Information security, compliance and the grant life cycle

October 10, 2013

Cyberinfrastructure Day
2013

Presenters

- Beth Chancellor, Chief Information Security Officer, Division of IT
- Jeremy Cox, Lead Accountant, Office of Sponsored Programs Administration
- Jennifer Duncan, Director, Office of Sponsored Programs Administration
- Jennifer May, Director of Research Compliance Services, Office of Research
- Michelle Wisdom, IT Compliance Officer & Health ISO, Division of IT

The Grant Lifecycle

- Pre-submission
  - External and Internal Influences
- Planning & Submission
- Post Award / Operational Compliance
- Close Out
- _____
- Importance of consolidated resources

External Influences - Standards, Laws and Regulations

- Federal Information Security Management Act (FISMA)
  - Nat'l Institute of Standards & Technology (NIST)
- FDA 21 CFR Part 11 (electronic records & electronic signatures)
- Office of Management & Budget (OMB) Circular A-130 (information resource management)
- Export Control
  - International Traffic in Arms Regulations
- Federal Acquisition Regulation (FAR) & Defense Federal Acquisition Regulation Supplement (DFARS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Research Classification
- Family Educational Rights and Privacy Act (FERPA)

Highlight on DFARS

- Defense Federal Acquisition Regulation Supplement
- Example Clauses that impact data use and security
  - DFAR 252.204-7000 (Dec 1991)
  - DFAR 252.204-7000 (Aug 2013)
- Proposed Rule that could impact data use and security
  - Safeguarding Unclassified DoD Information (DFARS Case 2011-D039)

Internal Influences – Policies, Programs and PI Self-categorization

- Management, Access and Use policy (BPM1201)
- Info Sec policy (BPM1203)
- Information Security Program
  - Data classification
  - Requirement to report
- IT Procurement policy (BPM1204)

- What's the value of research data and information?
  - Data integrity
  - IP
  - Tech transfer
  - Your life's work
- How should it be protected regardless of formal classification?

UNC Mammography Registry Breach

newsobserver.com

Subscriptions

Search New

Home News Sports Business Politics Living Opinion Communities Local Deals

UNC, researcher settle dispute over hacker attack

Submitted by eferreri on 04/15/2011 - 20:33

Tags: Campus Notes | Bonnie Yankaskas | Carolina Mammography Registry | hacker | higher education | UNC | UNC-CH

SHARE

A prominent UNC-Chapel Hill researcher has settled a dispute with the university, re-gaining her credentials and full salary while agreeing to retire at the end of the year.

Bonnie Yankaskas, a noted epidemiologist, had been demoted, her pay cut essentially in half, after a hacker infiltrated a computer server that she, as the principal investigator for a massive breast cancer study, oversaw.

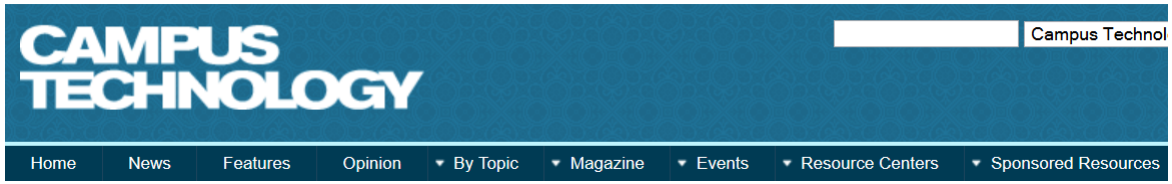
Yankaskas has overseen the Carolina Mammography Registry, a federally funded project that compiles and analyzes mammogram data submitted by dozens of radiology offices across North Carolina to improve breast cancer screening.

The university held her responsible for the breach and first tried to fire her before later recommending the demotion from full to associate professor and the pay cut.

Under the terms of a settlement announced Friday, Yankaskas has regained her status as a full professor and her full salary of $175,000 has been restored.

She agreed to retire Dec. 31 of this year, according to a news release issued late Friday.

Higher Ed Data Breaches Continue to Rise



Security | News

Higher Ed Data Breaches at Near-Record High in 2012

By Dian Schaffhauser ▪ 03/21/13

Nobody knows who will win the NCAA Men's Division Basketball Championship; the final game won't happen until April 6. But just as surely as bracket mania strikes the country this month in response to college basketball, so too does Application Security release the final rankings of this year's dubious roster of higher education "data breach madness" winners. These are colleges and universities that have experienced a notable data breach in 2012.

This year's declared winner is the University of Nebraska, which reported a breach of 654,000 records on May 25, 2012. Rounding out the data breach "Final Four" were the University of North Carolina (350,000), Arizona State University (300,000), and Northwest Florida State College (279,000). Three of those breaches also made the top 10 higher ed data breaches of all time.

Planning & Submission

- Think ahead to the end
  - If there happens to be an audit, can you show adequate documentation for:
    - Pre-award activities
    - Financial activities
    - Security measures
    - Communication/delegation to sub-recipients
    - Data Use and Reporting

Planning & Submission

- What regulations, laws, policies, procedures apply to your work?
- How do you ensure that you can meet the requirements pre-submission?
- What IT resources are planned for ahead of time?
  - Storage, Collaboration tools, sharing/file transfers, access control technologies, outsourced services such as cloud-based tools

Planning & Submission

- Do you ever have to "certify" that information/data is secure?
  - Already seeing an increase and likely to see more
  - Signature required by a security official
- Do you ever have to submit security plans to the sponsor?
  - Technology controls
  - General workplace security (http://infosec.missouri.edu/pdf/wism-form.pdf)

Adobe cloud service breached

USA TODAY

Adobe loses 2.9 mil customer records, source code

CYBERTRUTH Byron Acohido, USA TODAY 1:56 a.m. EDT October 4, 2013

(Photo: Adobe)

TAGS

Seattle

SEATTLE – Adobe has become the latest big-name data breach victim.

The company that mainstreamed desktop publishing admitted in a statement that hackers gained unauthorized access to 2.9 million customer accounts and stole part of the source code that underlies its products.

"The Adobe breach shows that everyone is fair game," says Eduard Goodman, chief privacy officer at risk management firm IDentity Theft 911. "The hackers went in and stole private consumer information in the form of card information, even if it was encrypted, and they stole intellectual property. Those are two valuable assets. "

This news was flushed out by Brian Krebs, author of the cybersecurity blog, krebsonsecurity.com.

Evernote cloud service breached

50 million compromised in Evernote hack

By **Doug Gross**, CNN
updated 4:34 PM EST, Mon March 4, 2013 | Filed under: Web

(CNN) -- Tens of millions of online note-takers found themselves worrying about their security Monday, as questions remained about a weekend hack of Evernote.

The online note-taking and archiving service began requiring its 50 million users to reset their passwords Saturday after announcing it was the victim of a security breach, making it the latest tech company in recent weeks to fall victim to hackers.

Evernote said the encryption coding they use to protect passwords is "robust," but still sent the password warning to users of the service, which is popular among college students and others who rely on taking notes for later use.

Sophos Security analyst Graham Cluley said in a blog post that it remains unclear how long the hackers had access to Evernote and how they managed to get in.

"What's not good news," he wrote, "is that the hackers now have access to the usernames and email addresses of Evernote customers. It is easy to imagine how this information could be abused -- for instance, the hackers could send out spam emails to those users claiming to come from Evernote, and trick them into visiting a malicious website.

Post Award and Operational Compliance

- Who manages the infrastructure and/or the services?
  - Data steward / data custodian, these are separate roles
    - Do they know their responsibilities?
    - Are they qualified?
    - What terms & conditions are in place with outsourced providers?
- What has been agreed to from an information security perspective?
  - Potential effects of non-compliance

Grant Close Out

- Reporting/Publishing
- Archival
  - If it's worth archiving, it's worth securing
- Return of data
- Disposal

What does all of this mean?

- Myriad of compliance hurdles to address, plus…
- A host of security implications
  - Data stewards / Data custodians
  - Data storage / Data encryption
  - Secure file sharing / transmission
  - Access Control technologies
  - Archival and Disposal

How can we help?

- Plan ahead and engage early
- Ask for expert help and advice
  - Look ahead for potential audit issues
  - Engage OSPA in audit requests
  - Leverage the Compliance Office
  - The DoIT security team can provide templates for security plans
  - ISOs should and can sign security certifications
  - Seek approval from an ISO to use outsourced technology services

How can you help?

- All of our eggs in one basket!
  - Scalability
  - Security standards
  - Highly trained security and technical staff
  - Management & administration
  - Encryption
  - Access control technologies and standard processes
  - Documentation

Support the efforts of the CIC!!!

Policies & Resources

- Information Security & Access Management Team
- Office of Sponsored Programs Administration
- Research Compliance Office
- Institutional Review Board (IRB)

- IT Management, Access and Use policy – BPM1201
- IT Security policy – BPM 1203
- IT Procurement policy – BPM1204
- Information Security Program
- Data Classification System

Contacts

Information Security Officers

- Beth Chancellor, Chief Information Security Officer
- Brandon Hough, Information Security Officer
- Michelle Wisdom, IT Compliance Officer/Health ISO