Cybersecurity Budgets

Scott Russell, Bob Cowles, Craig Jackson

Indiana University Center for Applied Cybersecurity Research
cacr.iu.edu

NSF Cybersecurity Center of Excellence
trustedci.org

August 17, 2016
2016 NSF Cybersecurity Summit

From 2015 NSF Summit Report

Recommendation 1: The NSF CI and Large Facility community should develop a broadly applicable strategy for information security budgets, including how, why, and where it does what it does in terms of spending.

Recommendation 2: The NSF CI and Large Facility community should support research on metrics that indicate whether spending on information security is sufficient and appropriately balanced with a project's science mission.

Outline

Introduction

Part 1: Review of Recent Cybersecurity Spending Surveys

a. Methodology
b. Results & Analysis
c. Recommendations

Part 2: Case Study, DOE Science Labs

a. Environment
b. Methodology
c. Analysis
    i. Cybersecurity vs. Lab budget
    ii. Cybersecurity vs. IT budget
d. Conclusions

Questions

Goals for this talk

1. Give you a strong sense of the cybersecurity budget benchmarking research that is out there, and to what extent it is useful. (Spoiler alert: Probably not.)

   https://goo.gl/JwwfEx

2. Give you insight into cybersecurity budgeting in a community with some similarities to this one. (Following our own awesome advice.)

3. Help us move beyond the benchmarking discussion (which has gotta happen) and into how spending much makes sense.

Part 1

Review of Recent Cybersecurity Spending Surveys

Why do an exhaustive review of cybersecurity spending research?

1. Lemming logic: Benchmarking makes sense up to a point. If someone isn't telling you exactly what to do, you look around at the crowd.
2. Always good to establish a description of the environment before dictating norms.
3. There's a bunch of this research 'out there' and a cursory look indicates it is not all the same quality and not all saying the same thing.
4. Masochism.
5. Spending norms might be important.

Methodology

Exhaustive keyword search for independent research papers

Fifty studies

Further narrowed results based on the following criteria:

1. Quantitative - % of IT budget, % of revenue, or $
2. Published Methodology
3. Publicly Available / commonly available to academic institutions
4. Recent (Jan. 2011 through Feb. 2016)

Eleven studies remained

Eight were broad spectrum; three sector specific

Results & Analysis

Studies show *some* consistency in findings…

Majority of cybersecurity budgets lie between 3% to 12% of the IT budget.

But that's quite a range. Big practical difference between $30k and $120k. Can we trust any of this?

Results & Analysis

Size matters!

"Small" organizations spend 2x to 4x more of their IT budget (percentage) than "large" organizations

Economies of scale & baseline costs at work?

Sector matters!

Finance and aerospace/defense sectors spend more

Makes little sense to focus on cross-sector averages

The utility of most studies is limited…

1. Methodological rigor (lots of "unsure", low response rates)
2. Often unclear what is and what is not "cybersecurity"; the scope will obviously impact the money spent there
3. Intra-study variability in results

Recommendations

1: Avoid over-reliance on benchmarking data

- Variability suggests limited validity and/or complete chaos in the wild
- "Does spend" vs. "should spend"… no reason to believe these are aligned well
- Concentrate instead matching spending to risk-to-mission (*see, e.g.*, AFCEA "The Economics of Cybersecurity")

2: Talk to peer organizations / look at case studies

- Seek out case studies rather than surveys
- Organizational size and sector are important
- Access to granular data is very important

3: Ignore all but the highest quality, most usable studies

- PWC "Global State of Information Security"; particularly data exploration tool

Part 2

Case Study - DOE Science Labs

http://science.energy.gov/laboratories/

Environment

DOE Office of Science funds 10 research labs
Government Owned, Contractor Operated (vs. NSF)
Federal Information System Management Act (FISMA)

Not included in cybersecurity

- Good business - personnel policies; good procedures
- Effective IT - DR/backup, config & patch mgmt, identity and access mgmt, log collection

Included in cybersecurity

- Monitoring, threat management, incident response

Unclassified Only

Classified and Unclassified

Methodology

Each year, the federal budget for each lab specifies the cybersecurity budget as a portion of the total budget for each lab.

http://energy.gov/sites/prod/files/2016/02/f29/FY2017BudgetLaboratoryTable_0.pdf

Each year, labs are required to describe their IT investments (OMB Exhibit 53) and this is reflected in a public DOE IT Dashboard

https://www.itdashboard.gov/drupal/summary/019

Analysis

Cybersecurity vs. Lab Budget

NAME	FY2017 Total	Cyber Funding	
Ames	46832	843	1.80%
Princeton	76882	816	1.06%
TJLab	125574	1119	0.89%
Fermi	394639	2560	0.65%
SLAC	543072	2458	0.45%
LBL	643886	2940	0.46%
Brookhaven	476992	2846	0.60%
PNNL	517782	4445	0.86%
Argonne	585279	2660	0.45%
ORNL	1058672	7504	0.71%

Analysis

Cybersecurity vs. Lab Budget

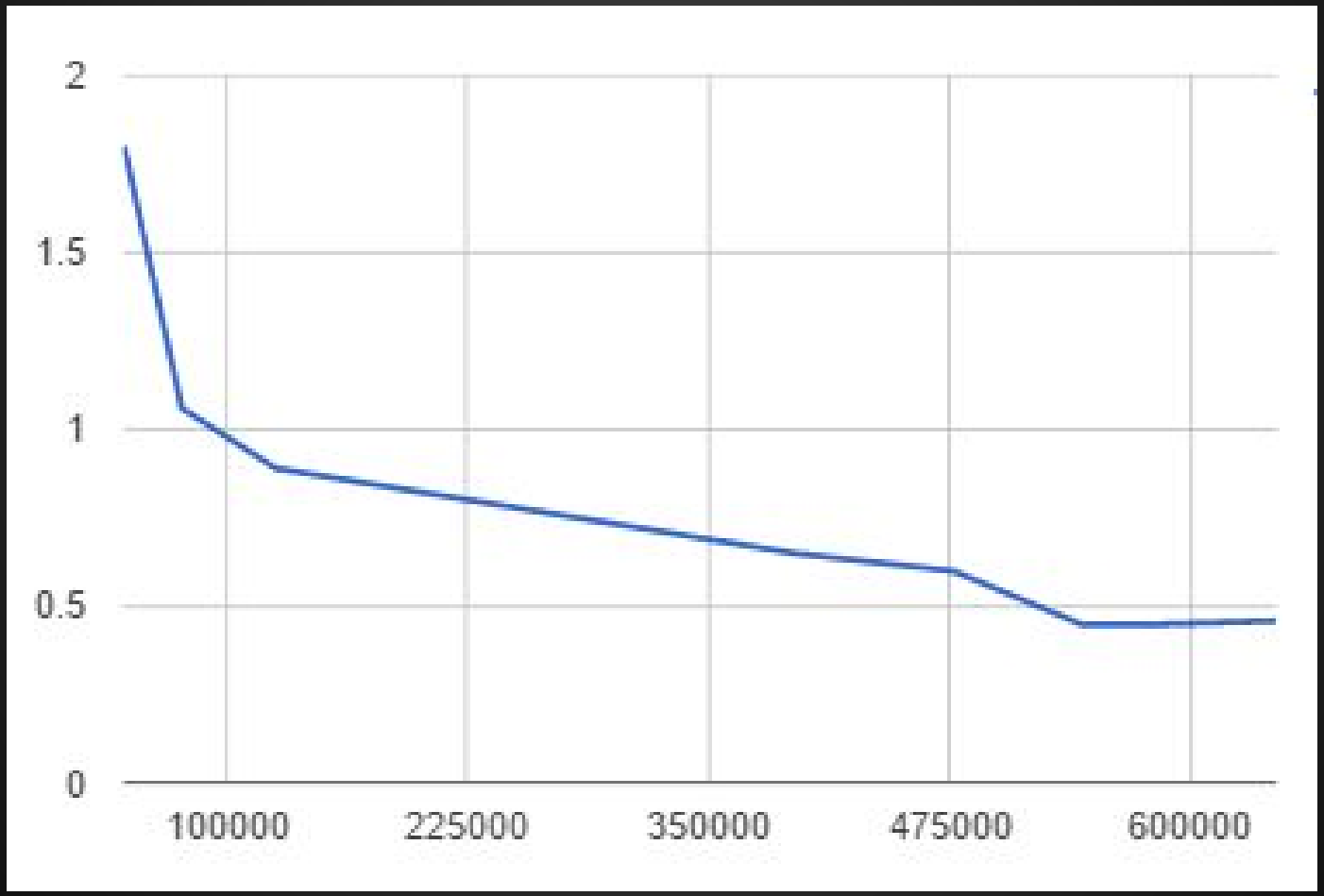
NAME	FY2017 Total	Cyber Funding	
Ames	46832	843	1.80%
Princeton	76882	816	1.06%
TJLab	125574	1119	0.89%
Fermi	394639	2560	0.65%
SLAC	543072	2458	0.45%
LBL	643886	2940	0.46%
Brookhaven	476992	2846	0.60%
PNNL	517782	4445	0.86%
Argonne	585279	2660	0.45%
ORNL	1058672	7504	0.71%

Analysis

If classified effort is relatively small …

NAME	FY2017 Total	Cyber Funding	
Ames	46832	843	1.80%
Princeton	76882	816	1.06%
TJLab	125574	1119	0.89%
Fermi	394639	2560	0.65%
SLAC	543072	2458	0.45%
LBL	643886	2940	0.46%
Brookhaven	476992	2846	0.60%
PNNL	517782	4445	0.86%
Argonne	585279	2660	0.45%
ORNL	1058672	7504	0.71%

Chart - % Cybersecurity vs. Total Lab Budget



Analysis

Cybersecurity vs. IT Budget

Name	Total IT	Cyber Funding	
Ames	3020	843	27.91%
Princeton	6866	816	11.88%
TJLab	10820	1119	10.34%
Fermi	30729	2560	8.33%
SLAC	25467	2458	9.65%
LBL	31801	2940	9.24%
Brookhaven	25582	2846	11.13%
PNNL	42318	4445	10.50%
Argonne	21863	2660	12.17%
Oak Ridge	29626	7504	25.33%

Analysis

Cybersecurity vs. IT Budget

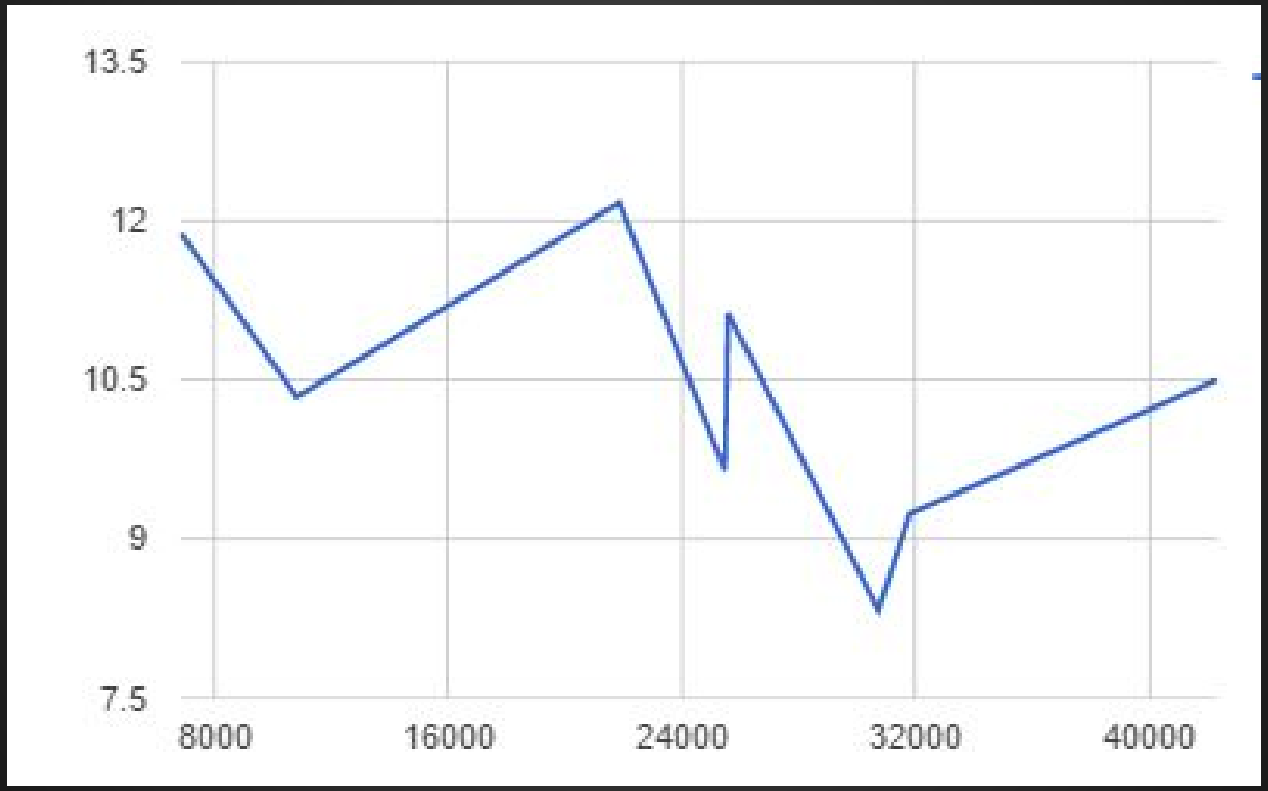
Name	Total IT	Cyber Funding	
Ames	3020	843	27.91%
Princeton	6866	816	11.88%
TJLab	10820	1119	10.34%
Fermi	30729	2560	8.33%
SLAC	25467	2458	9.65%
LBL	31801	2940	9.24%
Brookhaven	25582	2846	11.13%
PNNL	42318	4445	10.50%
Argonne	21863	2660	12.17%
Oak Ridge	29626	7504	25.33%

Analysis

Scientific IT is not included in reported investment

Name	Total IT	Cyber Funding	
Ames	3020	843	27.91%
Princeton	6866	816	11.88%
TJLab	10820	1119	10.34%
Fermi	30729	2560	8.33%
SLAC	25467	2458	9.65%
LBL	31801	2940	9.24%
Brookhaven	25582	2846	11.13%
PNNL	42318	4445	10.50%
Argonne	21863	2660	12.17%
Oak Ridge	29626	7504	25.33%

Chart - % Cybersecurity vs. IT Budget



Part 2 Conclusions

1. What is included in the IT budget and what is included in the cybersecurity budget is not consistent and must be viewed carefully when working with the data.

2. We see a trend of decreasing cybersecurity spending as a percentage of increasing total lab or IT budgets (economy of scale)

3. For larger labs cybersecurity spending is about 0.5% of total budget and 8-12% of IT budget - consistent with the reviewed surveys.

And so....

1. Security costs money. Difficult to reach economy of scale without joining forces and sharing practices and information.

2. Distinguish between good practices (business and IT) and actual cost of cybersecurity.

3. Complete the survey at trustedci.org/survey.

Thank you…. Questions?

Draft paper: https://goo.gl/JwwfEx
Final to be published with summit report

Craig Jackson (scjackso@indiana.edu)
Bob Cowles (bob.cowles@gmail.com)

The authors thank the Indiana University Center for Applied Cybersecurity Research and the Center for Trustworthy Scientific Cyberinfrastructure for supporting this work. This material is based in part on work supported by the National Science Foundation under Grant Number ACI-1547272 and OCI-1234408.