Higher Ed Cyber Roundup: Disruptions, Financial Loss, Data Breaches

Jan – June 2016

Disruptions

The **remote print feature was disabled on all campus printers** after an individual or group **hacked into multiple printers** and printed an anti-Semitic flyer.

DePaul University / March 2016 / Story

The **online W-2 service was shut down** following an investigation that revealed W-2 information for over **300 employees was accessed from suspicious locations**. SSNs and birthdates are the only information required to login—information likely obtained from an unrelated data breach. Approximately **150 employees** reported **problems filing taxes** this year.

Northwestern University / May 2016 / Story / Story2

Financial Loss

Thirteen employees had their **direct deposit payments misdirected to another account.** Over **$50,000** was involved. The online service used to modify bank routing information for direct deposits was suspended to "preserve payroll data integrity."

Illinois State University / March 2016 / Story

Higher Ed Cyber Roundup: Disruptions, Financial Loss, Data Breaches

Jan – June 2016

Data Breaches

Personally identifiable information including names, mailing addresses, university ID numbers, and Social Security numbers of **38,000 current and former students** was exposed through a "**sophisticated phishing scam.**"

North Carolina State University
June 2016 / Story

Approximately **63,000 current and former students and employees** had their **social security numbers stolen** via a breach of the University's computer network.

University of Central Florida
February 2016 / Story

W-2 information for University employees was **accidentally provided to a cyber-criminal** after a University employee **fell victim to a phishing scam.** Approximately **1,300 employees'** names, addresses, incomes, and Social Security numbers were exposed. One of the **victims is suing the University over the breach,** citing the University as willful and reckless in exposing the personal information.

Rockhurst University
May 2016 / Story / Story 2

W-2 information for over **600 current and former employees was fraudulently downloaded from a third party vendor,** W-2Express, an online service operated by Equifax. As with the Northwestern University case listed above, it appears SSNs and birthdates were obtained elsewhere and used to login to the online W-2 service.

Stanford University
May 2016 / Story

A component of the University's **human resource system was infiltrated** via a **phishing attack. W-2 information** of over **1,400 employees** was put at risk; direct deposit information of 40 employees was also exposed.

University of Virginia
January 2016 / Story

Employees' **W-2 information** was **mistakenly e-mailed to a cyber-criminal impersonating a senior executive.** The Academy purchases **two years of credit monitoring** for affected individuals.

Academy of Art University
April 2016 / Story