http://security.bsd.uchicago.edu

In this issue of the BSD ISO Cybersecurity Newsletter…

- The conclusion of the unfortunate story told in the January BSD ISO newsletter involving Dr. John Smith and a security incident that resulted in the disappearance of a year worth of research data. Please read the following story called "False Security" and ask what you could do to prevent the same occurrence in your department.
- Business Impact Analysis (BIA) Questionnaire: Tool to assess risks in your department.
- Laptop Encryption Acceleration Program (LEAP) Update.

False Security

Dr. John Smith found all the data from an important study missing, and learned a hard lesson about constantly monitoring account privileges. "Is there any way to get the data back?" he asked.

"Well...it depends," said the security officer. "Did you have a backup?" Dr. Smith breathed a sigh of relief. His laboratory had installed their own backup a year ago, after a hard drive crash wiped out important data from another study. His pulse returning to normal, Dr. Smith accessed his backup drive, feeling a glimmer of optimism as he found all the familiar data folders in their right place. But clicking into the "lost" study folder, his chills returned. "Oh no," Dr. Smith groaned, "There's still data missing here. Months of data. Why didn't the backup work?" "Well, how often did you have it set up for automated backups?" asked the security officer. "Uhhh…."

"Dr. Smith had failed to establish continuity -- regular backups on a daily or weekly basis"

When he self-installed the backup, Dr. Smith had failed to establish continuity -- regular backups on a daily or weekly basis that captures new data added to the system. Without it, the backup was merely a snapshot of the files at the time of its installation, and the missing data added afterwards could not be easily restored.

With all the simple solutions exhausted, there remained only one option to recover the data...at great cost. Through an outside

Preventative Measures

- The STA-01-BSD Minimum Security Standards for Systems specify that all important data should be backed up to a BSD-approved network storage.
- Laboratory system admins must establish a regular, procedure to carry out and verify regular backups.
- Labs should document restoration procedures, and periodically execute trial restores to ensure data continuity.
- The Center for Research Informatics can help meet these standards by housing your data and preventing unauthorized access by outside parties and providing automatic backup services. For more on the CRI, visit http://cri.uchicago.edu.

firm, the security office obtained a quote for saving Dr. Smith's lost data: over $10,000, and months of time that could have been avoided with a few minutes of proper set-up.

An already-thin laboratory budget would have to be stretched even more, sacrificing future work just so the last year of painstaking research could be saved. A series of seemingly small oversights had seriously derailed the progress of Dr. Smith's laboratory. "Why!?!," he shouted to the ceiling, fists clenched and raised. "Why didn't I follow the BSD Minimum Security Standards for Systems!!!!"

NEXT MONTH: A lost laptop creates big problems in...Tales from the Encrypt.

Business Impact Analysis (BIA) Questionnaire

The BSD ISO has created the Business Impact Analysis (BIA) Questionnaire as a tool to help the BSD Executive Administrators assess risks in their departments. Completing the BIS Questionnaire will ensure the continuity of critical business processes in the event a disaster should occur. The BIA Questionnaire is now available for use and can be downloaded from the BSD ISO website at http://security.bsd.uchicago.edu/For Faculty And Staff.

Laptop Encryption Acceleration Program (LEAP)

The Laptop Encryption Acceleration Program (LEAP) is in the final stage and the inventory collection process is considered complete. All users in possession of a laptop must now ensure they satisfy the BSD directive to encrypt BSD-owned laptops. In general, there are three options -Self-Service Portal, Encryption by Appointment, Do It Yourself- which users can pursue. For more information about LEAP and the three laptop encryption options go to http://security.bsd.uchicago.edu/Encryption.

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

Contact the BSD-ISO team via the following phone numbers or e-mail addresses:
You may also send an e-mail to the BSD Security mailbox: security@bsd.uchicago.edu
Visit the BSD-ISO website: http://security.bsd.uchicago.edu

Plamen Martinov, Director of BSD Information Security	O: 773-834-1714	pmartinov@bsd.uchicago.edu
Bruce Thompson, IT Security Operations Analyst	O: 773-834-5398	bthompson@bsd.uchicago.edu
Travis Le, IT Risk and Security Analyst	O: 773-834-7127	tle2@bsd.uchicago.edu
Kim Cooke, IT Security and Compliance Analyst	O: 773-834-7897	kcooke3@bsd.uchicago.edu