



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.



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.



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**

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



Ransomware Is Coming to Medical Devices

November 19, 2015 // 06:00 AM EST

Written by J.M. FORUP



PENNS STATE

College of Eng network disabled to sophisticated

Plans in place to allow teaching continue as University moves

HOME U.S. NEWS MARKETS INVESTING TECH SMALL B

Computer expert briefly says plane fly sideways

AM ET



IRPLANE HACKED?

Symantec Security

Symantec Official Blog

Digital Extortion Rise

By: Roger Park

Created 20 Apr 2015

engadget

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

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



The Washington Post

Hacks of OPM databases compromised 22.1 million people, authorities say

Digital subscriptions

SUBSCRIBE

888

engadget

Old Intel chips are vulnerable to a fresh security exploit

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



Science must be trustworthy and reproducible

06 Feb 2017 08:00 AEST



Australian Synchrotron User Portal

Home » login

Recently the Australian Synchrotron Research Portal was impacted by a security incident. ANSTO has been working to resolve the situation.

Please reset your password by utilizing the 'Forgotten your Password?' link below. Should you have any questions or concerns please do not hesitate to contact the Australian Synchrotron User Office at user.office@synchrotron.org.au.

Understanding Science

how science really works

EXPLORE AN INTERACTIVE REPRESENTATION OF THE PROCESS OF SCIENCE.

The science checklist applied: Cold fusion

Fusion occurs when two light atoms, like hydrogen, join together, or fuse, into a single heavier atom, releasing a lot of energy in the process. In 1989, chemists Stanley Pons and Martin Fleischmann excited the world with claims that they had produced fusion at room temperature — "cold" fusion compared to the high temperatures the process was thought to require. Their discovery seemed to offer a potential solution to the energy crisis: cheap energy, without pollutants or radioactive waste.

Science cannot be absolutely defined; however, scientific endeavors have a set of key characteristics, summarized in the Science Checklist.

LSC Scientific Collaboration

Home Español LIGO Lab Join LSCInternet

News Magazine Advanced LIGO LIGO science Educational resources For researchers Multimedia

latest news news archive upcoming events press releases press information past events blog sites

"BLIND INJECTION" STRESS-TESTS LIGO AND VIRGO'S SEARCH FOR GRAVITATIONAL WAVES

Biotech giant publishes failures to confirm high-profile science

Amgen posts three studies at new online channel for discussing reproducibility.

Monya Baker

04 February 2016

231,004 people like this. Sign Up to see what your friends like.

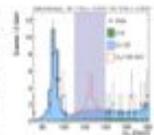
Recent

- 1. **Tasmanian bushfires threaten iconic ancient forests**
Nature | 04 February 2016
- 2. **Forests not equal when it comes to climate**
Nature | 04 February 2016
- 3. **Humour on the brain: Robert Newman reviewed**
Nature | 04 February 2016

Blinding and unblinding analyses

CMS performs searches for new particles by looking for signals amidst a background of known physics. If the data begin to indicate something more interesting than merely background — for instance, more decay events than expected in a certain region — it is important to make sure that the observation is statistically significant by collecting and analyzing more data.

"There is however a human tendency, sometimes at a subconscious level, to optimize one's analysis based on what is already seen," says Albert De Roeck, co-convenor for the CMS Higgs group. To avoid such bias while analyzing new data, physicists draw "blinds" over the region where an excess of decay events is expected; this region is only "unblinded" when they are satisfied with their procedures. This ensures objectivity when it comes to looking for much-sought-after signs of new physics, and gives confidence in the ultimate result. The procedure is similar to that used by medical researchers when testing a new treatment.



ADAM MANN SCIENCE 02.22.12 6:01 PM

FASTER-THAN-LIGHT NEUTRINO RESULTS MAY BE DUE TO BAD CABLES

“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!”

REUTERS EDITION: U.S. SIGN IN | REGISTER Search Reuters

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS MONEY LIFE PICTURES VIDEO

Scan, track, and monitor hundreds of IPv4 & IPv6 addresses... for free. solarwinds.com/netfree

Mon Mar 7, 2016 9:18am EST Related: TECH, CYBERSECURITY

Apple users targeted in first known Mac ransomware campaign

BOSTON | BY JIM FINKLE

EDITOR'S CHOICE

Apple users targeted

What it feels like to be 32% more productive.

An Apple iPhone is pictured next to the logo of Apple in Bordeaux, southwestern France, February 18, 2016. REUTERS/REGIS DUVERNAY

Apple Inc (AAPL.O) customers were targeted by hackers over the week

ars technica DYMO XTL INDUSTRIAL LABELING MADE SIMPLE WITH THE DYMO® XTL™ 300

MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS

RISK ASSESSMENT / SECURITY & HACKTIVISM

Hospital pays \$17k for ransomware crypto key

Hollywood Presbyterian says systems were restored after 10-day lockout.

by Sean Gallagher - Feb 18, 2016 10:17am EST

Share Tweet Email 141

Hollywood Presbyterian Medical Center, the Los Angeles hospital held hostage by crypto-ransomware, has opted to pay a ransom of 40 bitcoins — the equivalent of \$17,000 — to the group that locked down

Symantec Security Insights Blog

Symantec Official Blog

Digital Extortion on the Rise

By: Roger Park SYMANTEC EMPLOYEE

Created 20 Apr 2015

+1 1 Votes

“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



CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE
The NSF Cybersecurity Center of Excellence

Thank You

trustedci.org

 [@TrustedCI](https://twitter.com/TrustedCI)

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

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, and Indiana University .

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.