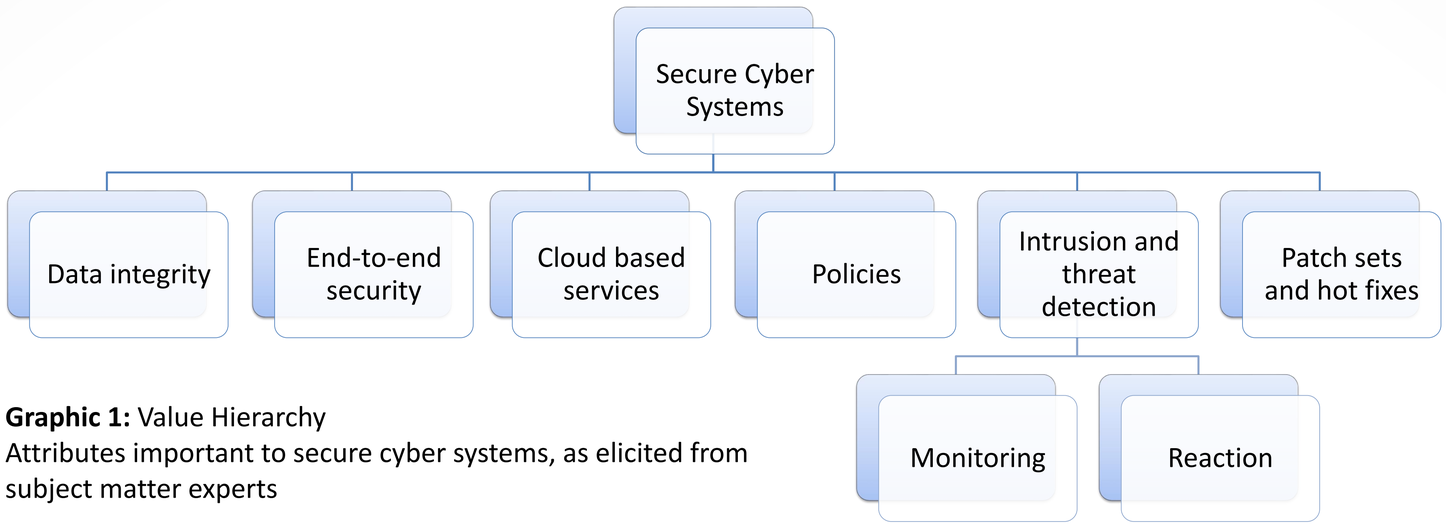
A Value Model for Implementing Cyber Metrics and Best Practices

Dr. Natalie Scala, Emil Manuel, Rachel Fredman, Jasmin Farahani, Towson University
Dr. Paul Goethals, United States Military Academy

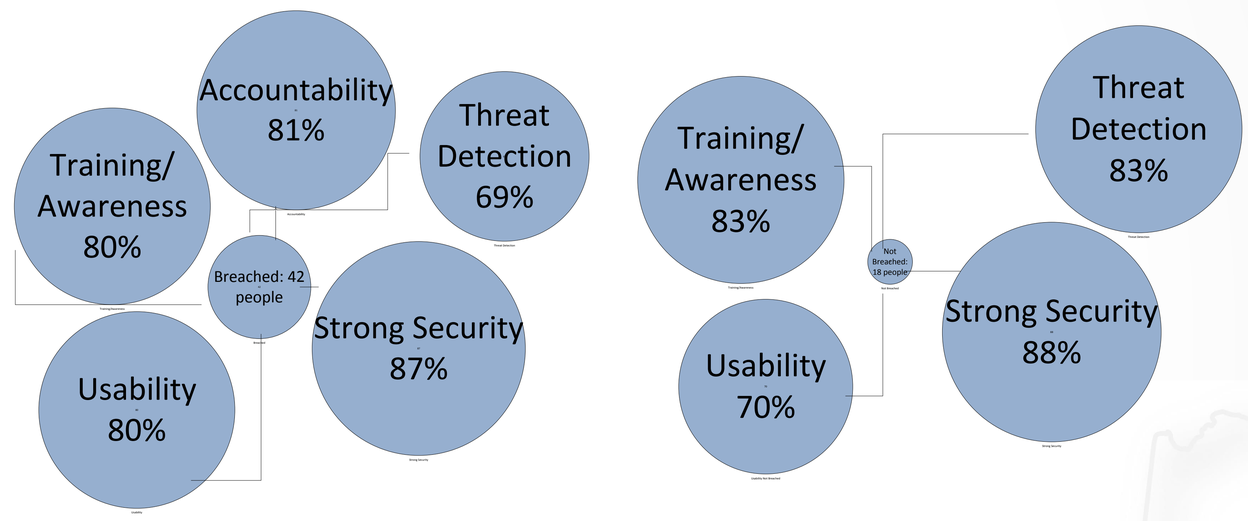
Amid security concerns and the sheer volume of options to address them, this research develops a value model that enables any organization to identify the most important security metrics and best practices to implement.



Graphic 1: Value Hierarchy
Attributes important to secure cyber systems, as elicited from subject matter experts

Data Integrity	
Existence of security and access permissions, existence of transaction or version logs, having and using audit process	100
Existence of security and access permissions, existence of transaction or version logs	80
Existence of security and access permissions, having and using audit process	70
Existence of transaction or version logs, having and using audit process	50
Existence of security and access permissions	50
Existence of transaction or version logs	30
Having and using audit process	20
None of these	0

Table 1: Sample Value Function
Elicited from subject matter experts



Graphic 2: Bubble Chart
From survey analysis, organizations that were either breached or not breached were consistent in their value of threat detection, training/awareness, and strong security. A notable difference is the additional value of accountability in organizations that were breached.

For each metric or best practice a, calculate score s:

$$s_a = \sum_{i=1}^{m} w_i v_{ia}$$

where w_i is the weight of measure i, and v_{ia} is the value function scale item for measure i and alternative a

Derive weights using the rank order centroid method:

$$w_i = \frac{1}{K}\sum_{k=1}^{K}\frac{1}{k}$$

where K is the number of measures, w_i is the weight for the i^{th} measure

- Normalize weights to sum to 1
- Buede (2009), Barron (1992), Barron and Barrett (1996)

Largest s_a denotes preferred alternative

Formulas: Calculating Value using Multiple Objective Decision Analysis (MODA)

Preliminary Ranking Results	
Control administrative privileges	1
Limit workstation-to-workstation communication	2
Take advantage of software improvements	3
Use anti-virus file reputation services	4
Enable anti-exploitation features	5
Use web domain name system reputation	6
Implement host intrusion prevention system (HIPS) rules	7
Segregate networks and functions	8
Application whitelisting	9
Set a secure baseline configuration	10

Table 2: Preliminary Rank Order Results
Using Top 10 Information Assurance Mitigation Strategies[1] as candidate metrics and best practices
[1]http://tinyurl.com/top10IAD

HoTSoS *Symposium and Bootcamp*
HOT TOPICS *in the* **SCIENCE OF SECURITY**
APRIL 4-5, 2017 | HANOVER, MARYLAND