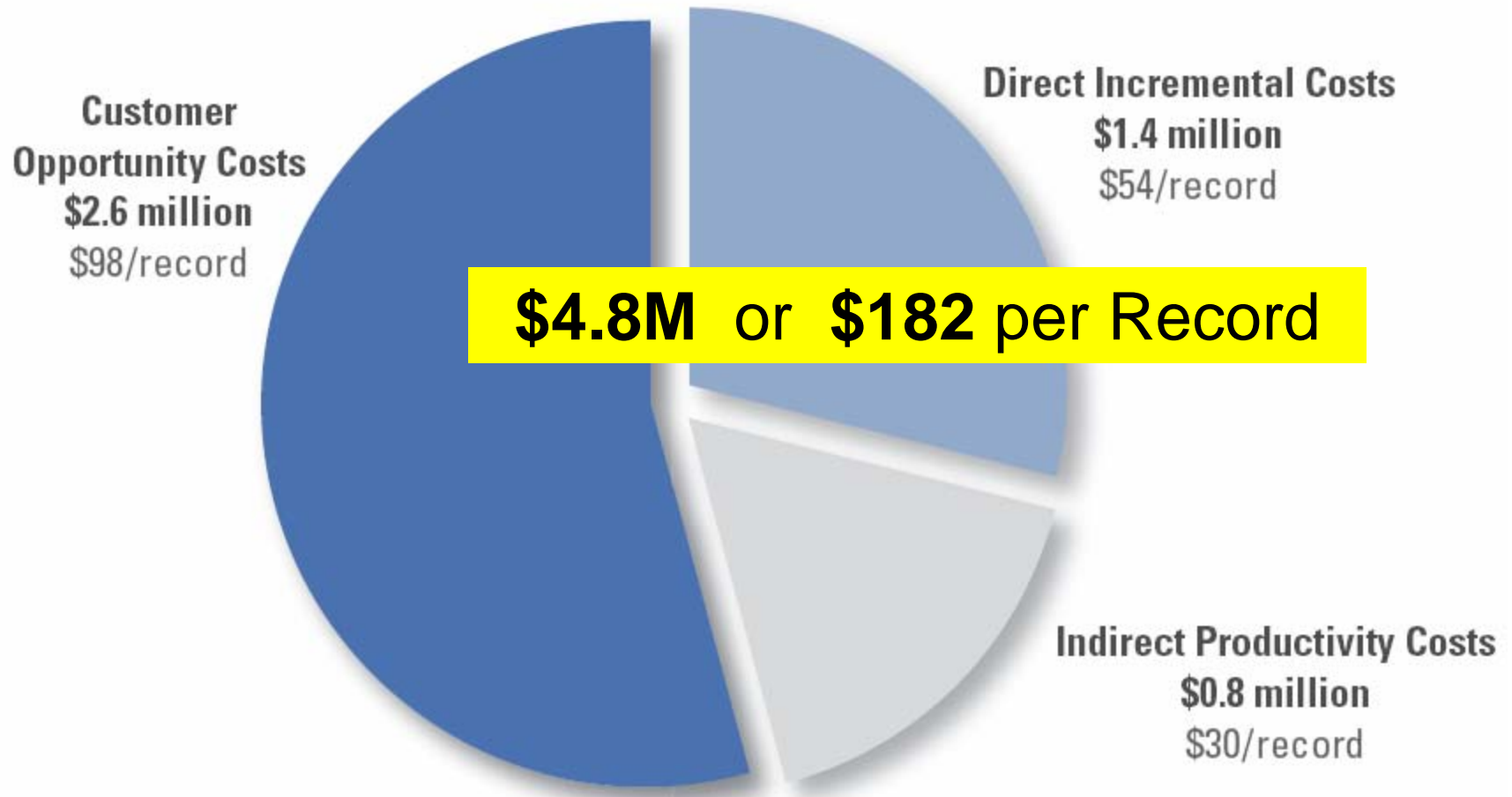
Data Breach Could Affect Millions of TJX Shoppers

By ERIC DASH

Published: January 19, 2007

Tens of millions of credit and debit cards might have been compromised by a computer security breach

Data Breach Costs Per-Incident



Data Breach Costs by Category

■ \$300K for Detection and Escalation

- Internal investigation
- Legal, audit, consulting

■ \$700K for Initial Notification

- Letters
- Emails
- Telephone
- Published media
- Website

■ \$1.2M for Post Notification

- Mail
- Emails
- Telephone to internal call center
- Telephone to outsourced call center
- Legal defense services
- Criminal investigations (forensics)
- Public or investor relations
- Free or discounted services

■ **\$2.6M for Brand Impact**

- Cost of turnover
- Cost of fewer new customers

2006 CERT /SEI Study on Insider Threat

- **Fraud – obtain property/services through deception or trickery**
 - Current Employees – non-technical; non-management positions
 - Many had privileged access – access during work hours
- **Theft of Confidential Information – stealing proprietary information from organization**
 - Current Employees – half with technical positions (and had accepted new positions)
 - Used own or compromised accounts – accessed during work hours
- **IT Sabotage Attack – intent to harm a specific individual organization or organization’s data or daily business**
 - Former Employees – highly technical position
 - Backdoor accounts, shared accounts, other employees accounts
 - Remote access outside normal work hours

CERT – A Risk Mitigation Model: Lessons Learned from Actual Insider Sabotage
Dawn M. Cappelli, Andrew P. Moore, Eric D. Shaw
Nov 7, 2006

**32% of Fraud/Theft is
Insider-based**

US-CERT Common Sense Guide

- Institute periodic enterprise wide risk assessment
- Institute periodic employee security awareness training
- Enforce separation of duties and least privilege
- Implement strict password and account management policies and practices
- Log, Monitor and audit employee online actions
- Use extra caution with system administrators and privileged users
- Actively defend against malicious code
- Use layered defenses against remote attacks
- Monitor and respond to suspicious or disruptive behavior
- Deactivate computer access following termination
- Collect and save data for use in investigations
- Implement secure backup and recovery processes
- Clearly document insider threat controls

CERT – A Risk Mitigation Model: Lessons Learned from Actual Insider Sabotage

Dawn M. Cappelli, Andrew P. Moore, Eric D. Shaw

Nov 7, 2006

The Role of Convergence



Step 1 of 3: Recognize Screen

To learn the screen, please use your magnifier and drag the magnifier and drop it on the screen of this application.

Learn Screen



Server information

OneSign Server process running
Number of requests handled by OneSign Server since start
Average Server response time

Convergence Hype

“Just a buzz word – has no real impact on security”

“Requires complex organizational changes”

“IT will run physical security”

“Only possible with an integrated Identity Management system”

“Just a means to improve operational efficiency”

“Will require overhaul of cards, door readers and access systems”

Many Definitions

**Convergence of
Identities**

**Convergence of
Systems & Workflows**

**Convergence of
Credentials**

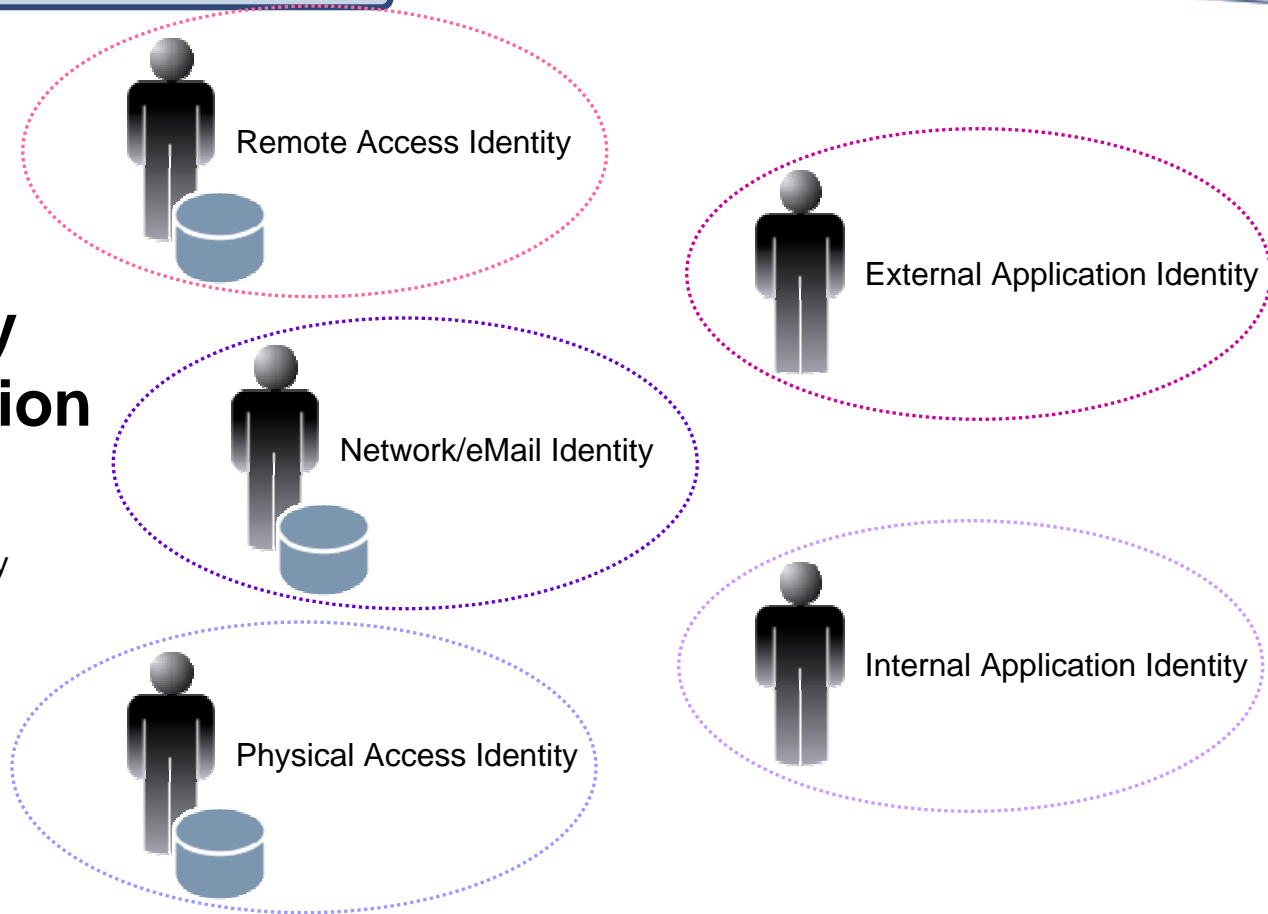
**Convergence of
Devices**

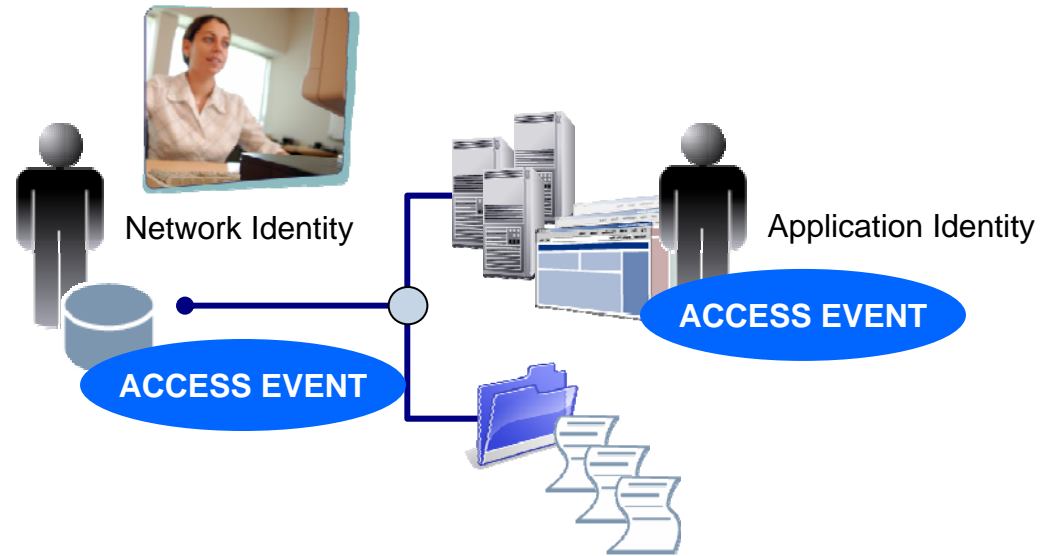
Convergence of Identities

Identity Proliferation

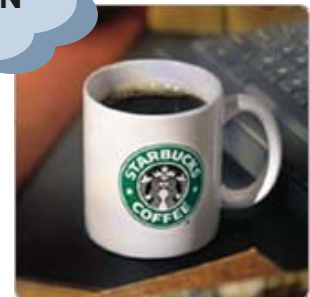


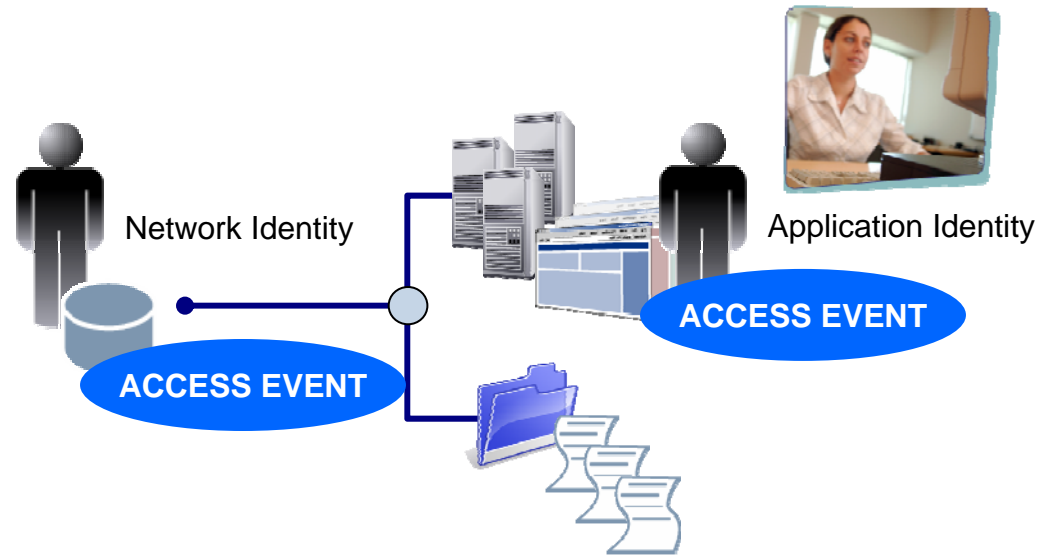
True Identity

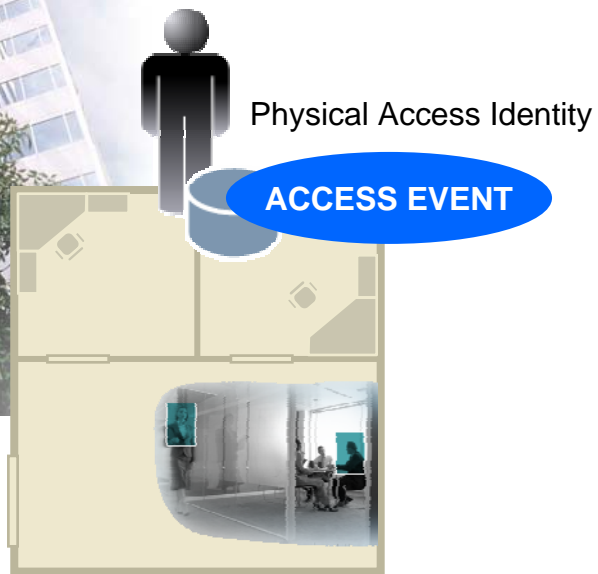
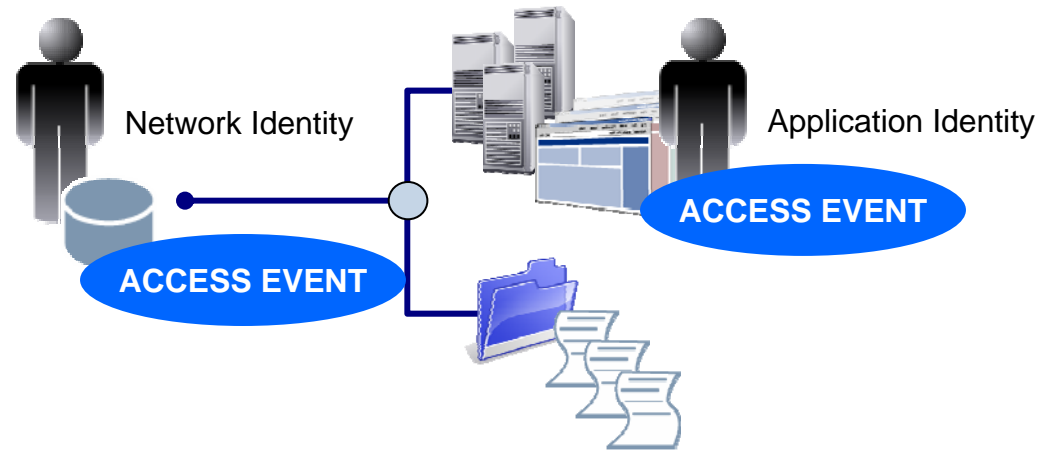


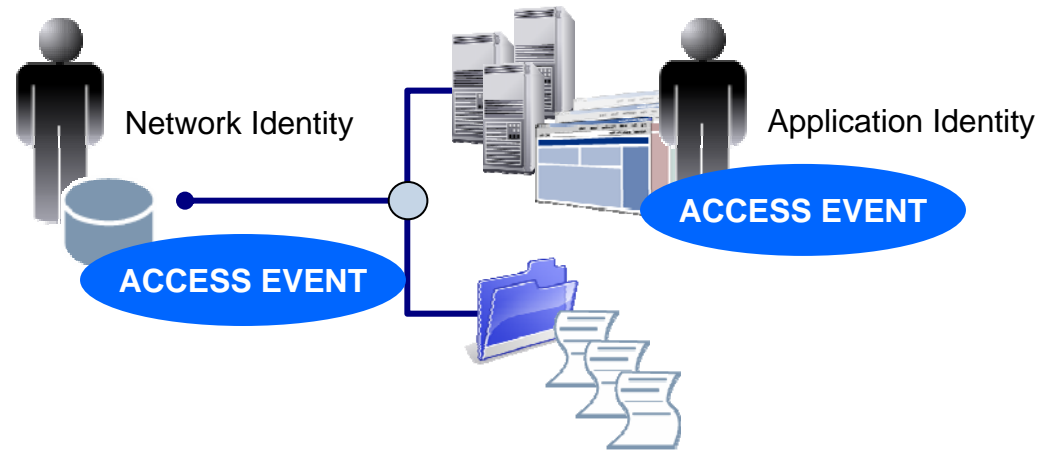


Remote VPN Access

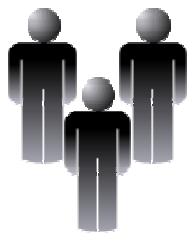








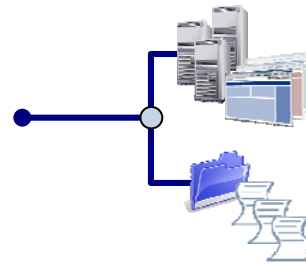
How do you safeguard information assets? How do you demonstrate compliance?



Disparate Identities



Disparate Locations

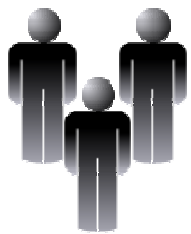


Discrete Systems



Discrete Access Events

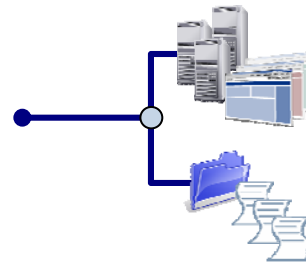
How do you safeguard information assets? How do you demonstrate compliance?



Disparate Identities



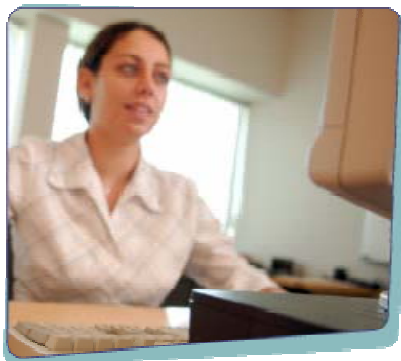
Disparate Locations



Discrete Systems

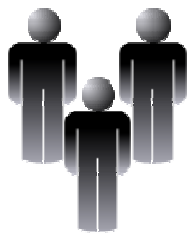


Discrete Access Events



Validate Identities

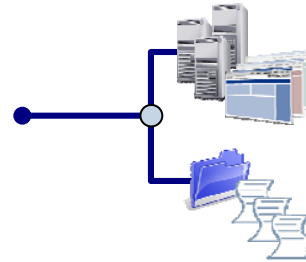
How do you safeguard information assets? How do you demonstrate compliance?



Disparate Identities



Disparate Locations



Discrete Systems

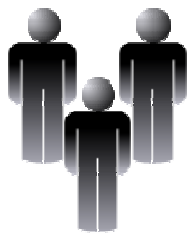


Discrete Access Events



Confirm location

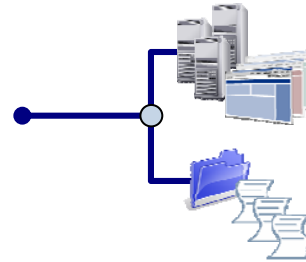
How do you safeguard information assets? How do you demonstrate compliance?



Disparate Identities



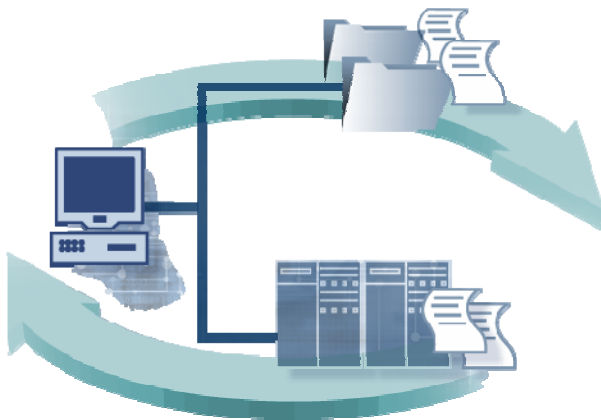
Disparate Locations



Discrete Systems

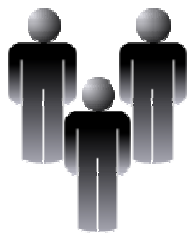


Discrete Access Events



Enforce Access Policy

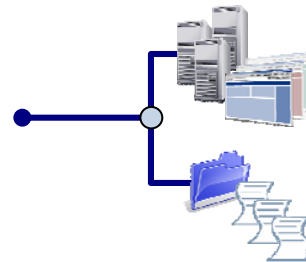
How do you safeguard information assets? How do you demonstrate compliance?



Disparate Identities



Disparate Locations



Discrete Systems



Discrete Access Events

Track, Trace, Report

8:15 AM
Entered building

8:27 AM
Entered Zone A

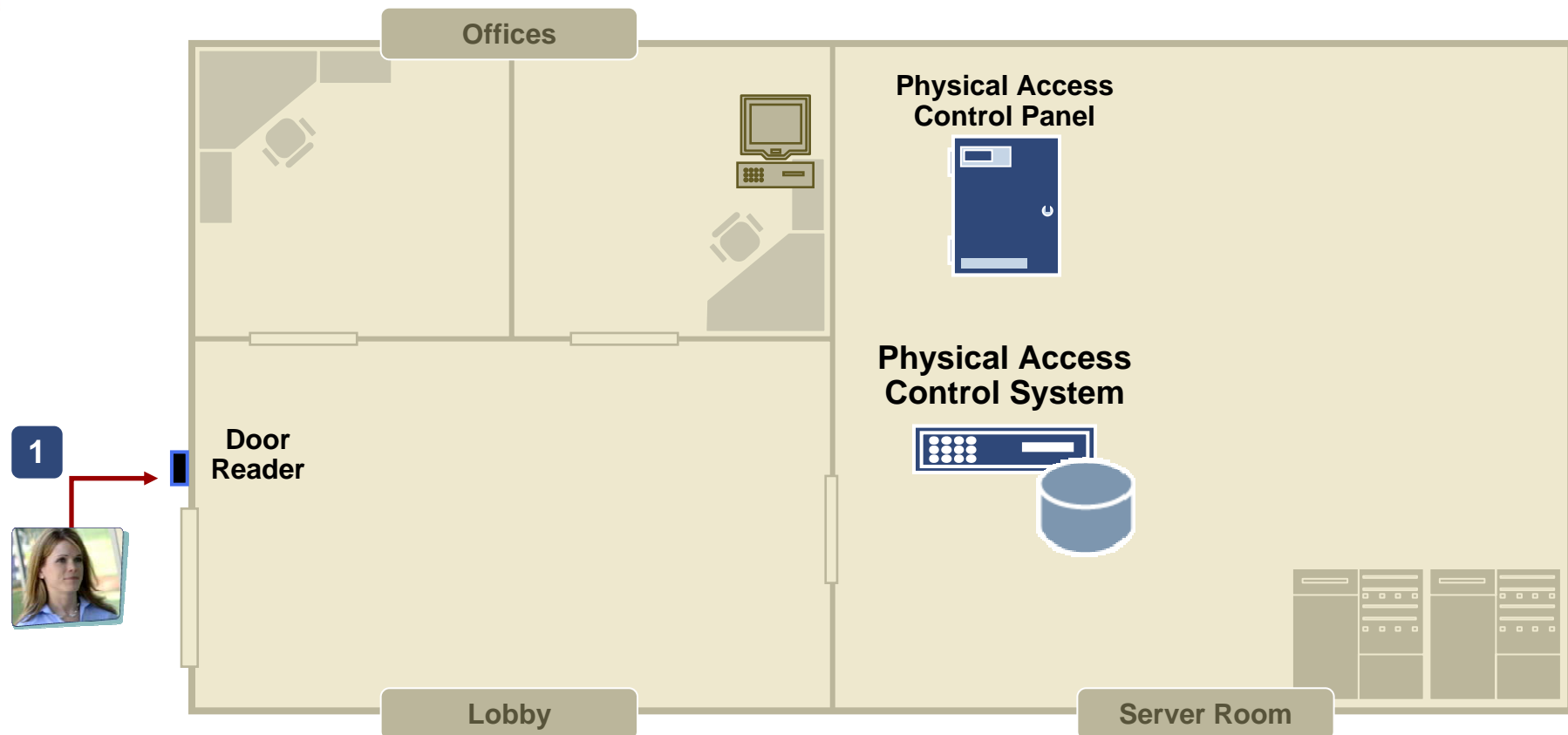
8:35 AM
Authenticated to Network

10:10 AM
Logged into Application Y

5:15 PM
Logged off Network

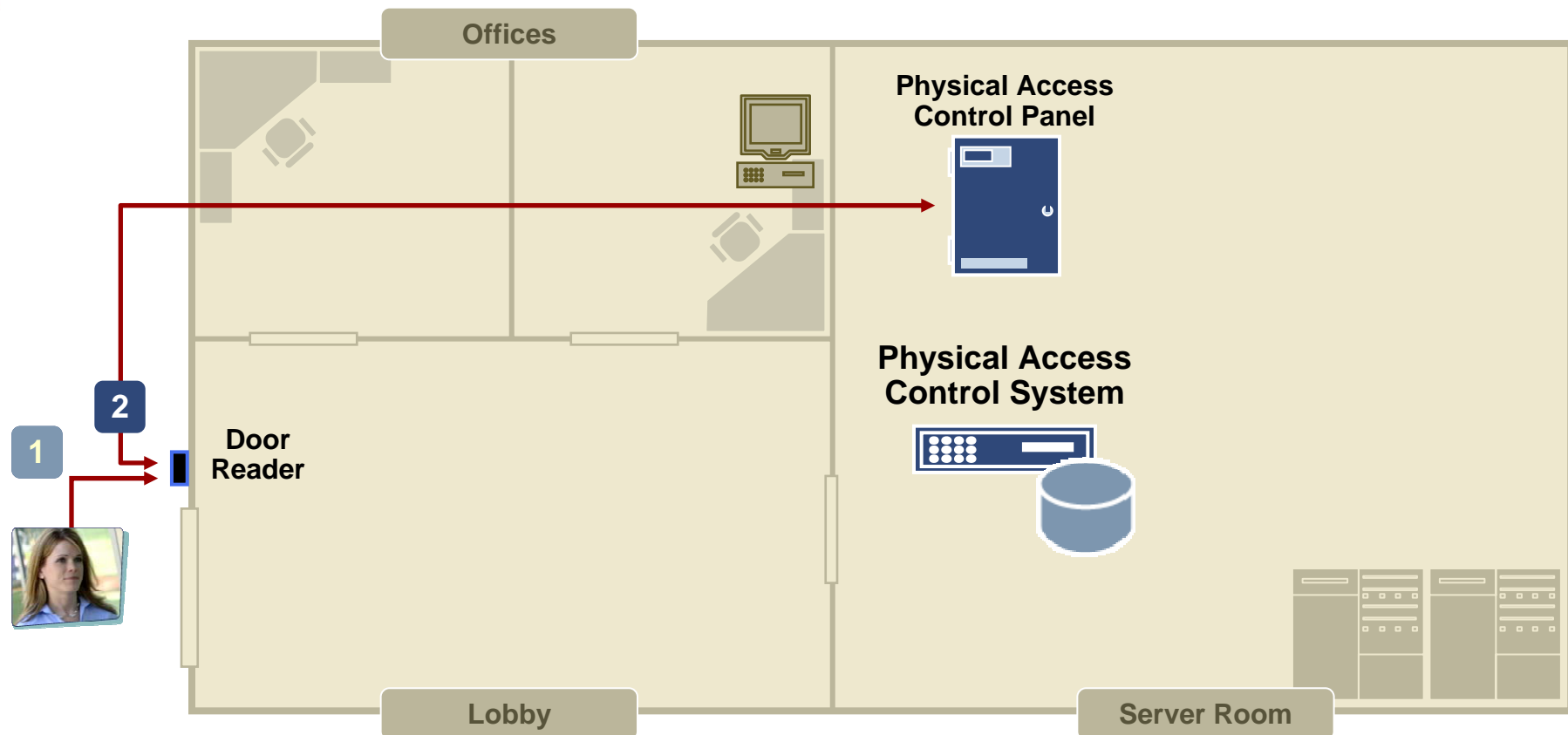
5:32 PM
Exited Building

Identity-based Convergence



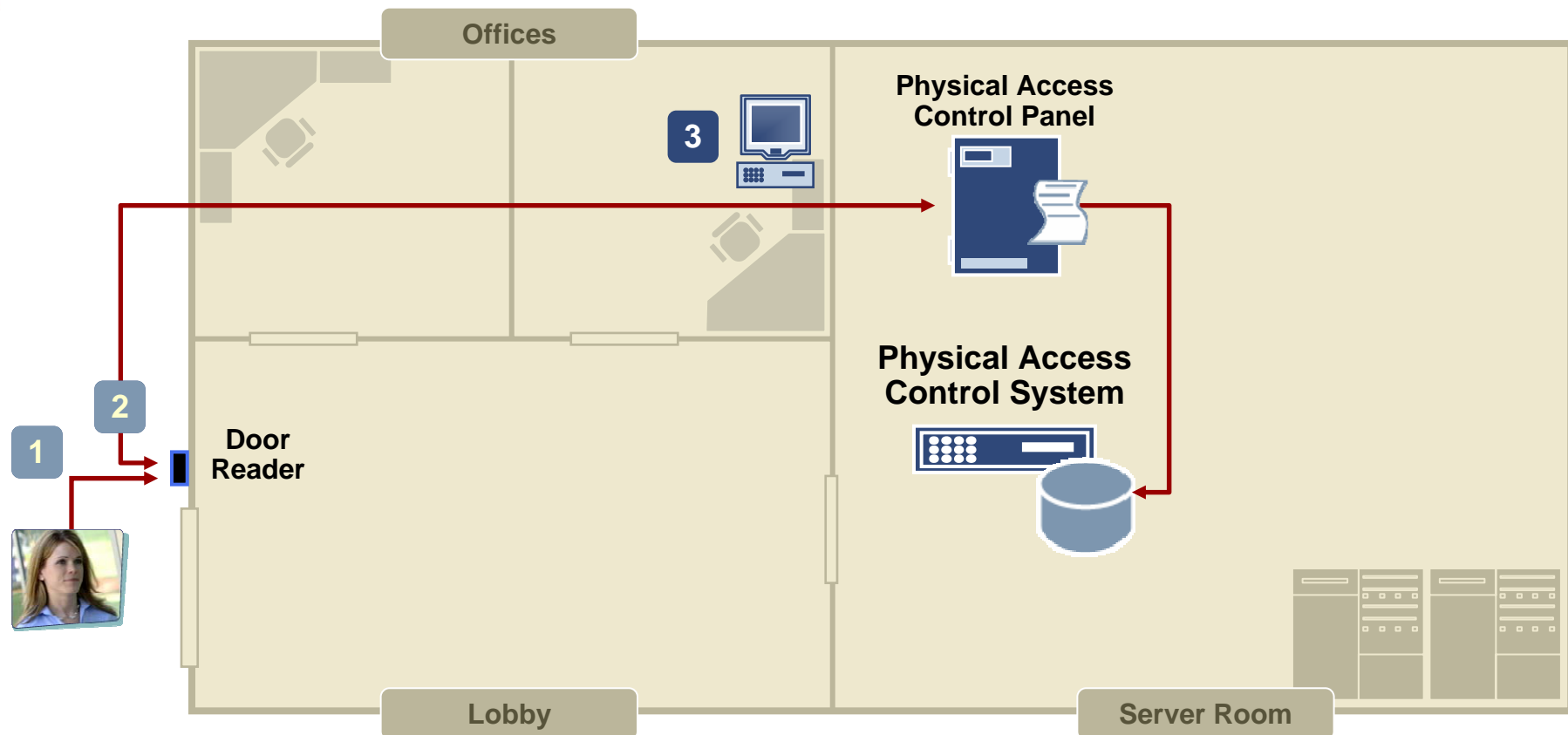
STEP 1: Employee attempts secure entry to building or workplace zone

Identity-based Convergence



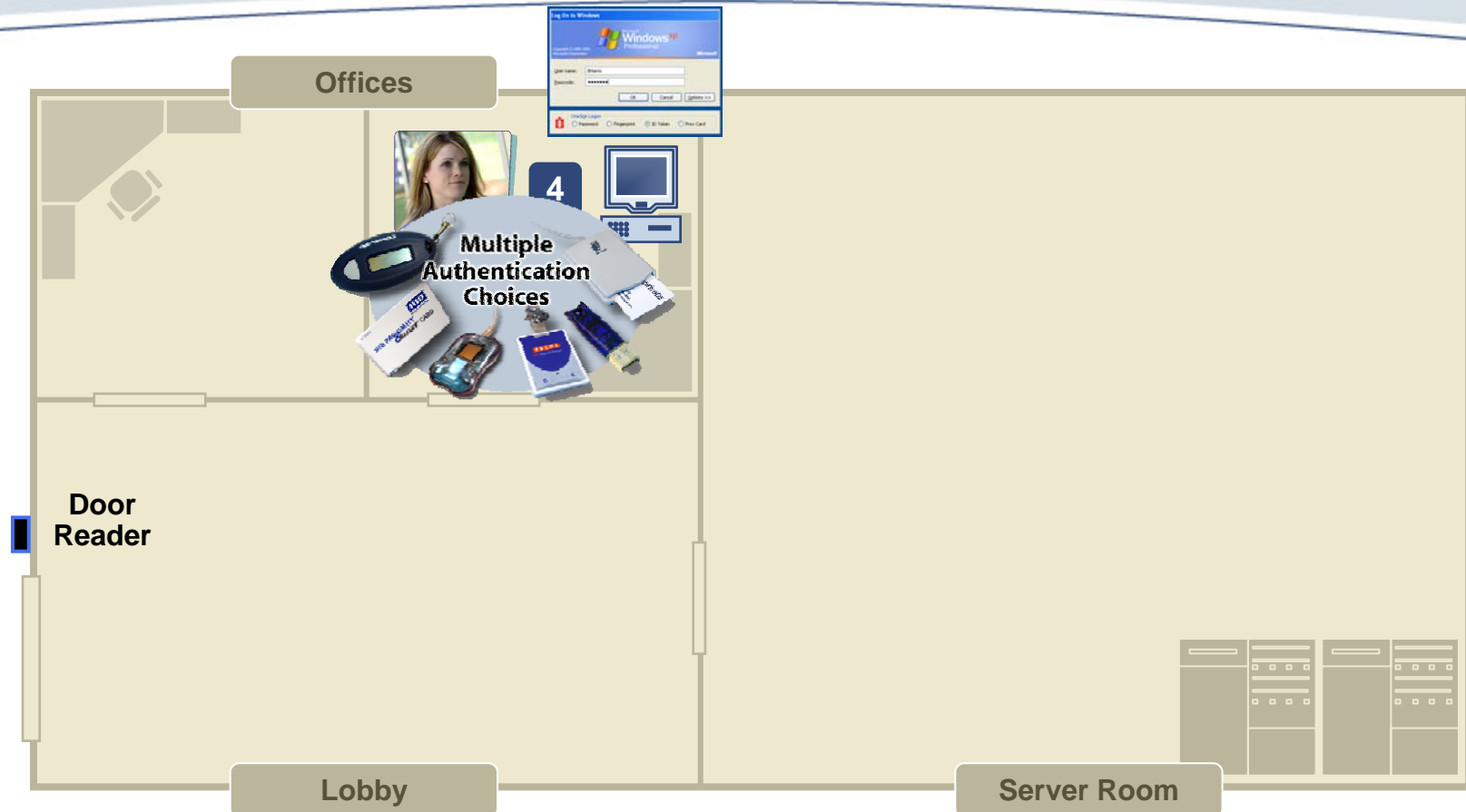
STEP 2: Physical Security system validates employee and unlocks door

Identity-based Convergence



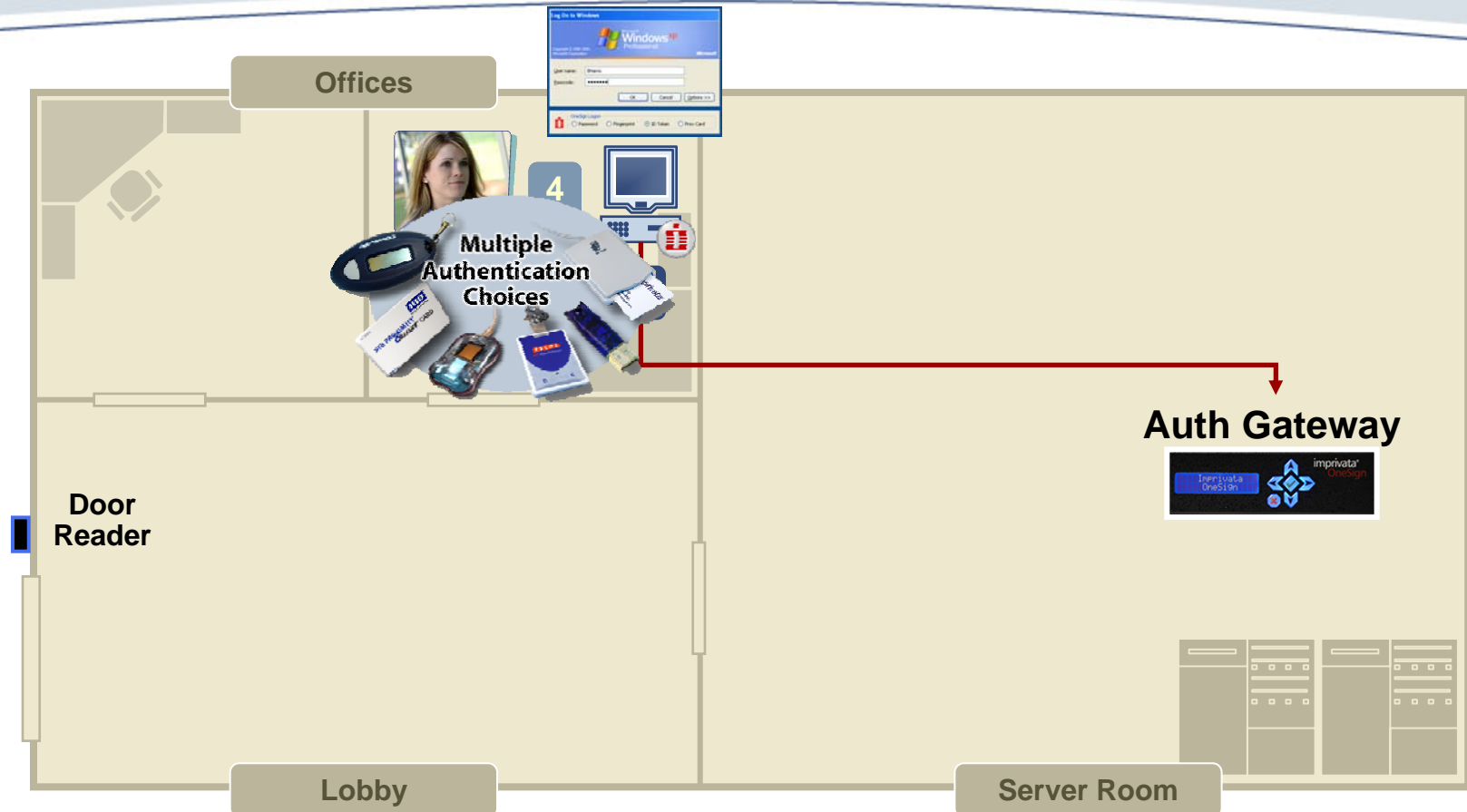
STEP 3: Employee enters workplace; entry log is recorded

Identity-based Convergence



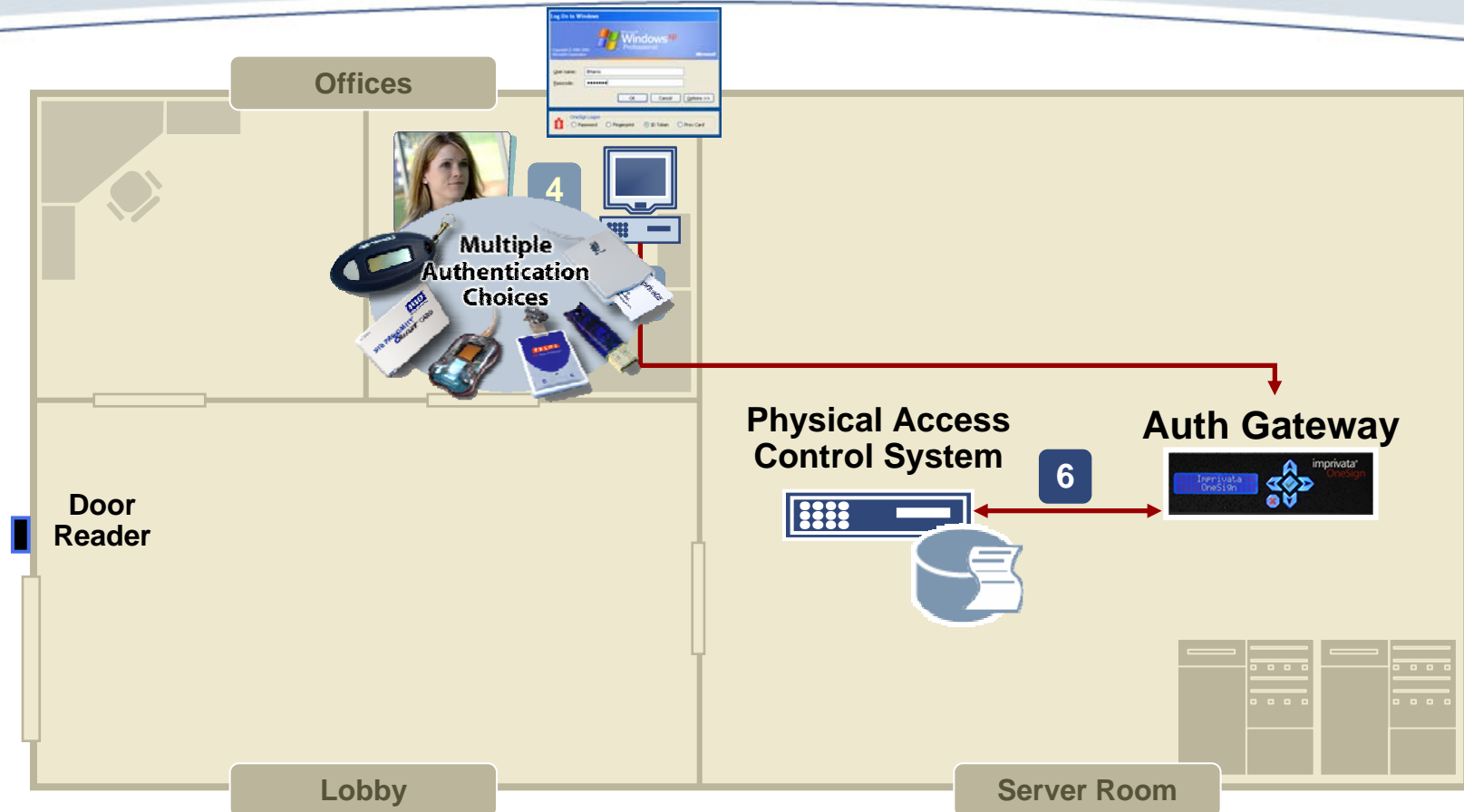
STEP 4: Employee attempts login to local network

Identity-based Convergence



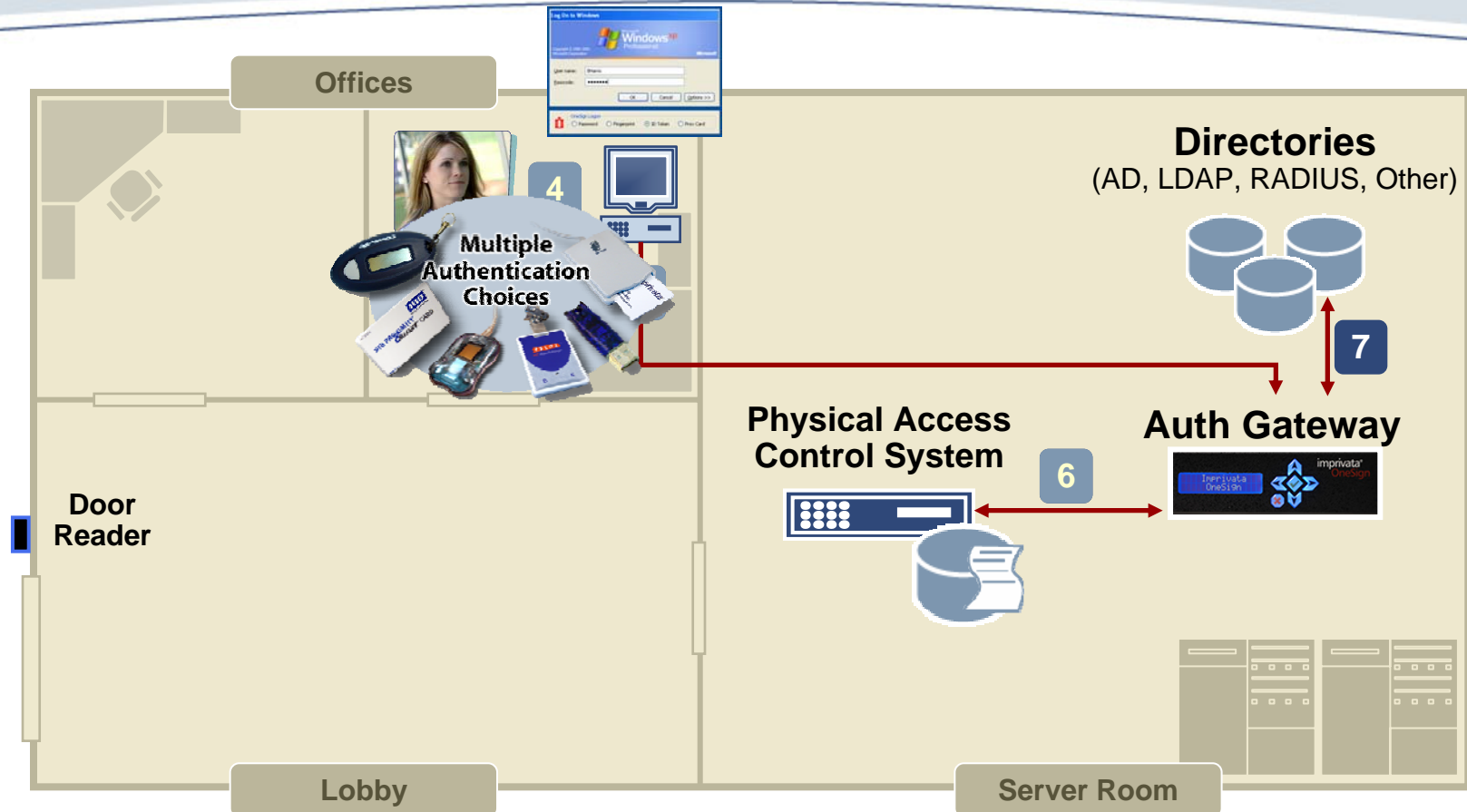
STEP 5: Logon Agent makes request to Authentication Gateway

Identity-based Convergence



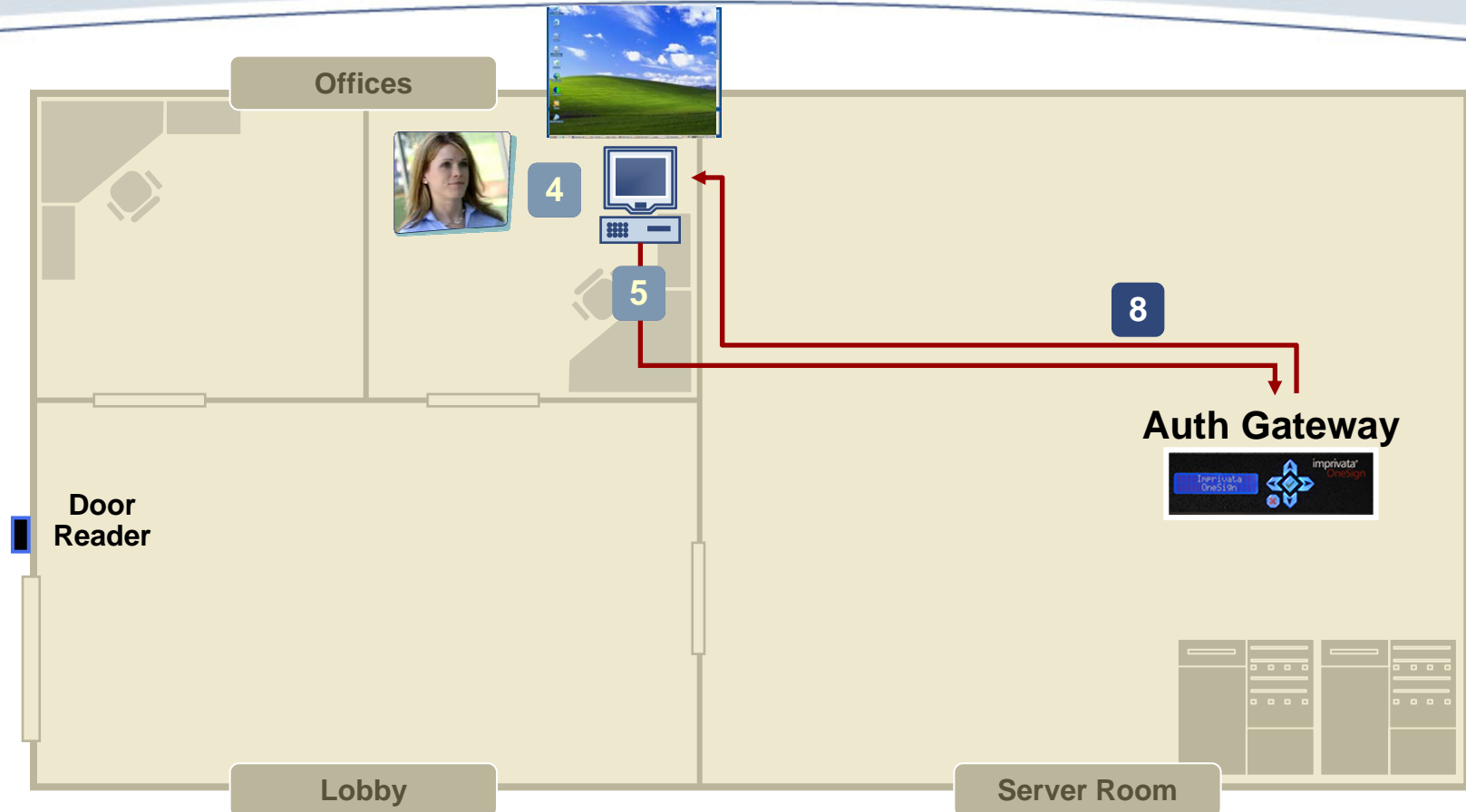
STEP 6: Authentication Gateway verifies that employee is active badge holder and has authenticated into workplace or zone

Identity-based Convergence



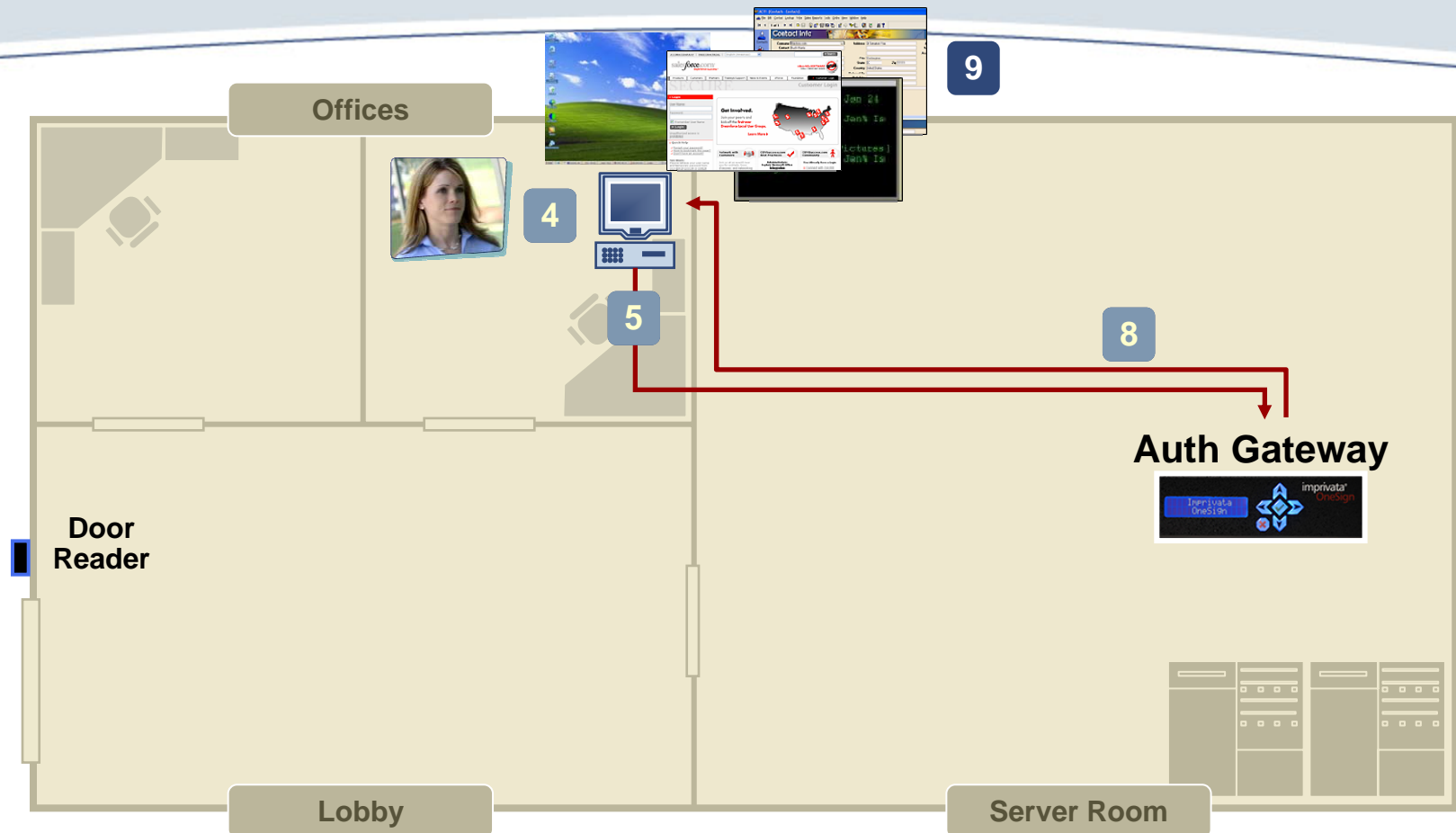
STEP 7: Authentication Gateway verifies employee's network privileges with IT directories

Identity-based Convergence



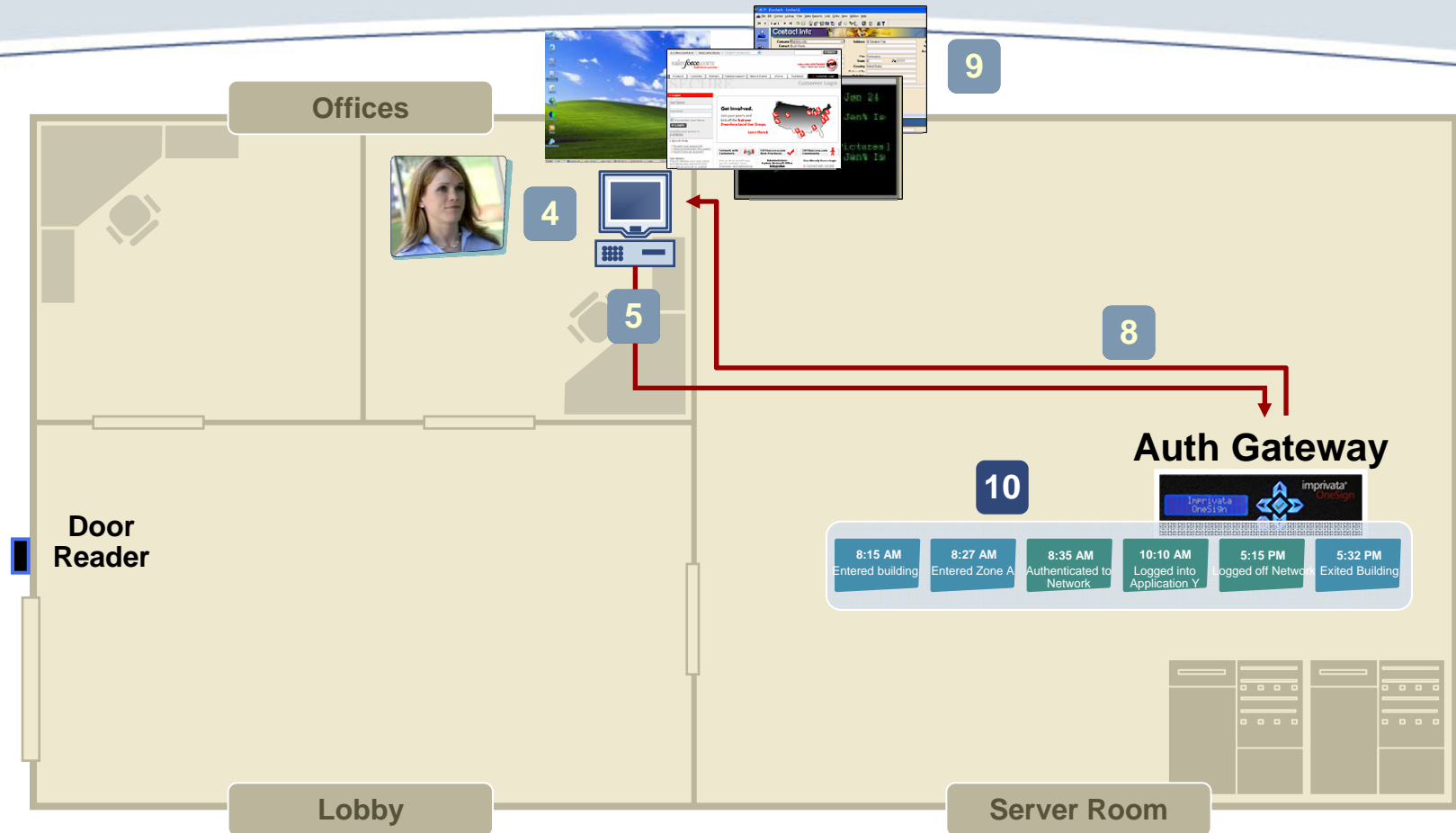
STEP 8: Logon Agent authenticates employee to the network or computer

Identity-based Convergence



STEP 9: Single sign-on enables seamless application access

Identity-based Convergence



STEP 10: Converged Login with real-time, integrated event reporting
(Who accessed what, when, and *from where*)

Information Security Requirements

- **Define an access policy for the individual independent of the identity**
- **Enforce the policy by:**
 - Increase confidence in identifying the user
 - Strong authentication
 - Location-based authentication
 - Aggregate information from all sources
 - Network, remote, physical access, application
 - Apply policy with as much information as possible
- **Control passwords to applications**
- **Deter malicious use through converged auditing back to true or network identity**
 - Who, what, where, when, how?
- **Act on real-time changes to the status of the user**

Consolidate Identities

■ Enforce policy

- Control choke points
 - Network, remote, application access logons
- Implement strong authentication
- Integrate location/user status location from physical access system
- SSO to automate entry of passwords to applications

■ Integrated auditing

Identity Convergence Applied Against CERT Common Sense Guide

- Institute periodic enterprise wide risk assessment
- Institute periodic employee security awareness training
- Enforce separation of duties and least privilege
- Implement strict password and account management policies and practices
- Log, Monitor and audit employee online actions
- Use extra caution with system administrators and privileged users
- Actively defend against malicious code
- Use layered defenses against remote attacks
- Monitor and respond to suspicious or disruptive behavior
- Deactivate computer access following termination
- Collect and save data for use in investigations
- Implement secure backup and recovery processes
- Clearly document insider threat controls

CERT – A Risk Mitigation Model: Lessons Learned from Actual Insider Sabotage

Dawn M. Cappelli, Andrew P. Moore, Eric D. Shaw

Nov 7, 2006

Questions?

