Pass or fail?

Data privacy and cybersecurity in higher education

McDonald Hopkins

A business advisory and advocacy law firm®

beazley

Introduction

Institutions of higher education are becoming prime targets for cyberattacks because of the vast amount of data they collect and maintain, and the openness of their online communities. As colleges and universities are leaders in education; likewise they should be leaders in cybersecurity and data privacy training and education.

Colleges and universities collect data from donors, trustees, board members, alumni, students, parents, applicants, faculty, staff, medical patients, consumers, and vendors. The type of data they collect and maintain is wide spread as well, including, sensitive research, financial, medical, employment, personal, and tax data. Colleges and universities also are not only institutions of higher education – they are financial institutions, medical institutions, and retail establishments, and subject to the state, federal and international regulations related to those industries.

As the costs of a data breach skyrockets well into the millions of dollars, colleges and universities are advised to assess their cyber insurance coverage, breach preparedness, incident response plans (IRP), and educate all groups that have access to and use data in their systems.

With just one incident a college or university could be dealing with as many as 75 to 100 different breach notice laws.

Data Privacy and Cybersecurity Risks for Higher Education

Diversity of residencies

Institutions of higher education draw students from across the country and around the globe. While a multicultural environment is a tremendous asset, the different permanent residencies of students complicate data breach response. It is essential that colleges and universities understand that the law of the state or country of residence of each student, alumni, staff, donor and impacted individual in a data breach governs. Currently, there are 47 state breach notice laws and numerous foreign countries that have their own breach notice laws. As such, with just one incident a college or university could be dealing with as many as 75 to 100 different breach notice laws. Those laws dictate what a breach is, what elements constitute personally identifiable information, when notice needs to be given, how to give notice, who receives notice, and what must be told to impacted individuals and applicable regulators. Many state attorneys general will commence an investigation of the incident, which means requests for specific policies, procedures and remedial measures implemented by the institution.

FERPA

Although the Family Educational Rights and Privacy Act (FERPA) does not have a strict requirement to provide notice of a data breach, direct student notification is advisable if the compromised data includes student Social Security numbers and other identifying information that could lead to identity theft. FERPA does require the institution to maintain a record of each such disclosure. Moreover, notifying the Family Policy Compliance Office about the breach is considered a best practice by the U.S. Department of Education. The Department of Education often will commence its own investigation of the incident and may request additional documentation.

HIPAA

Many colleges and universities have independent hospitals and clinics that collect and maintain protected health information (PHI) as a covered entity subject to the Health Insurance Portability and Accountability Act (HIPAA). If a breach at an institution of higher education involves PHI and it is deemed to be a covered entity, HIPAA will require the institution to comply with its breach notification rule requirements, which include a host of notice requirements in addition to, and different from, state breach notice laws. If the institution is a covered entity, the U.S. Department of Health and Human Services Office for Civil Rights likely will commence an investigation if the breach impacts 500 or more individuals.

Retail regulations
Colleges and universities also are retail establishments with various retail entities on campus including food venues, book stores, clothing, and other retail operations subject to the Payment Card Industry Data Security Standards.

Research establishments
University systems can be a jumping point to government computers or corporate networks due to the collaborative research efforts between colleges and universities and government and corporate America in developing cutting edge research.

Open online communities
Further complicating the cybersecurity risks, colleges and universities are known for maintaining open online communities, with network systems that have multiple points of access including multiple departments and various users, as well as third party vendors. Many colleges and universities are staffed with students in their IT departments with limited experience, yet wide access. Further, students access college and university systems through wired and wireless internet portals, with extensive use of unsecured social network sites. Moreover, colleges and universities have a significant user turnover with students graduating or transferring schools.

Unique Features of Higher Education

Amount of data to be protected
"From social security and credit card numbers to health care records and intellectual property produced by research departments, colleges and universities house a vast amount of sensitive data."[1]

- **Personal and financial information:** Colleges and universities receive personal and financial information of donors, alumni, students, parents, faculty, staff, and prospective students which is collected and stored on college and university servers.
- **Health information:** Colleges and universities collect and maintain PHI of students, employees, and other patients at campus medical systems. In addition, colleges and universities collect and maintain medical information of employees as employers.
- **Intellectual property:** Colleges and universities are at the forefront of sensitive research, many times collaborating with the government and/or corporate America. They collect and maintain sophisticated research in engineering, sciences, and other disciplines, new or emerging technologies and innovation, of which other countries are interested.
- **Government data:** Certain higher education institutions are actively engaged with government programs, such as the Department of Defense. As a result, these colleges and universities have highly confidential information that, if leaked, may pose a threat to national security.
- **Employment-related records:** Colleges and universities collect and maintain employment related data for all employees, including personal and tax related information.
- **Retail establishments:** Colleges and universities also include campus retail establishments thereby subjecting the university to many of the point of sale data security issues and related regulations.

[1] Boyer, Stephen, BitSight. Cofounder and CTO.

Open communication and information sharing disrupts the incident response process

The learning environment on college campuses encourages open communication and information sharing – both of which are crucial to a student's education. Unfortunately, institutions of higher education often desire to structure their data breach responses with that same openness and sharing in mind.

Responding to a privacy incident is one time when a college or university could cause more damage than good by overly communicating or sharing information too quickly. The beginning stages of a breach investigation often include a complex forensic investigation, and breach response, while often fluid, can be time consuming given the complexities of today's intrusions and compromises. While it can be tempting for an incident response team (IRT) to share everything it knows about an incident with the campus community, colleges and universities must learn only to share information on a need to know basis. There are many times when an incident never rises to the level of a full-blown data breach requiring public notice. Before a college or university publicly communicates about the incident or breach, it should be able to respond to these questions – otherwise it should not be publicly communicating about the incident at all.

- What happened?
- How did it happen?
- Who is impacted?
- What are you doing for those impacted?
- How are you preventing this from happening again?

A breach response that is done correctly withstands the temptation of sharing information outside of the IRT until the investigation and legal analysis is complete and the messaging is consistent and agreed upon.

Decentralization complicates incident response planning and breach response

Multiple campus locations, a variety of employees with diverse knowledge and levels of expertise, and different colleges/schools or offices making independent decisions contributes to the decentralization of institutions of higher education. While the decentralized nature works for campuses, it complicates incident response planning and responding to a breach. Assembling an IRT on a campus is often a battle, but getting all of the IRT members on the same page for one unified response can be all out war. It is, therefore, essential that the IRT meet at least twice a year to conduct a breach response workshop and tabletop exercise. During these workshops and exercises, the IRT will have the opportunity to sort through the issues of decentralization and narrow the various decision points the IRT will face during a real-life data breach. It is best to practice while things are calm!

Assembling an incident response team (IRT) on a campus is often a battle, but getting all of the IRT members on the same page for one unified response can be all out war.

Costs for Higher Education

The costs of a breach for colleges and universities can be high. The institution risks losing funding based on negative public relations, losing donors who don't want to submit financial information that cannot be kept secure and losing research grants from corporations or the government when collaborating opens the door for a hacker to gain access to their system. Financial loss also could occur if a cyber thief transferred university funds after gaining access to university financial systems through malware on, for example, the controller's computer.

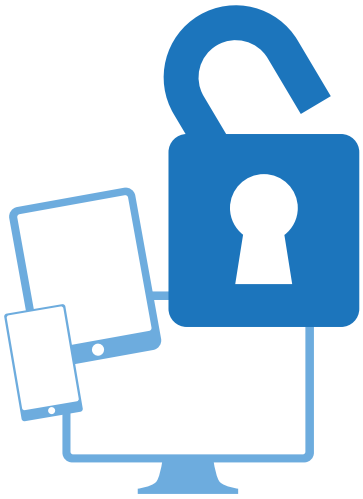
Universities also suffer reputational harm as a result of the public's loss of confidence and trust in the university. Consumer studies have shown:

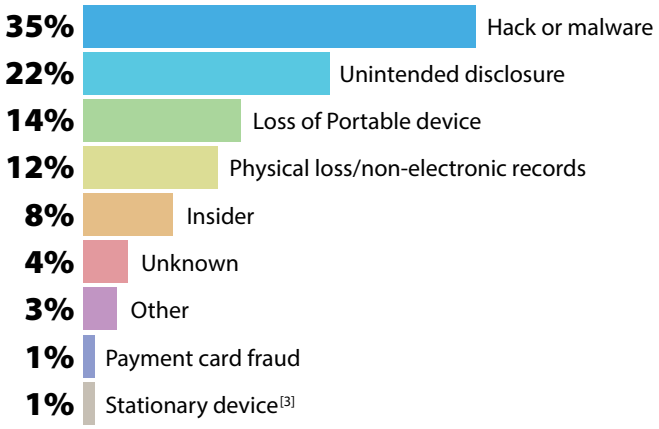
- 62% said breach notification decreased trust and confidence in the organization.
- 15% would terminate their relationship with the notifying organization (39% would consider terminating).
- 94% believe the reporting organization is solely to blame for breach.
- 72% thought organizations do a poor job communicating and handling a data breach. [2]

In the first few months of 2016 there has already been a 50 percent increase in higher education breaches.

Causes of Higher Education Data Breaches

In 2015, there were multiple causes of data breaches at colleges and universities, including:





Many data breaches at colleges or universities still result from lost or stolen devices that are unencrypted (i.e., laptops, USBs, portable storage devices). But the main cause of intrusions into a campus network is through phishing emails sent to university employees whose everyday job is not to worry about data security. The hackers take advantage of these vulnerabilities and send targeted spear-phishing emails to university employees and subsequently obtain valid usernames and passwords to gain access to the university system, which is another reason why breach response workshops, tabletop exercises and training employees is crucial.

There also has been a rise in hacking into college IT systems by other countries to obtain access to sensitive research data.

Colleges and universities should monitor their third-party vendors and service providers that are granted access to sensitive and personal information. Vendor breaches continue to increase and often are the most costly to a university.

[2] Ponemon Institute & Experian Data Breach Resolution.

[3] Beazley Breach Response.

2016 Higher Education Breach Statistics

In the first few months of 2016 there has already been a 50 percent increase in higher education breaches.[4] Data breaches in higher education institutions cost approximately $300 per record, second only to the cost of health care breaches. (Most other breaches average $150 per record.[5]) The cost per record has increased annually for the past several years. In 2014 cost per record was only $200 in higher education breaches.

Recent examples of breaches in the higher education sector include:[6]

- **Southern New Hampshire University:** 140,000 records, including student names, email addresses and IDs, course names, selection, and instructors, due to third party vendor configuration error.
- **University of Central Florida:** 63,000 records, due to unauthorized access into the university system. The data compromised included financial, medical, grades and Social Security numbers. The university provided one year free credit monitoring for those affected.
- **University of Virginia:** 1,440 records including personal and financial data, due to cyberattack of the human resources system. The attack was initiated by a phishing email to an employee asking for usernames and passwords to their HR system and one or more employee fell for the phishing scam. The information compromised included data from W2 forms. The FBI-led investigation resulted in arrests.
- **Penn State College of Engineering:** Servers were hacked on two occasions by hackers believed to be based in China and may have exposed at least 18,000 individuals' sensitive data. Notification was sent to employees and faculty. The university asked affected individuals to change user name and password, and set up a VPN with a two factor authentication.
- **University of California Berkeley:** Notified individuals of a data breach in their real estate division that resulted in unauthorized access to servers used to support a number of real estate programs and work station. The data included names, Social Security numbers, credit card numbers and driver's license numbers. The university offered one year of free credit monitoring.
- **University Development and Alumni Relations at the Penn State College of Medicine:** Penn State notified 1,176 individuals of a data breach of their personal information, including Social Security numbers.
- **Maricopa County Community College District:** Breach response cost over $26 million and required notification to 2.3 million people, including current and former students, staff and vendors from as far back as 30 years. Data hacked included Social Security numbers and banking information.

The risk of exposure includes records for all individuals who come in contact with higher education services, including, donors, alumni, students, prospective students, virtual students, parents, employees, faculty, medical patients, athletes, and third party vendors.

Data breaches in higher education institutions cost approximately $300 per record.

[4] Privacy Rights Clearinghouse. 2016

[5] Ponemon Institute's 2015 Global Cost of Data Breach Study Reveals Average Cost of Data Breach Reaches Record levels. May 27, 2015. PRNewswire

[6] Privacy Rights Clearinghouse. 2016.

Considerations

While higher education institutions are making progress in data privacy and cybersecurity, they need to focus more attention on breach preparedness, including:

- **Personal information review –** Identify what sensitive and personal information the institution has, where it is stored, and who has access.
- **Policy and program development –** Review (and revise) policies for handling, storing, managing, and destroying personal information. Ensure the university has a well-drafted written information security program that identifies the administrative, technical and physical safeguards the institution has in place for sensitive and personal information. Colleges and universities should take a closer look at their policies covering computers and electronic devices usage, document retention/destruction, telecommuting, social media, and access control policies.
- **Limit user & administrator privileges –** Too often universities and colleges allow open file sharing and collaboration, which can lead to vulnerabilities on which a hacker will capitalize. It is important to limit user and administrator privileges and control access on a need-to-know basis.
- **Training –** Colleges and universities have a plethora of personal information on their students, donors, staff, faculty, parents, alumni, medical patients, athletes, and vendors. The institution should implement specific data privacy and cybersecurity training for individuals who have access to and/or handle personal and sensitive data collected and maintained by the college or university on its stakeholders, as well as general awareness training for all individuals who use, access or connect to the institution's systems. Coupled with ongoing security awareness, the training of university groups at all levels that have access to confidential information, is key to reducing cybersecurity risk.
- **Vendor management –** Given the rise in breaches caused by service providers, it is critical to ensure vendors maintain appropriate security measures and that assurances are provided in vendor contracts. Such agreements also should be vetted for a service provider's protocol for breach response obligations.
- **IRT and IRP practice –** Developing an incident response team and incident response plan prior to a data security incident is critical to successful incident response. The institution will be far better positioned if they have the opportunity to practice hypothetical breach exercises with their IRT using their IRP as a guide, before the real-life breach occurs. Don't let the IRT always know ahead of time when the exercise will occur. It is a great test of the IRT and IRP when the element of surprise is present!

In 2016, higher education institutions are no longer judged because they have a breach. Rather, they are judged on how they respond to the data breach and the steps they take to ensure their stakeholders are fully informed and protected. Be an institution that passes the cybersecurity and data privacy test.

Too often universities and colleges allow open file sharing and collaboration, which can lead to vulnerabilities that a hacker will capitalize on.

McDonald Hopkins

A business advisory and advocacy law firm®

beazley

Questions about data privacy and cybersecurity in higher education? Contact any one of these McDonald Hopkins attorneys.

James J. Giszczak
248.220.1354
jgiszczak@mcdonaldhopkins.com

Sherri A. Krause
248.593.2946
skrause@mcdonaldhopkins.com

Dominic A. Paluzzi
248.220.1356
dpaluzzi@mcdonaldhopkins.com