# University Cyber Roundup: Disruptions, Data Breaches, Financial Loss

Jan – Jun 2018

## Disruptions

MVSU IT Department was **forced to shut down the school's internet service** after a **ransomware attack** hit the school.

*Mississippi Valley State University / Mar 2018 / Story*

A data breach at the University of Alaska allowed **a third party hacker to change the email addresses of 50 users, locking them out of their accounts.**

*University of Alaska / Feb 2018 / Story*

## Data Breaches and Disclosures

Patients of Purdue University Pharmacy were alerted to a potential breach of their private information when an **unauthorized access file** was found on a pharmacy computer. Affected data included **patient names, identification numbers, dates of birth, dates of service.** Further, **a second case of malware was found on a Pharmacy computer,** jeopardizing **driver's license numbers and Medicare information.**

*Purdue University Pharmacy / May 2018 / Story*

NetID, the University of Vermont portal that **grants access to email, class registration, and grades,** was breached. Approximately **37,000 current and former faculty and staff** were affected.

*University of Vermont, VT / May 2018 / Story*

Students and staff at the University of Toledo received a letter in May informing them that a **USB flash drive containing their personal information was lost** in January. Information on the flash drive included **names, addresses, social security numbers, and possibly birth dates.**

*University of Toledo, OH / May 2018 / Story*

Close to **2,700 current and former students and staff** at the University of Buffalo had their **login information compromised.**

*University of Buffalo, NY / May 2018 / Story*

Personal information, including **names, Social Security numbers, and dates of birth,** of current and former Global University students was **compromised** when a **misconfiguration of database** left it **open on the Internet.**

Global University, MO / *May 2018 / Story*

The **names and social security numbers** of **46 employees and their families** were displayed in error on an internal website.

Columbia College / *Mar 2018 / Story*

A **hard drive** containing the **personal data of 15,000 people was stolen** from Fresno State University. Personal information on the drive included **names, addresses, phone numbers, birth dates, credit card numbers, driver's license numbers, and full or partial Social Security numbers.**

*Fresno State University / Mar 2018 / Story*

An associate professor at the University of Washington **accidentally emailed** a spreadsheet to 85 students, faculty, and staff that contained **name, gender, citizenship status, and ethnicity of 9,000 applicants.**

University of Washington / *Mar 2018 / Story*

A **spreadsheet** containing **names, email, ID numbers, and home addresses of 362 students** was **sent in an email attachment.**

*St. Louis Community College / Mar 2018 / Story*

A **former employee inappropriately accessed** a University of North Georgia **database containing name, ID number, gender, major, concentration, dorm or commuter status, class, address, phone number, adviser name, email and campus.**

University of North Georgia / *Feb 2018 / Story*

A **school laptop was stolen** out of an employee's car. The laptop contained **names, Social Security numbers, dates of birth, subscriber member numbers and/or health insurance information of over 2,500 individuals.**

*California College of Arts / Feb 2018 / Story*

## Financial Loss

The **email account** of the CFO of Northwest University **was compromised,** allowing hackers access to the account. A **legitimate payment of $60,000 was re-routed** by the hackers.

Northwest University, WA / *May 2018 / Story*