Learn from Your Peers: Metrics Success Stories

Joshua Beeman, CISO, University of Pennsylvania
Cathy Hubbs, CISO, American University
Eric Schmidt, CISO, Butler University
University Fun Fact
In the 60’s our on campus food joint, The Tavern, was the largest seller of beer in the District of Columbia.

Speaker Fun Fact
Trapeze “catch” on first try!

Median InfoSec Spend as % of Central IT Spend 2016

<table>
<thead>
<tr>
<th></th>
<th>My institution</th>
<th>All nonspecialized U.S.</th>
<th>AA</th>
<th>BA</th>
<th>MA public</th>
<th>MA private</th>
<th>DR public</th>
<th>DR private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Institutional Responses, 2016 EDUCAUSE Core Data Service
Butler University

Hinkle Fieldhouse was constructed in 1928 as the then-largest basketball arena in the nation, and it was named a National Historic Landmark in 1987. Hinkle served as the setting for the iconic sports movie Hoosiers and is home to the Butler Bulldogs, members of the Big East Conference.

- Named the Most Innovative School in the Midwest by U.S. News and World Report, Butler is a nationally recognized comprehensive university encompassing six colleges: Arts, Business, Communication, Education, Liberal Arts and Sciences, and Pharmacy and Health Sciences
- Butler offers more than 60 undergraduate areas of study, eight pre-professional programs, and 19 graduate programs
- About 4,700 students are enrolled at Butler, representing 45 states and 49 countries

Speaker Fact

Has run many ultramarathons including three 50 mile races and dozens of 32 mile races.

*Fun Fact*

Has run many ultramarathons including three 50 mile races and dozens of 32 mile races.
UPenn

“By The Numbers”
Annual University Budget: $8.78 Billion
Number of IT staff: 900
Number of (Central) InfoSec Staff: 10

Median InfoSec Spend as % of Central IT Spend 2016

- My Institution: 5%
- All nonspecialized U.S.: 3%
- AA: 3%
- BA: 2%
- MA public: 3%
- MA private: 2%
- DR public: 4%
- DR private: 4%

University Population
- Staff: 12,356
- Faculty: 4,645
- Full-time students: 21,563
- Part-time students: 3,313

- University Fun Fact
  Penn researchers introduced ENIAC, the world’s first electronic, large-scale general-purpose digital computer.

- Speaker Fun Fact
  Was on reality-tv show “Trading Spaces”
Why Metrics?

‘You cannot improve what you cannot measure.’
Lord Kelvin, paraphrased by Andrew Jaquith

Enable decision makers to take action.

Metrics can be used to educate and raise awareness.

Contribute to answering questions your executives may have. For example:

How is the effectiveness of the cybersecurity program measured?
Is the organization spending appropriately on security priorities?
How does the organization’s security program compare to that of its peers?
What Works? What Matters?

Decide what matters (and to which audience) and then work backwards to create the metric.

Your metrics will mature - but only if you start somewhere first

Contextually specific* - relevant enough to decision makers to take action

*Source: Andrew Jaquith, Security Metrics
Data Gathering

Begin with data that you have available to you easily and automatically.
Consider the:
- Accuracy
- Repeatability
- Reliability
- Auditability

Augment your program over time with additional data.
Driving Accountability

- Observing changes in behavior
- Use this to focus yourself and management
- Be mindful of unintended consequences
Review Effectiveness of Your Metrics

Seek to improve and refine cybersecurity metrics.

Periodically check in with the consumers of your metrics.
  Are they still providing value?

Maintain historical data and capture trends.
Summary and Additional Discussion

Metrics for different levels - **Decide what matters (and to which audience) and then work backwards** to create the metric. The perfect is enemy of the good. **Start with the data that you can collect and the tools you have** and move forward; automation is key; don’t design something so heavy that it’s not functionally workable.

Consider **where you want to hold yourself accountable**

**Metrics are education.** A pretty graph that you explain once and show every quarter educates your board/senior management.

Be sure you **review your metrics**--they are worthless if you don’t look at them regularly to understand how they change over time, and it’s OK if they mature over time.
Questions?