What's Your Number?
Measuring the Maturity of Your Security Program with HEISC's New Assessment Tool

EDUCAUSE Annual Conference
Wednesday, October 16, 2013

David Escalante | Boston College
Cathy Hubbs | American University
Privacy Month Reminder

• National Cyber Security Alliance will host an event during Data Privacy month.
• Watch for special EDUCAUSE events starting in late January.
Talking Points

• History
• Developing the Tool
• Demo
• Using the Tool at Your Institution
• Analyzing the Results
• Future Versions
History of the Tool

• Information Security Governance (ISG) tool (2004)

• HEISC Strategic Plan (2011)
  – Management Assessment Tool (not Audit tool)
  – Assess a Security Program relative to:
    • Industry standards
    • Higher Education values and practices

• Collaborate with DoE if possible
Developing the Tool (1)

- Leveraged ISO 27002
  - Why 27002 as framework?
- Informed by
  - ISG Tool
  - NIST 800-53
  - Cloud Security Alliance Cloud Controls
  - DoE comments and contributions
- Reviewed NIST 800-53 and mapped to ISO
Developing the Tool (2)

- Deciding on Maturity Levels
- Performed pilots with HEISC working groups
## Comparing Maturity Levels

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>ISO 21827</th>
<th>Carnegie-Mellon Capability Maturity Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Not Performed</td>
<td>Non-existent</td>
</tr>
<tr>
<td>1</td>
<td>Performed Informally</td>
<td>Ad hoc</td>
</tr>
<tr>
<td>2</td>
<td>Planned</td>
<td>Repeatable</td>
</tr>
<tr>
<td>3</td>
<td>Well Defined</td>
<td>Defined &amp; Implemented</td>
</tr>
<tr>
<td>4</td>
<td>Quantitatively Controlled</td>
<td>Managed</td>
</tr>
<tr>
<td>5</td>
<td>Continuously Improving</td>
<td>Optimized</td>
</tr>
</tbody>
</table>
Demo Time...
Who Should Complete the Assessment?

• System
• Central IT
• Departments
  – U. California got good preliminary feedback
• Market Basket (peer comparison)
  – Anonymity vs. inter-institutional sharing
  – Tool does not consolidate auto-magically
How Long Will It Take?

• Set aside 2 hours
  +/- 1 hour
  – That’s “per fill” not “per institution”

• Analysis will take longer...
Sample Report Card - Processes

DEPTH OF SECURITY PROGRAM

BREADTH OF SECURITY PROGRAM


AVG
Sample Report Card - Technical

DEPTH OF SECURITY PROGRAM vs BREADTH OF SECURITY PROGRAM

- Risk Management
- Security Policy
- Organization
- Asset Mgmt
- H/R Security
- Physical
- Comm + Ops Mgmt
- Access Control
- System Development
- Incident Mgmt
- Business Continuity
- Compliance

AVG
Your Number...

• How the scoring works today
• Alternate approaches
  – Average across questions
  – Weighted average
• A high score is reason to be suspicious – even non-EDUs with strong security programs aren’t going to score a 4.75...
Validating Results Using Institution’s Risk Assessment

• Best practices versus risk mitigation
  – Which is more important? Which is “Right”?  
  – Do the results fit together?

• Solving the assessment’s variances
  – How to compare?

YMMV
Your Mileage May Vary
## Risk Assessment for “Party”

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Risk Name</th>
<th>Probability (1-3)</th>
<th>Impact (1-3)</th>
<th>Risk Score</th>
<th>Mitigation</th>
<th>Contingency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guests</td>
<td>The guests find the party boring</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>Invite crazy friends, provide sufficient liquor</td>
<td>Bring out the karaoke</td>
</tr>
<tr>
<td>Guests</td>
<td>Drunken brawl</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>Don’t invite crazy friends, don’t provide too much liquor</td>
<td>Call 911</td>
</tr>
<tr>
<td>Nature</td>
<td>Rain</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>Have the party indoors</td>
<td>Move the party indoors</td>
</tr>
<tr>
<td>Nature</td>
<td>Earthquake or fire</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>Start the party with instructions on what to do in the event of fire or earthquake</td>
<td>Implement the appropriate natural disaster response plan</td>
</tr>
<tr>
<td>Food</td>
<td>Not enough food</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>Have a buffet</td>
<td>Order pizza</td>
</tr>
<tr>
<td>Food</td>
<td>Food is spoiled</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>Store the food in deep freezer</td>
<td>Order pizza</td>
</tr>
</tbody>
</table>
## Mapping Party Risks to ISO

### Significant Risks Identified by Risk Assessment

<table>
<thead>
<tr>
<th>ISO Area</th>
<th>Party Boring</th>
<th>Drunken Brawl</th>
<th>Rain/Quake / Fire</th>
<th>Not Enough Food</th>
<th>Food Is Sponted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Policy</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Organization</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Asset Management</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>H/R Security</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical &amp; Environmental Security</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications &amp; Operations Management</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Access Control</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems Acquisition, Development, and Maintenance</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Incident Management</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Continuity</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Mapping Actual Risks to ISO

## Significant Risks Identified by Risk Assessment

<table>
<thead>
<tr>
<th>ISO Area</th>
<th>Loss of Regulated Data</th>
<th>Disclosure of Internal Info</th>
<th>Password Exposure</th>
<th>Improper Storage of Data</th>
<th>Failure to Produce Critical Data</th>
<th>Systems Unavailable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Asset Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>H/R Security</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Physical &amp; Environmental Security</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications &amp; Operations Management</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Systems Acquisition, Dev. &amp; Maintenance</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Incident Management</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Continuity Compliance</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
HEISC Security Program Assessment With Risk Assessment Overlay
Now What?
Alternative Assessment Methods

- Benchmarking
- Metrics
- Spending
- Compliance
Improving the Current Tool

• Working group had representation from both large and small schools
• The more input, however, the better
  
  security-feedback@educause.edu
• Are the questions apropos?
• Is the scoring reasonable?
• Is the documentation adequate?
Future Features of the Tool

• Inter-institutional benchmarking
  – Pros and Cons
• Charts
Links & Credits

• educause.edu/security/assessment-tool
• Send feedback to:
  security-feedback@educause.edu
• HEISC-ASSESS subcommittee:
  Julia Allen  Patrick Feehan  Rodney Petersen
  Silvio Balzano  Bridget-Anne Hampden (DoE)  Adam Vedra
  Cathy Bates  Cathy Hubbs  Valerie Vogel
  Kathy Bergsma  Barron Hulver  Cheryl Washington
  David Escalante  Doug Markiewicz
Questions?