Cybersecurity for Research on Campus: Not Just HIPAA & FISMA

Jim Basney\textsuperscript{1} and Anurag Shankar\textsuperscript{2}

\textsuperscript{1}National Center for Supercomputing Applications, University of Illinois at Urbana-Champaign
\textsuperscript{2}Center for Applied Cybersecurity Research, Indiana University

Internet2 Global Summit
May 7, 2018
MISSION STATEMENT

Washington University in St. Louis' mission is to discover and disseminate knowledge, and protect the freedom of inquiry through research, teaching, and learning.

Washington University creates an environment to encourage and support an ethos of wide-ranging exploration. Washington faculty and staff strive to enhance the lives and livelihood of the people of the greater St. Louis community, the nation, and the world.

Excellence in education and research, a global community, and a commitment to helping people near and far

These tenants guide what we do every day, as we fulfill the promise of UU.

Our mission

Indiana University is a major multcampus public research institution, grounded in the liberal arts and sciences, and a world leader in professional, medical, and technological education.
Regulated vs Open Research

Regulated research is guided by compliance.
E.g. HIPAA, FISMA, NIST 800-171

Open research is not guided by compliance.
E.g. Astronomy, climate, physics, geology

A sizeable fraction or even majority of research is open.
If no medical school, probably majority.
Why worry about open research risks?

➢ Because compliance is not the only driver
➢ Integrity and available are concerns even when confidentiality is not
➢ Can result in reputational harm and funding loss
➢ Researchers on campus have worries and appreciate your help
Open Research Risks
Data Integrity

Data integrity is important for public impact and scientific reproducibility.
Availability of data and Instruments

Eco-loons hack Thirty Meter Telescope website to help the 'natives'
Search for little green men finds them rather close to home

Cyber attack threatened WA astrophysicists' shot at gravitational waves, colliding neutron stars
By Nicolas Perpich
Updated 17 Oct 2017, 3:44am

WATCH

VIDEO: In a galaxy 130 million lights years away two neutron stars collide (ABC News)
Non-regulated but Confidential Data

Endangered species location data.
Maintain confidentiality before “going public” with big news.

Risks:

➢ Release of early research results can mislead

➢ Allow time for peer review & confirmation of results

➢ Properly credit collaborators, related work

➢ Establish commercialization plans (patents, licensing)
Ransomware makes Availability into an attack that works on anyone.

- Research happens online
- Sharing data, programs, etc., with remote collaborators enables research but introduces risks
- Researchers travel with laptops to conferences around the world
- Ransomware or other computer compromise causes:
  - research data loss
  - loss of researcher productivity
Reputation: Collaboration is built on trust

Need trustworthy tools for distributed scientific collaborations.

- Sharing preliminary research results
- Writing grant proposals, research papers
- Managing research subcontracts, budgets, project personnel

Poorly handled security incidents can damage research collaborations.

- Continued/future funding at risk
- Future partnerships at risk
- Allow for questioning of data integrity
Financial: Valuable data and instruments

- Data tampering hinders reproducibility, dissemination of results
- Data may be expensive (or impossible) to reproduce
- Scientific instruments are expensive to replace
- Compromise of controllers can damage instruments or take them offline - harming research productivity on limited budgets
- Scientific instrument productive use often outlasts vendor support (security patches)
Financial: Path to Commercialization

➢ Industry partnerships and commercial technology transfer fund research activities and enable impact
➢ Access to proprietary data enables leading edge research
➢ Risks: industrial espionage, invention disclosure prior to patent application or technology licensing
➢ Poor security practices can lead to loss of industrial partnership opportunities
Another perspective: NSF PI Survey
2018 Clemson survey of 700 NSF PIs*:  

<table>
<thead>
<tr>
<th>Where do your cybersecurity requirements come from?</th>
<th>Not sure</th>
<th>18%**</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use common sense or make up own</td>
<td>33%</td>
</tr>
<tr>
<td></td>
<td>From the university</td>
<td>58%</td>
</tr>
<tr>
<td></td>
<td>From regulations</td>
<td>36%</td>
</tr>
</tbody>
</table>

⇒ 64% get their security requirements from other than regulation.
But those researchers have concerns...
From same 2018 Clemson survey...

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>15%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you aware of attacks against you?</td>
<td>Yes</td>
<td>15%</td>
</tr>
<tr>
<td>Does cybersecurity impact your work?</td>
<td>Yes</td>
<td>60%</td>
</tr>
<tr>
<td>Does cybersecurity seriously impact your ability to work?</td>
<td>Yes</td>
<td>2%</td>
</tr>
<tr>
<td>Are you interested in cybersecurity training?</td>
<td>Yes</td>
<td>26%</td>
</tr>
<tr>
<td>Would you like a confidential security evaluation?</td>
<td>Yes</td>
<td>24%</td>
</tr>
</tbody>
</table>
Risk Summary

➢ No guidance means ambiguity.
➢ Integrity, Availability often more important than Confidentiality.
➢ Each project is different.
➢ There is motivation among the researchers.
Cybersecurity and Open Research: The Challenge of Connecting
"We’re a new research project"

Publish or Perish! Our big risk is being beaten to publication. We need to get the collaboration up now!

"We’re a 200-year old university"

Research is great, but we need to keep paychecks printing and stay out of the newspapers for the wrong reasons!
The Research Sprint

➢ Research tends to be a series of sprints.

➢ A sprint to write a proposal.

➢ Then when/if funded, a sprint to research.
The Researcher

➢ Probably knows that cybersecurity needs attention, but doesn’t know where to start.

➢ Is being inundated by advice from the media, experts, etc.

➢ It’s human nature when anxiety and uncertainty meet to cope by ignoring.
Unusual Software, Hardware, Data, etc.

IT for research tends to be different.

➢ E.g. Secure Shell access to shared computers.
➢ E.g. Uploading virtual machines.
➢ E.g. Distributed, high performance files systems, networks, etc.
Collaboration

It’s common for researchers to span universities and even countries. They will want to define their teams, change those definitions and share access. Collaborators won’t all be in your directories. This can lead to “shadow IT” or use of Cloud to support collaborations.
Cybersecurity and Open Research: How to Connect
Listen and Understand
Get to Know your Research Facilitators And Research Computing Group

They will interact with more researchers than you do.

Let them know what to look for (e.g. PHI) to bring to your attention.

Spend some time learning from them common cybersecurity challenges researchers face on your campus.

Image credit: https://aciref.org/facilitators/what-we-do/
Think Balanced

Old days: We thought we could prevent all attacks.

Now: Balanced approach to risk management is needed:

- Prevention
- Detection
- Mitigation
- Response
- Recovery
Trusted CI can help

Contact us to request help, from small questions to month-long engagements:

https://trustedci.org/help/

See also:
https://trustedci.org/situational-awareness/
https://trustedci.org/webinars/
https://trustedci.org/ctsc-email-lists/
http://blog.trustedci.org/
@TrustedCI
Conclusions

➢ Cybersecurity for unregulated research is important.
➢ Risks to unregulated research often involve integrity, reputation, availability.
➢ Listen to researchers, offer balanced approach, leverage your research computing staff.
➢ Trustedci.org is a source of help.
Acknowledgments

Jill Gemmill, Clemson University
Katie Morris, Office of Research Administration, Indiana University
Von Welch, IU/CACR

Trusted CI, the NSF Cybersecurity Center of Excellence is supported by the National Science Foundation under Grant ACI-1547272. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.