University Cyber Roundup: Disruptions, Data Breaches, Financial Loss

Jan – Jun 2019

Data Breaches

A Temple University employee uploaded a document containing **160 students' dates of birth, cell phone numbers, and passport information to the University's public website.**

Temple University / *Jun 2019* / Story

A Seattle University laptop containing **more than 2,000 social security numbers of former faculty, staff, and their dependents** was left on a public bus.

Seattle University / *Apr 2019* / Story

The University of Alaska took **over a year to notify potential victim**s of a data breach. In February 2018, it was discovered that an unauthorized user accessed and changed the passwords of UAOnline users. Further investigation found that an **unauthorized user accessed email accounts containing names, government issued identification numbers, dates of birth, digital signatures, driver's license numbers, usernames and/or passwords, financial account numbers, health and/or health insurance information, passport numbers, and UA student identification numbers.** Social security numbers were also compromised for some users.

University of Alaska / *Apr 2019* / Story

A public records request led to the **public dissemination of improperly redacted information** including **social security numbers** of Community College of Allegheny County former students.

Community College of Allegheny County, *PA / Apr 2019* / Story

An employee of St. Louis Community College **accidentally e-mailed** the personal information (**name, personal address, college identification number, phone number, race and more**) of **4,000 students** to a local school district's employees.

St. Louis Community College / *Mar 2019* / Story

Hackers broke into three **colleges' admissions database using the password reset system and offered to sell applicants their files.**

Grinnell College, Hamilton College, Oberlin College / *Mar 2019* / Story

A Stanford student discovered a **flaw in a third-party system** that **allowed access to student records by changing the numeric ID in the URL**. Information compromised included sensitive information such as **students' ethnicity, legacy status, home address, citizenship status, criminal status, standardized test scores, personal essays and financial aid status.**

Stanford University / *Feb 2019* / *Story*

An employee **inadvertently attached a spreadsheet** containing personal information of **4,557 current students.** Personal information included **names, addresses, email addresses, gender, ethnicity, academic standing, and GPA.**

Cal Poly Pomona / *Feb 2019* / *Story*

Over **200 students had their personal information, such as first name, last name, school account username, student identification number, date of birth, driver's license number and/or partial/full Social Security number, compromised** when an **email account was accessed by an authorized user.**

Pellissippi State Community College / *Feb 2019* / *Story*