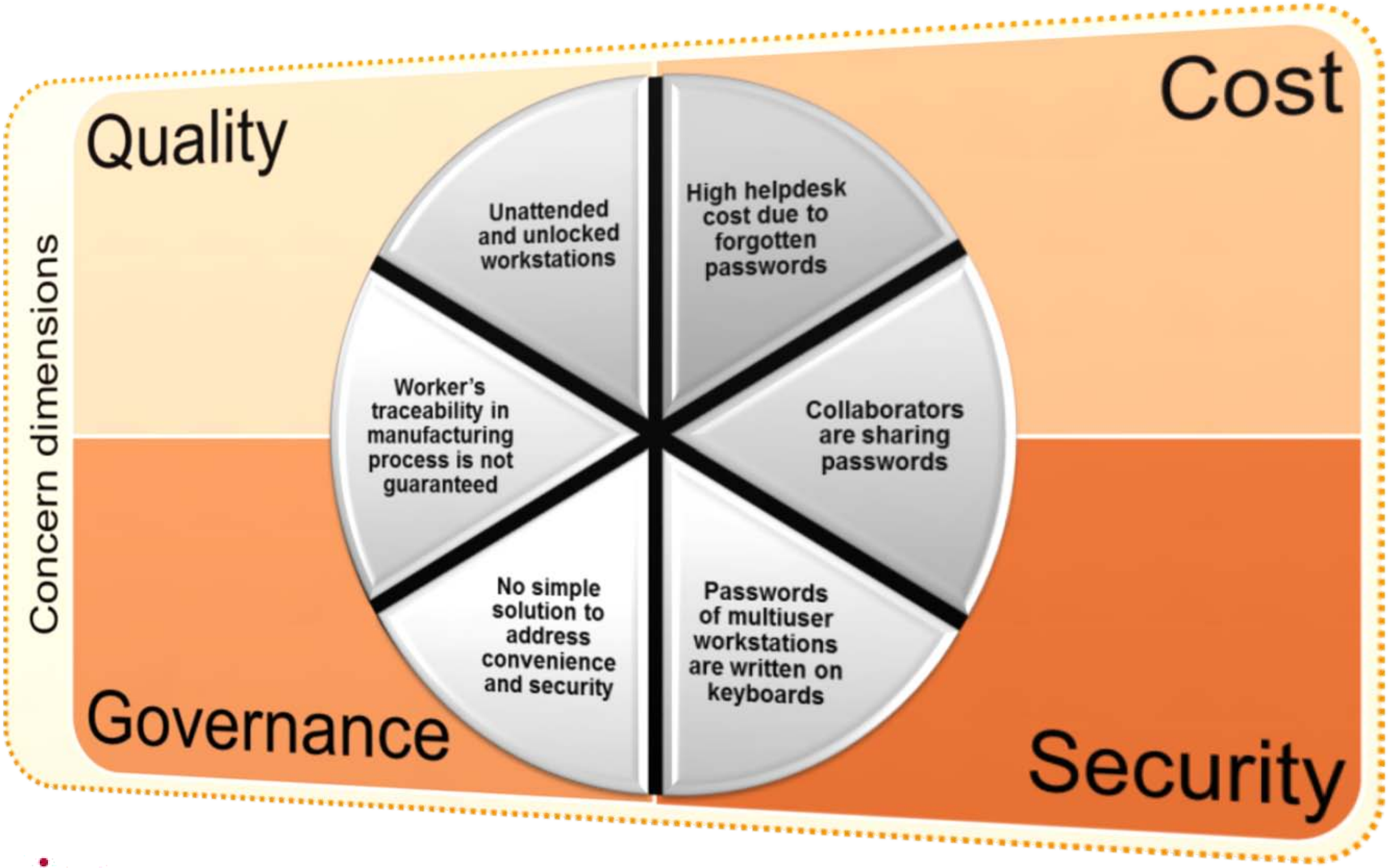
uLogon Solution

Your Hand is the Password

Overview

- Today's reality – *Your Business & Your Environment*
- Think about the problems you need to solve
- The Impact – problems to avoid, opportunities to realize
- The benefits to be gained
- Unisys uLogon Solution and Biometrics
- Unisys uLogon clients look like
- Appendix

Today’s Business Reality



Quality
Cost
Concern dimensions
Unattended and unlocked workstations
High helpdesk cost due to forgotten passwords
Worker’s traceability in manufacturing process is not guaranteed
Collaborators are sharing passwords
No simple solution to address convenience and security
Passwords of multiuser workstations are written on keyboards
Governance
Security

UNISYS

Today's Reality

Helpdesk Cost

"Password problems and resets generally constitute between 25% and 40% of total help desk incidents" – Forester Research, - Chip Gliedman with John Ragsdale, Jessica Harrington.[1]

Usability / Convenience

Temporary / Part-time workers tend to forget their passwords every time they are back to work

Enable secure multi-user access to shared workstations

Freedom from remembering (complicated / multiple) passwords

Audit and Compliance

Audit preparations are not just expensive but disruptive as well. It is quite a task to reconcile password event logs across multiple systems

Password sharing / unattended and unlocked PCs increase risk of non-compliance with regulations (including Sarbanes-Oxley (SOX) Act, Electronic Signatures in Global and National Commerce (E-SIGN) Act, Basel II)

Security

Weak passwords can easily be guessed or hacked: Password policies are often not enforced

Strong password policies can actually reduce security: Users often write and store passwords in obvious locations

Security and privacy compromised by non-compliant practices (e.g.: unattended and unlocked PCs)

[1] As quoted in PRWeb's "Reduce Help Desk Costs Using Password Management Software", November 2011

Today's Authentication Challenges…

We see organizations trying to…

- **Secure Identity**
  Data security and identity management have never been more critical in the healthcare industry. With the passage of Health Insurance Portability and Accountability Act (HIPAA), medical organizations are now required to use two or more forms of authentication in order to access electronic health records and other sensitive data

- **Secure Shared Infrastructure**
  The need for secure workstations in specialised, multi-user manufacturing facilities is forcing manufacturers to implement authentication solutions to track user activity and smoothen assembly based processes.

- **Meet Regulatory Challenges**
  Banking industry is facing a deeper problem with increased regulation on data security and auditing such as the Basel Accords, Sarbanes Oxley and EU Data Protection Directive.

- **Enhance Productivity**
  Retailers are on the look-out for technologies (biometrics) that have a positive impact on the employee output. Retailers expect a 300%* return on investment during the first year of using biometric technology and a tremendous boost in employee productivity, by reducing time spent in repeated log-in and log-out procedures.

UNISYS

*Ponemon Institute

Cyber criminals can hack what you have (Passwords), But can't hack who you are (Biometrics)….

Protect the Enterprise
Integrate with Enterprise Security
Authenticate the User
Track & Monitor

…Yet you can Track who is accessing what and where

- **Can't look for point Solution -** It's about integrating the solution into your existing security posture, so that you get enterprise grade security with ease of management of a point solution.
- Don't think about securing the transaction. **Authenticate the user** –once you do that, from that moment on you have the right user accessing the system.
- **Look beyond Passwords -** Multifactor Authentication is the way forward

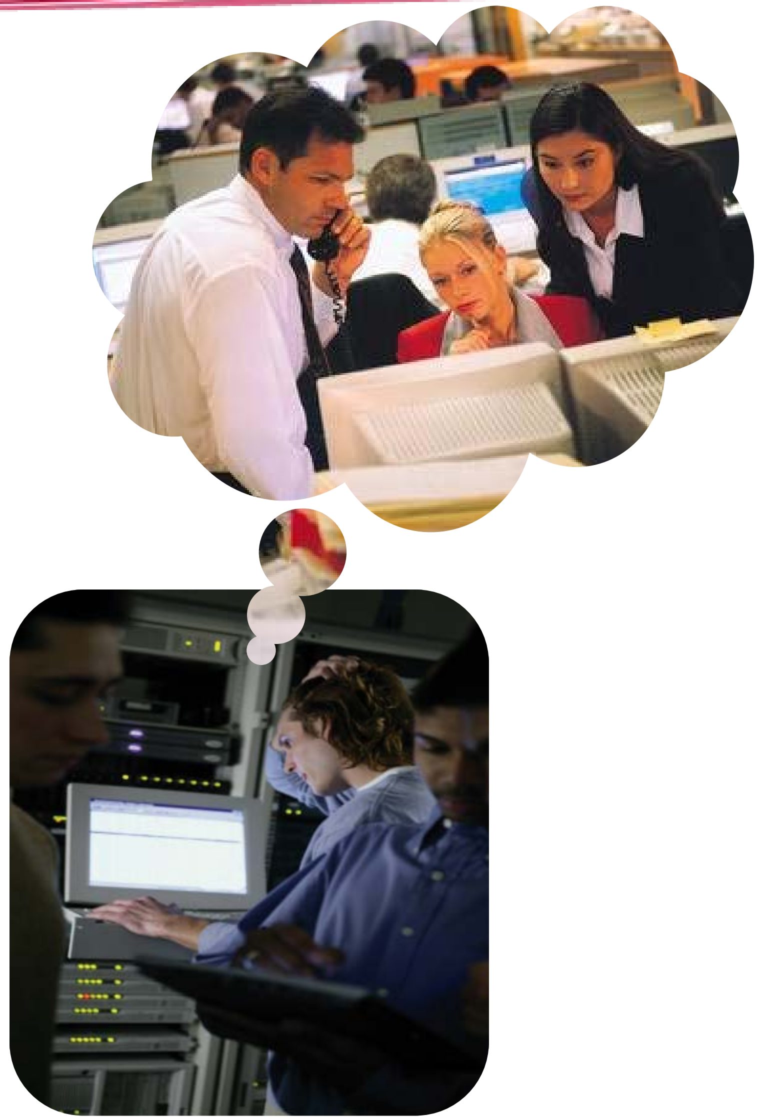
The Dark Authentication Reality Check

- 44 % of employees share work devices without supervision.
- 18 % of employees share passwords with co-workers.
- 11 % of employees reported that they or fellow employees accessed unauthorized information and sold it for profit *~ Market Research Firm – InsightExpress*

- The average organizational cost per data breach in 2011 was $5.5 million and the cost per compromised record was $194. *~ The Ponemon Institute*

- 39% organizations reported “negligent insiders” as the root cause of data breaches. *~ The Ponemon Institute*

- 59% of respondents report that employees circumvent or disengage security features, such as passwords and key locks
- 51% of the organizations experienced data loss resulting from employee use of unsecured mobile devices *~ The Ponemon Institute Global Study on Mobility Risks*



Can you afford…?

- Forgotten passwords and scheduled password changes can account for up to 25 percent of a helpdesk's activity.**Can you afford employees calling the helpdesk for password resets?**
    - Roughly 30 percent of all help desk calls are for password resets – and cost between *$25 to $50 per call*. [1]
- With increasing pressure from government agencies to meet compliance and increased cost of non-compliance. **Can you afford to take chances at being non-compliant?**
    - The extrapolated average cost for organizations that experience non-compliance-related problems is $9.4 million. Adjusting total cost by organizational headcount (size) yields a per capita compliance cost of $222 per employee.[2]

~ *1 T*he Help Desk Institute,
~ *2 Ponemon Institute, True cost of Compliance Report, 2011*

Unisys Approach

- Eliminate the resource sapping password reset infrastructure
- Mitigate challenges of constantly meeting audit and compliance requirements
- Eliminate complex architecture and infrastructure changes to meet your authentication challenges
- Enhance user productivity by reducing time spent on repeated sign on processes in a multi-user environment

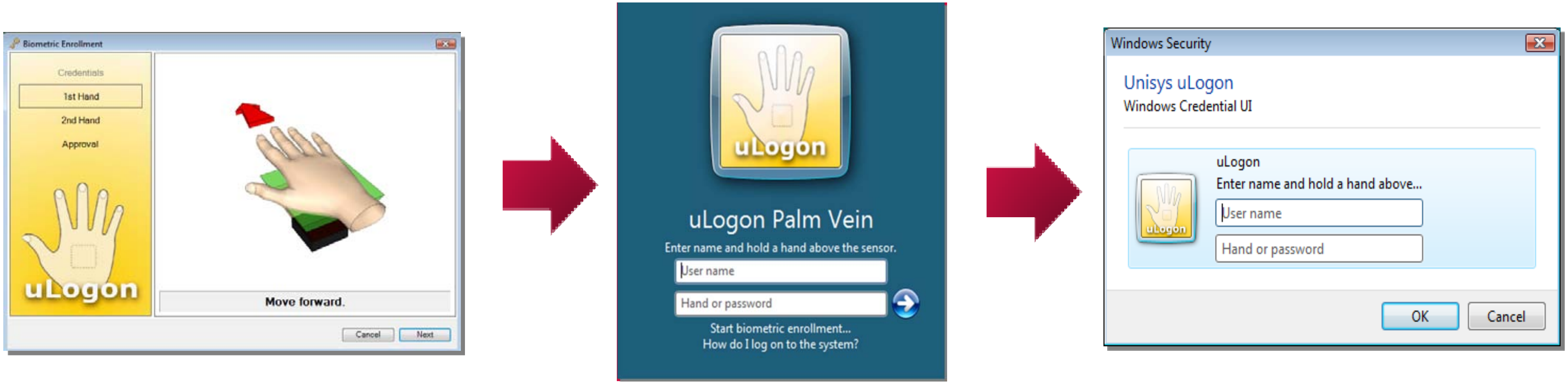
UNISYS

uLogon Solution

Enrollment Simplified through biometrics…

Easy to implement and operates on the self-enrollment concept.

Using a hand vein sensor, the uLogon software allows users to self-enroll on any Windows workstation by storing the encrypted vein image in the identity store.



Biometric Enrollment

Credentials

1st Hand

2nd Hand

Approval

Move forward.

uLogon Palm Vein

Enter name and hold a hand above the sensor.

User name

Hand or password

Start biometric enrollment...

How do I log on to the system?

Windows Security

Unisys uLogon

Windows Credential UI

uLogon

Enter name and hold a hand above...

User name

Hand or password

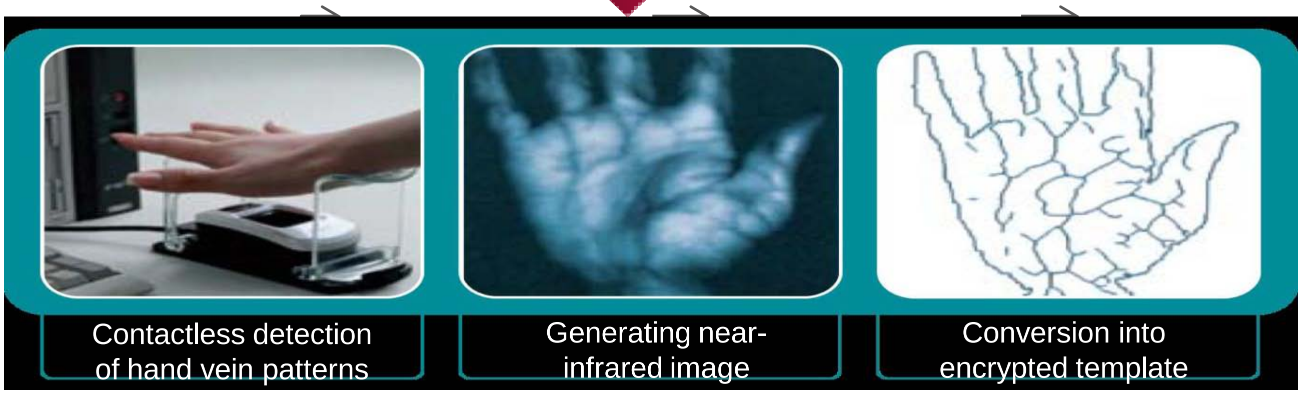
Users can initiate the enrollment process without even touching the sensor. The hand-vein sensor automatically detects the hand, captures an infrared image and extracts the biometric features. Post enrollment, the biometric template is encrypted and stored for verification purposes.

uLogon Solution:

Authentication Simplified through biometrics…

uLogon works on a role-based access mechanism.

Role-based access control takes the privileges associated with a user and maps them to the systems used for accessing IT resources.



Contactless detection of hand vein patterns

Generating near-infrared image

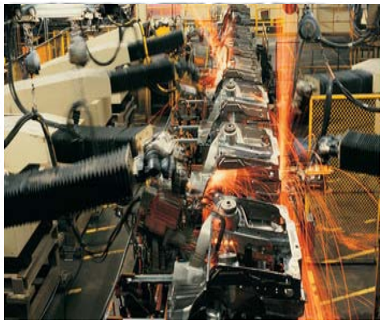
Conversion into encrypted template

The strong authentication using palm vein biometrics is used as a service for different applications. The applications will receive the authenticated identity in form of a signed SAML ticket. This ticket can provide a proven identity and additionally add relevant trusted information in form of claims. The data inside the claims can be age, email address, role information or any other requested information.

Unisys uLogon Clients Look Like….

A National Hospital

A Technology Manufacturing Company



A National Postal Service

Luxury Watch Manufacturers

UNISYS

A National Postal Service

- **Business challenge**
  - Usability Issues: Temporary / part-time workers, come back having forgotten their passwords
  - Cost Issues: High help desk costs for password reset
  - Complexity of the password to change every time
  - Security Issues:
    - Weak passwords can easily be guessed or hacked
    - Strong password policies can actually reduce security- users often write and store passwords in obvious locations

- **Solution**
  - Biometric uLogon Solution with Palm vein scanner in the mice, keyboards and as a standalone devices

- **Results and benefit**
  - 650K$/year of cost saving in password resets
  - Automatic “Rights” Management by Integration with Active Directory
  - Freedom of not remembering your password
  - Biometrics ensure beyond any doubt that users are who they claim to be

A Swiss Watch Manufacturer

- **Business challenge**
  - Security: All workstation on the shop floor are in an open space and shared across many users, anybody can quickly enter and exit and read sensitive data on products
  - Productivity:
    - Several hundred employees sharing half as many PCs' to enter the watch serial numbers into the ERP system
    - Too much time to log on and log off

- **Solution**
  - uLogon Screenlocker Solution with contactless chip and RFID

- **Results and benefit**
  - Allows only legitimate users to access sensitive data
  - Improved communication within the organization and shortened response times to clients and customers
  - Improved productivity by significantly reducing the time spent on log in/log off, and in password administration and maintenance
  - Compliance with regulations by enabling secure user access and providing a proven method for protecting internal data and networks
  - Improved quality through full traceability and the creation of a consequent performance reward programme

A National Hospital

- **Business challenge**
  - Publicly shared, multi user kiosks that are constantly exposed to security breaches
  - Waste of precious time in logging-on, waiting for applications to load and logging-off
  - Subsequent users denied access as previous users accidently lock workstations and walk away

- **Solution**
  - uLogon Screenlocker Solution

- **Results and benefit**
  - Allows only legitimate users to access sensitive data
  - Improved productivity by significantly reducing the time spent on log-in/log-off.
  - Compliance with regulations by enabling secure user access and providing a proven method for protecting internal data and networks using existing RFID badges.
  - Improved quality through full traceability

A Technology & Manufacturing Company

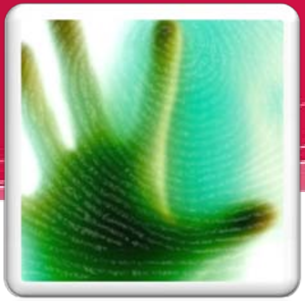
- **Business challenge**
  - Usability issues: Windows logon in protected areas is complex
  - Complexity of the password to change every time
  - Security Issues:
    - No traceability of who accessed the workstation
    - Weak passwords can easily be guessed or hacked
    - Strong password policies can actually reduce security - users often write and store passwords in obvious locations

- **Solution**
  - uLogon solution with RFID readers for Windows Logon

- **Results and benefit**
  - Automatic “Rights” Management by Integration with Active Directory
  - Freedom from remembering your password - easy to handle with existing badges, password change is automated with no user interaction required
  - The password is stored securely in the Legic badge

Appendix

Biometrics – What is it ?



Biometrics is the automated technique of measuring a physical characteristic or personal trait and comparing it to information in a database or on a token for the purposes of positive identification of a person

Identity Concepts – How can you prove who you are ?

1. **With Something You Have** - Driver license, passport, token (PKI), Smartcard …
2. **With Something You Know** - PIN, Password, family name, date of birth, word/phrase
3. **But best of all, with Something You Are** (Biometrics) - Physical and Behavioral Characteristics

Some Types of Biometric:

- Facial Recognition
- Iris Recognition
- Voice
- Keystroke dynamics (how you depress the keyboard)
- Vein and Vascular Patterns
- Fingerprint
- Hand Geometry
- Skin texture
- Palm Print
- Handwritten signature
- Gait (how you walk)

UNISYS