Exploring Converged Access of IT Security and Building Access

Today, Tomorrow and the Future

Julian Lovelock

ActivIdentity,
part of HID Global

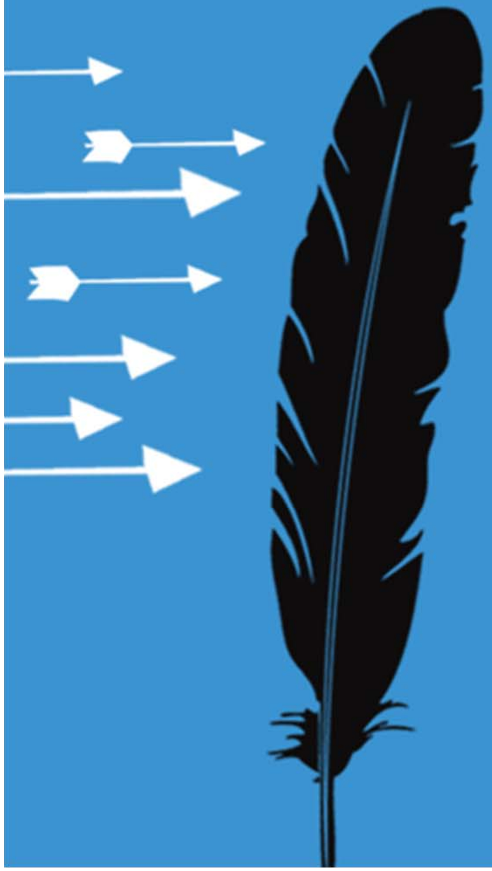
Session ID: SPO2-106

Session Classification: Intermediate

RSACONFERENCE2012

Synopsis

- Domains of Physical & IT security have hitherto been separate worlds
- This is changing, albeit differently across different verticals
- Technology & economics are driving factors.
- These changes bring opportunities for better security at reduced cost



The stereotypes

Stereotypes - Physical Security

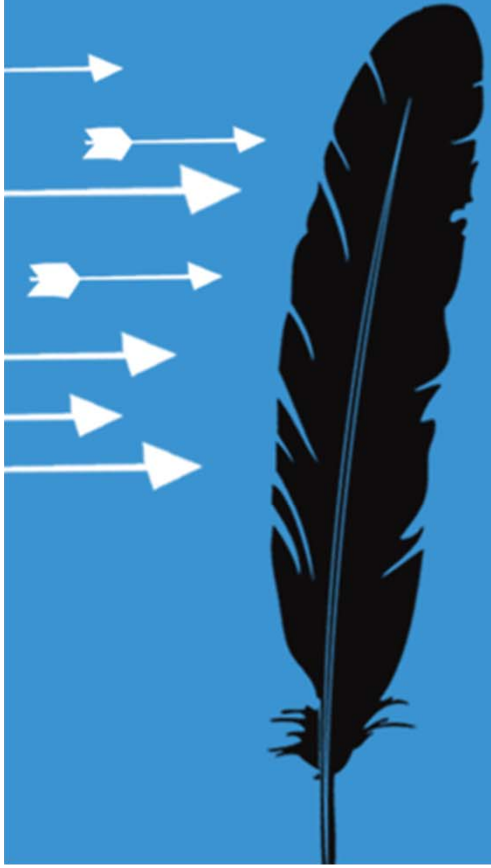
In the blue corner,

- Ex-Cop or Military
- Likes dogs, guns and fences
- Doesn't trust computers

Stereotypes – IT Security

In the red corner..

- Doesn't understand the practical issues
- Thinks corporate security is mainly about firewalls
- Gets all the budget
- Not good with people



The reality

Corporate Security is concerned with a broad range of critical Security Issues

- Agriculture / farming / food manufacturing
  - Food Defense/Supply Chain, Workforce protection

- Arenas/stadiums/leagues/entertainment
  - Crowd control, Game integrity, Terrorism

- Business services
  - International travel, Counter intelligence / espionage

Source: Securitymagazine.com Nov 2011 edition

Critical Security Issues (cont)

- Construction/Real Estate/Property Management
  - Organized crime, Workplace violence, Theft
- Education
  - Talent Management, Bullying
- Energy (Oil & Petroleum)
  - In country civil unrest, Facility Threats

Source: Securitymagazine.com Nov 2011 edition

Critical Security Issues (cont)

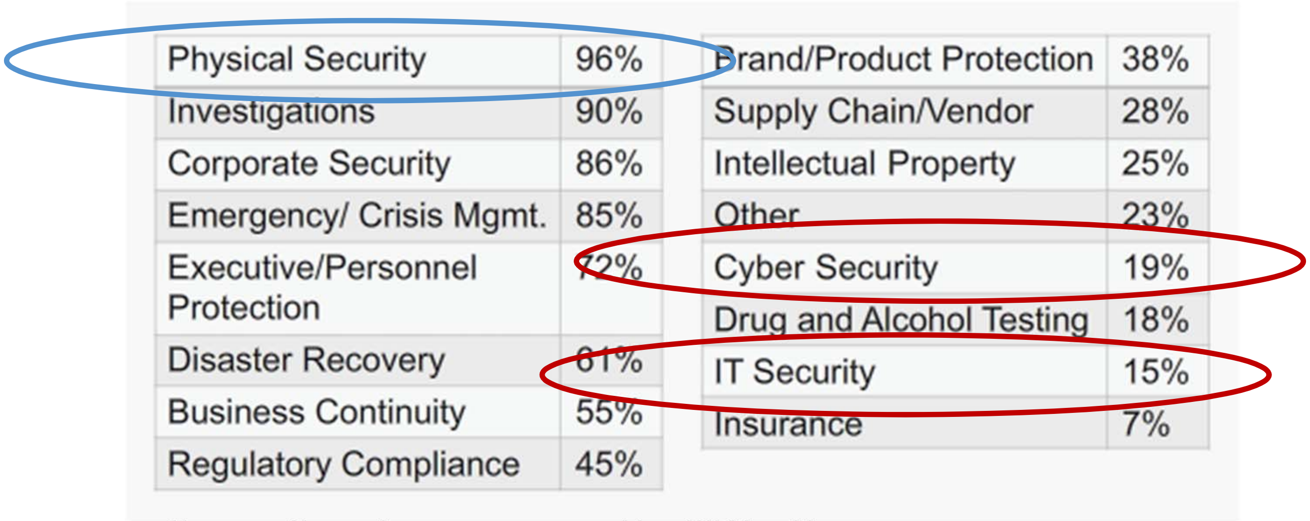
The list goes on across a range of 19 sectors…

Including: Finance/Banking/Insurance, Government, Healthcare, Hospital/Medical Centers, Hospitality/Casinos, Industrial/Manufacturing, IT/ Communications / Media, Ports/Terminals, Retail, Transportation & Logistics, Utilities

63% cited Cyber-Crime as a Critical Issue.

Source: Securitymagazine.com Nov 2011 edition

CSO Responsibilities



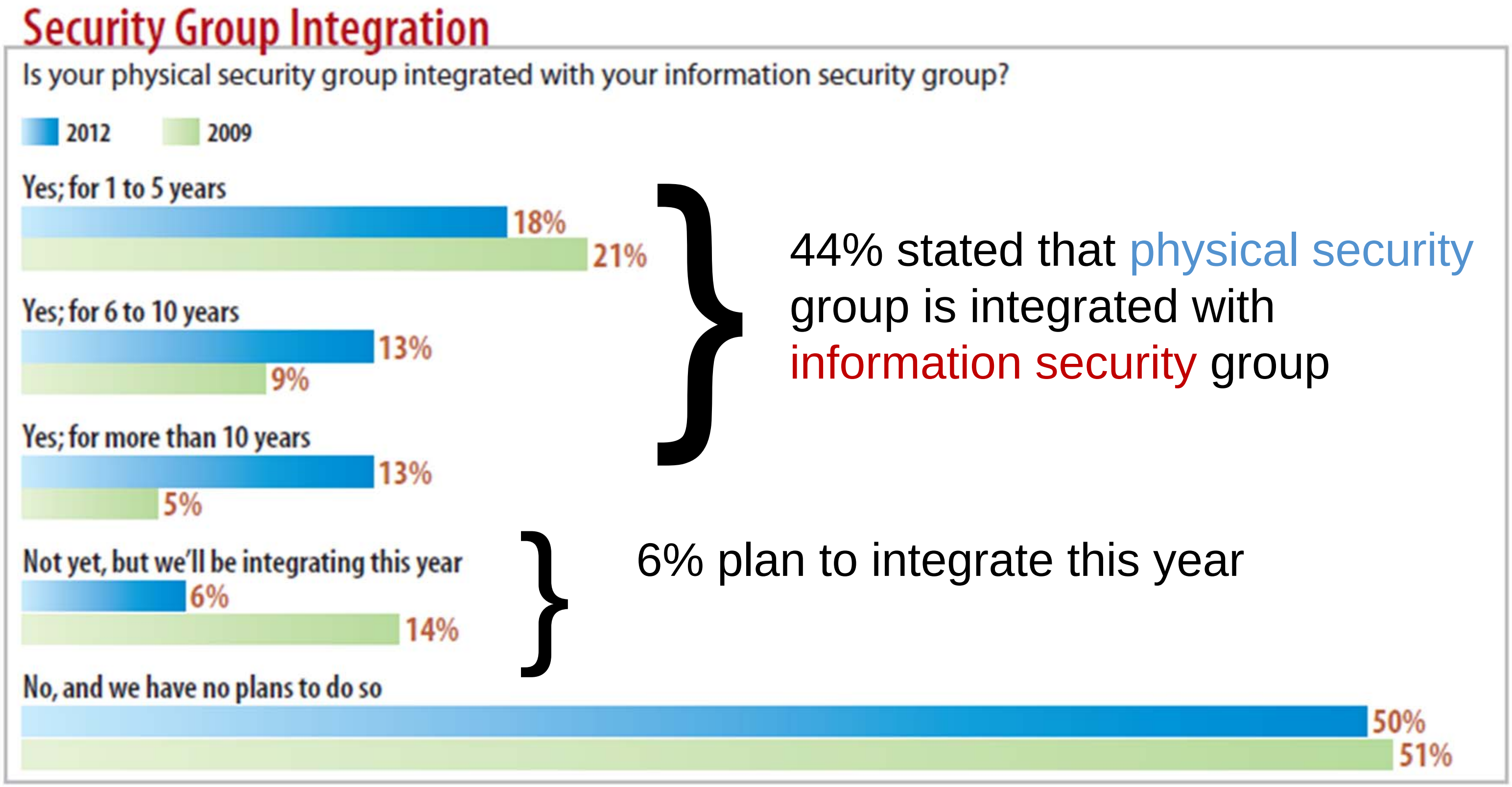
Physical Security	96%
Investigations	90%
Corporate Security	86%
Emergency/ Crisis Mgmt.	85%
Executive/Personnel Protection	72%
Disaster Recovery	61%
Business Continuity	55%
Regulatory Compliance	45%

Brand/Product Protection	38%
Supply Chain/Vendor	28%
Intellectual Property	25%
Other	23%
Cyber Security	19%
Drug and Alcohol Testing	18%
IT Security	15%
Insurance	7%

Source: Securitymagazine.com Nov 2011 edition

Less than 50% of CSOs listed IT/Cyber security as a responsibility

Departmental Integration



44% stated that physical security group is integrated with information security group

6% plan to integrate this year

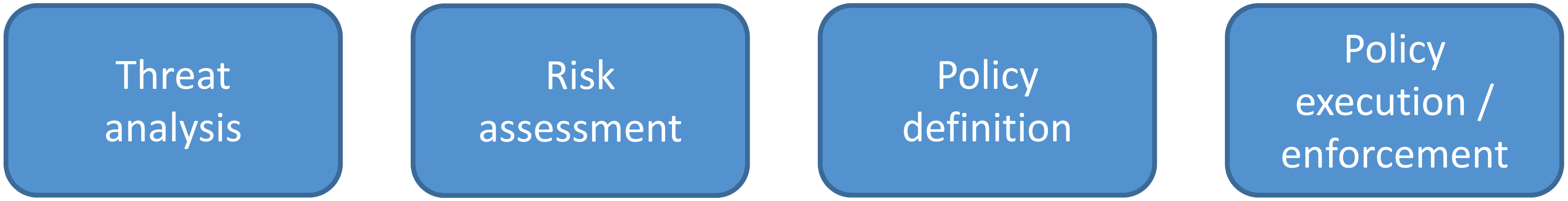
Base: 334 respondents in September 2011 and 314 in February 2009 R3621111/4
Data: *InformationWeek* Physical/Logical Security Survey of business technology professionals

Addressing Cyber Threats

Across those responsible for Corporate Security

- Majority identified IT security as a critical issue
- Minority control the IT security budget

Addressing Cyber threats requires a mix of “traditional” security skills and IT expertise.



Threat analysis

Risk assessment

Policy definition

Policy execution / enforcement

Organizations are faced with three options

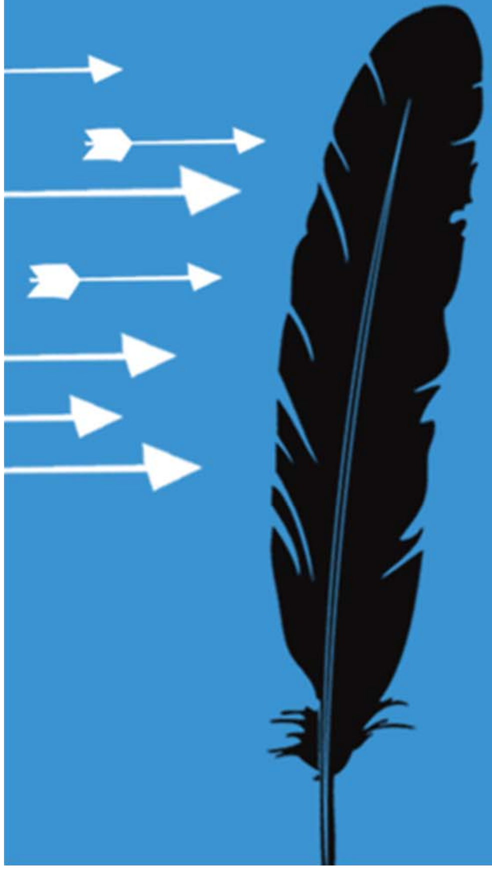
1. Re-organize
2. Collaborate
3. ~~Fail to address the issue~~

To get started...

- Physical Security needs to become “IT savy”
  - Substantial systems inter-dependencies
  - Physical security is impacted by IT security

  20% of physical security teams highlighted lack of knowledge of IP based systems as an issue – Information week survey 2012

- IT security dependent on corporate security policies
  - Almost all “cyber attacks” rely on human failing
  - IT should not publish a separate security policy



Market Trends

Technology & Market Trends

- Integrators, value added resellers and distributors addressing both
- Convergent User Management
- Convergent Credential – Common Access Card
- Convergent Logging
- Network interdependencies
- Context based access rules
- Evolution of physical access control solutions

Relative Market Maturity

	Physical Access Card Entry Systems	IT Security Strong Authentication Solutions
Already Implemented	78%	39%
Currently evaluating / considering implementing	9%	23%
No intention of implementing	13%	29%

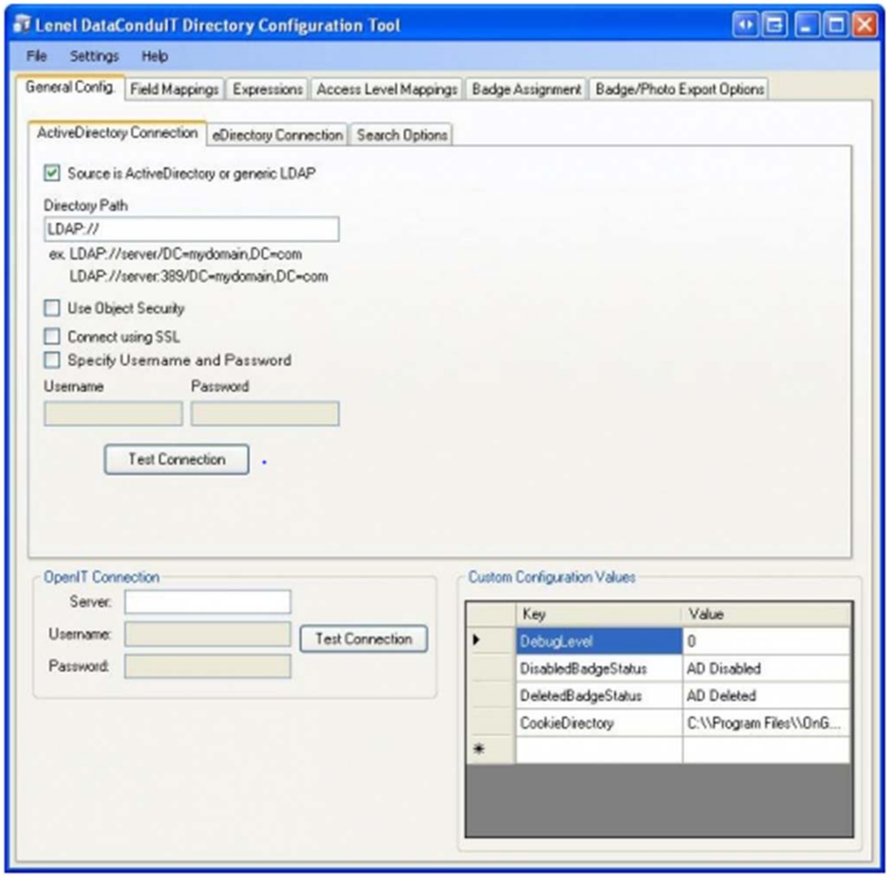
Source: CSO Market Pulse: Two-Factor Authentication Adoption

Technology & Market Trends

- Integrators, value added resellers and distributors addressing both
- Convergent User Management
- Convergent Credential – Common Access Card
- Convergent Logging
- Network interdependencies
- Context based access rules
- Evolution of physical access control solutions

Convergence of User management

- Integration with Active Directory
- Identity and PACS roles are defined and managed in AD



☑ Source is ActiveDirectory or generic LDAP

Directory Path: LDAP://

ex. LDAP://server/DC=mydomain,DC=com
LDAP://server:389/DC=mydomain,DC=com

□ Use Object Security

□ Connect using SSL

□ Specify Username and Password

Username:

Password:

Server:

Username:

Password:

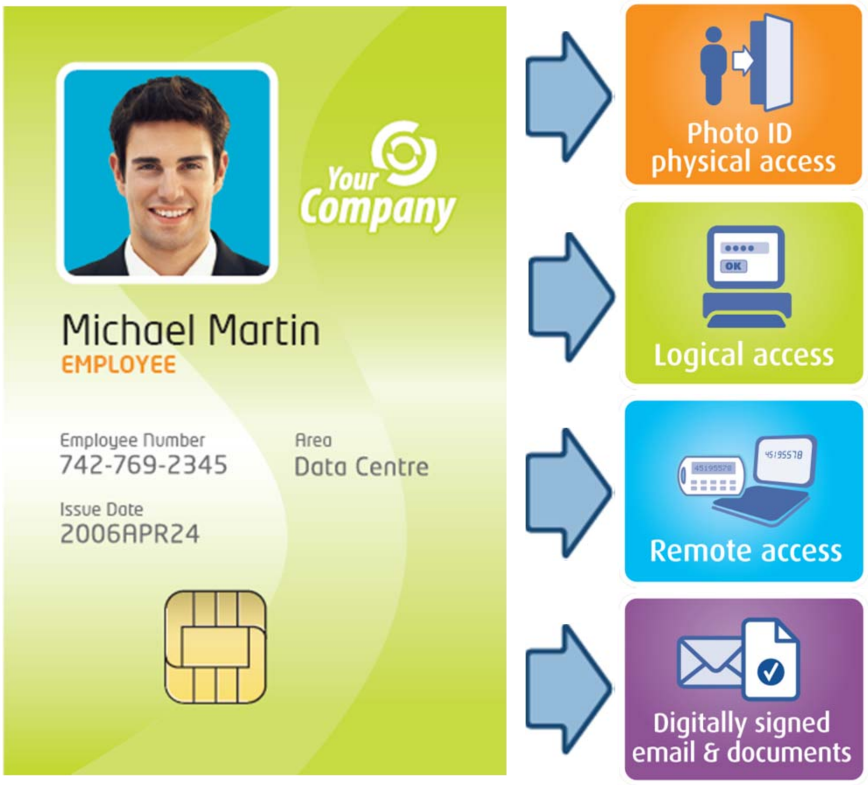
	Key	Value
▸	DebugLevel	0
	DisabledBadgeStatus	AD Disabled
	DeletedBadgeStatus	AD Deleted
	CookieDirectory	C:\\Program Files\\OnG...
*		

Physical Identity and Access Management (PIAM)

- Enterprises often manage several brands of physical access control and manually synchronize information among the systems making regulatory compliance (NERC, FERC,etc) a challenge

- PIAM vendors automate the process enabling a single trusted source for identity information and access rules

One card for physical and logical convergence

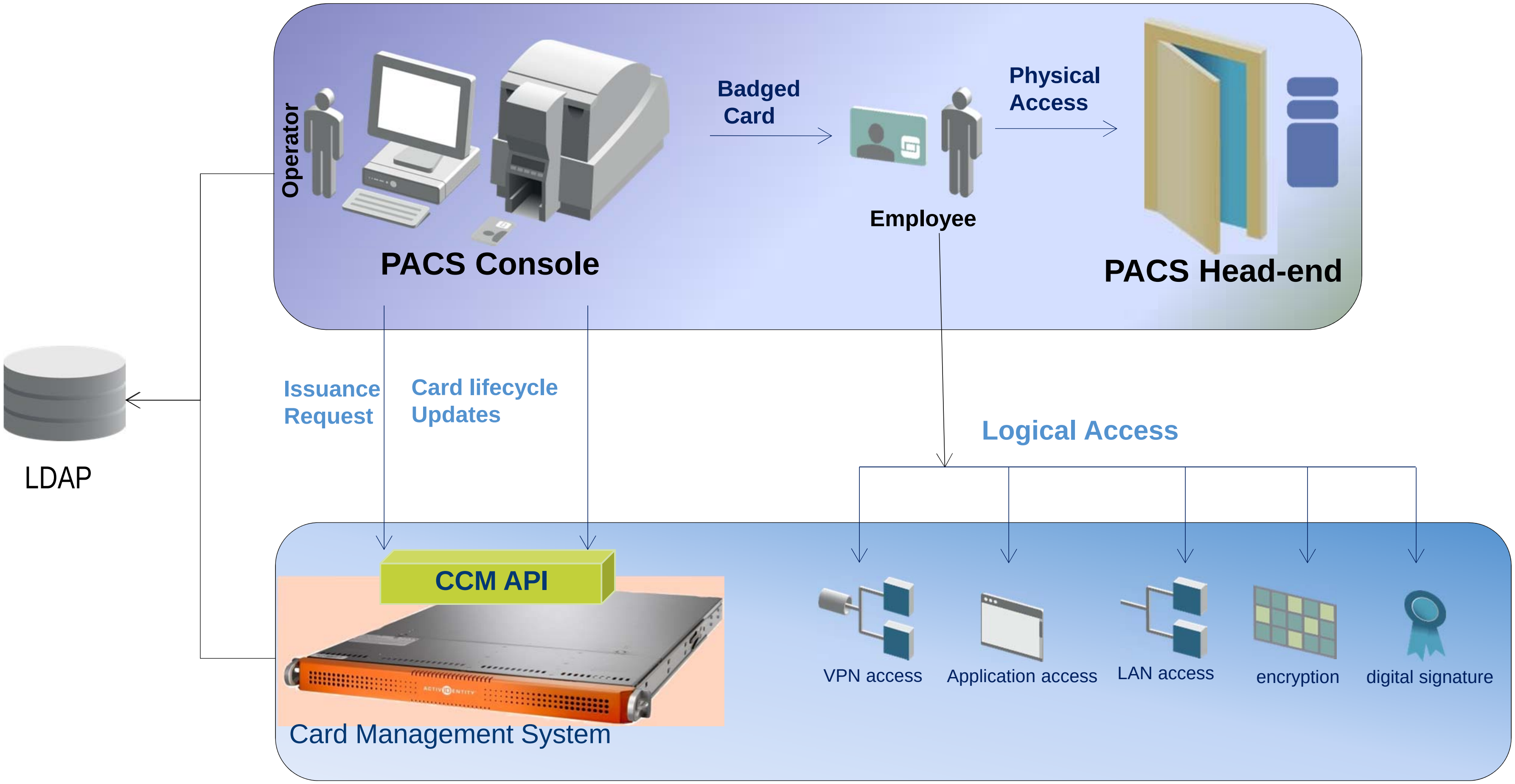


A single ‘smartcard’ gets you into the building,

logs you onto your workstation

authenticates you to the applications you need

Integrated Solution for Enterprise



Analytics Convergence – PSIM tools

- Proliferation of connected physical access devices – cameras, locks, sensors
  - Generates wealth of data
- Requires analytics software to convert data to information
- Data analytics require IT and BI skills to deploy, administer and generate value

Convergent audit logging

- Enables a consolidated forensic view
  - Entered building on Saturday at 5.30am through side entrance
  - Opened office at 5.35am
  - Logged onto network at 5.48am
  - Logged onto CRM application at 6.01am
  - Logged off system at 6.25am
  - Left building at 7.02am

PSIM + SIEM

Technology & Market Trends

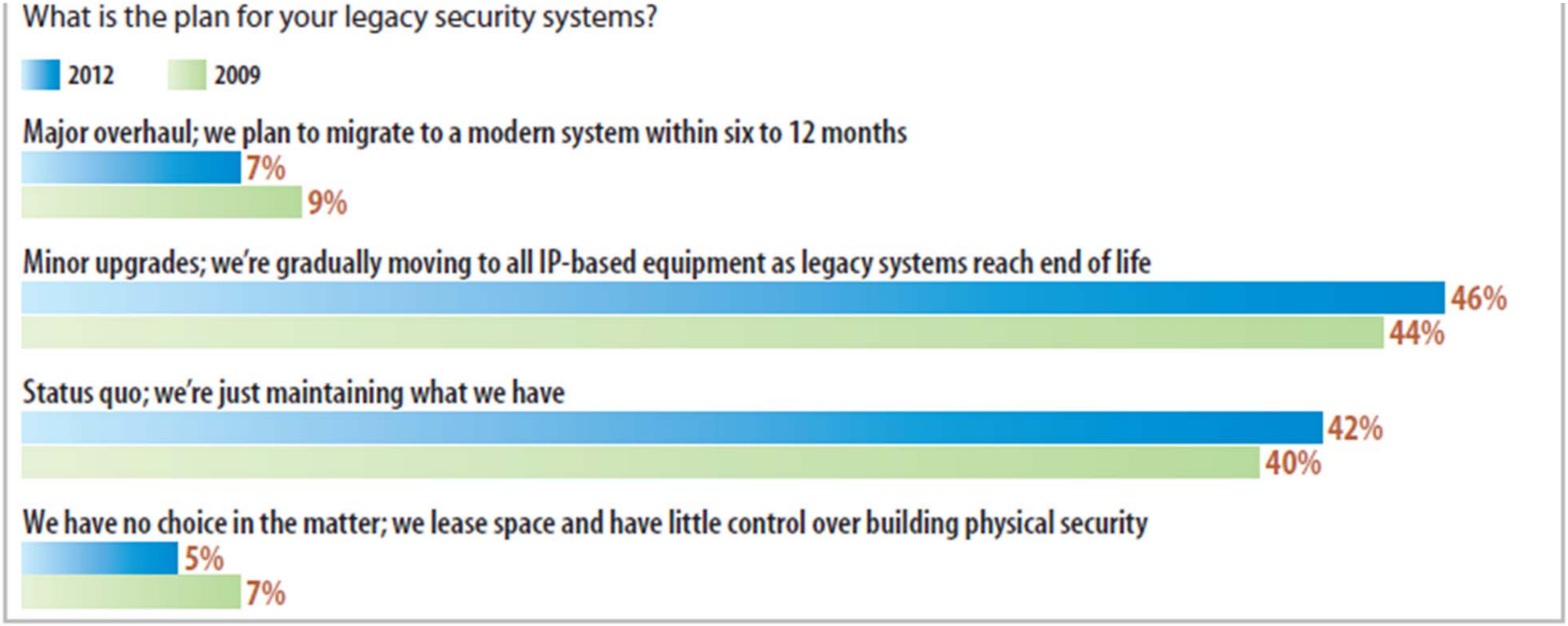
- Integrators, value added resellers and distributors addressing both
- Convergent User Management
- Convergent Credential – Common Access Card
- Convergent Logging
- Network interdependencies
- Context based access rules
- Evolution of physical access control solutions

Network Interdependencies

- IP based readers, e.g. HID Edge device range
- Heavy network dependency generated by growth in video

IT department is now heavily involved in the deployment of a Physical Access Control system, video surveillance, sensors

Trend in Physical Access to IP based



Base: 171 respondents in September 2011 and 169 in February 2009 with legacy security systems R3621111/3
Data: *InformationWeek* Physical/Logical Security Survey of business technology professionals

InformationWeek :: reports

I need to use your network

What are your bandwidth requirements?

Technology & Market Trends

- Integrators, value added resellers and distributors addressing both
- Convergent User Management
- Convergent Credential – Common Access Card
- Convergent Logging
- Network interdependencies
- Context based access rules
- Evolution of physical access control solutions

Context based access rules

- Consider Physical Access context for Logical Access Control decision
  - Is the user known to be the building / room?
  - Check PACS credential status
  - Prevent tailgating
  - Another tool for increasing security in depth

Context based access rules

- Consider Logical Access context for Physical Access Control decisions
  - Did the employee log in to the VPN from a foreign country 3 hours prior to badging into the building
  - Is the employee currently logged in from a different location

Technology & Market Trends

- Integrators, value added resellers and distributors addressing both
- Convergent User Management
- Convergent Credential – Common Access Card
- Convergent Logging
- Network interdependencies
- Context based access rules
- Evolution of physical access control solutions

Arizona State University Pilot

- Mobile phone replaced card
- For access to buildings on campus
- Almost 90% said they would like to use their smartphone to open all doors on campus

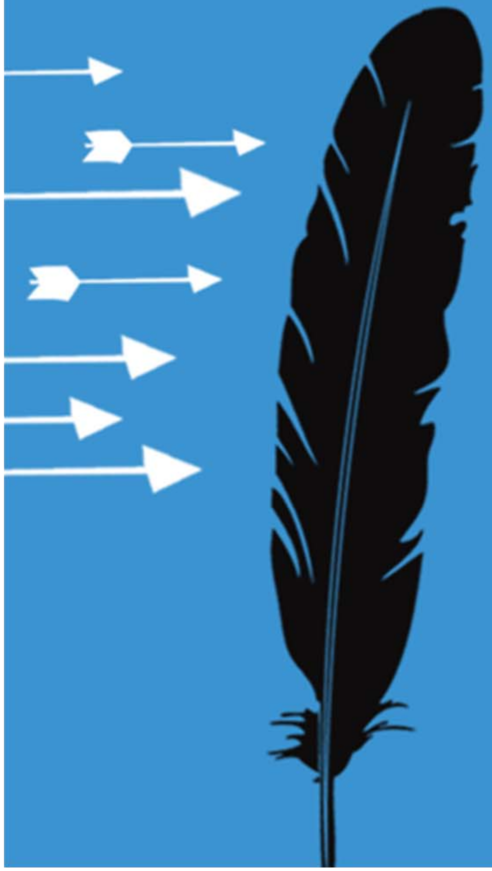
Mobile Credentials

BlackBerry
HID
HID & BLACKBERRY OPEN DOORS
NFC DIGITAL KEYS COME OF AGE FOR ACCESS CONTROL

- Embedding credentials on NFC enabled smartphones
- Requires physical access administration (assigning access levels, ordering and provisioning credentials) be aligned with IT and communications administration (ordering and provisioning mobile phones)
- Decouples the credential management from the device management

PKI at the door

- The federal government has now issued PIV credentials to ~ 90% of their employees
- Federal government will begin updating their PACS in FY12 to support PKI based credentials
- Federal contractors will follow the government's lead



Benefits and opportunities of convergence

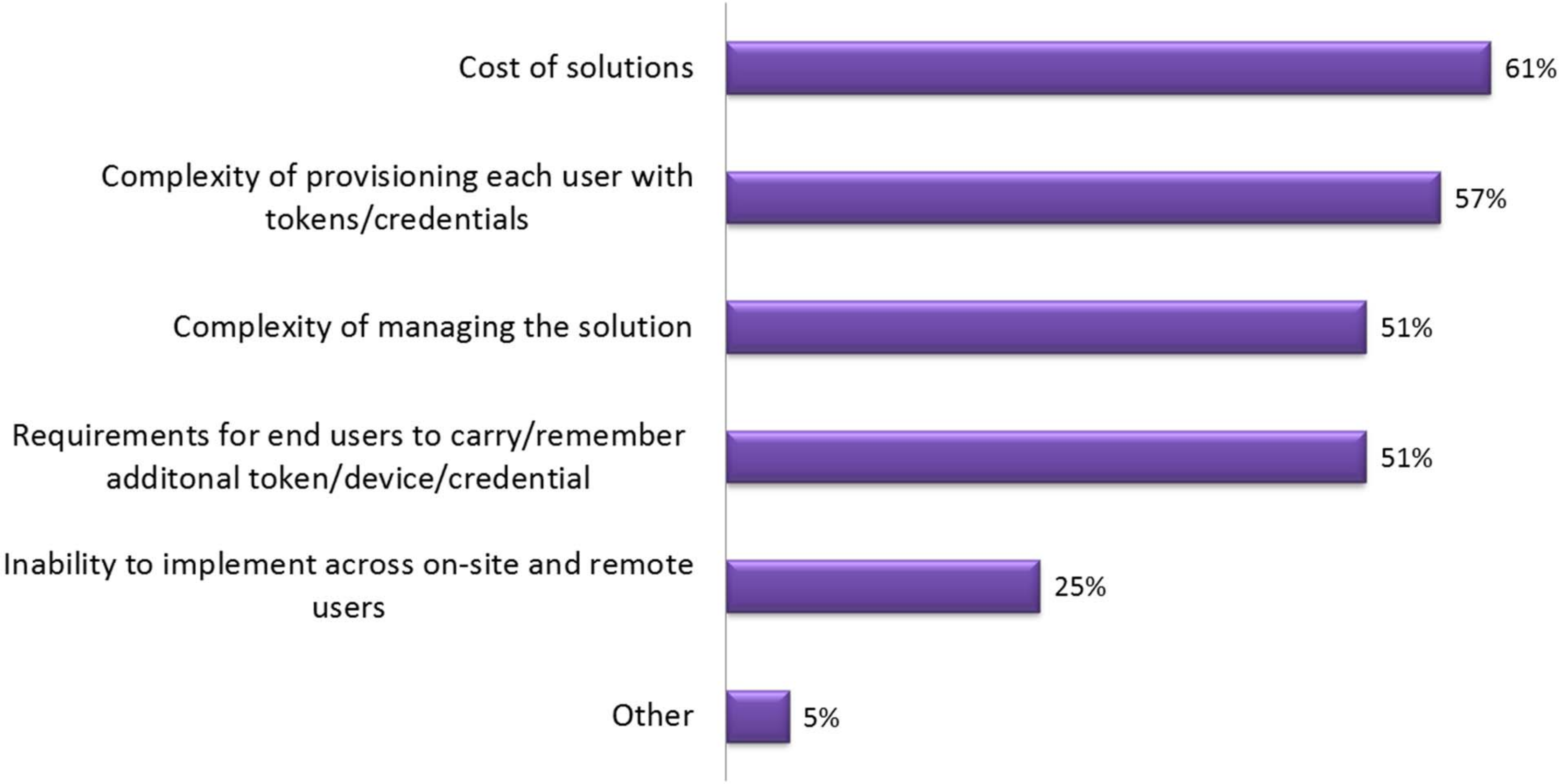
1. *One security policy*

2. *One credential*

3. *One audit log*

Top Challenges/Barriers Associated with Implementation of Two-Factor Authentication Solution

Q6: What are the top challenges or barriers your company associates with the implementation of a two-factor authentication solution? (Please check all that apply.)
Base: 112 qualified respondents



Benefits of a convergence

USABILITY

- One card gets you into the building
- Logs you onto the computer
- Gives you access to the applications you need to do a days work
- Authenticate for remote access

No more passwords
No more multiple devices
One card does it all

Happy Users

Investment

- Leverage investment in physical access card for system security (or vice versa)
- Replace two sets of admin processes with one

Cost of converged smartcard
Is considerably less than
Cost of PACS card + token

Happy CFO

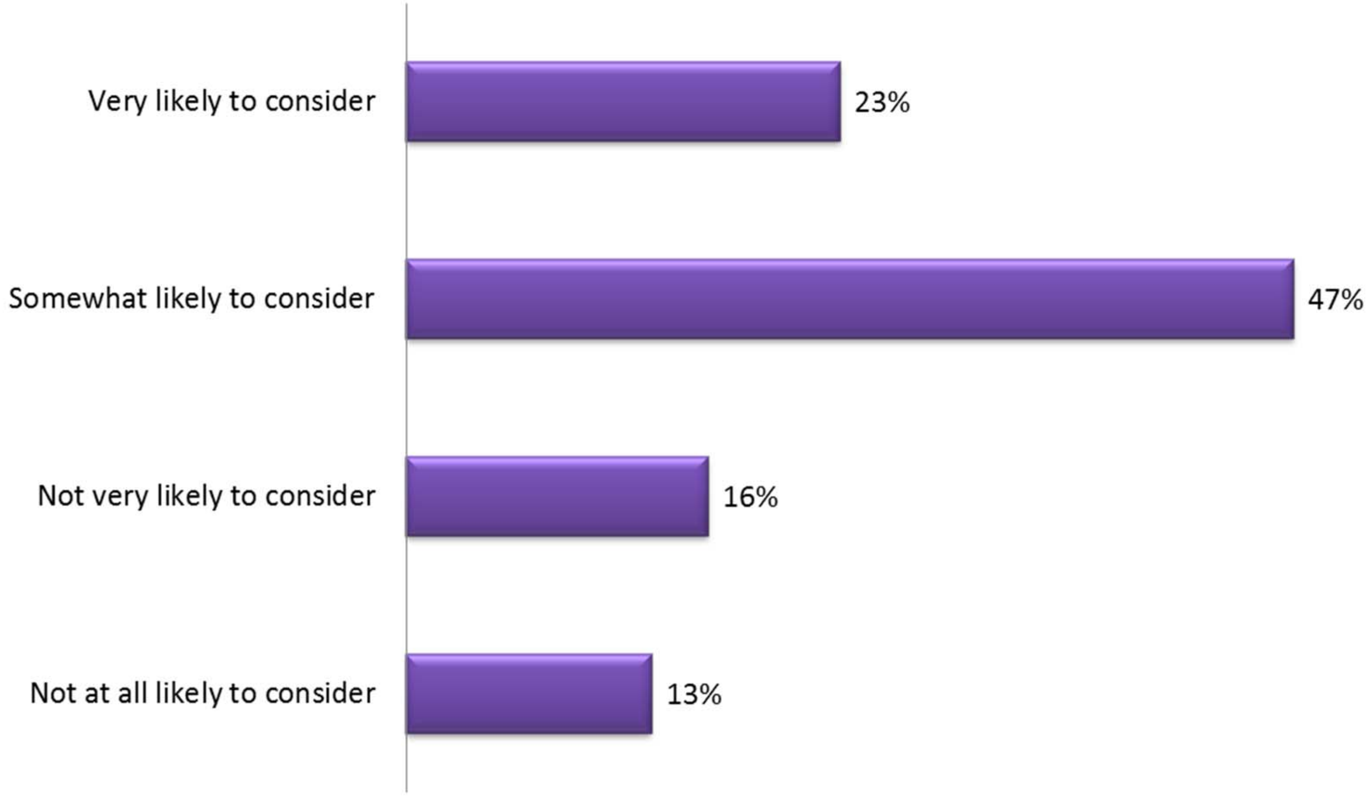
Assurance

- Buildings access and system access privileges are collectively withdrawn
- Credentials are not easily shared

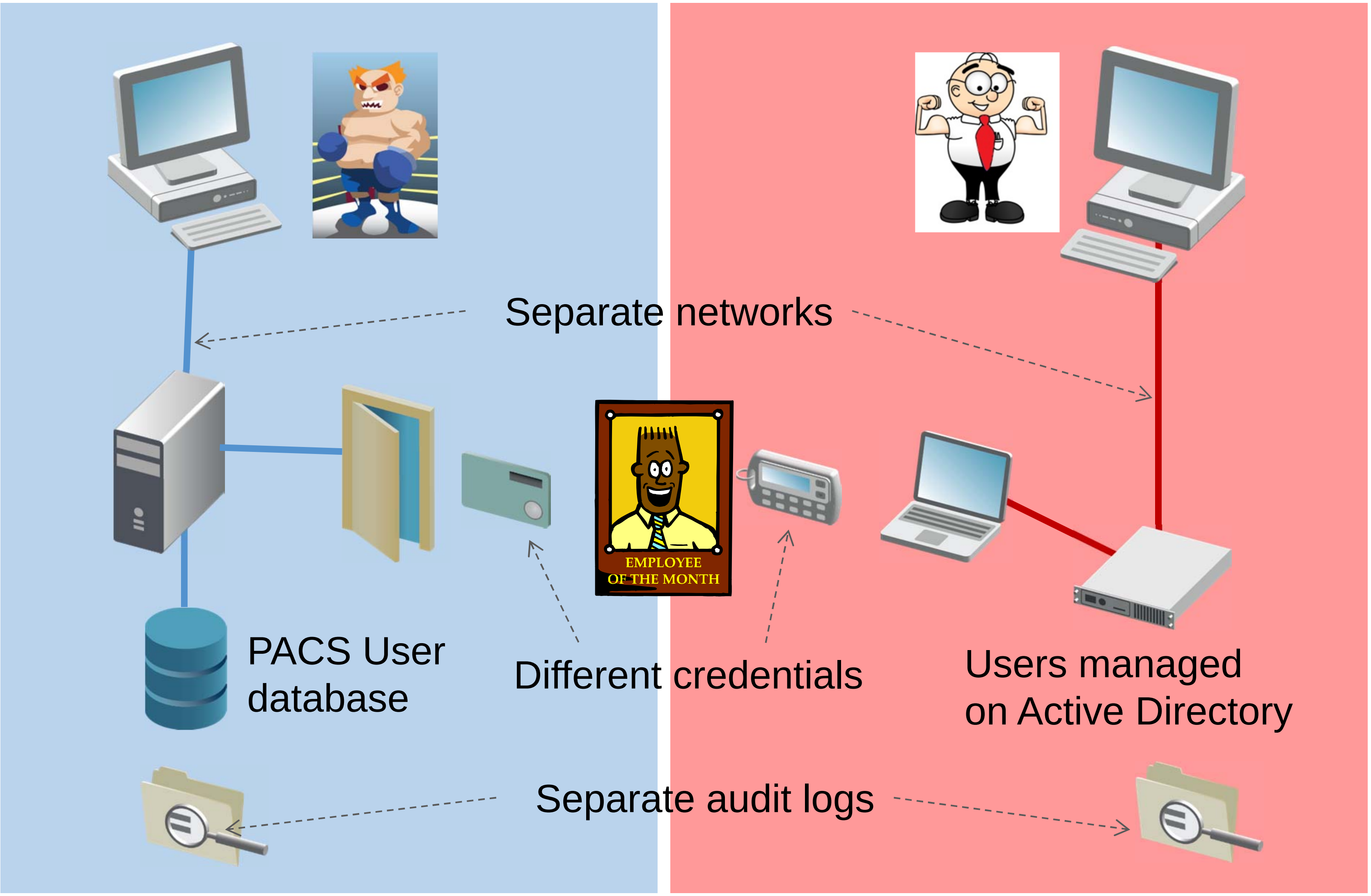
Compliance
Accountability

Happy CSO

Likelihood of Company to Consider a Two-Factor Authentication Solution that Makes Use of Existing Card Access System



Q10: How likely would your company be to consider a two-factor authentication solution that could make use of an existing physical access card system?
Base: 112 respondents



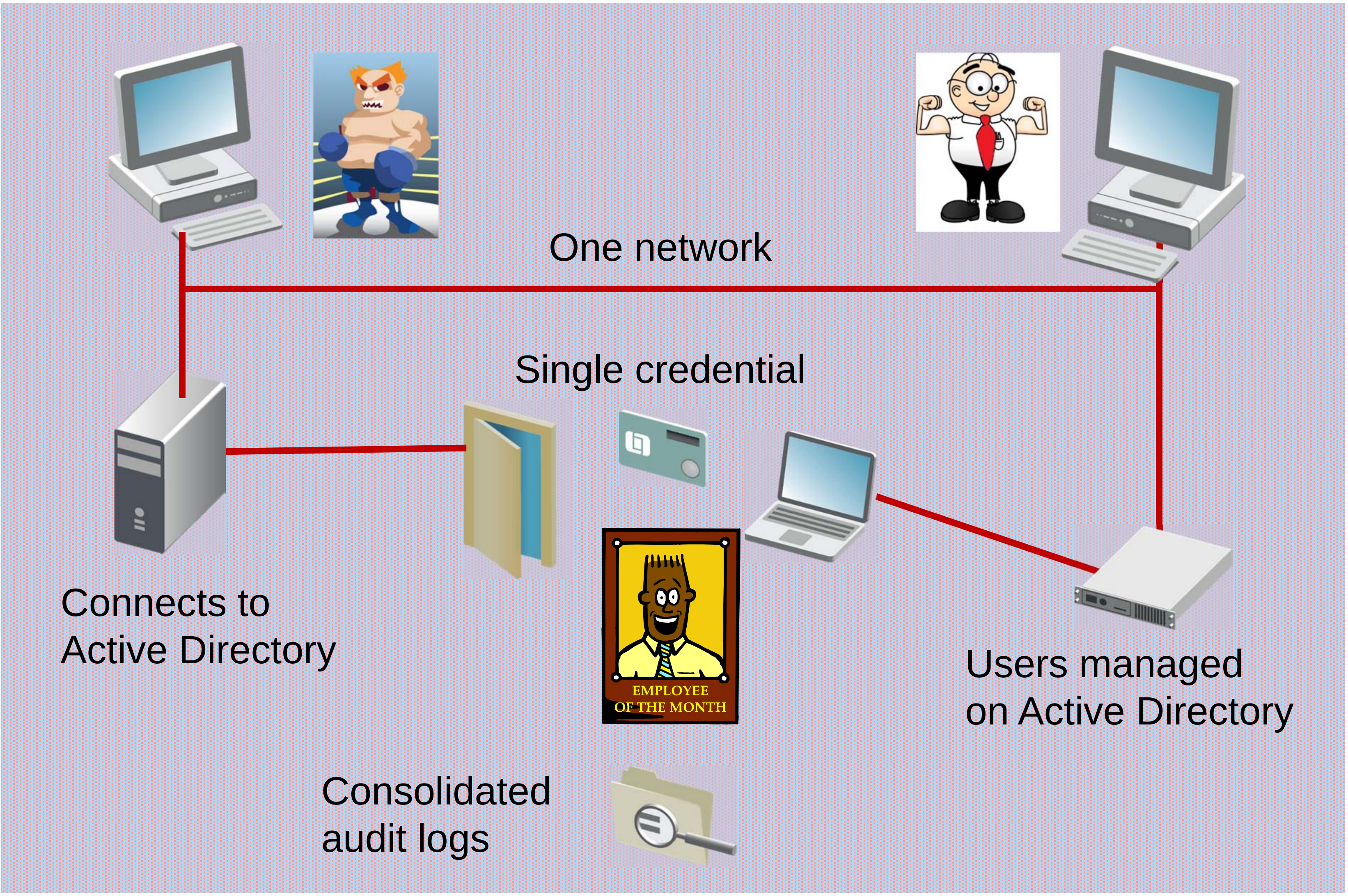
Separate networks

PACS User database

Different credentials

Users managed on Active Directory

Separate audit logs



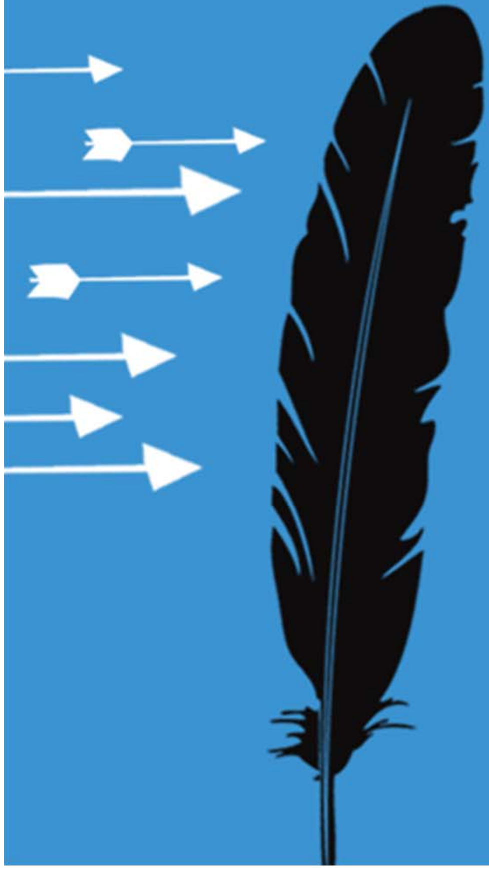
One network

Single credential

Connects to
Active Directory

Users managed
on Active Directory

Consolidated
audit logs



Apply

Apply Slide

- Introduce "physical access" team to the "IT security" team
- Identify common goals & shared concerns
- Establish a unified security policy
  - Not one for physical access & another for IT access
- Review potential cost savings and security benefits opportunity through converged credentialing