The Auditor’s Dilemma: Audit Issues for Higher Education in the Information Age

Richard N. Katz
EDUCAUSE
May 23, 2006
Boulder, Colorado
Agenda

• Framework to think about the future
• Some interesting technologies and trends
• Possible audit challenges
• One deep example: identity management
• Summary
Framework for Thinking about the Future


Mainframe Computing

Physical Connectivity

Logical Connectivity

Embedded Connectivity

Personal Computing
Interesting Technology Trends

• Services Oriented Architectures
• E-Portfolio/Personal Digital Repository
• Open Source
• Identity Management
• Mobility
• Embedded Intelligence
  – Sensors, RFID
Interesting Social and Economic Trends

• Increasing Regulation
• Potential for Disintermediation
• Increasing Localization, Personalization and Virtualization of data, transactions, software, services, etc.
• Miniaturization of Devices
• Mobility of Devices and Workers
Some emerging audit quandaries

• SOAs: Dynamically distributed systems
  – the “system” is a snapshot of the services available & called at a given moment

  *Glendower:* I can call spirits from the vasty deep.

  *Hotspur:* Why so can I, or so can any man, but will they come when you do call for them?

  -- William Shakespeare, *Henry IV Part I*
Some emerging audit quandaries

Regulation

– Severe (& inconsistent) penalties for data exposure since California SB 1386

– IT culture is probably more favorable today to central processes & standards than in Y2K era

– Will SOX/GLB/transparency come to higher education?
  • Academic accountability?

– Digital rights management & IP
  • Libraries have historically mediated a lot of IP relationships that will now be distributed—but institution will still be liable in the end
Some emerging audit quandaries

E-Portfolio

- Individual, not the institution is locus of control
- Access management is an individual act
- Constraints on institutional uses of individual data
- Carried on iPod? Network?
Some emerging audit quandaries

Embedded Intelligence

- Massive decentralization of data collection, management, and use
- Unprecedented privacy issues
- Spoofing of Sensors
Some emerging audit quandaries

Open Source

- Business model

- No corporate owner
  (liability management?)

- Economic sustainability?

- Privacy?
Some emerging audit quandaries

Devices

– Far less standardized than the PC

– Constant, ubiquitous, “pretty good” connectivity

– Handheld processing & storage N years (5? 7?) behind PCs
Some emerging audit quandaries

Identity

– May be the single greatest weakness of Internet 1.0

– Will be:

• Fortified by new public infrastructure (RealID Act, HSPD-12)
• Diversified by user ability to define/present digital identities
• User-centric (MS InfoCard, OASIS XRI spec)
• Federated
  – shared, cross-institutional pools & constituent pools

Spy vs. Spy, Mad Magazine
Knock, knock. Who is there?

- Internet users grew from 45 million to over 1 billion 1995-2005
- Annual cost of U.S. identity theft is about $50 billion
- Native Internet identity mechanisms are weak to nonexistent
- Legacy identity mechanisms are embedded, scale poorly, non-interoperable

Sources: eTForecasts; US Federal Trade Commission; Privacy Rights Clearinghouse
Identity Management: What is it?

*The business processes and infrastructure required to support the creation, maintenance, and use of digital identities.*  
*(Courtesy The Burton Group)*

Key functions:
- establishing identity
- user authentication and authorization

Supporting infrastructure:
- enterprise directory
- reduced or single sign-on
- automated role-based authorization
- federated identity
Establishing Identity: Limited Differentiation

For faculty and staff in sensitive roles, do you require stronger identity proofing than for those not in sensitive roles?

For different groups of off-campus affiliates (e.g., parents, alumni), do you use different methods of identity proofing?

For different groups of on-campus visitors and guests, do you use different methods of identity proofing?
## Motivation to pursue IdM

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security/privacy best practices</td>
<td>80.9</td>
</tr>
<tr>
<td>Enhanced user services and satisfaction</td>
<td>60.8</td>
</tr>
<tr>
<td>Regulatory compliance (e.g. HIPPA, GLB Act, FERPA)</td>
<td>42.7</td>
</tr>
<tr>
<td>Strategic value/opportunities</td>
<td>22.8</td>
</tr>
<tr>
<td>Improvements in our technical environment</td>
<td>20.3</td>
</tr>
<tr>
<td>Keeping current with generally accepted IT directions</td>
<td>18.9</td>
</tr>
<tr>
<td>Cost reduction/increased efficiencies</td>
<td>18.6</td>
</tr>
<tr>
<td>Position the institution for implementation of federated identity</td>
<td>14.6</td>
</tr>
<tr>
<td>Strategy of early adoption/experimentation</td>
<td>1.2</td>
</tr>
<tr>
<td>Reduce vendor dependencies</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Total percentage of respondents ranking item as first, second, or third highest motivation
The IdM capability gap

1=very low, 2=low, 3=medium, 4=high, 5=very high

Respondents uniformly rated benefit importance higher than institutional capability to deliver
Senior management understanding of IdM

- Understands benefits: 9.5% Strongly Agree, 31.8% Agree, 23.3% Neutral, 31.3% Disagree, 4.1% Strongly Disagree
- Understands the costs: 2.8% Strongly Agree, 14.1% Agree, 26.7% Neutral, 46.7% Disagree, 9.7% Strongly Disagree
- Willing to address related policy issues: 8.9% Strongly Agree, 46.2% Agree, 31.3% Neutral, 11.2% Disagree, 2.3% Strongly Disagree
Institution providing needed resources for IdM?

- Strongly Agree, 6.3%
- Agree, 25.6%
- Neutral, 32.0%
- Disagree, 30.2%
- Strongly Disagree, 5.8%
IdM documentation

- **Documented data owners/custodians**
- **Documented data definitions, reconciling differences**
- **Risk assessment of data access security and privacy practices**
- **Released an RFI or RFP for Identity Management**

**Legend**
- Completed
- In progress
- Planning to do
- Not planning to do
- Don’t know
## Authentication technologies

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Using (%)</th>
<th>Planning to use (%)</th>
<th>Not planning to use (%)</th>
<th>Don’t know (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conventional password/PIN</td>
<td>91.1</td>
<td>2.1</td>
<td>6.5</td>
<td>0.3</td>
</tr>
<tr>
<td>Strong password</td>
<td>55.0</td>
<td>23.8</td>
<td>16.5</td>
<td>4.7</td>
</tr>
<tr>
<td>Kerberos</td>
<td>26.2</td>
<td>11.5</td>
<td>46.1</td>
<td>16.1</td>
</tr>
<tr>
<td>PKI certificate (software) without PIN</td>
<td>7.1</td>
<td>7.4</td>
<td>58.9</td>
<td>26.5</td>
</tr>
<tr>
<td>PKI certificate (software) with PIN</td>
<td>4.8</td>
<td>10.6</td>
<td>55.9</td>
<td>28.7</td>
</tr>
<tr>
<td>PKI hardware token without PIN</td>
<td>0.6</td>
<td>2.8</td>
<td>68.9</td>
<td>27.7</td>
</tr>
<tr>
<td>PKI hardware token with PIN</td>
<td>1.8</td>
<td>7.6</td>
<td>62.2</td>
<td>28.4</td>
</tr>
<tr>
<td>SecuRId-style onetime password</td>
<td>12.7</td>
<td>11.8</td>
<td>54.6</td>
<td>20.9</td>
</tr>
<tr>
<td>Other multi-factor authentication methods</td>
<td>6.5</td>
<td>17.9</td>
<td>48.7</td>
<td>27.0</td>
</tr>
<tr>
<td>Biometric identification</td>
<td>3.3</td>
<td>12.6</td>
<td>66.1</td>
<td>18.0</td>
</tr>
</tbody>
</table>

Percentage of respondents choosing category
Plenty of IdM work on the table

- 64% of respondents were either implementing enterprise directories, reduced or single sign on, or role-based authorization, or planning to in some time frame
- Majority with operational enterprise directories plan to enhance them
- Almost nobody entirely rules out at least considering these technologies
- Aggressive tech adopters & institutions with data warehouses and portals report more advanced adoption
When will you need a federated identity solution? (N=398)

<table>
<thead>
<tr>
<th></th>
<th>DR</th>
<th>MA</th>
<th>BA</th>
<th>AA</th>
</tr>
</thead>
<tbody>
<tr>
<td>We do not envision a need</td>
<td>6.1</td>
<td>19.8</td>
<td>18.9</td>
<td>17.0</td>
</tr>
<tr>
<td>We have a need now</td>
<td>30.3</td>
<td>6.3</td>
<td>6.8</td>
<td>10.6</td>
</tr>
<tr>
<td>In the next 12 months</td>
<td>11.1</td>
<td>4.5</td>
<td>8.1</td>
<td>0.0</td>
</tr>
<tr>
<td>Between one and two years from now</td>
<td>19.2</td>
<td>15.3</td>
<td>14.9</td>
<td>8.5</td>
</tr>
<tr>
<td>Between two and three years from now</td>
<td>19.2</td>
<td>16.2</td>
<td>16.2</td>
<td>8.5</td>
</tr>
<tr>
<td>More than three years from now</td>
<td>5.1</td>
<td>11.7</td>
<td>10.8</td>
<td>10.6</td>
</tr>
<tr>
<td>Don’t know</td>
<td>9.1</td>
<td>26.1</td>
<td>24.3</td>
<td>44.7</td>
</tr>
</tbody>
</table>

Percentage of respondents in category
Expected central IT spending on IdM projects in the next 3 years (N=339)

<table>
<thead>
<tr>
<th>Category</th>
<th>Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>$50,000 or less</td>
<td>26.5</td>
<td>26.5</td>
</tr>
<tr>
<td>$50,001 to $100,000</td>
<td>20.6</td>
<td>47.2</td>
</tr>
<tr>
<td>$100,001 to $500,000</td>
<td>28.3</td>
<td>75.5</td>
</tr>
<tr>
<td>$500,001 to $1 million</td>
<td>5.9</td>
<td>81.4</td>
</tr>
<tr>
<td>Between $1 million and $2 million</td>
<td>2.9</td>
<td>84.4</td>
</tr>
<tr>
<td>Between $2 million and $5 million</td>
<td>1.5</td>
<td>85.8</td>
</tr>
<tr>
<td>More than $5 million</td>
<td>0.3</td>
<td>86.1</td>
</tr>
<tr>
<td>Don’t know</td>
<td>13.9</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Percentage of project-active respondents choosing each category
IdM project sponsorship

Percentage of project-active respondents selecting item; multiple responses allowed.
How IdM projects are paid for

- Annual central IT budget
- Bundled w. other projects
- Not yet determined
- One time campus budget allocation
- Contributions from other central units
- Partnerships or grants

Percentage of project-active respondents selecting item; multiple responses allowed
## What matters?

<table>
<thead>
<tr>
<th></th>
<th>Sr mgmt understanding of costs</th>
<th>Sr. mgmt willing to address policy issues</th>
<th>Tech adoption strategy</th>
<th>Institution IT goals</th>
<th>Resource sufficiency</th>
<th>Selected documentation, policy, &amp; planning activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IdM capability score</strong></td>
<td><strong>X</strong></td>
<td><strong>X</strong></td>
<td><strong>X</strong></td>
<td><strong>X</strong></td>
<td><strong>X</strong></td>
<td><strong>X</strong></td>
</tr>
<tr>
<td><strong>Cost savings</strong></td>
<td><strong>X</strong></td>
<td><strong>X</strong></td>
<td><strong>X</strong></td>
<td></td>
<td></td>
<td><strong>X</strong></td>
</tr>
</tbody>
</table>

**Significant associations between higher/better outcomes and other measures**
Key findings

- It isn’t just hype—respondents are highly engaged with identity management
- But preparations and adoption are light on completed work, heavy on in-progress work & “planning to plan”
- Respondents rate the importance of IdM higher than their capability to deliver it
- AuthN remains heavily dependent on passwords
- IdM is still IT-centric in sponsorship & funding
- Resources don’t match ambitions
- Completers think investments are worth it—but can’t necessarily show $ savings
Summary

• IT is now enabling new business models that will challenge (demolish?) existing ideas about internal control, audit trail, and other basic concepts.

• Higher education’s cost competitiveness may depend on our ability to shed business processes, infrastructures, etc.

• Managing identity and authenticity is a big and growing challenge. IT and internal audit are natural allies here.

• Unmanaged decentralization will pose new and surprising risks.