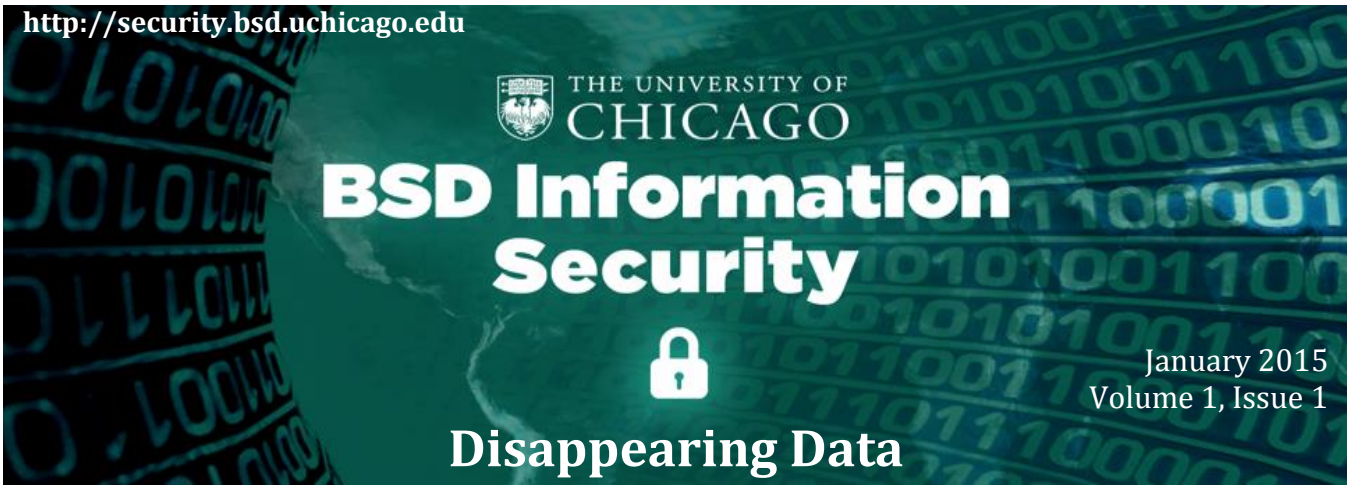

From the Desk of the BSD Information Security Office

A warm welcome to the first issue of the BSD Information Security Office's Newsletter!

The BSD Information Security Office will publish a monthly newsletter designed to raise awareness of information security related issues and concerns. This newsletter will include stories about IT security incidents and suggestions on how to avoid future incidents that could jeopardize the confidentiality, integrity and availability of BSD systems and data. Please enjoy this first story called "Disappearing Data" and ask what you could do to prevent the same occurance in your department.

The Disappearing Data

It had been a long, difficult study, but finally Dr. John Smith was ready to conduct the final data analysis and write his manuscript. The last 12 months of recruitment and retainment, making sure each volunteer showed up for their three required laboratory visits, had pushed his research team to its limit. But with enough subjects to power the study, it was time to bring this project across the finish line, Dr. Smith thought as he clicked through to his laboratory's data folder and found nothing. His heart skipped a beat, his stomach twirled. A year of data, vanished, gone. Beads of sudden sweat appearing on his brow, Dr. Smith quickly clicked up and down the directory, looking in every folder to see if the data had somehow moved. But it was nowhere. All that hard work erased, without a trace. Leaning back in his chair with his head in his hands, Dr. Smith frantically thought back to how this could happen. Only a handful of people in his lab could access the server, and all of them would be just as crushed by the disappearance as he was. Who else could have gotten to the data, and who could possibly have a reason to delete it?

Dr. Smith sat up suddenly, remembering a particularly bad day last month. After his funding was unexpectedly reduced, he was forced into a tough decision: end the project early, or let one of his lab staff go. The research assistant he chose had been with the lab for two years, and took the layoff hard, leaving the laboratory in tears. At the time, Dr. Smith chalked the threats up to understandable disappointment and put it aside, but now…

There was no option left except to call the BSD Information Security Office, who confirmed his worst fears -- the assistant had logged in last night, and shortly thereafter, the data files were deleted. In all the emotions surrounding the layoff, he had forgotten to revoke the research assistant's permissions. They had been able to later log in to the server from a remote location and take their revenge. With a deep sigh, Dr. Smith asked the question he dreaded to ask, "Is there any chance of recovering the data?"

In the long pause that followed from the other end of the call, Dr. Smith saw his academic career flash before his eyes. How would he explain the loss of data to his lab members? To his funding agency? To his tenure review committee? Finally, the security officer responded in a voice filled with hesitance. "Well...it depends. Did you have a backup?"

TO BE CONTINUED…

How could Dr. Smith have avoided this terrifying situation?

The STA-01-BSD Minimum Security Standards for Systems requires laboratory supervisors to maintain strict account control for their research IT system System administrators must have a documented process for granting, revising, and terminating access to these systems, and all account types that are no longer being utilized must be disabled immediately. In addition, accounts should be regularly reviewed and access removed when an account no longer needs to access the system. For more information, visit http://security.bsd.uchicago.edu.

The Center for Research Informatics can help meet these standards by housing your laboratory's data server and securing it, preventing unauthorized access by outside parties and providing automatic backup services. For more on the CRI, visit cri.uchicago.edu.

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