Coping with Cyber Attacks and Data Breaches: Legal and Operational Issues

Lawrence White
Vice President and General Counsel
University of Delaware
Newark, Delaware

Table of Contents

| I.  | The Prevalence of Cyber Attacks and Data Breaches in Higher Education Today | 2 |
| II. | How to Prepare For, and Minimize the Impact of, a Data Breach               | 4 |
|     | A. Before a data breach                                               | 4 |
|     | B. What to do when (and after) a breach occurs                         | 6 |
| III.| The Legal Obligation to Provide Timely Notice                           | 7 |
|     | A. State notification laws                                             | 7 |
|     | B. Federal statutory and regulatory notice requirements                 | 9 |
COPING WITH CYBER ATTACKS AND DATA BREACHES:  
LEGAL AND OPERATIONAL ISSUES

I. THE PREVALENCE OF CYBER ATTACKS AND DATA BREACHES IN HIGHER EDUCATION TODAY

A. “Security experts like to say that there are now two types of company: those which know they have been hacked and those which have been hacked without realising it.” 

B. University computer systems are particularly inviting targets for hackers, for several reasons:


(2) Open architecture. In contrast to for-profit corporations, which tend to operated proprietary systems with limited access, college and university computer systems embrace access, including access by some users—think teen-aged students—who cherish access from all points at all times with a minimum of security interference. As a result, central computer systems are notoriously difficult to secure, are prone to cyber attack, and—in a mutually reinforcing cycle—are known to be prone to attack, which increases their visibility as targets.
Some universities cut corners in times of budget-cutting and financial austerity. In 2006, an information technology official at Emory University named Jay Flanagan prepared a report titled *Surveying the Steps to a Secure Emory University*. Mr. Flanagan surveyed institutions to identify what he called the “barriers to effective security.” From that report:


Cost vulnerability manifests itself in one other way. University IT departments tend to use hundreds or even thousands of software programs and platforms, many procured from large national vendors. Those platforms must be updated or “patched” constantly as data security experts identify new vulnerabilities. When patch announcements are posted on vendor web sites, hackers almost instantaneously get to work attacking vulnerabilities. If there is a delay—even one measure din seconds or minutes—in downloading and installing the latest patch, chaos can ensure. “Information officers say they have also learned the hard way that when a software publisher like Oracle or Microsoft announces that it has discovered a security vulnerability and has developed a ‘patch’ to correct it, systems need to apply the patch right away. As soon as such a hole is disclosed, hacker groups begin designing programs to take advantage of it, hoping to release new attacks before people and organizations get around to installing the patch. ‘The time between when a vulnerability is announced and

II. HOW TO PREPARE FOR, AND MINIMIZE THE IMPACT OF, A DATA BREACH

[Note: In 2000 EDUCAUSE, with assistance from Internet 2, organized an important working group known as the Higher Education Information Security Council, or “HEISC.” HEISC’s mission is to improve information security, data protection, and privacy programs in higher education. The extraordinary HEISC web site (http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative/about) offers an extraordinary array of resources, model policies, and practical advice for organizing institutions’ approaches to data security and coping with data breaches. Foremost among these resources is the Information Security Guide: Effective Practices and Solutions for Higher Education, available at https://wiki.internet2.edu/confluence/display/itsg2/Home. This section of this outline borrows heavily from concepts and organizing themes in the Guide.]


(1) Establish and, if resources permit, staff an “Information Security Program.” Ideally, one full-time person would be designated as the institution’s IT Security Director with responsibilities to stay current in the field and ensure that institutional policies are up to date.

(2) Develop and disseminate a comprehensive “Security Awareness Plan” that sensitizes users to the need for security vigilance. Be sure the plan addresses security concerns emanating from student use of social media, which is absolutely ubiquitous on campus today.

As part of the plan, organize a security awareness web site. For content and design hints, see Developing Your Campus Information Security Website, https://wiki.internet2.edu/confluence/display/itsg2/Developing+Your+Campus+Information+Security+Website.

(3) Pay attention to simple, memorable, well-tested ways to spread the message—e.g., punchy phrases (see http://www.nativeintelligence.com/ni-free/awareness-slogans.asp) and campus posters (see https://web.chapman.edu/information[-]securityuploadcontestresults.aspx and the illustrative example below).
(4) Be sure vendor contracts are negotiated carefully and with due regard for institution-protective guarantees and warranties on data security. Prepare requests for proposals carefully and with input from counsel experienced in drafting them. From Data Protection Contractual Language, https://wiki.internet2.edu/confluence/display/itsg2/Data+Protection+Contractual+Language:

Consider the following when drafting or reviewing an RFP:

- Clearly define the data to be protected.
- Define specifically your information security requirements (needs) and clearly differentiate between what is needed and what is wanted. The items below depend from these first two points.
- To the extent possible, include all security requirements in a separate and clearly identified section of the RFP. If security requirements are dispersed throughout multiple sections of the RFP it is difficult to identify and consider them as a separate evaluation criteria.
- Not only tell vendors what you require but ask them how they propose to meet the requirements. Also, consider asking what alternatives are available in case requirements cannot be met. Just listing the requirement or asking a Yes/No question will not elicit meaningful and specific responses.

(5) Do some basic business continuity planning. See Business Continuity Planning, https://wiki.internet2.edu/confluence/display/itsg2/Business+Continuity+Planning. At its most rudimentary, continuity planning involves:

- Establishing an emergency operations team, the members of which can be summoned on short notice. Key members of the team might include the IT Director, General Counsel, Communications Director, Public Safety Director, and (if the institution has one) IT Security Director.
- Co-locating backup IT services.
- Preparing (and constantly updating) an inventory of computer systems and servers, identifying for each one the sensitive personal data it contains and the business functions that need access to the system.

B. What to do when (and after) a breach occurs. From Sensitive Data Exposure Incident Checklist, https://wiki.internet2.edu/confluence/display/itsg2/Incident+Checklist:

STEP 1: Identification

Verify that an incident has actually occurred. This activity typically involves the Unit systems administrator and end user, but may also result from proactive incident detection work of the Security Office or central IT operations. If it is determined that an incident has occurred, inform appropriate authorities.

STEP 2: Damage Containment and Data Exposure Assessment

Identify an Incident Response Lead and assemble an incident response team charged with limiting further damage from the incident. Conduct a thorough assessment of the type and scope of data exposed following applicable laws, regulation and policy.

STEP 3: Eradication and Recovery

Take steps to remove the cause of the exposure, reduce the impact of the exposure of the sensitive data, restore operations if the incident compromised or otherwise put out of service a system or network, and ensure that future risk of exposure is mitigated.
Often, this step involves difficult judgment calls about whether and when to take a system offline. Doing that can result in sudden dysfunctions in critical administrative and academic computing systems. Figuring out how to notify users and how to estimate how long systems will be down can be a high-stress endeavor.]

STEP 4: Notification

Determine the need to give notice to individuals whose data may have been exposed by the incident. Swiftness in notifying those affected by a breach of personally identifiable information (PII), as well as informing certain government entities, is legally mandated in many states and, depending on the nature of the data, also federal law. Speed is also important from a public relations standpoint. To this end, many of the sub-steps can and should be undertaken in parallel to accommodate these needs.

[This is the subject of the next section of this outline.]

[Important policy question: Should notification be undertaken using internal resources, or should the institution retain an outside vendor with expertise preparing and delivering required notices?]  

STEP 5: Follow-up

Identify lessons learned from the incident, implement any remediation needs, and securely store a complete record of the incident.

III. THE LEGAL OBLIGATION TO PROVIDE TIMELY NOTICE

[Note: For an excellent summary of data breach notification requirements, see Gina Stevens, Data Security Breach Notification Laws (Congressional Research Service, April 10, 2012), reprinted at http://www.fas.org/sgp/crs/misc/R42475.pdf. That reference work informed this part of the outline, and is liberally cited in what follows as “Stevens.”]

A. State notification laws. “Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have laws requiring notification of security breaches involving personal information. Federal statutes, regulations, and a memorandum for federal departments and agencies require certain sectors (healthcare, financial, federal public sector, and the Department of Veterans Affairs) to implement information security programs and provide notification of security breaches of personal information. … Alabama, Kentucky, New Mexico, and South Dakota do not have security breach notification laws.” Stevens i, 4.
“State security breach notification laws generally follow a similar framework and can be categorized into several standard elements: (1) delineating who must comply with the law; (2) defining the terms ‘personal information’ and ‘breach of security;’ (3) establishing the elements of harm that must occur … for notice to be triggered; (4) adopting requirements for notice; (5) creating exemptions and safe harbors; (6) clarifying preemption and relationships to other federal laws; and (7) creating penalties, enforcement authorities, and remedies.” Id. 5.

How quickly notice must be given after discovery of a breach is a recurring issue of some significance in construing state notice statutes. From one exemplar, Delaware’s recently enacted law on data security breaches, 6 Del. C. § 12B-102(a), http://delcode.delaware.gov/title6/c012b/:

Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

An interesting table: when the University of Delaware suffered a fairly large-scale hacking incident in the summer of 2013, we did some research on elapsed time between detection and notice at colleges and universities, as reported in newspaper and media accounts. Here is an expurgated version of the summarizing table we prepared:

<table>
<thead>
<tr>
<th>Institutional descriptor</th>
<th>Reported date of breach</th>
<th>Reported date of awareness</th>
<th>Date notice sent</th>
<th>Approximate no. of notices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community college</td>
<td>3/1/11</td>
<td>1/1/13</td>
<td>3/25/13</td>
<td>3,300</td>
</tr>
<tr>
<td>Regional state university</td>
<td>2/19/13</td>
<td>2/19/13</td>
<td>3/11/13</td>
<td>25,000</td>
</tr>
<tr>
<td>Regional state university</td>
<td>5/21-9/24/2012</td>
<td>10/5/12</td>
<td>10/8/12</td>
<td>279,000</td>
</tr>
<tr>
<td>Large state flagship university</td>
<td>6/6/12</td>
<td>8/1/12</td>
<td></td>
<td>34,000</td>
</tr>
<tr>
<td>Large state flagship university</td>
<td>5/23/12</td>
<td>5/23/12</td>
<td>5/25/12</td>
<td>655,000</td>
</tr>
<tr>
<td>Community college</td>
<td>3/28/12</td>
<td>3/28/12</td>
<td>4/23/12</td>
<td>87,000</td>
</tr>
<tr>
<td>Large public research university</td>
<td>10/19/11</td>
<td>10/24/11</td>
<td>11/10/11</td>
<td>176,000</td>
</tr>
<tr>
<td>Large state flagship university</td>
<td>5/25/11</td>
<td>6/25/11</td>
<td>8/10/11</td>
<td>79,000</td>
</tr>
<tr>
<td>Ranch campus of a large state flagship university</td>
<td>3/15/11</td>
<td>6/9/11</td>
<td>12,000</td>
<td></td>
</tr>
<tr>
<td>Private university</td>
<td>12/12/10</td>
<td>12/13/10</td>
<td>12/20/10</td>
<td>12,000</td>
</tr>
<tr>
<td>Large state flagship university</td>
<td>Late 10/2010</td>
<td>12/15/10</td>
<td>760,000</td>
<td></td>
</tr>
<tr>
<td>Large state flagship university</td>
<td>10/26/10</td>
<td>11/30/10</td>
<td>60,000</td>
<td></td>
</tr>
<tr>
<td>Regional state university</td>
<td>9/24-9/29/2010</td>
<td>9/29/10</td>
<td>10/15/10</td>
<td>107,000</td>
</tr>
<tr>
<td>Private university</td>
<td>6/1/10</td>
<td>7/16/10</td>
<td>93,000</td>
<td></td>
</tr>
<tr>
<td>Large public research university</td>
<td>7/28/10</td>
<td>7/13/10</td>
<td>34,000</td>
<td></td>
</tr>
<tr>
<td>Large public research university</td>
<td>4/5/10</td>
<td>4/8/10</td>
<td>7,000</td>
<td></td>
</tr>
<tr>
<td>Regional state university</td>
<td>11/11/09</td>
<td>12/11/09</td>
<td>2/22/10</td>
<td>170,000</td>
</tr>
</tbody>
</table>
A few interesting summarizing data:

- The lapse between date of breach and date of detection ranged from instantaneous to almost two years, and typically ran to about a week.
- The lapse between detection and notice to affected individuals was typically a few weeks and was occasionally—rarely, but occasionally—more than a month.
- The number of persons to whom notice was sent ranged from a low of a few thousand to a high of three-quarters of a million. The average number was about 150,000.

B. **Federal statutory and regulatory notice requirements.** “The legal and regulatory framework for the protection of personally identifiable information is complex because businesses, governments, and individuals who process data must comply with the requirements of many differing privacy, information security, and breach notification laws. No single federal law or regulation governs the security of all types of sensitive personal information. Determining which federal law, regulation, and self-regulatory guidance is applicable depends in part on the entity or sector that collected the information, and the type of information collected and regulated.” Stevens 7.

1. **HIPAA-protected health information.** “Part C of the Health Insurance Portability and Accountability Act of 1996[, 42 U.S.C. §§1320d et seq.] (HIPAA) requires ‘the development of a health information system through the establishment of standards and requirements for the electronic transmission of health information.’” … [HIPAA] require[s] the Secretary of Health and Human Services to adopt national standards to facilitate the electronic exchange of information … [and] protect the privacy of individually identifiable health information …. HIPAA covered entities—health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically—are required to comply with the national standards and regulations.” Id. 11.

In compliance with HIPAA, the Department of Health and Human Services has adopted two “rules”—a euphemism for lengthy, arcane sets of federal regulations—that apply to institutions that collect and store so-called “protected health information” (“PHI”):

(a) **The HIPAA Privacy Rule.** The Privacy Rule imposes three distinct obligations on institutions that collect PHI:

1. The Privacy Rule requires a covered entity to maintain reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.
(2) The Privacy Rule limits the circumstances under which PHI may be used or disclosed. A covered entity is permitted to use or disclose protected health information without patient authorization for treatment, payment, or health care operations; otherwise, PHI cannot be used or disclosed except with authorization from the subject of the records.

(3) If the institution engages companies to store or otherwise have access to PHI, the institution must enter into a formally structured “business associate agreement” with each such company establishing minimum privacy protections for PHI.

(b) The HIPAA Security Rule. This rule, which applies only to PHI in electronic form (“E PHI”), requires a covered entity to ensure the confidentiality, integrity, and availability of all EPHI the covered entity creates, receives, maintains, or transmits. “Covered entities must protect against any reasonably anticipated threats or hazards to the security or integrity of such information and any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule and ensure compliance by their workforces.” Id. 12-13.

(2) The HITECH Act. “The Health Information Technology for Economic and Clinical Health Act (HITECH Act) was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA). As part of this new law, sweeping changes to the health information privacy regime were enacted. Most of the privacy provisions are additional requirements supplementing the HIPAA Privacy and Security Rules, but a few provisions deal specifically with electronic health records (EHRs). The HITECH Act … established new limits on the use of protected health information for marketing and fundraising purposes; provided new enforcement authority for state attorneys general to bring suit in federal district court to enforce HIPAA violations; increased civil and criminal penalties for HIPAA violations; required covered entities and business associates to notify the public and HHS of data breaches; changed certain use and disclosure rules for protected health information; and created additional individual rights.” Id. 13.

For our purposes, the most important provisions in the HITECH Act are the ones that impose breach notification requirements on covered entities. “The HITECH Act requires covered entities, business associates, and vendors of PHRs to notify affected individuals in the event of a ‘breach’ of ‘unsecured protected health information.’ A ‘breach’ is defined as the ‘unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information ….” Id. 15.
(3) *Gramm-Leach-Bliley.* “Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) requires financial institutions to provide customers with notice of their privacy policies and requires financial institutions to safeguard the security and confidentiality of customer information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. Financial institutions are defined as businesses that are engaged in certain ‘financial activities, … [including] traditional banking, lending, and insurance functions, along with other financial activities.’”