



CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

Trustworthy Computational Science: Lessons Learned and Next Steps

Von Welch

*2015 NSF Cybersecurity Summit for Large Facilities and
Cyberinfrastructure
August 18th, 2015*

trustedci.org

Anthem

Home FAQ A Le

How to Access & Sign Up For Identity Theft & Credit Monitoring Services

engadget

Old Intel chips are vulnerable to a fresh security exploit

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



The Washington Post

Federal Eye

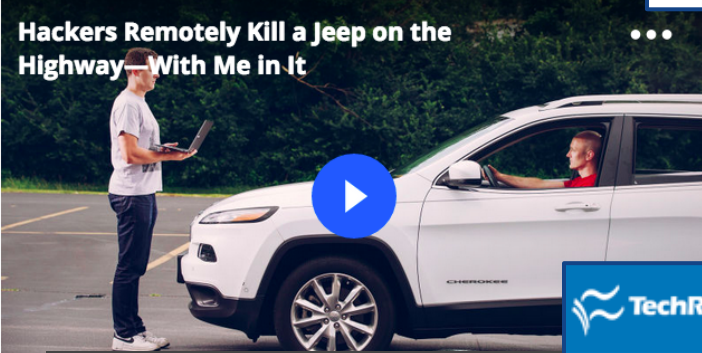
Hacks of OPM databases compromised 22.1 million people, federal authorities say

By Ellen Nakashima July 9



HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

wired.com



HACKING AMERICA

FBI: Computer expert briefly made plane fly sideways

Elizabeth Weise
Sunday, 17 May 2015 | 11:45 AM ET

USA TODAY

TechRepublic

MOBILITY


Major flaw in Android texting discovered

A recent SMS vulnerability affects millions of Android phones. This article explains the flaw and offers up a temporary (although not permanent) fix.

By Jack Wallen | August 10, 2015, 8:12 AM PST

Hollywood THE BUSINESS

Sony Hack: WikiLeaks Publishes More Than 30,000 Documents



Getty Images

Symantec Security Insights Blog

Symantec Official Blog

Digital Extortion on the Rise

By: Roger Park | SYMANTEC EMPLOYEE

Created 20 Apr 2015

Hitting close to home...

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

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

PENN STATE



Stay Connected

For the Media

Contact Us

Search Penn State

News for:

> STUDENTS

> BUSINESS & INDUSTRY

> VISITORS & NEIGHBORS

> ALUMNI

> FACULTY & STAFF

News from:

> CAMPUSES

> COLLEGES

Saturday, August 15, 2015

PENN STATE NEWS

Home Research Academics Impact Campus Life Athletics Administration

College of Engineering network disabled in response to sophisticated cyberattack

Plans in place to allow teaching, research in the college to continue as University moves to recover

May 15, 2015

Cyberattack hits UVA

[Click here to sign up for breaking news alerts »](#)

■ Portions of UVA systems targeted in Chinese hack

Story Comments

Print Font Size: + -

Recommend 95 Tweet 47 +1 1 Pin it 0 Share 11

Hackers targeted 2 employees' emails

No personal, financial or medical information

UVA email will be inaccessible

Upgrade expected to be complete Sunday evening

dailyprogress.com

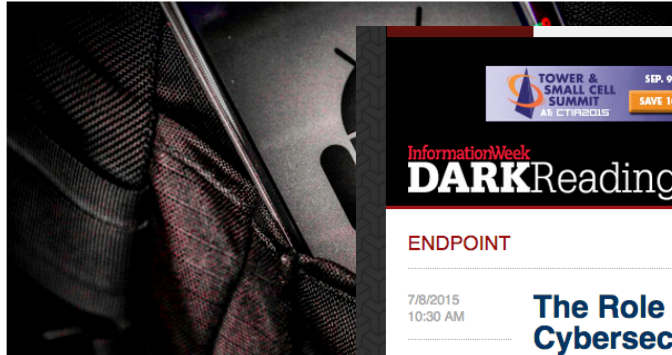
Posted: Friday, August 14, 2015 4:59 pm

Any Good News?

Yes!

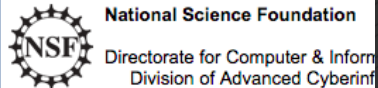
BIG ANDROID MAKERS WILL NOW PUSH MONTHLY SECURITY UPDATES

wired.com



Cybersecurity Innovation

PROGRAM SOLICITATION NSF 15-549



Full Proposal Deadline(s) (due by 5 p.m. pro

June 02, 2015

TOWER & SMALL CELL SUMMIT SEP. 9-11, 2015 | LAS VEGAS
SAVE 10% WITH CODE **RMK2015**

InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

ENDPOINT

7/8/2015
10:30 AM



Jason Straight
Commentary



1 COMMENT
[COMMENT NOW](#)



The Role of the Board In Cybersecurity: 'Learn, Ensure, Inspect'

Board members of the most forward-thinking U.S. companies are not just throwing money at the mounting problem of managing cyber risk.

It wasn't long ago that cybersecurity was considered the exclusive domain of IT departments, a matter of purchasing and deploying the right technology to defend against intrusions into the network. In case you haven't heard, those days are over. In the wake of devastating and embarrassing incidents at Target, JPMorgan Chase, Home Depot and dozens of other established and widely respected brands, executive management and boards of directors are now acutely aware that the responsibility for safety, security and integrity of their networks and data sits

hackingtheuniverse.com

NIST Adds New SP-1800 series

NIST (National Institute of Standards and Technology) has announced a new Special Publications (SP) series of documents called SP-1800, intended to augment the SP-800 series.

SPECIAL PUBLICATIONS - [nist.gov]

SP 1800, NIST Cybersecurity Practice Guides (2015-present): A new subseries created to complement the SP 800s; targets specific cybersecurity challenges in the public and private sectors; practical, user-friendly guides to facilitate adoption of standards-based approaches to cybersecurity;

The first draft document in the 1800 series has been released for comment:

[Securing Electronic Health Records on Mobile Devices](#) - [nist.gov]



Two Factor Auth (2FA)

List of websites and whether or not they support 2FA. Add your own favorite site by submitting a pull request on the [GitHub repo](#).

App and Sync	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
Dropbox	↗					✓
Apple iCloud	↗	✓				✓
Dropbox	↗	✓				

Google Online Security Blog

The latest news and insights from Google on security and safety on the Internet

Announcing Project Zero

Posted: Tuesday, July 15, 2014

[g+](#) 946



Posted by Chris Evans, Researcher Herder

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

continuousassurance.org

Government and Courts increasing their role.

U.S. Food and Drug Administration

Search FDA

back to [Safety Alerts for Human Medical Products](#)

Symbiq Infusion System by Hospira: FDA Safety Communication - Cybersecurity Vulnerabilities

THE WALL STREET JOURNAL. | THE CIO REPORT

CIO Journal

Exclusive reporting and analysis for corporate-technology executives

CIO REPORT | CONSUMERIZATION | BIG DATA | CLOUD

5:18 pm ET
Jul 23, 2015 | PRIVACY

Appeals Court Revives Neiman Marcus Data Breach Suit

ARTICLE | COMMENTS (1)

DONNA SEYMOUR | NEIMAN MARCUS | OFFICE OF PERSONNEL MANAGEMENT

Email | Print | Facebook | Twitter | Google+ | LinkedIn

By KIM S. NASH

Neiman Marcus Group LLC is back in court over a 2013 cyberattack, as a U.S. appeals court reinstated on Monday a case that had been dismissed last year. The reversal highlights the complicated legal issues companies confront when customer data is breached, including questions concerning the degree to which customers can hold companies, and their executives, liable.

ing
Homeland Security's Industrial
Response Team (ICS-CERT), and Hospira
associated with the Symbiq Infusion
are facilities transition to alternativ
these pumps.

WIRED | Lifelock Once Again Failed at Its One Job: Protecting Data | SUBSCRIBE

BUSINESS | DESIGN | ENTERTAINMENT | GEAR | SCIENCE | SECURITY

KIM ZETTER | SECURITY | 07.21.15 | 6:41 PM

LIFELOCK ONCE AGAIN FAILED AT ITS ONE JOB: PROTECTING DATA

GETTY IMAGES

SHARE

3375 | 1377

CUSTOMERS WHO HIRED the infamous ID theft-protection firm Lifelock to monitor their identities after their data was stolen in a breach were in for a surprise. It turns out Lifelock failed to properly secure their data.

According to a [complaint filed in court today](#) by the Federal Trade Commission, Lifelock has failed to adhere to a 2010 order and settlement that required the company to establish and maintain a comprehensive security program to protect sensitive personal data users entrust to the company as part of its identity-theft protection service.

How does computational science navigate all of this?



The Challenge for Science Cybersecurity

Shifting landscape of threats.

Constantly changing, often insecure, technology.

Very open, collaborative environment.

Need to demonstrate value to science productivity.

No one-size fits all silver bullet.

Cybersecurity Program Goal

Minimize:

Cost of breaches/incidents +

Cost of cybersecurity program +

Negative impact on science productivity

Paraphrased from: “The Defender's Dilemma. Charting a Course Toward Cybersecurity” http://www.rand.org/pubs/research_reports/RR1024.html

Treat Cyberthreats as other Disaster Risks

Not “if” but “when.”

If not you, then something you count on.

Prevention, detection, response, and recovery all important.

Risk Assessment

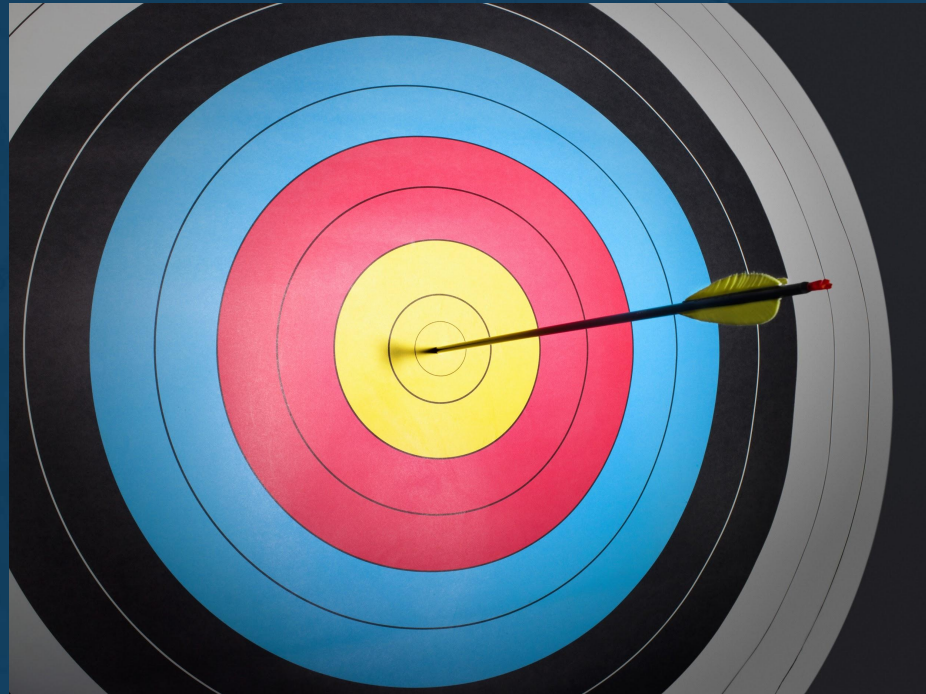
Channeling Willie Sutton: Why do people hack computers?

Because that's where the data is.



Understand where to focus

Know key liabilities and assets critical to science mission and can put focus there.



Caution:

“Our data is public” doesn’t save the day

Reputation, trust, and other “intangibles” matter.

Integrity and availability of data

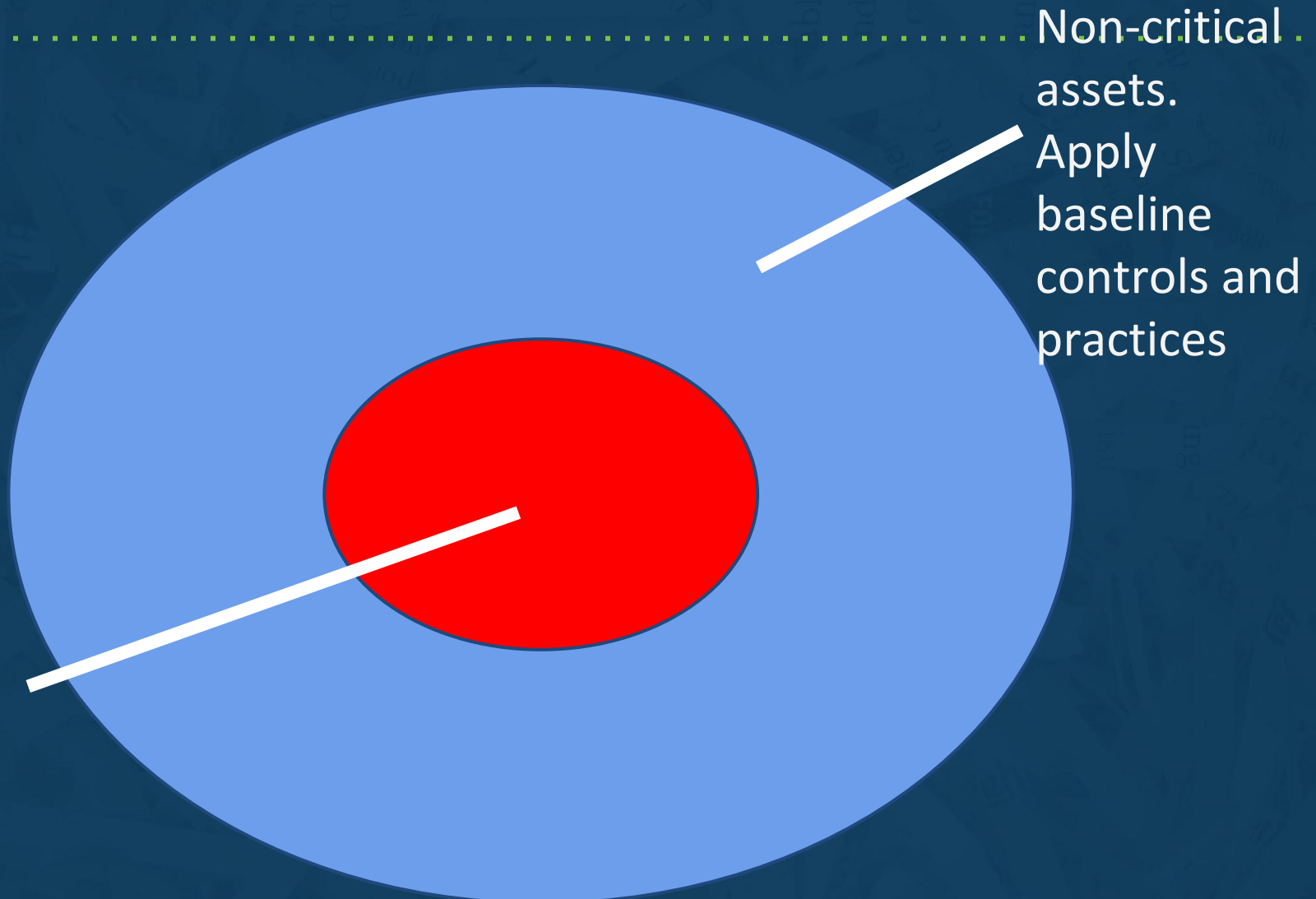
Illicit use of systems

Availability of instruments

Hacktivism

Etc.

The Big Picture Cybersecurity Program



CI Threat Profile

CICI Cybersecurity Center of Excellence will develop a Threat Profile. My advice...

Think of how worse cases scenarios may arise where public loses trust in our science products.

Focus on understanding different data categories for different science communities and their confidentiality, integrity, availability risks.

Determine key points of CI that need hardening.

Can we leverage Science's controls?

The LIGO Scientific Collaboration and the Virgo Collaboration completed detection capabilities at their recent joint collaboration meeting in Arcadi. Virgo's most recent observation run revealed evidence of the elusive sig black hole. The collaboration knew that the "detection" could be a "blind data without telling the analysts, to test the detector and analysis. None under the assumption that the signal was real, and wrote and approved a breaking discovery. A few moments later, according to plan, it was revealed injection.

While the scientists were disappointed that the discovery was not real, th compelling demonstration of the collaboration's readiness to detect grav scientists are looking forward to observations with the advanced detecto real signals from the distant reaches of the universe.

GRAVITATIONAL WAVES:

There's a lot at stake here. Gravitational waves, a firm prediction of Einst have never been directly detected, although there is convincing indirect precise timing of the orbits of binary pulsars in the Galaxy. The direct de distortions of space-time that they produce when they arrive at Earth fro be a major scientific milestone, and would open up the new field of grav

Checks for bias, error....
(Aka Insider Threat)

Cybersecurity Resources for the NSF Community

The NSF Bro Center of Excellence

- Bro support for NSF projects & Higher-Ed
 - Oct 2013 launch at Summit
- Development work for these communities
 - E.g. SDN & Science DMZ is important to them (PACF)
- Research
 - Can't save 3 months of pcaps, run analysis live
- Outreach
 - BroCon & NSF Cybersecurity Summit
 - Partnering with CTSC & ESNet on projects
 - 1-on-1 engagements
- <https://www.bro.org/nsf/>

Assistance Provided

- Troubleshooting & Optimizing
 - Cluster setups & tap/agg aren't easy
 - CPU affinity and Hyper-threading?
- Planning & reviewing designs for NSM
 - Where should I tap? What are pros/cons?
 - How much hardware should I start with?
 - Should I design for peak or average?

Engaged communities:

- LIGO
- National Center for Atmospheric Research
- Ice Cube
- Many universities...

Center for Trustworthy Cyberinfrastructure

trustedci.org

Cybersecurity program guide and program review

Secure software design/review

Peer review facilitation

Training, best practices, guidance

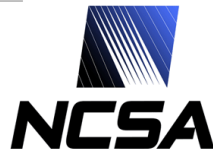
Engaged communities:

CyberGIS, DataONE, Pegasus, Globus, OOI, Gemini, HUBzero, DKIST, Ice Cube, LIGO, SciGaP, CC-NIE (Utah, PSU, Pittsburgh, Cincinnati, Oklahoma), NTF, PerfSonar...



CENTER FOR APPLIED
CYBERSECURITY RESEARCH

INDIANA UNIVERSITY
Pervasive Technology Institute



THE UNIVERSITY
of
WISCONSIN
MADISON



The Community

Ask for and share program documents, advice, lessons learned, etc.

Reciprocal peer reviews of cybersecurity programs.

Use this Summit CFP to share your experiences.



CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

Thank You

Von Welch (vwelch@iu.edu)



[trustedci.org](https://www.trustedci.org)

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

Image credit: Thinkstock