RISE
Enable • Protect
Research-centric Information Security Enablement Program

BSD Information Security Office Cybersecurity Newsletter

January 2017 | SECURITY.BSD.UCHICAGO.EDU | Volume 3, Issue 1

Inside this Issue:

Upcoming Enhancement Reminder: Encryption for XMail ***(Page 1)***

Automated Incident Response (AIR) Launch & Tabletop Exercise ***(Page 1)***

Million Dollar Download ***(Page 2)***

Upcoming Enhancement Reminder: Encryption for XMail

What: Privacy and security controls for mobile devices are being enabled on the University's email system for BSD faculty and staff.

Why: Consequences of unencrypted lost data include fines, identity theft, compromised research data, endangered federal grant status, and risk to the reputation and image of the organization. To avoid these issues and align with regulatory requirements, mobile devices connecting to the e-mail system will require encryption.

What to do: Encrypt your mobile device before February 28, 2017.

Directions for encrypting BSD mobile devices:
http://security.bsd.uchicago.edu/bsd-mobile-device-encryption/

Directions for BSD e-mail encryption:
http://security.bsd.uchicago.edu/bsd-e-mail-encryption/

Automated Incident Response (AIR)

In January 2017, stakeholders from many departments across the BSD met to run through a tabletop exercise demonstrating the new automation incident workflow by discussing and reacting to mock incidents.

AIR is planned to go-live on February 6, 2017.

What is Automated Incident Response (AIR)?

A working group consisting of University of Chicago stakeholders and industry experts was established to develop an Incident Response (IR) program to automate the process for tracking and reporting on cybersecurity incidents within the Biological Sciences Division (BSD). The automation capabilities of the program provide notifications to key stakeholders as incidents are tracked and remediated. This program is designed to augment, and where possible, replace the current workflow, which requires manual human intervention to validate that appropriate approvals are acquired before remediation activities occur.

The IR project was initiated to address cybersecurity gaps in the existing BSD cybersecurity program and aid in automation. The BSD ISO currently implements security controls from the NIST Cybersecurity Framework, commonly referred to across many industries as "the Framework". Modeling policies and procedures after the industry standards laid out within the Framework, the BSD ISO has been able to develop a greater understanding of the current state of cybersecurity programs across all BSD departments. The academic and research elements of the departments were reviewed to determine current approaches for addressing cybersecurity concerns as outlined in the Framework. Utilizing best practices, the BSD ISO developed a risk-informed target state profile to model the ideal security posture.

This target state profile identified the types of policies, procedures, and practices needed across the BSD to mitigate cybersecurity risk to an acceptable level. After performing a gap analysis between the current and target security state, it was identified that improving and automating IR would best improve the BSD's cybersecurity program.

Million Dollar Download

It only takes one click in a phishing attack to lose confidential Biological Sciences Division data which could result in large sums of money paid for regulatory fines and penalties. Please read the story below about how Bruce and his organization fell victim to a phishing attack.

It had all looked so legit. Bruce, a laboratory technician for an academic hospital, considered himself a pretty computer-savvy guy. He had heard all about hacking, phishing, and malware, and stayed vigilant about the personal and financial information he posted online. But the e-mail he received late one Friday afternoon didn't set off any of those alarm bells. It came from a .gov address, the official logo of a federal agency was at the top of the message, and there were none of the obvious misspellings or punctuation errors of your typical e-mail scam.

The message said to simply download and open a Word document to review new instructions for reporting health benefits on this year's tax forms. Seemed simple enough, Bruce thought, as he clicked the attachment. When he tried to open the file, Word took forever to open...but that wasn't unusual for his work

computer. Glancing at the clock, Bruce decided he'd log out and read it on Monday. He gathered his stuff and dashed for the bus. It was a decision he'd long regret.

By the time he returned to work three days later, Bruce had a bad feeling. Logging back in, he found that the document still wasn't loading, and thinking back, he didn't feel so good about the origin of that e-mail any more. Swallowing his pride, he dialed up IT and admitted what he'd done. The concerned voice on the phone was just the beginning of a landslide of consequences.

First, the IT experts determined that Bruce had in fact downloaded a malicious program, one that was left free to operate over the weekend. Even worse, his computer could access to tens of thousands of electronic medical records, leaving patient information including names, billing, social security numbers, insurance, and more vulnerable to the software. It was the worst-case scenario.

While there was no hard evidence (yet) that any of this data had been stolen or used for fraud, the hospital had no choice but to disclose the breach to those affected. Local and national media covered the story, quoting patients angered and disappointed at the invasion of their privacy. The official press release only named an anonymous "single employee" as the source of the breach, but Bruce felt like everyone at the hospital knew it had been him.

As the media storm died down, it was replaced by the glare of a different, harsher spotlight: federal investigations. The FBI looked into the origins of the e-mail and the Department of Health and Human Services (DHHS) examined the hospital's security procedures. Bruce was the subject of several difficult and humiliating interviews. Eventually, the hospital settled the case with DHHS for nearly $1 million, promising to install new security protections and employee training to prevent another incident. It was a heavy price tag for one bad decision, but one that Bruce would never forget...or repeat.

Visit http://security.bsd.uchicago.edu/phishing/ for more information on how to avoid a phishing attack.

What to do if you become aware of an information security incident?

Contact the BSD ISO Team via email at security@bsd.uchicago.edu.