IT Risk Bulletin

THE UNIVERSITY of ALABAMA SYSTEM

A joint publication of the UA, UAB, UAB Health System, and UAH Chief Information Security Officers and The University of Alabama System

Spring 2016 Issue No. 14

FOR MORE INFORMATION:

ASHLEY EWING
Information Security Officer
UA
205-348-6524
aewing@ua.edu

CHIEF INFORMATION SECURITY OFFICER
UAB
205-975-3117
CISO@uab.edu

ROB FERRILL
Chief Information Security Officer
UAB Health System
205-975-9911
rferrill@uabmc.edu

RUSS WARD
Chief Information Security Officer
UAH
256-824-2623
ciso@uah.edu

CHAD TINDOL
Director of Risk Management
UA System
205-348-5889
ctindol@uasystem.ua.edu

MURIEL FOSTER
Director of IT Audit
Office of Internal Audit, UA System
205-934-4105
mjfoster2@uasystem.ua.edu

To access current and past IT Risk Bulletins, go to the "Office of Risk Management" page on www.uasystem.ua.edu.

Lessons from Recent Data Breaches

Guest Author: Erin Owen, Project Specialist, The University of Alabama System

According to Bloomberg News, since 2005, there have been more than 75 million-record data breaches. And those are just the ones we know about. Below are details on some recent major data breaches and what universities can learn from these examples.

Premera Blue Cross/Blue Shield

Premera Blue Cross/Blue Shield, a major health insurer, experienced a data breach in February 2015 that resulted in one of the largest thefts of medical records to date.

- According to NetworkWorld.com, Premera Blue Cross/Blue Shield's data breach compromised approximately 11 million subscribers' and vendors' records and included information such as names, birth dates, Social Security numbers, bank account information, addresses, and other information.
- It is believed that the hackers accessed the information from Premera by using phishing to lure employees to sites that downloaded malware.
- **The Lesson:** As has been mentioned in previous issues of the *IT Risk Bulletin*, phishing takes place regularly, and every employee must be vigilant to protect their personal information and their access to University resources.

University of California, Berkeley

According to NetworkWorld.com, The University of California-Berkeley has disclosed, in accordance with California law, three data breaches since late 2014.

- The most recent data breach in December 2015 could have compromised Social Security numbers and bank account information for approximately 80,000 current and former faculty, staff, students, and vendors.
- UC-Berkeley has prided itself on cutting-edge cybersecurity research and has received millions of dollars from the Hewlett Foundation for cybersecurity policy research.
- **The Lesson:** Any organization, no matter how sophisticated or focused on cyber-security, can fall victim.

Army National Guard

In July 2015, the Army National Guard announced that a data breach may have exposed the private information, including names, Social security numbers, dates of birth, and home addresses, of current and former Army National Guard members since 2004.

- According to a quote from Maj. Earl Brown, a spokesman for the National Guard Bureau, in an article on TheHill.com, the data containing this personal information was "inadvertently transferred to a non-DoD-accredited data center by a contract employee."
- **The Lesson:** It is important that all employees are informed of your institution's rules and procedures for saving and transferring data, especially those including the personal information of students and/or employees.