NACUA NOTES
National Association of College and University Attorneys October 12, 2018 | Vol. 17 No. 1

TOPIC:

KEY ISSUES IN MANAGING DATA BREACH RISK IN HIGHER EDUCATION: PRACTICAL TIPS FOR BEFORE, DURING, AND AFTER

AUTHORS:

Sandra A. Brown, Esquire, and Scott D. Schneider[1]

INTRODUCTION:

Colleges and universities are known for innovation, collaboration, and knowledge sharing. These qualities contribute to U.S. economic growth, yet these same qualities expose institutions to great risk of theft of sensitive information and intellectual property. Colleges and universities store sensitive student and personnel records as well as financial records and data that have significant value, in addition to valuable intellectual property from cutting-edge research. Moreover, many institutions operate medical schools and health centers, storing personally identifiable health records. Hackers, identity thieves, and, unfortunately, malicious insiders[2] increasingly see colleges and universities as potential "gold mines" because of the sensitive data[3] and intellectual property they store.[4]

The risks for higher education institutions may be higher than for many industry counterparts for several reasons. Much of the work of these institutions—especially academic research—relies on collaboration and the free flow of information between people both inside *and* outside the institution. In addition, much of this work is done in a decentralized way. In particular, academic research is typically conducted by professors or in departments with very little, if any, institutional oversight. As a consequence, university administrators and information technology (IT) personnel may not know where all sensitive data is stored and likely will not know what is going on across all parts of their computer networks at any particular time.

This combination of large quantities of valuable assets and a decentralized, collaborative culture makes colleges and universities particularly attractive to hackers. Recent high-profile anecdotes illustrate the type of information hackers target, the myriad motivations for targeting higher education institutions, and the ways in which hackers can significantly disrupt business operations:

- Seeking to steal the intellectual property of Pennsylvania State University's College of Engineering, hackers from China infiltrated the University's computer systems, gaining usernames and passwords in what Federal Bureau of Investigation (FBI) investigators described as a sophisticated cyberattack that lasted more than two years.[5]

- While installing and testing a security patch for a defect in a commercial software system, the University of California at Berkeley became aware of a cyberattack potentially impacting the Social Security and bank account numbers of approximately 80,000 current and former faculty, staff, students, and vendors.[6]

- At Rutgers, the State University of New Jersey, a cyberattack knocked the University's computer network offline four times during the 2014-2015 school year. The hacker who claimed responsibility for the attacks boasted that he or she was paid $500 an hour in Bitcoin by a client who held a grudge against Rutgers and wanted to disrupt the University's computer systems.[7]

In addition to being targeted by outsiders, organizations are at risk for both inadvertent and malicious activity by current or former employees and even students with access to computer networks. As an example of malicious activity by an insider, in June of 2018, Tesla filed a lawsuit against a former employee alleging sabotage and intellectual property theft.[8] In the complaint, the electric car manufacturer accused the former employee of hacking the automaker's computer systems and stealing company secrets. Tesla's CEO, Elon Musk, alleges that the defendant, while an employee, managed to conduct "quite extensive and damaging sabotage" to the company's operations by changing the software code to internal products and exporting proprietary data to outsiders.[9]

As cyber threats evolve, so too must incident prevention, detection, and response strategies. Increasingly, these strategies force colleges and universities to wrestle with entrenched operating procedures and cultural norms. Strategies such as proactive collaboration and intelligence sharing with law enforcement, testing for user-based vulnerabilities, mandated security controls, and comprehensive network and system monitoring can thwart threats and mitigate their impact when they occur. Getting approval to implement the strategies, however, may be challenging. University counsel and key clients will be well served by reviewing trending threats and threat actors, local susceptibility to those threats, and emerging threat mitigation strategies to enhance protections for sensitive information, including information regulated by various legal regimes.

This NACUANOTE will briefly summarize various data privacy laws that require institutions to implement measures to safeguard data. It will then provide key suggestions for in-house counsel to assess and assist with institutional data-breach prevention efforts and to guide mitigation efforts both during and after a data breach.

DISCUSSION:

A. Brief Summary of the Applicable Law

This section of the NACUANOTE briefly summarizes various privacy laws that impose compliance obligations on colleges and universities regarding the acquisition and storage of personally-identifiable data.[10]

1. Family Educational Rights and Privacy Act (FERPA)

FERPA is the overarching regulatory framework for student records in higher education, although it does not impose detailed, prescriptive legal obligations to secure data in specific ways (unlike more modern statutes such as GLBA and HIPAA, discussed below). FERPA applies to educational institutions that receive funds for programs administered by the Department of Education.[11] In the absence of an applicable statutory exception, an educational institution subject to FERPA may not disclose the education records of students, or personally identifiable information from such records, without a student's written consent.

Beyond this general obligation to safeguard education records, FERPA does not impose on colleges and universities specific data security requirements. In one instance, though, when discussing disclosures pursuant to "legitimate educational interests," the FERPA regulations oblige colleges and universities to adopt "reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests."[12] These regulations specify: "An educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to education records is effective and that it remains in compliance with the legitimate educational interest requirement in paragraph (a)(1)(i)(A) of this section."[13] Although this language affords flexibility to institutions, it seems to suggest something more than passive protection, instead implicating that colleges and universities have an affirmative obligation to implement data security protocols to protect education records.[14]

2. Gramm-Leach-Bliley Act (GLBA)

To the extent that an educational institution engages in lending funds (whether to students, parents, faculty, or employees), collecting loan payments, or facilitating the process of applying for financial aid, the institution may be a covered "financial institution" subject to GLBA regulations.[15]

There are two categories of compliance requirements under GLBA: (1) the Privacy Rules and (2) the Safeguarding Rules. The Privacy Rules govern the use and disclosure of personal nonpublic information (NPI) while the Safeguarding Rules set forth requirements with respect to the manner in which covered institutions are expected to protect NPI in their custody or control.

The Safeguarding Rules require covered institutions to develop, implement, and maintain a comprehensive security program consisting of administrative, technical, and physical safeguards to protect against the unauthorized use or disclosure of NPI. Generally speaking, these rules require the institution to:

- designate one or more employees to coordinate the information security program;

- identify and assess the risks to customer information and evaluate the effectiveness of the current safeguards for controlling these risks;

- design and implement a safeguards program and regularly monitor and test it; and

- evaluate and adjust the program in light of relevant circumstances, including changes in the institution's business or operations, or the results of security testing and monitoring.

Colleges and universities that comply with FERPA are considered to be in compliance with the GLBA Privacy Rules.[16] However, there is no similar safe harbor with respect to the Safeguarding Rules, which means covered institutions are required to implement the comprehensive written information security program referenced above as part of their GLBA security compliance efforts.

3. Fair and Accurate Credit Transactions Act (FACTA)

In addition, if a higher education institution does any of the following, it is likely a "creditor"[17]under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") and is covered by certain rules promulgated pursuant to FACTA known as the "Red Flag Rules:"

- participates in the Federal Perkins Loan program

- offers institutional loans to students, faculty, or staff

- offers a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.

The Red Flag Rules' most significant compliance obligation is the requirement to develop and implement a written identity theft prevention program in connection with new and existing "covered accounts." "Covered accounts" means accounts offered or maintained by covered creditors "that involves or is designed to permit multiple payments or transactions" and "[a]ny other account that the . . . creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the . . . creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks."[18]

The required program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft.

4. Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act

Higher education institutions can also be "covered entities"[19] under HIPAA if they provide self-insured health plans (to employees and/or retirees), or employ staff that provide health services to individuals other than employees.[20] The HIPAA Privacy and Security Rules[21] oblige covered entities to safeguard the privacy of protected health information (PHI)[22] and to comply with security standards regarding patient information maintained in electronic form. To satisfy this broad obligation, the Administrative Safeguards provisions in the HIPAA Security Rule require covered entities to perform ongoing risk analysis. In this analysis, institutions regularly

evaluate the likelihood and impact of potential risks to PHI, implement appropriate security measures to address the risks identified in that risk analysis, and periodically evaluate the effectiveness of the security measures put in place following the risk analysis.

The HITECH Act[23] amended the HIPAA security breach notification rules and required that covered entities notify individuals when their "unsecured" PHI had been breached. In addition, pursuant to the HITECH Act, business associates of covered entities (for instance, third-party administrators, consultants, and pharmacy benefit managers) are covered under HIPAA and are subject to breach notification requirements. The HIPAA Breach Notification Rule requires covered entities to provide notification of a breach involving PHI to affected individuals, the Secretary of the United States Department of Health and Human Services, and, in certain circumstances, the media. Covered entities are also required to have in place written policies and procedures regarding breach notification, to train employees on these policies and procedures, and to develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

5. European Union General Data Protection Regulation

In April 2016, the European Union (EU) formally adopted the General Data Protection Regulation (GDPR) with an effective date of May 25, 2018. The GDPR, which replaces the EU's Data Protection Directive of 1995, "represents a significant expansion of personal privacy rights for EU residents."[24] The GDPR defines its scope as protecting all "personal data" of all individuals within the territory of the EU. The definition of "personal data" is exceptionally broad and includes educational, financial, employment-related, and health data; photographs; personal phone numbers; IP addresses; and "sensitive personal data," including racial and ethnic origin, religion, sexual orientation, and political views.

The GDPR is fundamentally different from U.S. data privacy and security laws in a number of respects. Most notably, GDPR covers all facets of information management, including the collection, retention, deletion, breaches, and disclosures of personal data. It also asserts personal consent as a fundamental requirement for almost all of these "processing" activities. Put another way, most collection, storage, uses, matching, and disclosures — including subcontracting of processing functions — of personally identifiable information must be based on the data subject's consent, either directly, or indirectly through a contract to which the data subject is a party. In addition, that consent must be freely given and specific to the transaction.

As written, the GDPR applies to all EU-based operations of non-EU entities, including semester-abroad programs, even if they primarily enroll US residents who may only be temporarily attending programs in one of the member states. Significantly for higher education institutions, and unlike its predecessor, the GDPR's coverage is asserted to extend to entities with no physical EU footprint if they "control" or "process" covered personal information of individuals physically within the EU (*e.g.*, when institutions solicit admissions applications from residents in the EU as well as distance education programs which target EU residents).[25]

With respect to data breaches, covered entities will be required to notify the relevant "supervisory authorities" within an EU state of any breaches within 72 hours of their discovery and to provide information on the remedial steps they have taken in response. It also requires breach notification to data subjects themselves "without undue delay."

6. State Data Breach Notification Laws

Most U.S. states have data security and breach notification laws that vary in scope and attendant obligations. These laws focus on personally identifiable information (PII) that would enable cyber criminals to commit identify theft and fraud by misappropriating credit card information and Social Security numbers. State statutes generally require notification in the event of breaches involving the following information: the consumer's name in combination with a unique identifier such as Social Security number, driver's license number, bank account number, credit card number, or access code. Some states go further to require notification in the event other types of information are accessed or acquired.[26]

For example, California has a Law on Notification of Security Breach[27] that requires notification to the affected individuals when a data breach of personal information occurs. It also has a data protection law[28] that covers information about a California resident, regardless of whether the business that owns or licenses the information conducts business in California.[29]

7. Statutory Penalties and Private Litigation

In addition to out-of-pocket costs and reputational harm that may result from unsecured data and operational disruption caused by cyberattacks, institutions that neglect their compliance obligations to safeguard certain types of data can face significant statutory penalties. For example, after learning of an alleged breach of unsecured electronic health information pertaining to roughly 10,000 individuals, the University of Mississippi Medical Center (UMMC) agreed to settle the resulting HIPAA-related breach investigation for $2.75 million.[30] During the investigation, the Department of Health and Human Services (HHS) Office for Civil Rights determined that UMMC had been aware of system vulnerabilities as far back as April 2005 but had not undertaking efforts to mitigate the risks until after the breach occurred.[31]

A similar investigation into Oregon Health & Science University (OHSU) led to a $2.7 million fine after OHSU reported four data breaches impacting more than 500 individuals each, as well as a breach "on a cloud-based server without a business associate agreement."[32] The breaches were discovered in 2013 by a faculty member, who came across PII that included data patient diagnoses, credit card and payment information, medical procedures, photos, driver's license numbers and Social Security numbers on Google's Gmail and Drive cloud services, after it had been placed there by a university physician.[33]

In addition to operational disruption and statutory penalties, institutions may also face legal liability through private rights of action, if they are available. Even when no private right of action is available pursuant to statute (*e.g.*, there is no private right of action available under FERPA or HIPAA), various parties injured by institutional data breaches have sought relief both individually and in class litigation pursuant to state law tort claims. For instance, following a data breach involving academic and personal data of millions of current and former students and employees of the Maricopa County Community College District, the District was sued in a class-action lawsuit alleging negligence, negligence *per se* under two Arizona state statutes, breach of fiduciary duty, and breach of the right of privacy.[34]

Finally, the HITECH Act now permits State Attorneys General to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules.[35]

8. Specific Contractual Requirements

Institutions that have entered into contracts with the United States government have additional requirements depending upon applicable contract clauses. Over the last couple of years,

cybersecurity guidance and requirements for government contractors have continued to evolve, particularly with respect to Department of Defense contractors. Most significantly, a new Defense Federal Acquisition Regulation Supplement (DFARS) clause was published that requires certain federal government contractors to apply 15 basic cybersecurity safeguarding requirements and procedures to protect their information systems. All safeguarding requirements are based on security requirements published in the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171.[36]

This DFARS clause amends the Federal Acquisition Regulation (FAR) by adding requirements for "basic safeguarding" of contractors' information systems and applies to "covered contractor information systems", which are defined as systems owned or operated by contractors that "process, store or transmit federal contract information." [37] Federal contract information is defined as any "information provided by or generated for the government under a contract to develop a product or service." Examples of federal contract information include, but are not limited to, financial, export control, procurement and acquisition data. It does not include information that is meant for public release."[38]

Although educational institutions are engaged in primarily fundamental research, which by definition is meant for public release, many of these institutions own and/or operate federally funded laboratories, research and development centers, and/or other units that operate information systems that process, store or transmit federal contract information. Compliance with all 109 controls outlined in NIST SP 800-171 was required by December 31, 2017.[39] As stated in the background section of the rule in the Federal Register, "this new rule is just one step in a series of coordinated regulatory actions" that are a part of the recent surge in regulatory activity providing the guidance needed to help strengthen contractors' controls and practices around protecting government data.[40]

B. Before: Assessing Prevention Efforts and Preparing For a Data Breach

As cyberattacks evolve, colleges and universities should implement robust cybersecurity plans to protect intellectual property, safeguard the institution from significant operational destructions, and fulfill compliance obligations. Especially with regard to that last goal—to satisfy statutory and regulatory compliance obligations—institutional counsel should be involved in developing and reviewing data protection plans and breach protocol. In particular, counsel can offer valuable perspective in reviewing policies, assessing vulnerabilities, developing incident response plans, acquiring cyber insurance, and aligning vendor contracts with breach notification requirements. This work will also prepare attorneys advising the university in the event of a breach.

1. Ensure that the Institution has a Strong Information Security Policy

First and foremost, every institution should have a strong written information security policy[41], the purpose of which is to protect the confidentiality, integrity, and availability of institutional data as well as any information systems that store, process, or transmit institutional data. The policy should be approved by the highest level of leadership possible and communicated and practiced from the top. It must apply to all members of the institution, including all external parties who contract to provide services to the institution. An individual should be designated to head the institution's information security and privacy efforts. This individual must be empowered to make decisions quickly when necessary to safeguard systems or data.

A good policy will address at a minimum (a) the institution's objectives; (b) authorities, responsibilities, and duties of various stakeholders in the institution; (c) classification of data, data ownership, and data retention; (d) the regulatory framework within which the institution is operating (*e.g.*, NIST); and (e) privacy policies/issues. It will also include a clearly identified reporting mechanism for data breaches and suspected misuse of data — whether that is a separate reporting mechanism for information security or a cross-reference to an existing reporting mechanism (*e.g.*, a reporting mechanism that exists under an institution's loss of electronics devices protocol or policy).

An information security policy often is a high-level policy that comprises numerous more specific sub-policies and/or practices. For example, a university's computing policy might define acceptable behavior with respect to the use of the university's computing resources as well as privacy expectations with respect to student, faculty, and staff data. Another sub-policy might address the regulatory requirements of the GLBA. All policies, of course, are informed by and must be in compliance with applicable law, necessitating that the need for policy-level changes be vetted by legal counsel. Because the cybersecurity landscape is changing so rapidly, the policy should be reviewed on a regular basis and revised accordingly.

2. **Assess Vulnerabilities and Prevention Efforts**

With the backdrop of a high-level Information Security Policy and integrated sub-policies, counsel should meet with key institutional stakeholders to assess the control regimes that are in place to prevent, detect, and respond to a data incident and be involved in determining whether a data breach has occurred. Counsel also should meet with program leaders and team members to educate the university community about common IT security risks and effective solutions and practices to mitigate those risks. Important questions and considerations are as follows:

- What steps are taken by the IT department to regularly monitor for ongoing breaches? Is IT monitoring recurring phishing scams and notifying members of the university community when warranted?

- Does the university perform campus-wide user vulnerability testing and training for phishing susceptibility?

- Does the university periodically organize tabletop exercises to identify and address security gaps with respect to people, processes, technology, and facilities?

- Does the university require multi-factor authentication for high-value assets to reduce the impact of a successful phishing campaign? (In this authentication protocol, a divulged password is useless to the attacker without the second factor.)

[42] IT should cover the basics of patching, anti-virus protection, verified backups, strong passwords and multi-factor authentication, operating with minimal privileges, and user training. Year after year, security researchers find that the same basic hygiene and informed user behavior would have prevented the vast majority of cyber-attacks.[43] Basic system and network configuration, back-up protocols, encryption protocols, privileged account use, system and application patching status, authentication strength, security monitoring, and end-user awareness are among the areas that should be assessed, remediated, and reassessed on an

on-going basis. Mindful of these standard practices, counsel can develop questions for cybersecurity teams designed to assess vulnerabilities and strengthen prevention efforts.

3. Develop a Data Breach Incident Response Plan

One common practice in data breach risk mitigation is adopting a comprehensive incident response plan that outlines steps to take if a breach is suspected or occurs. Among other things, such a plan or protocol typically identifies who is responsible for what action when an institution becomes aware of an incident that could constitute a data breach. For instance, who is responsible for notifying the university president and general counsel? Also, who will be responsible for determining reporting obligations, remediating the breach, and the like? Who has the ultimate authority to determine whether a data breach has occurred? These plans typically detail vendors that may be needed or involved in responding to a breach, including contact information and pertinent contract details, such as response times or responsibilities in the event of an incident.

Counsel's role in the event of a data breach typically involves providing advice about:

- when and whether breach notification to affected individuals is required,
- whether insurance notification requirements are triggered,
- what state law and other notification requirements are triggered,
- whether law enforcement should be contacted,
- whether a forensic investigation should be conducted (and, if so, by whom), and
- whether any internal review will be conducted and whether the review can or should be subject to attorney-client privilege.

For institutions that have not yet created such a plan, various universities have posted detailed plans that could serve as templates.[44] Once developed, these plans ought to be tested periodically and revised regularly to account for, among other things, personnel changes.

4. Consider Cyber Insurance

Various providers offer insurance coverage that have been dubbed "cyber insurance" policies. Their scope of coverage varies widely, and counsel should review such policies carefully before an incident occurs to gain a realistic sense of whether the institution is protected and to what extent it is covered. In addition, protections provided by such policies typically have preconditions that institutions must comply with before coverage kicks in — in particular, notification requirements — that counsel should understand prior to an incident.

When considering whether to purchase cyber insurance or assessing coverage, counsel and other institutional officials may want to consider the following questions:

- Does the policy cover the cost of issuing notices to those impacted by a breach? If so, does the coverage give the institution the right to control how those notices are given?

- Does the policy refuse to cover or outright prohibit the institution from providing notifications that are not expressly required under a state data breach notification statute (i.e., "voluntary" notifications)?

- Does the policy cover the cost of providing credit monitoring, identity restoration services, or identity-theft insurance to those impacted by a breach? If so, are there any restrictions on when such items are covered?

- Does the policy cover regulatory proceedings and litigation costs that may result from a breach? If so, what are the coverage retentions and limits?

- Does the policy permit the organization to retain an attorney of its choice to help the organization investigate and document an incident, retain investigators if needed, identify statutory obligations to notify consumers and regulators, and advise the organization concerning steps that may reduce the likelihood of litigation or a regulatory investigation?

5. **Consider Data Breach Obligations When Drafting Vendor Contracts**

Institutions of higher education routinely share sensitive data with third-party providers, and data security is an important subject that should be addressed when writing and renewing contracts with any third party that will have access to sensitive institutional data. In addition to standard indemnification, limitations of liability, and insurance requirements, considerations in contract negotiations typically include the following:

- Conducting due diligence when comparing possible third-party providers to assess a provider's security infrastructure and environment

- Determining what will happen with data in the vendor's possession upon contract termination

- Requiring immediate notification of all breaches in security and sensitive data and making clear who is responsible for responding to the security breach, including the decision as to whether public disclosure is required

- Acquiring the right to monitor and/or audit the vendor's performance of its obligations, including the ability to allow the university's third-party auditors to conduct reviews on-site at the vendor

- Requiring university notification of all requests for disclosure of personal data by any party, including law enforcement or other government representatives, and providing the university with some degree of control over the response

- Acquiring and reviewing a copy of the vendor's privacy policy

- Requirements for returning or destroying data at the end of the contract

The Department of Education has also informally weighed in on this topic by identifying "Model Terms of Service" for "Protecting Student Privacy While Using Online Educational Services."[45]

C. During and After: The Role of Counsel When Put on Notice of a Data Breach

What are the key questions and considerations in-house university counsel should assess when receiving notice that the university has experienced a possible breach?

1. Immediate Mitigation and Incident Analysis

In all cases when there is a data breach, the institution's incident response team (or other group designated in the institution's Information Security Policy) should conduct straightforward mitigation efforts immediately, beginning with identifying the scope of the breach, assessing how the breach occurred, and taking immediate steps to limit further data loss. Of course, assessment of the extent of a breach may involve issues that require the assistance of specialized consultants to perform forensic analysis. Further, since insurance may cover only the cost of third party providers and not the internal response team, it is important to ensure that potential consultants are identified, under retainer, and equipped to rapidly assist.

2. Notify Insurer

Counsel or institutional risk management personnel should immediately review any applicable insurance coverage and notify the insurance carrier in accordance with policy requirements.

3. Consider Legal Obligations With Respect to Research Sponsors and Vendors

Depending upon the source of the breach, agreements with the federal and/or state government as well as private companies may be implicated. Counsel should immediately identify the relevant provisions of such agreements and fulfill any reporting or other obligations with respect to them.

4. Assess Notice Obligations to Those Impacted by Breach

Since the content of the compromised data may give rise to different legal obligations, early identification of the impacted data will significantly aid an assessment of reporting requirements and other obligations. This invariably is the most cumbersome and complicated issue for counsel to navigate. As a practical matter, counsel will need to know the geographic areas (i.e., the states) in which those potentially impacted by the breach are located as well as the type of information compromised, in order to assess institutional legal obligations.

Today, there is no national data breach notification law[46]; rather, legal notification requirements are state specific. As alluded to previously, while 47 states have developed their own data breach laws, those laws are more similar than not, and coverage typically hinges on an assessment of the following two questions:[47]

- Does the state data-reporting statute apply to the college or university?
- Does the disclosed personally identifiable information trigger notification? Keep in mind that some statutes do not require notification where the information could not reasonably be understood to have been accessed by unauthorized persons, such as the media was destroyed (e.g., a laptop fell in a volcano), or the data was unreadable through encryption. [48]

If coverage is established, institutions then typically wrestle with the following issues:

- When must notice be provided?
  Few state laws prescribe specific deadlines to provide impacted individuals with notice. Generally, though, the notification must occur in the "most expedient time possible and without unreasonable delay"[49]

- What information does the notice have to include?
  Many state laws do not provide any instruction or requirements concerning the content of a notification, leaving the content to the discretion of the organization. Other states mandate that specific information be included in the notification letters. Of course, to the extent states differ in the information that must be provided to those impacted, the content of notification letters will differ.

- How must the notice be provided?
  The majority of states require that those impacted by a breach be notified in writing. While email notice can provide substantial cost savings, notification through email is permitted only in approximately one-third of the states, and in those states there are restrictions on when email notice is permissible. In addition, there may be requirements to post to websites if physical addresses are not available. There are various vendors schools can use to manage this process as well as staff call centers to respond to queries prompted by the notice.

- Is notification required to any other parties?
  Various state statutes also require third-party notification. For instance, some states will require the organization to notify the three major credit-reporting agencies in the event of a breach involving a minimum number of affected persons. Others require notification to a state's Attorney General's office. Still others require law enforcement to be notified.

EDUCAUSE provides very helpful online resources/toolkits to assist higher education IT in this area.[50]

5. **Notify Law Enforcement**

The majority of cyber incidents involve a crime that has been committed or is in the process of being committed. For example, when someone attempts to hack into an organization's network to steal intellectual property or to obtain sensitive personal information, that person may be committing criminal trespass, theft, attempted identity theft, computer fraud, wiretapping, or economic espionage, among a host of other statutory violations. When a crime is being committed, the organization should consider reporting it to law enforcement. Contacting law enforcement may help stop the criminal behavior and can make available services to protect networks from further attack or provide intelligence that can help in building a resilient defense.

There is no single federal or state law enforcement agency with jurisdiction over data breaches. However, the FBI has a Cyber Task Force in each of its 56 field offices. During an incident, the Cyber Task Force can deploy personnel such as a Computer Analysis Response Team, a Cyber Action Team, and other investigators and analysts with expertise in addressing cyber incidents that may affect a network. Working with the FBI does not mean that the collaboration

will lead to an investigation. The FBI coordinates with each organization to determine the best course of action to address an incident.[51]

6. **Mitigation and Remediation**

Given the potential financial exposure and reputational harms associated with data breaches, it is essential to consider possible ways to mitigate these damages as promptly as possible. Ensuring that there is a crisis communications strategy is essential in mitigating reputational harm. Regarding mitigating potential financial exposure, many higher education institutions offer remediation services to assist affected persons immediately following a data security breach. These typically include credit monitoring services, identity theft insurance, identity theft help information packets, and/or compensation for identity theft.

CONCLUSION:

All industries are susceptible to data breaches, but the challenges facing institutions of higher education are unique because of the amount of sensitive data and valuable intellectual property generated by these institutions and the decentralized and collaborative ways in which these institutions operate. College and university leaders can serve their institutions best by educating the appropriate offices about the risks and the legal frameworks and supporting the policies and planning that will enable the institution to handle what increasingly seems to be an inevitable risk of maintaining an IT infrastructure.

END NOTES:

[1] Sandra A. Brown is assistant general counsel and assistant vice president of Carnegie Mellon University and general counsel to the Software Engineering Institute. Scott D. Schneider is a partner in the Austin office of Husch Blackwell LLP and a member of the firm's Education team.

[2] A malicious insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. "Common Sense Guide to Mitigating Insider Threats, Fifth Edition," *Carnegie Mellon University* (Dec. 2016).

[3] According to a report from McAfee Labs, various records have market prices on the "Dark Web." For instance, credit card numbers coupled with the three-digit value printed on the back of the cards fetch around $5-$8 for each number. If a hacker can secure the cardholder's date of birth, the value increases to $15. If full information on the cardholder is available—*i.e.*, full name, billing address, Social Security number, mother's maiden name—the market price is $30. McAffee, "The Hidden Data Economy: The Marketplace for Stolen Digital Information," *McAfee Labs* (Dec. 2015).

[4] Joshua Bolkan, "Education Data Breaches Double in First Half of 2017," *Campus Technology* (Sep. 20, 2017).

[5] Nicole Perlroth, "Penn State's College of Engineering Hit by Cyberattack," *The New York Times* (May 15, 2015).

[6] Janet Gilmore, "Campus Alerting 80,000 Individuals to Cyberattack," *Berkeley News* (Feb. 26, 2016).

[7] Kelly Heyboer, "Who Hacked Rutgers? University Spending up to $3M to Stop Next Cyberattack," *NJ.com* (Aug. 23, 2015).

[8] Drew Harwell, "Former Employee Sued by Tesla Says he was a Whistleblower, Alarmed by Company Practices and Elon Musk," *The Washington Post* (June 21, 2018).

[9] Lora Kolodny, "Elon Musk Emails Employees about 'Extensive and Damaging Sabotage' by Employee," *CNBC* (June 18, 2018).

[10] The space constraints of this NACUANOTE do not allow for a detailed treatment of the applicable laws in the area. For more comprehensive treatment of the applicable laws, see John L. Nicholson and Meighan E. O'Reirdon, *Data Protection Basics: A Primer for College and University Counsel*, 36 J.C. & U.L. 101 (2009); Katie Beaudin, *College and University Data Breaches: Regulating Higher Education Cybersecurity Under State and Federal Law*, 41 J.C. & U.L. 657 (2015).

[11] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

[12] 34 C.F.R. §99.31 (a)(1)(ii).

[13] *Id.*

[14] While FERPA does not have a required data-breach protocol, in June 2017, the Department of Education published extensive practical guidance and "best practices" regarding steps institutions should take to protect students' education records, including how to respond to various data breach scenarios involving educational records. *See* U.S. Dep.'t of Education Technical Assistance Center and the Family Policy Compliance Office, Data Breach Response Training Kit (last updated June 2017).

[15] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq.

[16] 16 C.F.R. § 313.1.

[17] The definition of "creditor" for purposes of FACTA "means a creditor as defined in Section 702 of the Equal Credit Opportunity Act (15 U.S.C. 1691a) that regularly and in the ordinary course of business (i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction; (ii) furnishes information to consumer reporting agencies . . . in connection with a credit transaction; or (iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds . . . . " 15 U.S.C. 1681m(e)(4).

[18] 16 C.F.R. § 681.1 (b) (3).

[19] A higher education institution may be a "covered entity" under HIPAA if it: (1) provides health care services *and* (2) engages in one or more covered electronic transactions. Electronic transactions include health care claims, health care payments, coordination of benefits, eligibility for a health plan, and enrollment in a health plan. Health Insurance Portability and Accountability Act, 45 C.F.R. §160.103.

[20] *Id.* at § 164.103. They are ordinarily "hybrid entities," with a health care component required to comply with HIPAA, and a non-healthcare component that does not have HIPAA compliance obligations. Proper designation, and periodic review and revision, of the healthcare and non-healthcare components is critical to ensure that data security measures are followed by the appropriate parts of the institution.

[21] Pub. L. 104-191.

[22] HIPAA specifies that "PHI" is any individually identified health information that relates to the individual's past, present, or future physical or mental health condition or any other information that can be used to identify the individual. 45 CFR § 160.103.

[23] The Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. § 300jj et seq.

[24] EDUCAUSE, "The General Data Protection Regulation Explained," (Aug. 28, 2017).

[25] The General Data Protection Regulation, Recital 14: "The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data."

[26] For an excellent summary of these state laws, see Foley and Lardner, LLP, "State Data Breach Notification Laws," (Sept. 10, 2018).

[27] California Civil Code, § 1798.82 (2014).

[28] *Id.* at § 1798.81.5 (2014).

[29] Whether such state laws can in fact be enforced against institutions domiciled in other states is an unsettled legal issue. *See e.g.*, *Daimler AG v. Bauman*, 571 US 117 (2014).

[30] U.S. Dep.'t of Health and Human Services, "Multiple Alleged HIPAA Violations Result in $2.75 Million Settlement with the University of Mississippi Medical Center (UMMC)," (content reviewed on July 21, 2016).

[31] *Id.*

[32] Joseph Conn, "Feds Settle Data Breach Case with Oregon Health and Science University for $2.7 Million," *Modern Healthcare* (July 20, 2016).

[33] *Id.*

[34] *See* Complaint, *Roberts, et al, v. Maricopa County Community College District*, No. 2014-007411 (Sup. Ct. Ax. Apr. 28, 2014)

[35] 42 U.S.C. 1320d-5(d).

[36] Defense Federal Acquisition Regulation Supplement, 48 CFR 252.204-7012.

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] Federal Acquisition Regulation; Basic Safeguarding of Contractor Information Systems, 81 FR 30439 (May 16, 2016).

[41] *See, e.g.,* Harvard University Information Security Policy; University of Louisville, Information Security Policy and Standards (originally adopted July 23, 2007).

[42] Beware, though, that this approach does not provide a "silver bullet." Multi-factor authentication is on the radar of attackers, and there have already been successful attacks in spite of its use.

[43] "The takeaway from the [2018] Verizon Data Breach Investigations Report is depressingly familiar: Of the 1,935 breaches analyzed, 88 percent were accomplished using a familiar list of nine attack vectors, meaning they could probably have been prevented by a few simple cyber-hygiene measures." Shaun Waterman, "Verizon's Annual Data Breach Report is Depressing Reading Again," *CyberScoop* (Apr. 27, 2017).

[44] *See, e.g.,* University of California, *Privacy and Data Security Incident Response Plan*, (updated July 1, 2012); New York University, IT Security Information Breach Notification Policy (July 19, 2006).

[45] U.S. Dep.'t of Education, Privacy Technical Assistance Center and the Family Policy Compliance Office, "Protecting Student Privacy While Using Online Educational Services: Model Terms of Service," (March 2016).

[46] This may change. Multiple data breach notification bills have been considered by Congress over the last several years including the Data Security and Breach Notification Act of 2015, which would require organizations to implement reasonable and appropriate cybersecurity measures and notify customers when personally identifiable information has been or may have been compromised. Majority support for such legislation seems to require the creation of a single, national data breach notification standard that would establish full preemption over individual state data breach laws.

[47] Mintz Levin, *State Data Security Breach Notification Laws* (June 1, 2018) (summarizing state-law data breach notice requirements).

[48] *E.g.*, New Jersey defines a breach as unauthorized access to personal information when access to the personal information has not been secured by encryption or by any other method or technology that

renders the personal information unreadable or unusable. New Jersey Identity Theft Prevention Act (2005).

[49] *See, e.g.* Del. Code Ann. tit 6 sec. 12B-101-104, as amended (2017).

[50] EDUCAUSE, Data Incident Notification Toolkit (last updated May 11, 2015).

[51] *See* The Federal Bureau of Investigation, "What We Investigate: Cybercrime," (last accessed Oct. 11, 2018) (describing how the FBI investigates and addresses cyberattacks).

NACUANOTES Issues | Contact Us | NACUA Home Page

NACUANOTES Copyright Notice and Disclaimer

Copyright 2018 by Sandra A. Brown, Esquire, and Scott D. Schneider. NACUA members may reproduce and distribute copies of NACUANOTES to other NACUA members and to persons employed by NACUA member institutions if they provide appropriate attribution, including any credits, acknowledgments, copyright notice, or other such information contained in the NACUANOTE.

This NACUANOTE expresses the viewpoints of the authors and is not approved or endorsed by NACUA. This NACUANOTE should not be considered to be or used as legal advice. Legal questions should be directed to institutional legal counsel.