

***RESEARCH COMPUTING,
INFORMATION SECURITY
COMPLIANCE REQUIREMENTS,
AND
IMPACTS TO COST ACCOUNTING***

August 28, 2018



With you today

Sarah T Axelrod

sarah_axelrod@harvard.edu

Jim Carter

jcarter@huronconsultinggroup.com

Wendy Meister

wmeister@huronconsultinggroup.com



INFORMATION SECURITY & COMPLIANCE



Questions Leaders are Asking



President, Chancellor, Provost

Are we in compliance with all of these regulations related to information security?

Do we know where all of our sensitive data is located today?



CFO

Are we adequately funding information security?

What are the costs of responding to impacts of attack?



CIO / CTO

Am I implementing solutions bigger, faster, cheaper and in a more secure way?

How do I balance the need for access and the need for protection?



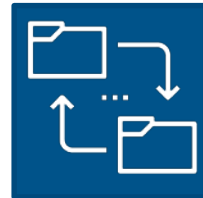
CISO

Is the institution enabling me to be successful?

How do I help educate and oversee an effective security program?

Risks by the Numbers

Dramatic increase in data security threats:



Increases

- **1% or 1 in 131** of all emails in 2016 contained malware (increase from 1 in 220 in 2015)
- **45%** increase in the number of reported data breaches from 2016 to 2017



Losses

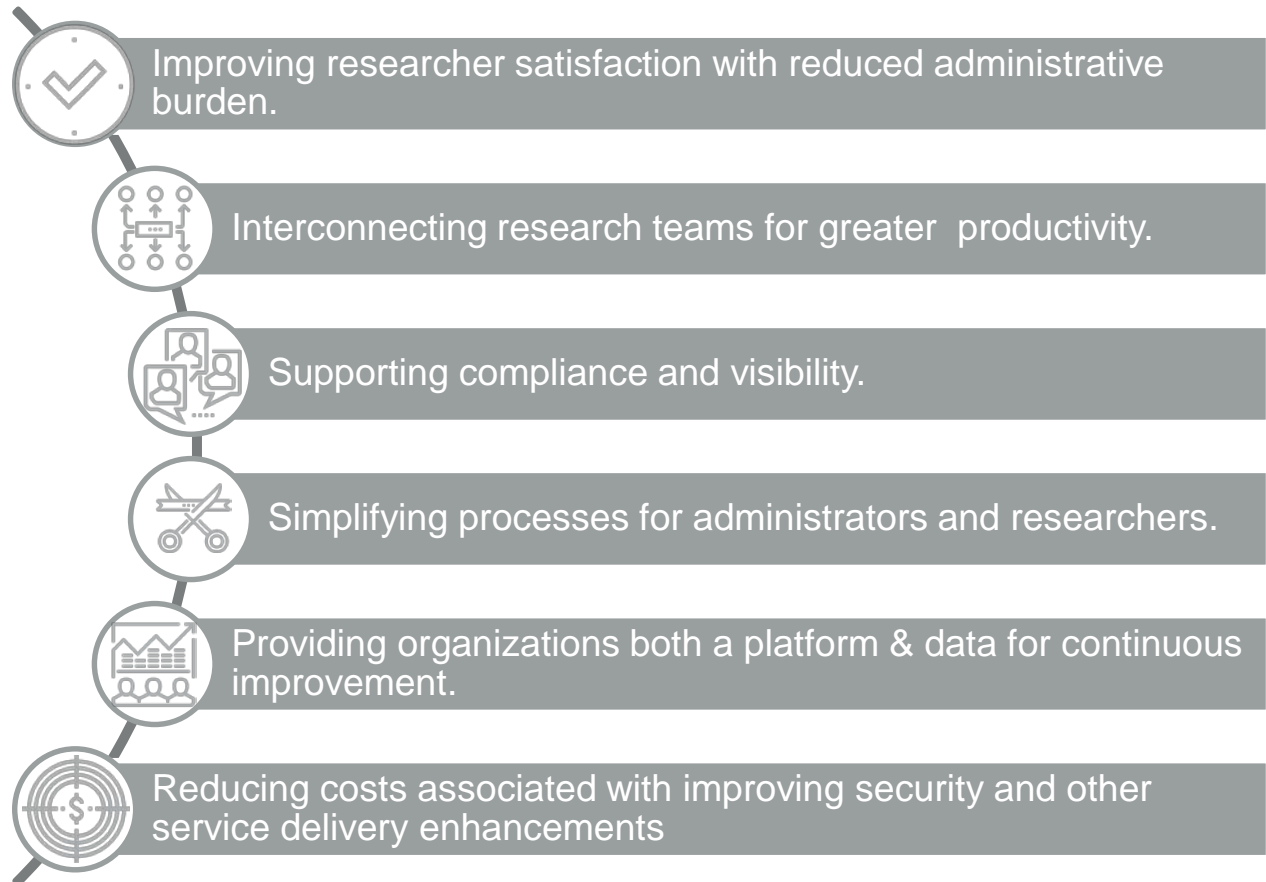
- **\$141** is the average cost incurred for each lost or stolen record containing sensitive or confidential information
- **\$360** is the approximate price of an Electronic Health Record on the black market compared to \$1 for a SSN

\$8T – Projected total cumulative cost of data breaches from 2017 - 2022

179M – Total number of records compromised by data breaches in the US 2017







A Greater Focus on Technology

Institutions are concentrating on:



IT Security Requirements

Snapshot: Compliance Crosswalk

	 HIPAA Health Insurance Portability & Accountability Act	 General Data Protection Regulation	 FERPA Family Educational Rights and Privacy Act	 PCI DSS COMPLIANT	 FISMA FEDERAL INFORMATION SECURITY MANAGEMENT ACT	 Welcome to CALIFORNIA The Golden State
Overview	<ul style="list-style-type: none"> + Privacy standards for the disclosure of protected health information + Security standards for the protection of health information + Breach notification rules 	<ul style="list-style-type: none"> + Key principles for the handling/storage of data for EU citizens or persons living in EU + Requirements for establishing lawful basis for processing + Individual rights + Security rules + Breach notification rules 	<ul style="list-style-type: none"> + Privacy standards for protection/disclosure of student education records 	<ul style="list-style-type: none"> + Security standards for handling of payment card information 	<ul style="list-style-type: none"> + Standards for implementing information security programs for federal agencies + Contains control-focused minimum security requirements 	<ul style="list-style-type: none"> + Customers are afforded the right to know what personal data are collected and why. + Broad definition of private data: personal identifiers, geolocation, biometric data, internet browsing history, psychometric data)
Overlaps other standards	<ul style="list-style-type: none"> + GDPR (Privacy, Security, Breach Notification) + FERPA (Privacy/Disclosure) + PCI (Security Control) + FISMA (Security Program, Security Control) 	<ul style="list-style-type: none"> + HIPAA (Privacy, Security, Breach Notification) + FERPA (Privacy) + PCI (Security Control) + FISMA (Security Program, Security Control) 	<ul style="list-style-type: none"> + HIPAA (Privacy/Disclosure) + EU GDPR (Privacy) 	<ul style="list-style-type: none"> + HIPAA (Security Control) + EU GDPR (Security Control) + FISMA (Security Control) 	<ul style="list-style-type: none"> + HIPAA (Security Program, Security Control) + EU GDPR (Security Program, Security Control) + PCI (Security Control) 	<ul style="list-style-type: none"> + HIPAA (Privacy, Security, Breach Notification) + FERPA (Privacy) + PCI (Security Control) + FISMA (Security Program, Security Control)
Mapping to best practices	<ul style="list-style-type: none"> + NIST CSF, SP 800-53 + ISO/IEC 27001 + ISO/IEC 27002 + ISO/IEC 29100 	<ul style="list-style-type: none"> + NIST CSF + ISO/IEC 27001 + ISO/IEC 29100 	<ul style="list-style-type: none"> + ISO/IEC 29100 	<ul style="list-style-type: none"> + NIST CSF, SP 800-53 + ISO/IEC 27002 	<ul style="list-style-type: none"> + FIPS (199, 200) + NIST CSF, SP 800-18/37/53/60) + ISO/IEC 27001 + ISO/IEC 27002 	<ul style="list-style-type: none"> + FIPS (199, 200) + NIST CSF, + ISO/IEC 27001 + ISO/IEC 27002

RESEARCH COMPUTING



Research Computing

In order to centralize and streamline the IT infrastructure, many institutions have established high performance computing centers to provide cutting edge technical capabilities to the research community across a variety of academic disciplines.

These services can include:

- High performance computing
- High throughput computing
- Cloud-based computing services
- Storage of large data sets
- Data backup and security
- Performance networking capabilities



High Performance Research Computing

IT costs have increased exponentially for services that benefit the entire research enterprise.

Establishing and maintaining high-performance computing centers can be extremely expensive for the institution.



Servers and other hardware

Software licenses and maintenance

Technical staff and IT security personnel

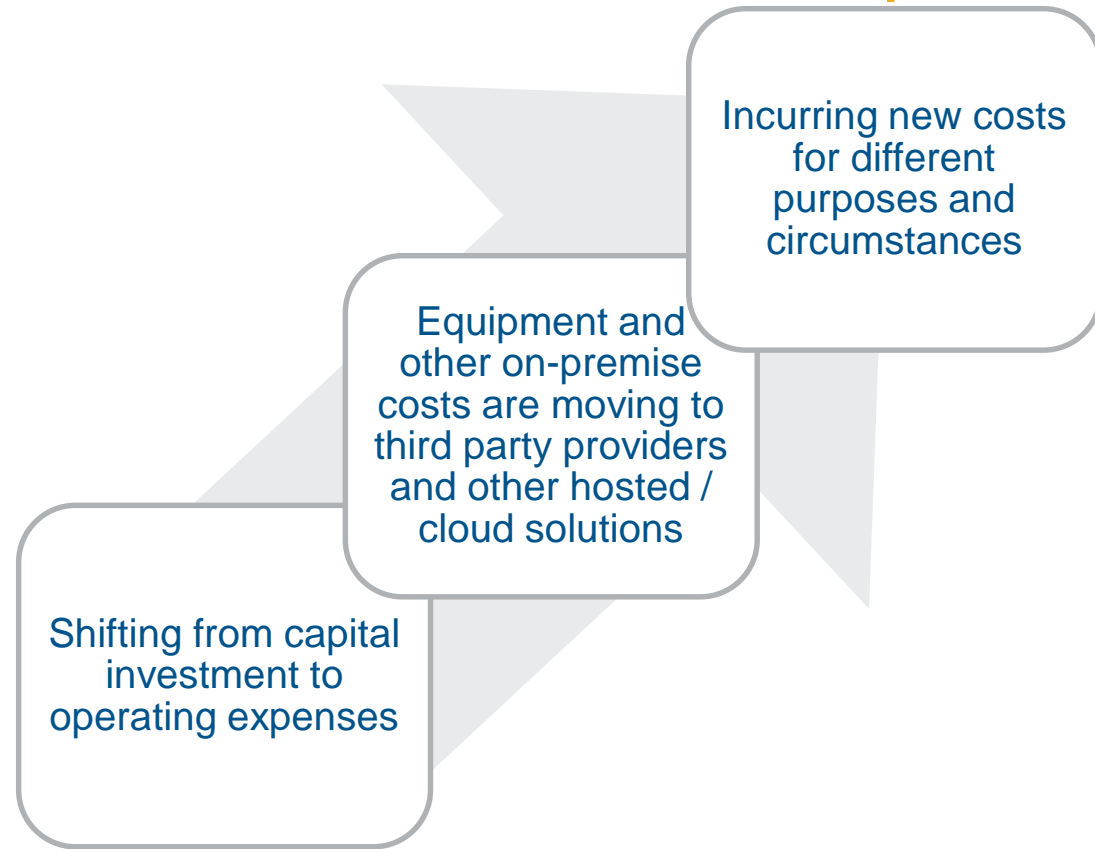
Facilities costs (can include the usage of space and utility costs)

→ **How can an institution recover some of these costs on an ongoing basis while continuing to provide critical support to the research mission?**

COST ACCOUNTING

Growth in Compliance and Research Computing Costs

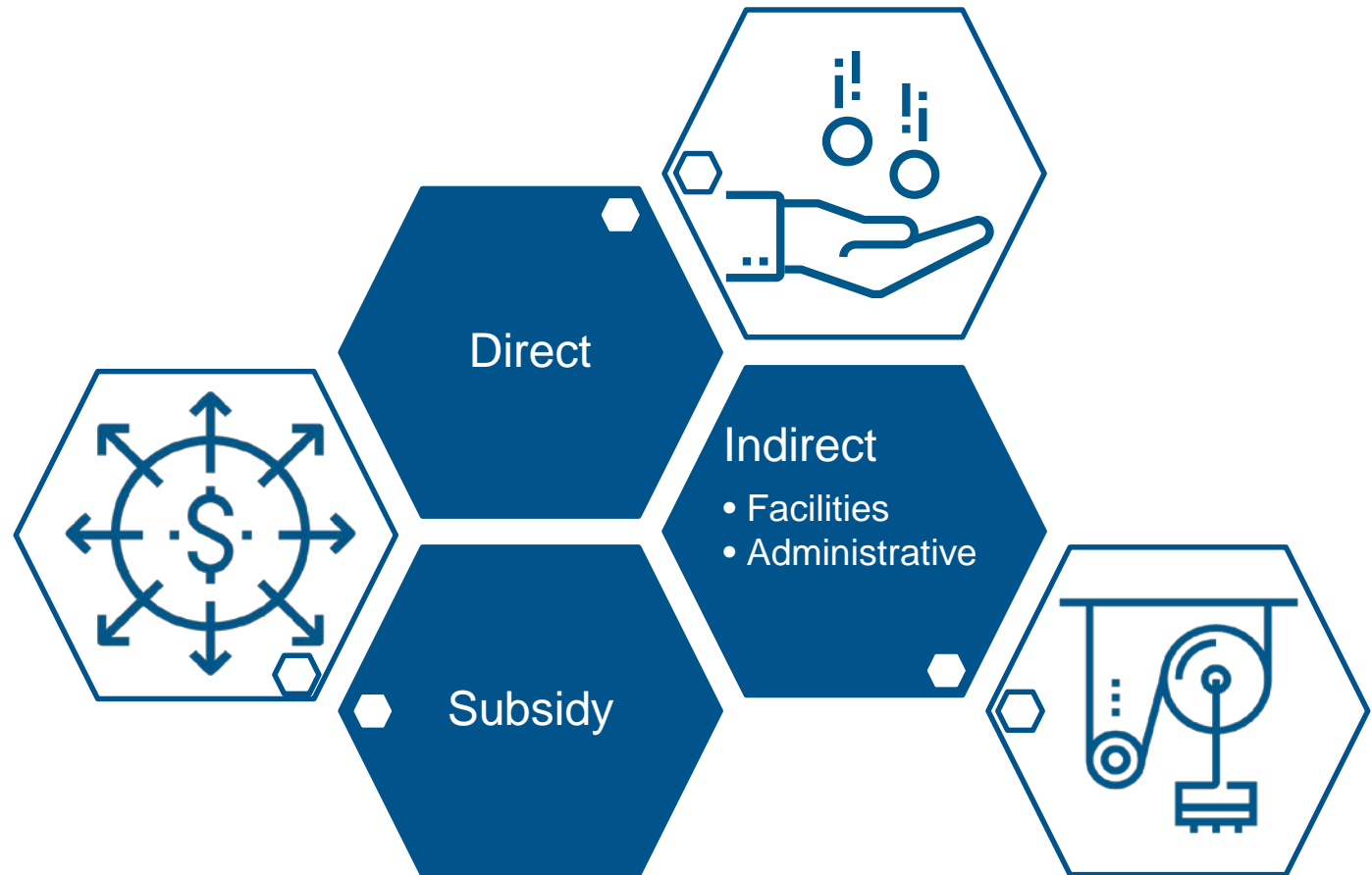
IT costs have increased exponentially for services that benefit the entire research enterprise.



→ How can we charge/allocate these costs for the government to pay its fair share?

How to Recover

Potential Options to Treat a Cost



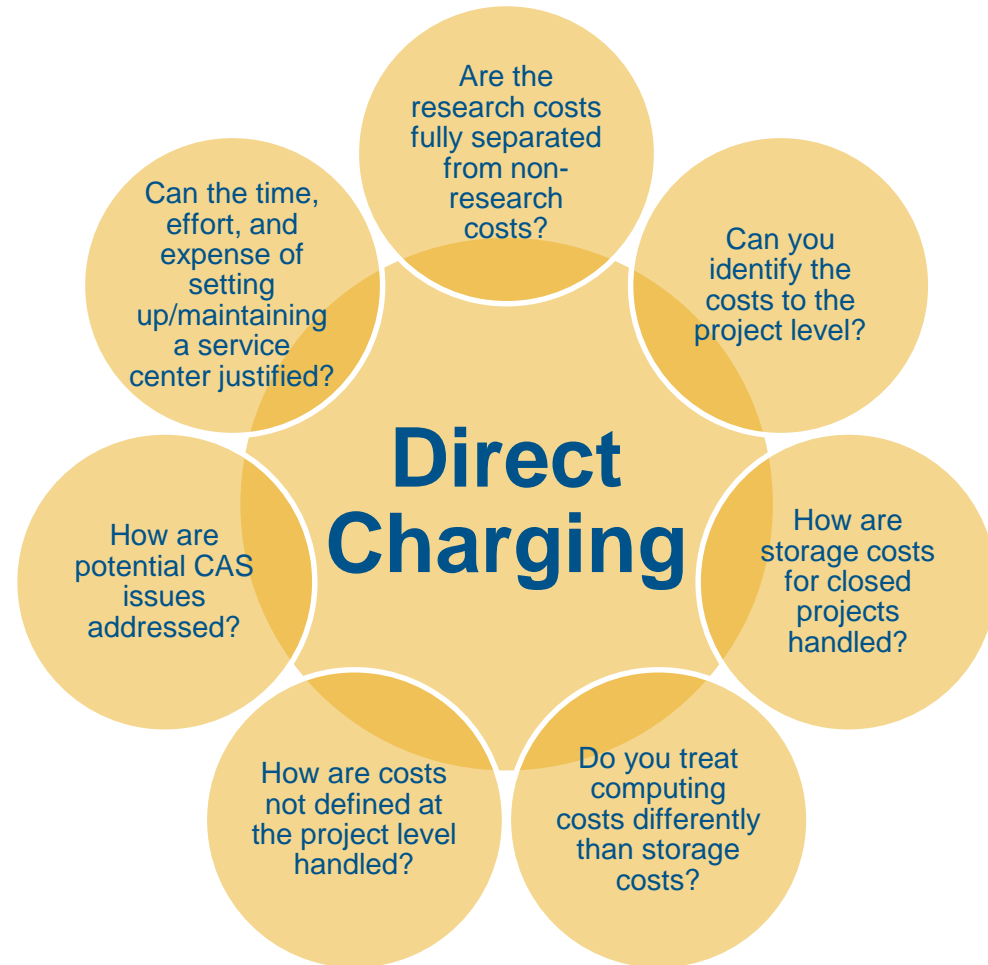
→ How do you quantify the 'effort / cost' associated with the treatment of potential recovery?

Survey Results

If your Institution offers High Performance Research Computing Services, do you:	Subsidize the entire operation, and include these costs in your F&A proposal				
	Operate this activity as a Service Center				
	Operate this activity as a Specialized Service Facility				
If you treat High Performance Research Computing as a Service Center or SSF, what are the rate(s) based on:					
	Server usage				
	Storage capacity				
	Annual payment				
Related to other IT Security costs such as FISMA, NIST, EU GDPR, etc. do you:	Subsidize the entire operation, and include these costs in your F&A proposal				
	1	2	3	4	5

Treatment of Compliance and Research Computing Costs

Challenges/Issues/Questions



Treatment of Compliance and Research Computing Costs

Considerations for Including Costs in F&A

Cost Separation

- How are administrative costs separated from facility costs?

Cost Allocation

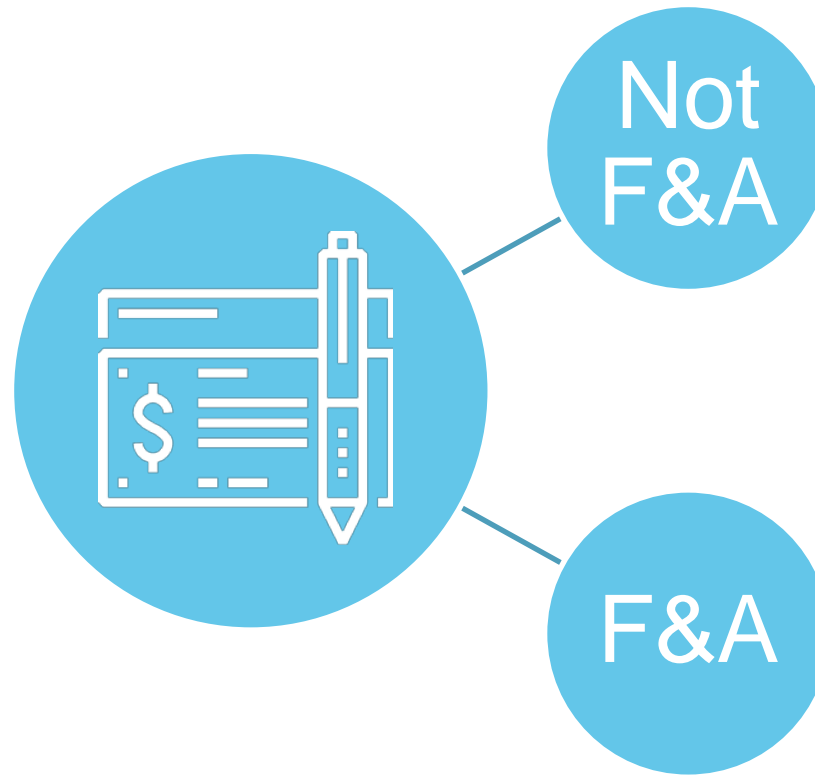
- What is the right basis for allocation of costs?
- Are there costs that may be directly allocated to specific awards?

Cost Incentivization

- If grants and PIs are not charged for research computing, how may behavior be incentivized (e.g. most economical manner of storage)?

Treatment of Compliance and Research Computing Costs

Considerations of IT Security Costs



- Are there other options for IT Security than to include it in an F&A rate?
- Could NIST or FISMA costs be charged directly?
- If not considered F&A, how is CAS compliance ensured?

- What components may be included in Facilities?
- Does IT security cover all institutional areas?

Additional Thoughts

Separating Services and Tracking Usage

- Should institutions charge for these services?
- Should these operations be subsidized?

- What costs should be included in the billing rates?
- What should be the rate base?

- What constitutes a specific “service?”
- How can the costs for each be separated?

THANK YOU



550 W Van Buren St #1700, Chicago, IL 60607



312-583-8700



www.huronconsultinggroup.com