Michael Best

July 29, 2019

Higher Education Data Breaches Draw Response from Federal Agencies

Higher education institutions have long been a target for cybersecurity attacks, in large part due to the sensitive personal, financial data and intellectual property assets that they hold. Recent events have risen to the attention of two of the most powerful federal regulatory agencies with oversight of colleges and universities. Specifically, last week the U.S. Department of Education issued a detailed warning regarding an ongoing cybersecurity attack that has, to date, affected at least 62 colleges and universities. In addition, the U.S. Office of Management and Budget recently issued robust information security audit requirements for educational institutions. These developments highlight the need for higher education institutions to stay current on cybersecurity legal developments and ongoing attacks and, at the same time, maintain an up-to-date, comprehensive information security program.

62 Colleges and Universities Affected by Cybersecurity Attack:

The U.S. Department of Education (the ED) posted a public security alert last week stating that they have identified at least 62 colleges and universities that were recently targeted by hackers exploiting a security vulnerability in the Ellucian Banner system, an Enterprise Resource Planning (ERP) web based application. The Ellucian Banner System is used by many colleges and universities to manage and customize their front facing web applications. The vulnerability exploited affected a module of Ellucian that is used to manage student user accounts. This vulnerability enabled hackers to create thousands of fake student accounts, some of which officials believe were leveraged almost immediately for criminal activity.

According to the ED's alert, victimized institutions have indicated that their implementation of the Ellucian Banner system affects all areas of academic administration, including the administration of financial aid. Officials are now urging colleges and universities using vulnerable versions of ERP

Related Industries

Higher Education

Related Practices

Privacy & Cybersecurity

modules to apply security patches and to consider implementing additional safeguards that segregate system functions affecting the ED's financial aid data. Impacted entities using these affected systems are encouraged to read the NIST Advisory in its entirety (see CVE-2019-8978) for more specific technical information.

New Information Security Audit Requirements Issued for Higher Education Institutions:

The U.S. Office of Management and Budget (OMB) recently issued its 2019 Compliance Supplement, containing first time audit objectives for higher educational institutions concerning compliance with the Safeguards Rule of the Gramm-Leach-Bliley Act (GLBA). This marks the first time that compliance with information security requirements has been expressly included as part of a Title IV audit process. The FTC has previously stated that they consider higher educational institutions that receive Title IV funds to be "financial institutions" subject to GLBA. The new audit objectives aim to determine whether an institution has developed and implemented an adequate information security program under the Safeguards Rule of the GLBA. The 2019 Compliance Supplement instructs auditors to verify that all institutions have the following three safeguards in place:

- Designation of an individual to coordinate the information security program;
- Completed risk assessment that covers employee training and management, networks and information systems, and incident response; and,
- Properly documented safeguards for every identified risk.

In order to comply with these audit objectives, educational institutions will be responsible for demonstrating that they have implemented these three core safeguards. We recommend that education institutions start working internally to assess their compliance, now, in order to work proactively to avoid security breaches and remediate any gaps prior to an audit.

The entire **2019 Compliance Supplement can be downloaded in full here.**

Michael Best has seasoned attorneys with substantial experience providing cybersecurity and privacy services to higher education institutions. Our attorneys can help universities and colleges assess applicable legal requirements and design and implement information security programs that comply with the law, mitigate the risk of a data breach and support successful completion of legally-required third party audits. For more information, please contact the Michael Best Privacy and Cybersecurity Team.

Related People

Adrienne Ehrhardt
Partner
asehrhardt@michaelbest.com
T 608.283.0131

Adrienne Ehrhardt, CIPP/US, CIPM
Partner
asehrhardt@michaelbest.com
T 608.283.0131

Rebecca Gerard
Associate
rlgerard@michaelbest.com
T 312.596.5872

José Olivieri
jaolivieri@michaelbest.com
T 414.225.4967

Elizabeth Rogers, CIPP/US
Partner
earogers@michaelbest.com
T 512.640.3164

Elizabeth Rogers
Partner
earogers@michaelbest.com
T 512.640.3164

Ryan Sulkin
Partner
rtsulkin@michaelbest.com
T 312.596.5836