Education & Outreach Moment

NSF PHASE I CENTER FOR ADAPTING FLAWS INTO FEATURES

NSFCAFF.ORG

Stony Brook University

Laboratory Data Security

Regulation & risks

- Research data of regulated science is guided by compliance (e.g., HIPPA, FISMA, NIST 800-1471).
- Open science is not guided by compliance.
- Data security is important for **productive**, **trustworthy**, and **reproducible** science.
- Ransomware encrypts the data to extort the user for access.
- Running science on a hacked computer?

Cyber attack threatened WA astrophysicists' shot at gravitational waves, colliding neutron stars

By Nicolas Perpitch

Posted Mon 16 Oct 2017 at 5:29pm, updated Tue 17 Oct 2017 at 3:44am

Professor Coward with the Zadko telescope. (Supplied: UWA)

Help keep family & friends informed by sharing this article

abc.net.au/news/cyber-att...

COPY LINK

SHARE

Astrophysicists at WA's Zadko telescope had just learned about the detection of a monumental deep space event involving two neutron stars colliding — which they had been hoping to find for years — when they came under sustained cyber attack.

At the critical and fleeting moment, they could not move their telescope to track the gigantic explosion 130 million light years away.

The first signs of the neutron star merger had been detected at 8:41am (WST) on August 31 by the LIGO observatory in the United States.

NEWS | IN DEPTH

CYBERSECURITY

U.S. blames 'massive' hack of research data on Iran

Targets included nearly 8000 professors in 22 countries

By Jon Cohen

"College professors are like shooting fish in a barrel."
Max Kilger, University of Texas

Stony Brook University

https://www.abc.net.au/news/2017-10-17/cyber-attack-almost-costs-team-look-at-colliding-neutron-stars/9055816

Cohen, J., Science2018, 359(6383), 1450-1450.

Laboratory Data Security

Best Practices

1. Secure Storage
   - Do not expose research infrastructure to the internet.
   - Encrypt sensitive data transmitted over a network.
   - Develop a central data backup service.
   - Destroy data that is no longer needed.
2. Encryption
   - Use the highest level of data encryption for rest and transit data.
3. Commercial Cloud Services
   - Use cloud services with two-factor authentication.

Stony Brook University

https://sharing.nih.gov/sites/default/files/flmngr/NIH_Best_Practices_for_Controlled-Access_Data_Subject_to_the_NIH_GDS_Policy.pdf
irtsectraining.nih.gov/publicUser.aspx

Laboratory Data Security

Best Practices

4. Hardware Security
   - Use an up-to-date OS with modern antivirus software.
   - A system with an old OS should be free of IP addresses.
   - Only authorized employees should use peripheral devices.
5. Application Security
   - Use two-factor authentication, passwords, and role-based access control.
6. Network Security
   - Use standard security measures like SSL.
   - Use laboratory information management systems (LIMS).
7. Personnel Security
   - Background checks, training, and compliance.

https://sharing.nih.gov/sites/default/files/flmngr/NIH_Best_Practices_for_Controlled-Access_Data_Subject_to_the_NIH_GDS_Policy.pdf
irtsectraining.nih.gov/publicUser.aspx