CTSC

CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Welcome to the CCoE Webinar Series. Our topic today is Practical Cybersecurity for Open Science Projects. Our host is Jeannette Dopheide.

The meeting will begin shortly. Participants are muted. You may type questions into the chat box during the presentation.

This meeting is being recorded.

The CTSC Webinar Series is supported by National Science Foundation grant #1547272.

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

CTSC

CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Practical Cybersecurity for Open Science Projects

The need for cybersecurity in science projects (at any scale) and first steps

Craig Jackson, Chief Policy Analyst, CACR and Co-PI, NSF CCoE

Susan Sons, Senior Security Analyst, CACR and NSF CCoE

Bob Cowles, CACR, NSF CCoE, Brightlite Information Security

Additional Contributors:

Von Welch, Director, CACR and PI, NSF CCoE

Randy Heiland, Senior Systems Analyst - Programmer, CACR and NSF CCoE

CCoE Webinar

27 February 2017

trustedci.org/trainingmaterials

Center for Trustworthy Scientific Cyberinfrastructure

The NSF Cybersecurity Center of Excellence

CTSC's mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science, and the information and know-how required to achieve and maintain effective cybersecurity programs.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

PITTSBURGH SUPERCOMPUTING CENTER

THE UNIVERSITY of WISCONSIN MADISON

NSF

Outline

1. Intro: Audience, Goals, Caveats, Terminology
2. Cybersecurity & Science
3. Cybersecurity Programs
4. Programmatic Must-Do's

-1-
Introduction

The audience for today's session

CTSC's work spans the full range of NSF-funded projects and facilities.

Today, we're focused on smaller science projects...

- Unlikely to have dedicated security personnel or security budget
- Unlikely to need tons of policy and process
- But, are still working with valuable and/or sensitive data and IT infrastructure.
- Relationships (*e.g.*, with host institution) are particularly important

Our hypothetical audience member is a clueful PI thinking, 'Hmm, do I need to worry about this cyber stuff?'

Goals of this session: Provide our hypothetical concerned researcher with . . .

1. A sense of cybersecurity's relevance to science.
2. A sense of cybersecurity's complexity and scope.
3. A sense of how a cybersecurity program can help you cope with that complexity (and protect your science project).
4. A few "must-do" action items that are doable and truly important.

And:

5. Get your questions on the table.

Caveats & Terminology

The views and conclusions contained herein are those of the author(s) and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the National Science Foundation.

Note on Terminology: We may use terms that have very specific meaning at your institution; if so, we are using those terms generally and are *not* referring to any local definitions.

E.g., “Sensitive Information”

Some more notes about terminology

- We use "information security" and "cybersecurity" more or less interchangeably. We often prefer the former, but have gotten trapped in the cybervortex.

- If we use a term that you don't understand, please ask for clarification in the webinar chat area!

-2-
Cybersecurity & Science

Our information technology world is stormy

engadget

Thirty Meter Telescope's website was hacked to protest its construction

by Mariella Moon | @mariella_moon | April 28th 2015 At 4

SUBSCRIBE

SCIENTIFIC AMERICAN

THE SCIENCES MIND HEALTH TECH SUSTAINABILITY EDUCATION VIDEO PODCASTS BLOGS STORE

nature

COMPUTING

"Ransomware" Cyber Attack Exposes Vulnerability of Universities

Security expert warns that schools' "Frankensteined" networks open doors for hackers

Nasa hack: AnonSec attempts to crash $222m drone, releases secret flight videos and employee data

By Mary-Ann Russon

February 1, 2016 13:05 GMT

2,127

PENNSTATE

PENN S

Home Research Academics Impact

College of Engi

network disabl

to sophisticate

Plans in place to allow teach

The Washington Post

Federal Eye

Hacks of OPM databases

omised 22.1 million people,

l authorities say

Digital subscriptions

SUBSCRIBE

888

HOME U.S. NEWS MARKETS INVESTING TECH SMALL B

MERICA

nputer expert briefly

ane fly sideways

AM ET

IRPLANE HACKED?

Symantec Securi

Symantec Official Blog

Digital Extortion Rise

By: Roger Park

Created 20 Apr 2015

engadget

Old Intel chips are vulnerable to a fresh security exploit

by Jon Fingas | @jonfingas | August 8th 2015 At 10:11pm

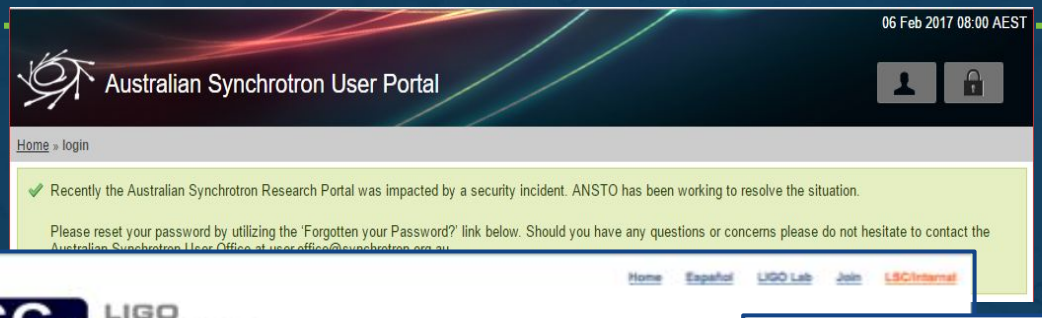
Ransomware Is Coming to Medical Devices

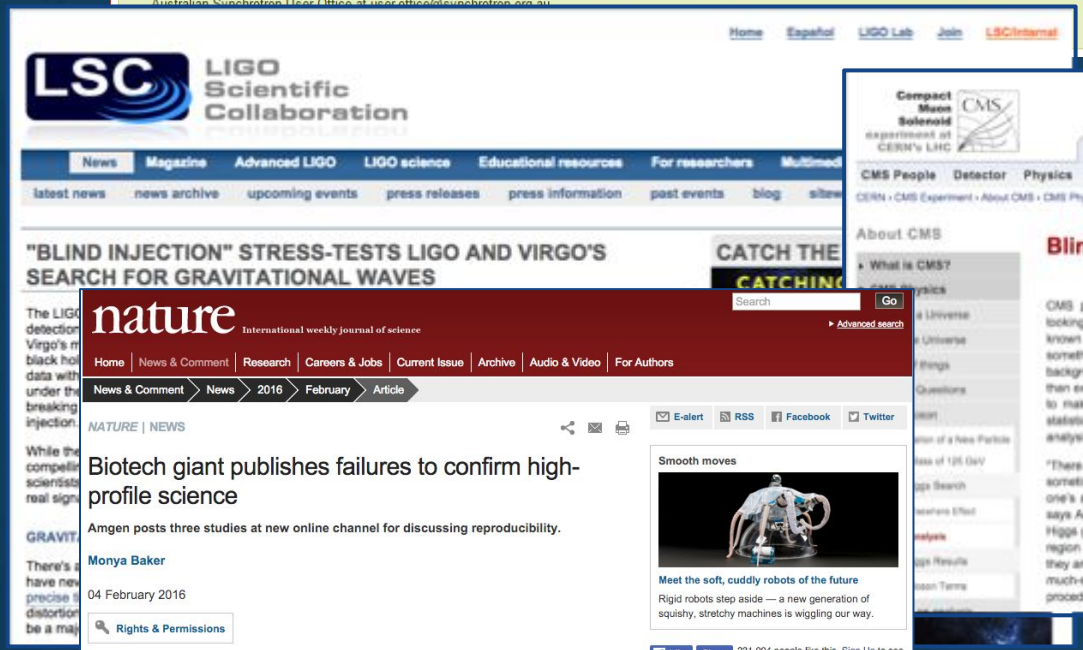
Written by J.M. PORUP

MOTHERBOARD

November 19, 2015 // 06:00 AM EST

Science must be trustworthy and reproducible



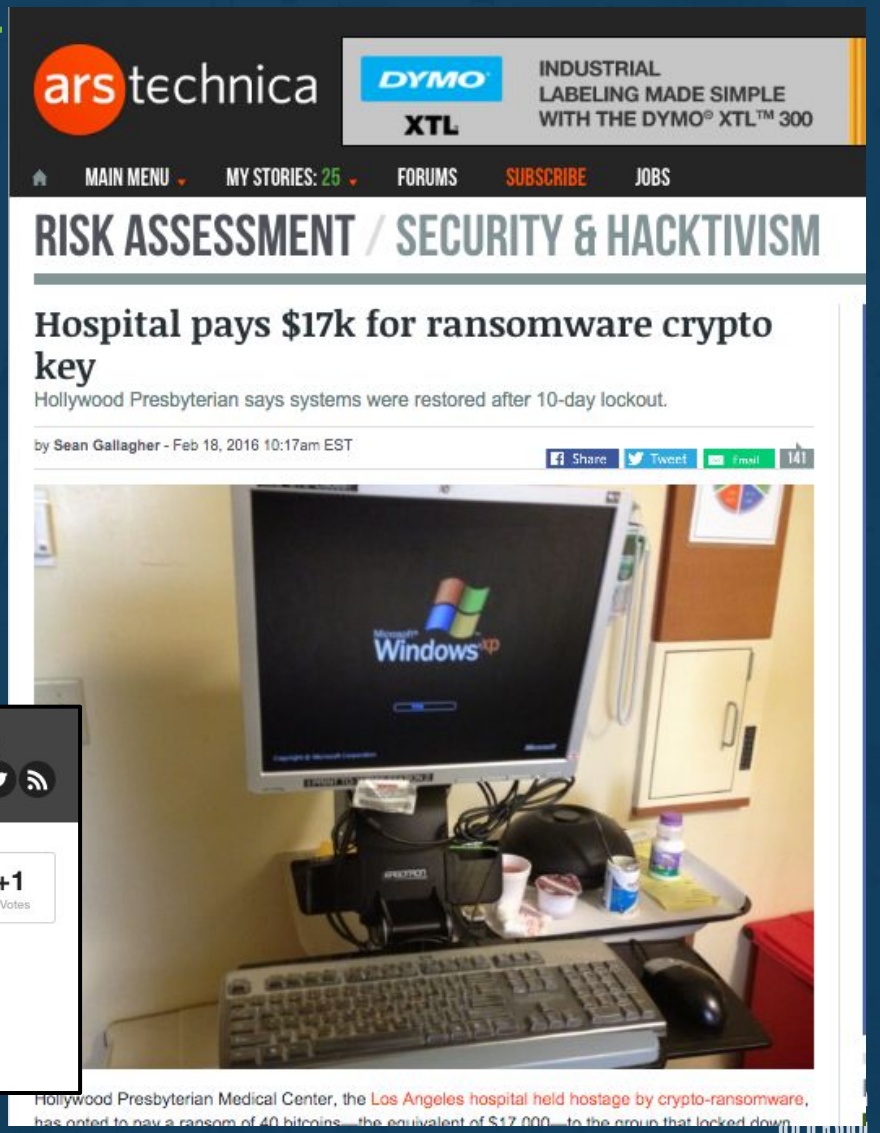


CTSC

“But I don’t handle sensitive data….”

- Security is more than than confidentiality; the integrity and availability of data and instruments is critical for science.
- Confidentiality before “going public” with big news.
- Valuable data and powerful IT.
- Everyone is a target… “internet noise”; ransomware; and open science is… open!
- Threats? More than criminals and rivals… environmental risks; lax management.

“My data isn’t valuable to anyone…”
“…except you!”



“Isn’t this just an IT problem?”

Sadly, you cannot plug in and switch on a “solution” for information security.

Information security is how you approach your information and technology in order to protect it. It’s just as broken if someone can dumpster dive for confidential information on paper, or if a misconfiguration nukes your entire research database and you have no way to recover the information, as it is if you are compromised by a network-based attack.

Information security has a positive impact on science even for smaller projects -- *it’s the science of protecting science!*

-3-
Cybersecurity Programs

So, what is a cybersecurity "program?"

It's not a plan; it's not a single project.

A cybersecurity program is a structured approach to develop, implement, and maintain an environment conducive to appropriate levels of information security and risk to the organization's mission [i.e., your science mission].

Cybersecurity programs are made up of ongoing activities and projects in the areas of: policies and procedures; controls and mitigations; control verification and assessment; threat monitoring and activity analysis; incident response and remediation; and training and awareness.

Cybersecurity programs should be scoped to the key assets, resources, and lifespan of organizations.

Bottom line:

Security programs are living, breathing things.

What does a PI or Project Manager want out of the cybersecurity program?

The program enables science impact, trust, and productivity by...

1. Ensuring the availability of key information systems and processes critical to the science mission
2. Guaranteeing the integrity of the data from accidental or malicious modification
3. Protecting the confidentiality of private or sensitive information from accidental or malicious disclosure
4. Obtaining these results while minimizing inconveniences and cost of the program

Advantages of Planning and Designing in Cybersecurity From Project Day 0

- Most effective, least expensive
- Make security a consideration of equipment, software, and service purchases.
- Get data storage/transport right so that you don't have to worry about trying to find/inventory later and wonder what was missed, mishandled, or stored outside project control.
- Avoid disturbing scientists' workflows in the course of retrofitting security measures after tech is in place.

For more information, templates, and tools …

trustedci.org/guide

and see also:

trustedci.org/ctsc-email-lists

trustedci.org/webinars

trustedci.org/useful-links

trustedci.org/trainingmaterials

-4-
Programmatic Must-Do's

Must-Do's

1. Determine what you have (parallel / iterative)
   - Inventory Assets
   - Identify Stakeholders
   - Categorize Data
   - Determine Project Information Flows
2. Determine what the institution provides
3. Determine who is responsible for controls
4. Fill Gaps
5. Ensure operational activities are covered

1a Inventory Assets

You can't secure what you can't identify and find.

Identify and inventory assets (information and information systems)

- Asset type
- Location
- Identifying Characteristics
- Protection Category
- Contact Information

1b Identify Stakeholders

- Project leadership. Involvement is essential.
- Institutions. Have requirements or provide resources
- Data subjects / research participants. Obligations?
- Funding agency. Involvement? Resources?
- Information system owners. Accept residual risk

1c Categorize (aka Classify) Data

Develop or tailor data categorization scheme

- No more than 3-4 categories
- Base on criticality to project & compliance req’ts
  - Availability & integrity are important issues
  - Specify rules for data location and protection level by category

1d Determine Project Information Flows

Carefully examine scientific processes

- Map information flows for your project
  - Where the data comes from and where it goes
  - Where the data is stored
- Determine owners of those processes
  - Knowledgeable, can determine acceptable risks
  - Default owner is project management

2 Determine What the Institution Provides

Don't reinvent what has already been done

- Many policies at the institution level will apply - *use them*
- Use existing procedures that are already familiar

3 Determine Who is Responsible for Controls

Don't duplicate operations unnecessarily

- Discuss operational support with institution cybersecurity group
- Many operational controls at the institution level will apply - *leverage them*

4 Fill Gaps

A little bit of spackle might be all that is required

- Make use of community resources
- Investigate other service providers (*e.g.,* cloud)
- Define your modest cybersecurity program
  - Policies
  - Basic controls

5 Ensure Operational Activities are Covered

- Authentication and access controls
- Configuration and vulnerability management
- Monitoring (logs and network activity)
- Incident response and remediation
- Data recovery and retention
- User training and awareness

Questions

Please take our survey

Bonus Material!

Authentication and Authorization

Also Identity and Access Management (IAM)

- Usernames and passwords
- Certificates

Controls access to software and data - who is able to create, read, write, update, or delete

Also -- processes for on-boarding and off-boarding

Configuration and Vulnerability Management

Default configurations are normally very insecure

- Use accepted frameworks to secure initial configurations -- see Security Technical Implementation Guides (ref: STIG in Wikipedia)
- Ensure configuration changes are approved and documented

Vulnerabilities in configuration or software arise on a continuing basis

- Do more than just scan - Patch!
- Prioritize remediation - everything is not the same

Monitoring

Compromises and intrusion WILL happen

Actively monitoring network traffic and logs can provide early detection

Pay close attention to outbound traffic for unexpected destinations

Incident Response and Remediation

Develop plan in advance; maintain an offline copy

Practice with table-top exercise

Have a good communication plan (who to notify, when, and by whom

Don’t be afraid to ask for help -- including institution, peers and law enforcement

Analyze for root cause of failure and repair

Data Recovery and Retention

Backups are necessary to limit impact of data loss (or ransomware)

Periodic testing data recovery process is essential for it to work when needed

Data retention policies and procedures can limit exposure in legal discovery cases

User Training and Awareness

Review key policies and expectations

Understand procedures and how to implement

Inform of the most recent methods of attack

Periodic training is necessary to remind and update

CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Thank You

trustedci.org

@TrustedCI

We thank the National Science Foundation (grant 1547272) for supporting our work.

About the CTSC Webinar Series

To view presentations, join the discuss mailing list, or submit requests to present, visit:

http://trustedci.org/webinars

The next webinar is March 27th at 11am Eastern

Topic: SDN and IAM Integration at Duke University

Speakers: Charley Kneifel

The CTSC Webinar Series is supported by National Science Foundation grant #1547272.

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

CTSC