Cybersecurity for Cyberinfrastructure...

and Science!

Von Welch (PI)
Susan Sons (HUBzero Engagement Lead)

Hubbub 2014
30 September 2014
trustedci.org
Cyberinfrastructure Ecosystem

Expertise
- Research and Scholarship
- Education
- Learning and Workforce Development
- Interoperability and operations
- Cyberscience

Computational Resources
- Supercomputers
- Clouds, Grids, Clusters
- Visualization
- Compute services
- Data Centers

Software
- Applications, middleware
- Software development and support
- Cybersecurity: access, authorization, authentication

Organizations
- Universities, schools
- Government labs, agencies
- Research and Medical Centers
- Libraries, Museums
- Virtual Organizations
- Communities

Scientific Instruments
- Large Facilities, MREFCs, telescopes
- Colliders, shake Tables
- Sensor Arrays
  - Ocean, environment, weather, buildings, climate, etc

Data
- Databases, Data repositories
- Collections and Libraries
- Data Access; storage, navigation management, mining tools, curation

Networking
- Campus, national, international networks
- Research and experimental networks
- End-to-end throughput
- Cybersecurity

Maintainability, sustainability, and extensibility

Image credit: Alan Blatecky/NSF
Science!

Distributed Scientific Community

NSF CI Project

- Multiple Universities and/or Research Orgs (IT and policies)
- CI, R&E, and Commercial Services
- CI and Open Source Software
- R&E Networks

Services, Risks, Policies

Requirements, Risks
So, what is cybersecurity for NSF science?
Cybersecurity Historically: Technology

Firewalls, IDS, encryption, logs, passwords, etc.
Cybersecurity supports an organization’s mission by managing risks to information assets.
Translating to NSF projects...

Cybersecurity manages risks to the performance and integrity of computational science.
Postdoc and Mentor Perpetuate Data Falsification and Fabrication In a Series of Published Articles

A former postdoctoral researcher and his mentor at a Colorado university perpetrated the apparent validity of research data after the postdoc had intentionally falsified and fabricated the original study. After coauthors on the original study were unable to replicate the postdoc’s research results, the mentor’s college—without informing university-level administration—conducted an informal inquiry and recommended that the issue be worked out in the literature rather than through a formal investigation. Although the mentor’s lab members had been able to repeat the results when the postdoc was there, after he left they could not do so.
The goal of CTSC is to provide the NSF community with a coherent understanding of cybersecurity, its importance to computational science, and the resources to achieve and maintain an appropriate cybersecurity program.
CTSC Activities

**Engagements**
LIGO, SciGAP, IceCube, Pegasus, CC-NIE peer review, DKIST, LTERNO, DataONE, SEAD, CyberGIS, HUBzero, Globus....

**Education, Outreach and Training**

**Leadership**
CTSC and HUBzero Engagement
HUBzero and cybersecurity

Used by 60+ communities, some with 10s or 100s of thousands of users.

Export control (ITAR) and HIPAA compliance requirements.

HUBzero approached CTSC to assess and improve their cybersecurity.
HUBzero/CTSC “Cybercheckup”

Initial week-long “cybercheckup” of existing HUBzero cybersecurity program.

Finding was a mature, robust cybersecurity program.

Identified places for improvement and further review: better documented physical security, use of two-factor authentication, access control, disaster/incident response plan, and vulnerability scan handling.
In-depth Review

- **Web Server Security Model**
  
  *Covers security measures—both technological and procedural—implemented by the HUBzero operations team.*

- **Disaster Recovery Plan**
  
  *Covers operational safeguards that ensure resiliency in case of a major failure, such as a hub hardware failure, and procedures for doing recovery operations.*
New Initiatives: Formalizing Procedures

- **CMS Security Model**
  
  *Codifies the design of access control and other security features of HUBzero’s CMS software for program longevity and so that they can be reviewed and improved upon.*

- **Vulnerability Management**
  
  *Formalizing the procedures for managing vulnerabilities discovered both in the CMS software and in HUBzero’s operations environment.*
Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects

http://trustedci.org/guide

Basis for CTSC evaluation.

Will be extended with vulnerability management as part of HUBzero engagement.
Thank You

trustedci.org

@TrustedCI

We thank the National Science Foundation (grant 1234408) for supporting our work.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.