THE RISKS AND LIABILITY OF GOVERNING BOARD MEMBERS TO ADDRESS CYBER SECURITY RISKS IN HIGHER EDUCATION

BY LUIS J. DIAZ, MARIA C. ANDERSON,
JOHN T. WOLAK AND DAVID OPDERBECK*

I. Introduction

Technological innovation now makes it possible to conduct business at the speed of thought. The resulting mass of data resulting from the "internet of things"[1] is stored on remotely-connected servers located throughout the world. While the benefits of this innovation revolution undoubtedly benefit society, business, and institutions of higher education, it also creates incremental risks in the form of data breach disasters when personally identifiable information (PII) and other sensitive information about customers, employees, and business partners is inadvertently disclosed.

Today, the news is filled with horror stories of such data breach disasters at some of the world's leading organizations. It seems that no one is immune from a data breach. In the aftermath of such an event, stock prices can plummet, public opinion shifts, and officers and directors can be terminated for failure to exercise best judgment in monitoring and mitigating those risks. The recent breaches at Target Corp.[2] and Parsippany, New Jersey-based Wyndham Worldwide Corp.[3] exemplify the tsunami of litigation that is likely to result when a major breach occurs. But, this is just the beginning as the duty of officers and directors relating to these global economy realities is just beginning to evolve. With the changing standards now emerging in the case law, it is reasonably foreseeable that there will be many more data breach related lawsuits in the future. As evidence of this fact, the Securities and Exchange Commission issued guidance in 2011 that it deems technology and privacy breaches as potentially material. SEC Chairwoman Mary Jo White has said that cyber threats are "of extraordinary and long-term

---

* Maria C. Anderson is Associate University Counsel for Montclair State University. Luis J. Diaz is a Director and Chief Diversity Office for Gibbons P.C., and focuses his practice on a broad range of technology related matters. John T. Wolak is a Director at Gibbons who focuses his practice on a broad range of commercial and insurance related matters. David Opderbeck is a Professor at Seton Hall University's School of Law and Director of the Gibbons Institute of Law, Science and Technology. In recognition of her extensive editorial assistance, the authors express gratitude to June Kim, Associate at Gibbons.

1 Peter T. Lewis, Speech, CONGRESSIONAL BLACK CAUCUS FOUNDATION 15TH ANNUAL LEGISLATIVE WEEKEND, September 1985. See also, International Telecommunications Union, ITU Internet Reports: The Internet of Things, November 2005, available at: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf.

2 See, infra, n. 6.

3 Federal Trade Commission v. Wyndham Worldwide Corporation, U.S. District Court for New Jersey, Civil Action No. 2:13-CV-01887-ES-JAD.

seriousness. They are first on the (SEC's) division of (market) intelligence's list of global threats, even surpassing terrorism."[4]

In light of these new world realities, officers and directors at all types of organizations, including colleges and universities, would be well advised to ensure that their organizations engage in a thoughtful process to implement adequate physical, electronic, and other security measures to prevent, manage, and respond to data breaches. The failure to do so can result in what happened at Target, where seven of ten directors were unseated because they failed to adequately manage cyber risks. Aside from the risk of breach-related litigation, it is also reasonably foreseeable that both federal and state regulators will become increasingly more aggressive in terms of regulatory compliance, fines, and monitoring activities.

Higher education institutions and their officers and directors are not exempt from these obligations. Many state laws impose a fiduciary duty upon boards of governors or trustees and administrators of public and private universities that require engaging in a robust due diligence process to ensure that cyber risks are properly identified and managed. This article seeks to provide some practical guidance concerning the federal and state laws applicable to higher education, and how officers and directors at these institutions can implement adequate policies, procedures, and practices to mitigate cyber risks and threats relating to potential data breaches.

II. Director and Officer Fiduciary Duties in the Face of Cyber Security Issues

Public awareness of director and officer liability for cyber attacks was elevated after a breach of consumer records at Target.[5] In reliance upon case law recognizing a board's obligation to oversee corporate risk post-Target, commentators suggested that liability for failure to monitor cyber-risk could be imputed to individual board members who were not discharging their fiduciary obligations by either: (a) "utterly" failing to implement "any reporting or information system or controls"; or (b) if such reporting or information systems were in place, consciously failing to monitor or oversee them so that board members were "disabled from being

4 Mary Jo White, Opening Statement at SEC Roundtable on Cybersecurity, U.S. SECURITIES AND EXCHANGE COMMISSION, March 26, 2014, available at https://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468.

5 After the breach of consumer records by Target, a shareholder derivative suit was filed in 2013 in the District of Minnesota alleging that board members breached their fiduciary duties to the company by failing to maintain adequate controls to ensure the security of data affecting as many as 70 million customers who shopped at Target between November 27, 2013 and December 15, 2013. See Kulia v. Steinhafel, No. 14-CV-00203 (D. Minn. July 18, 2014). An audit commissioned through Institutional Service Shareholders recommended seven out of Target's ten board members be removed after the data breach. See Kavita Kumar, Most of Target's Board Members Must Go, Proxy Advisor Recommends, Star Tribune, May 29, 2014, http://www.startribune.com/most-of-target-s-board-should-go-proxy-adviser-recommends/260960251/. The data breach required Target to defend its board members under public scrutiny in response to pressure from an influential shareholder. See Kavita Kumar, Target Board Defends its Role, Before and After Data Breach, Star Tribune, June 4, 2014, http://www.startribune.com/target-board-defends-its-role-before-and-after-data-breach/261527581/. Although the Board remained intact, Target replaced its Chief Executive Officer following the breach and appointed a new Chief Information Officer. See Kavita Kumar, Target's 10 Member Board Survives Vote of Shareholders, Star Tribune, July 2, 2014, http://www.startribune.com/june-12-target-s-board-survives-vote-of-shareholders/262727811/.

informed of risks or problems requiring their attention."[6] Therefore, University officials should be mindful of the legal risks posed to the members of their governing boards by ensuring they take an active role in the assessment of risk associated with information security systems selected for implementation and are regularly updated through reporting systems.[7]

In the United States, there are a multitude of sources that may impose liability upon board members for lapses in judgment related to cyber security. These sources may be found in federal laws – such as the Fair Credit Reporting Act, the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), Family Educational Right to Privacy Act (FERPA), and the Federal Information Security Management Act (FISMA) – or state and common laws. Potential plaintiffs include the Federal Trade Commission, the U.S. Securities and Exchange Commission, the Department of Justice, state attorneys general, and the individuals or companies whose data has been breached.[8] Higher education is particularly vulnerable to data breaches because, as the U.S. Department of Education has noted, "[c]omputer systems at colleges and universities [are] favored targets because they hold many of the same records as banks but are much easier to access."[9]

In a survey conducted by the Association of Governing Boards of Universities and Colleges and United Educators found that, while full boards have been increasingly engaged in risk discussions, "conflicting answers on the amount and quality of information boards receive on risk raised questions about the value of that information."[10] While 60 percent of respondents to that survey reported that the information boards received – particularly in connection with financial risks – was adequate, only 39 percent strongly agreed that enough information was shared to fulfill their legal and fiduciary duties."[11] Accordingly, because the failure of a board to actively address cyber risk management and information security risks can impose liability upon individuals,[12] members of governing boards must be provided adequate information in order to discharge their fiduciary duties.[13]

---

6 Eduardo Gallardo and Andrew Kaplan, Board of Directors' Duty of Oversight and Cybersecurity, Delaware Business Court Insider, August 20, 2014 (citing Stone v. Ritter, 911 A.2d 362, 370) (Del. 2006) and relying upon In re Caremark Int'l Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996)).

7 Foley and Lardner LLP, Taking Control of Cybersecurity: A Practical Guide for Officers and Directors, March 11, 2015, available at http://www.foley.com/taking-control-of-cybersecurity-a-practical-guide-for-officers-and-directors-03-11-2015/.

8 See Noah G. Susskind, Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know, 11 N.Y.U. J. L. & Bus. 573, 603 (2015).

9 Family Educational Rights and Privacy Act, 73 Fed. Reg. 74806, 74843 (Dec. 9, 2008) (codified at 34 CFR §99) available at http://www2.ed.gov/legislation/FedRegister/finrule/2008-4/120908a.pdf.

10 See Association of Governing Boards of Universities and Colleges, A Wake-Up Call: Enterprise Risk Management at Colleges and Universities Today at 2 (2013), available at http://agb.org/sites/agb.org/files/RiskSurvey2014.pdf.

11 Id.

12 Susskind, supra note 5, at 603.

13 Salar Ghahramani, Fiduciary Duty and the Ex Officio Conundrum in Corporate Governance:

Although the Sarbanes-Oxley Act has limited application to higher education, it has raised expectations of accountability in governance, regardless of whether a governing board manages a corporation or not-for-profit institution.[14] Members of not-for-profit governing boards who fail to meet the expectations of this Act may find themselves subject to removal or may not be indemnified in the event of suit by affected students, alumni, or employees.[15] Board members of not-for-profit institutions, whether public or private universities, may be subject to director and officer liability suits for failing to discharge their duties by broader classes of plaintiffs that may include other board members, donors, employees, students, vendors, contractors, other not-for-profit entities working in collaboration with the institution, and/or government agencies with regulatory authority over the institution.[16] While suits based upon such causes of action have thus far largely settled or been dismissed based upon failure to demonstrate causation or damages related to identity theft, suits continue to be filed, and the technological capacity to identify the use of such information continues to develop and requires constant monitoring to evaluate its evidentiary potential in damage claims.[17]

Governing boards of higher education institutions are commonly referred to as "the guardians" of the university and, as such, owe fiduciary duties of care and loyalty similar to their counterparts at for-profit corporations.[18] The degree of their fiduciary obligations vary, depending upon the institution's bylaws. However, as a general rule, board members must promote the institution's best interest, disclose

---

The Troublesome Murkiness of the Gubernatorial Trustee's Obligations, 10 Hastings Bus. L.J. 1, 11 (2014).

14 Lyman P.Q. Johnson & Mark A. Sides, Corporate Governance and the Sarbanes-Oxley Act: The Sarbanes-Oxley Act and Fiduciary Duties, 30 Wm. Mitchel L. Rev. 1149, 1223-1224 (2004).

15 See N.Y. Not-for-Profit Corp. Law § 722 (2014). See also, Vacco v. Diamandopoulos, 715 N.Y.S. 2d 269 (N.Y. Sup. Ct.,1998) (defendants, as former university trustees, were held financially accountable for mismanagement of the university's assets and held to violate the duties of care and loyalty owed to the university). See also, N.Y. Not-for-Profit Corp. Law § 717 (directors are required to discharge their duties in good faith and "with the care an ordinarily prudent person in a like position would exercise under similar circumstances").

16 Joseph Anthony Valenti, Know the Mission: A Lawyer's Duty To a Nonprofit Entity During An Internal Investigation, 22 St. Thomas L. Rev. 504, 509 (2010).

17 Erin Kenneally & John Stanley, Beyond Whiffle-Ball Bats: Addressing Identity Crime In An Information Economy, 26 J. Marshall J. Computer & Info. L. 47, 130 (2008). Although most data breach class actions have been unsuccessful because of the plaintiffs' inability to plead an "actual or imminent" injury that is sufficient to establish Article III standing, on December 18, 2014, the U.S. District Court for the District of Minnesota ruled that a class of consumers could proceed with a majority of their claims against Target arising from the data breach it suffered in late 2013. See In re: Target Corporation Customer Data Security Breach Litigation, MDL No. 14-2522, U.S. Dist. LEXIS 175768 (D.M.N. Dec. 18, 2014). In addition, a class action filed against AvMed, Inc. settled for $3 million (after being dismissed twice by a Florida District Court and reinstated by the U.S. Court of Appeals for the Eleventh Circuit) and did not require class members to prove actual damages, suggesting damages may not require proof or causation. See Philippa Maister, After the Breach: Plaintiffs Secure a Settlement that Doesn't Require Proof of Damages, Corporate Counsel, July 2014, at 15.

18 Salar Ghahramani, Fiduciary Duty and the Ex Officio Conundrum in Corporate Governance: The Troublesome Murkiness of the Gubernatorial Trustee's Obligations, 10 Hastings Bus. L.J. 1, 7 (2014).

to fellow board members any material information that may not be readily known, and exercise good faith duties of care and loyalty toward the institution.[19]

A. The Duty of Care

The duty of care relates to the governing board member's competence in performing his/her functions and requires the use of care that an ordinarily prudent person would exercise in a like position under similar circumstances.[20] The duty of care also requires the board member to exercise his or her responsibilities and decision-making in good faith and with due diligence.[21] The duty of care does not allow a board member to fail to supervise the organization or, even when acting in good faith, neglect to make informed decisions.[22] Finally, the duty of care requires that board members are well-equipped with information that is required in order to make informed decisions.[23] A recent survey found that only 12 percent of board members frequently receive briefings and reports on cyber-threats.[24] If a board member is not regularly informed as to the institution's cyber security policies, procedures, and risks, he or she may not effectively oversee or approve institutional initiatives that may result in a breach of the duty of care.[25]

B. The Duty of Loyalty

19 Id. at 13.

20 Id.

21 Id.

22 Id.

23 Id.

24 Ponemon Institute LLC, Cyber Security Incident Response: Are We as Prepared as We Think?, January 2014, available at https://www.lancope.com/sites/default/files/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf.

25 The vast majority of states provide that the members of a board of a not-for-profit are held to the same standards as those applicable to the board of a for-profit corporation. See 15 Pa. Cons. Stat. § 5712 (2014). See also Ariz. Rev. Stat. § 10-830 (LexisNexis 2014), Ark. Code Ann. § 4-28-618 (2014), Cal. Corp. Code § 5231 (Deering 2014), Colo. Rev. Stat. 7-128-401 (2014), Conn. Gen. Stat. § 33-1104 (2014) (director must discharge his duties "in a manner he reasonably believes to be in the best interests of the corporation); Fla. Stat. § 617.0830 (2014), Ga. Code Ann. § 14-3-830 (2014), Haw. Rev. Stat. § 414D-149 (2014), Idaho Code Ann. § 30-3-80 (2014), Ind. Code Ann. § 23-17-13-1 (2014), Iowa Code § 504.831 (2014), Ky. Rev. Stat. Ann.§ 273.215 (LexisNexis 2014), La. Rev. Stat. Ann. § 12:226 (2014), Me. Rev. Stat. tit. 13-B, § 717 (2014), Mass. Ann. Laws. ch. 180, § 6C (LexisNexis 2014), Minn. Stat. § 317A.251 (2014), Miss. Code Ann. § 79-11-267 (2014), Mo. Rev. Stat. § 355.001 (2014), Mont. Code Ann. 35-2-416 (2014), Neb. Rev. Stat. Ann. § 21-1986 (LexisNexis 2014), Nev. Rev. Stat. Ann. § 82.221 (2014), N.J. Rev. Stat. § 15A:6-14 (2014)(trustees and members of any committee designated by the board are required to "discharge their duties in good faith and with that degree of diligence, care and skill which ordinary, prudent persons would exercise under similar circumstances in like positions"); N.M. Stat. Ann. § 53-8-25.1 (LexisNexis 2014), N.C. Gen. Stat. § 55A-8-30 (2014), N.D. Cent. Code § 10-33-45 (2014), Ohio. Rev. Code Ann. § 1702.30 (LexisNexis 2014), 15 Pa. Cons. Stat. § 5712 (2014) (a director of a not-for-profit corporation is held as a fiduciary and must perform his or her duties in good faith and with such care as a person of ordinary prudence would use under similar circumstances); R.I. Gen. Laws § 7-6-22 (2014), Tenn. Code Ann. § 48-58-301 (2014), Tex. Bus. Orgs. Code Ann. § 22.221 (2014), Utah Code Ann. § 16-6a-822 (LexisNexis 2014), Vt. Stat. Ann. tit. 11B, § 8.30 (2014), Va. Code Ann. § 13.1-870 (2014), Wash. Rev. Code Ann. § 24.03.127 (LexisNexis 2014), W. Va. Code § 31E-8-830 (2014).

The duty of loyalty requires a member of a governing board for a higher education institution to act in what he or she reasonably believes to be in the best interests of the organization, in light of its stated purposes.[26] This requires the trustee to affirmatively protect the interests of the organization and to refrain from doing anything that would be injurious to the organization.[27] The duty of loyalty requires the board member to place the interests of the institution above his or her own, and is largely concerned with addressing direct or indirect conflicts of interest between the board member and the organization.[28] As with the duty of care, the vast majority of state laws provide that board members of a not-for-profit are subject to a duty of loyalty, just as board members of a for-profit corporation are.[29]

III. Summary of Legal Obligations to Facilitate A Board's Duty of Care and Loyalty

A. The Applicability of FERPA, HIPAA, and FISMA to Higher Education

Higher educational institutions must comply with FERPA,[30] FISMA,[31] and, if applicable, HIPAA,[32] in order to regulate the security of their student records or other data.[33] FERPA sets the standard for student privacy, and federal funding may be withheld from any institution with a policy or practice of disclosing student

---

26 Id. at 15.

27 Id.

28 Id.

29 Supra note 24.

30 20 U.S.C. § 1232g. Regulations under FERPA are codified at 34 C.F.R. § 99 (2011). In addition to FERPA, some other federal laws also implicate the privacy of educational records and should be considered during the due diligence phase. See, e.g., Individuals with Disabilities Education Act, 20 U.S.C. §§ 1400-1487; Protection of Pupil's Rights Amendments, 20 U.S.C. § 1232h (1978); USA Patriot Act, Pub. L. 107-56 (2001); Privacy Act of 1974, 5 U.S.C. Part I, Ch. 5, Subch. 11, Sec 552; and Campus Sex Crimes Prevention Act, Pub. L. 106-386.

31 FISMA requires that every federal agency develop and implement an agency-wide program to provide information security for the information systems and information that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. See 44 U.C.S.A. §3544, et. seq. This requirement is often passed through to higher education institutions as a condition of grants or contracts with federal agencies funding research. Charles H. Le Grand, Handbook for Internal Auditors §23.07 (Matthew Bender & Company Inc. 2014).

32 See 42 U.S.C. §§ 1320d, et. seq. HIPAA required the Secretary of the U.S. Department of Health and Human Services (the "Secretary") to adopt national standards to, inter alia, protect the privacy of individually identifiable health information and maintain administrative, technical, and physical safeguards for the security of health information.42 U.S.C. §§ 1320d-2(a)–(d). Health plans, health care clearinghouses, and health care providers who engage in standardized transactions and transmit financial and administrative claims electronically are covered entities under HIPAA and must comply with its standards and regulations. See 42 U.S.C. § 1320d-4(b).

33 The U.S. Department of Education established a Privacy Technical Assistance Center as a resource to assist institutions with ensuring the protection of data, compliance with privacy laws, and development of confidentiality and security practices associated with technology systems. See U.S. Department of Education Privacy Technical Assistance Center, Home, http://ptac.ed.gov/. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems.

information without authorization.[34] Because FERPA ensures that the privacy of student educational records[35] is protected by regulating to whom and under what circumstances such records may be disclosed, its provisions have important application when those records are shared with cloud software services providers.[36]

Directory information may be made public after an institution gives notice of the categories of directory information to all students and provides students an opportunity elect to keep such information private.[37] Non-directory information is all other information related to a student and maintained by a higher education institution, including, without limitation, social security numbers or student identification numbers.[38] The disclosure of non-directory information or PII to a third party is only permitted if it qualifies as one of FERPA's defined exceptions.[39]

---

34 FERPA applies to all educational institutions that receive funding under any program administered by the Department of Education, which encompasses virtually all public schools and most private and public postsecondary institutions, including medical and other professional schools. See 20 U.S.C. § 1232g (requires higher education institutions that receive federal funds administered by the Secretary of Education to ensure certain minimum privacy protections for educational records); 34 C.F.R. § 99.1 (FERPA defines an educational institution to include "any public or private agency or institution which is the recipient of funds). See also, Jennifer C. Wasson, FERPA in the Age of Computer Logging: School Discretion at the Cost of Student Privacy?, 81 N.C.L. Rev. 1348, 1353 (2003).

35 An educational record subject to FERPA is "directly related to a student" and "maintained by an educational agency or institution or by a party acting for such agency or institution." See 34 C.F.R. § 99.3. Some examples of educational records include student files, student system databases kept in storage devices, or recordings and/or broadcasts. See 20 U.S.C. § 1232g(a)(4)(A).

36 FERPA does not prohibit the use of cloud computing but requires higher education institutions to use reasonable methods to ensure the security of any information technology solutions, including cloud computing. See U.S. Department of Health & Human Services & U.S. Department of Education, Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records Nov. 2008, available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hipaaferpajointguide.pdf. FERPA does not, however, affirmatively require schools to implement specific procedures for cloud computing or to provide notification in event of a data breach. Notification by the institution in the event of a data breach may nonetheless be required pursuant to state law or even the institution's own internal policies.

37 Directory information may include "the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student." See 20 U.S.C. § 1232g(a)(5)(A).

38 See, e.g., 34 C.F.R. § 99.3. See also, 20 U.S.C. § 1232g(b). Information disclosed in combination with a student ID number, rather than a student name, is considered PII under FERPA and subject to heightened protection; only when an education institution removes all PII and assigns the records non-personal identifiers are disclosures to outside parties permitted without prior consent. See 20 U.S.C. § 1232g(a)(5).

39 One exception is pragmatic, permitting disclosures in connection with confidential and anonymous studies undertaken on behalf of the educational institution. See 20 U.S.C. § 1232g(b)(1)(F) (such studies must be "for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction"); see also 34 C.F.R. § 99.31(a)(6)). This information must be destroyed when no longer needed for the purposes for which the study was conducted. See 34 C.F.R. § 99.31(a)(6)(iii)(B). The educational institution must enter into an agreement with the organization conducting the study that limits the use of the PII and requires the organization to maintain confidentiality and anonymity and to destroy the PII once it is no

Faculty, staff, and other officials of the institution may access non-directory information under FERPA if they have a legitimate academic interest to do so.[40] The school official exception applies to third party cloud providers who are given access to student education records regulated by FERPA[41] so long as they agree: (1) to not redisclose the information without the student's prior consent,[42] and (2) to use the information only "for the purposes for which the disclosure was made."[43]

Higher education institutions providing academic programs that include the operation of medical hospitals or other treatment centers and submit claims for reimbursement of medical expenses to third parties are generally subject to HIPAA.[44] HIPAA requires a receiving party to maintain the confidentiality of protected health information (PHI) that includes individually identifiable health information[45] transmitted by, or maintained in, electronic, paper, or any other medium.[46] The HIPAA Privacy Rule requires that a covered entity maintain reasonable and appropriate administrative, technical, and physical safeguards to protect PHI privacy.[47] The Privacy Rule also requires covered entities to enter into business associate agreements with third party vendors who create, receive, maintain, or transmit PHI on their behalf.[48] Under the Privacy Rule, covered

longer needed. See 34 C.F.R. § 99.31(a)(6)(iii)(C)(1)–(4). Another exception provided by FERPA is in connection with audits and evaluations of programs conducted by local, federal, or state officials and their authorized representatives. See 20 U.S.C. § 1232g(b)(1)–(5).

40 20 U.S.C. § 1232g(b)(1)(A). See also, 34 C.F.R. § 99.31(a)(1).

41 34 C.F.R. § 99.31(a)(1)(i)(B) (third party must (i) "perform an institutional service or function for which the…institution would otherwise use employees"; (ii) "[be] under the direct control of the…institution with respect to the use and maintenance of education records"; and (iii) be subject to certain FERPA requirements governing the use and re-disclosure of PII in educational records.

42 34 C.F.R. § 99.33(a)(1).

43 34 C.F.R. § 99.33(a)(2).

44 HIPAA established a national health information privacy rule, which required the Secretary to issue final Standards for Privacy of Individually Identifiable Health Information, known as the Privacy Rule. See 45 C.F.R. Part 164 Subpart E. The Privacy Rule applies to health plans, health care clearinghouses, and health care providers who transmit financial and administrative transactions electronically to third parties for reimbursement of medical expenses, including medical universities that offer health care to individuals in the normal course of business or the fulfillment of academic credentials (i.e., through a university medical hospital or faculty/physician practice). See U.S. Department of Health and Human Services and U.S. Department of Education, supra note 35.

45 "The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that – (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and – (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." 42 U.S.C. §1320d(6).

46 45 C.F.R. §160.103.

47 45 C.F.R. § 164.530(c). This regulation also provides specific requirements regarding the structure around such safeguards, including designating a privacy official, training the workforce, providing a mechanism for documentation of complaints, avoiding retaliation and sanctions, and other important structural components.

48 Pursuant to the Privacy Rule, a covered entity must receive satisfactory assurances

entities may only use or disclose PHI without patient authorization for treatment, payment, or health care operations.[49] For other purposes, a covered entity must obtain patient authorization prior to using or disclosing PHI, albeit subject to certain exceptions.[50]

In addition, and pursuant to HIPAA, a national security standard for the protection of individually identifiable health information was established ("Security Rule").[51] The Security Rule regulates electronic PHI (ePHI) and requires any entity subject to it to adopt policies and measures to ensure the confidentiality, integrity, and availability of any ePHI created, received, maintained, or transmitted.[52] As with FERPA, covered entities must also enter into written agreements with third parties who create, receive, maintain, or transmit ePHI on their behalf that are consistent with the obligations under the Security Rule.[53] Consequently, if a higher

---

from its business associate that the business associate will appropriately safeguard the protected health information before sending PHI to the third party or having it create PHI on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate. See 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e). For further information about business associates in the HIPAA context, visit the HHS website. Business Associates, U.S. Dep't. of Health and Human Services, available at

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.

49 45 C.F.R. § 164.506.

50 45 C.F.R. § 164.508. Among these exceptions, PHI may be used or disclosed without patient authorization or prior agreement for public health, judicial, law enforcement, and other specifically enumerated purposes. See 45 C.F.R. § 164.512(a)-(l). "When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally." See 45 C.F.R. § 164.512. For some situations that might otherwise require authorization, a covered entity may use or disclose PHI without authorization so long as the individual was given the prior opportunity to object or agree. See 45 C.F.R. § 164.510 (e.g., for use in a directory, under emergency circumstances, for use in the care of the individual, for disaster relief, or for when the person is dead).

51 42 U.S.C. §§ 1320d-2 and (d)(4). HHS issued the these standards in 2003.

52 45 C.F.R. § 164.306(a). See also, 42 U.S.C. §§ 1320d-2(d) (requiring covered entities to protect the electronic PHI against any reasonably anticipated threats or hazards to the security or integrity of such information, as well as any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule). See also, 42 U.S.C. §§ 1320d-2(d)(2)(C) (covered entities are also responsible for ensuring compliance by their employees).

53 Under such agreements, the third party must: implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the covered entity's electronic PHI; ensure that its agents and subcontractors to whom it provides the PHI do the same; and report to the covered entity any security incident of which it becomes aware. See 45 C.F.R. § 164.504 (e)(2). The contract must also authorize termination if the covered entity determines that the third party has violated a material term. See 45 C.F.R. § 164.504 (e)(2)(iii). Additionally, if a covered entity's third party business partner violates the Security Rule, the covered entity is not liable unless it knew that the third party was engaged in a practice or pattern of activity that violated HIPAA and failed to take corrective action. See 45 C.F.R. § 164.504 (e)(1). The HITECH Act extended application of some provisions of the HIPAA Privacy and Security Rules to the business associates of HIPAA-covered entities, in particular, making those business associates subject to civil and criminal liability for improper disclosure of PHI; establishing new limits on the use of PHI for marketing and fundraising purposes; providing new enforcement authority for state attorneys general to bring suit in federal district court to enforce HIPAA violations; increasing civil and criminal penalties for HIPAA violations; requiring covered entities and business associates to

education institution is subject to HIPPA and intends to use cloud computing to manage its ePHI, the written agreement with the third party vendor must be drafted to protect the institution from liability from improper disclosures.

Notably, the Security Rule anticipates that covered entities will be permitted some "flexibility" in their approach to implement security protocols.[54] As part of that flexible approach, covered entities are required to consider the following factors: (1) the size, complexity, and capabilities of the covered entity or business associate, (2) the covered entity's or business associate's technical infrastructure, hardware, and software security capabilities, (3) the costs of security measures, and (4) the probability and criticality of potential risks to electronic protected health information.[55] Penalties for violations of HIPAA can be severe and may include criminal charges as well as significant civil penalties.[56]

B. State Laws and Data Security

In the United States, there is no comprehensive, uniform set of laws in either the federal or state systems to regulate data privacy and the collection, use, and disposal of personal information.[57] There are, however, hundreds of privacy and data security laws that govern the collection and use of personal information, all with varying obligations and degrees of scope.[58] States have individual data privacy and security laws directed toward the protection of student or employee

---

notify the public and HHS of data breaches; changing certain use and disclosure rules for protected health information; and creating additional individual rights. See 78 Fed. Reg. 5566–5702.

54 Covered entities and business associates may use any security measures that allow them to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart." See 45 C.F.R. § 164.306 (b)(1).

55 45 C.F.R. § 164.306 (b)(2)(i)–(iv).

56 The Office of Civil Rights in HHS enforces compliance with the Privacy Rule. 65 Fed. Reg. 82381. The Secretary of HHS must assess a civil monetary penalty on any covered entity or person failing to comply with the national standards and regulations. See 42 U.S.C. § 1320d-5(a). The minimum fine for a violation is $100 per violation, but can be up to $25,000 for all violations of an identical requirement or prohibition during a calendar year. 42 U.S.C. § 1320d-5(a)(1). The maximum fine for a violation is $50,000 per violation and up to $1.5 million for all violations of an identical requirement or prohibition during a calendar year. See 42 U.S.C. § 1320d-5(a)(1). Criminal penalties may imposed if a person knowingly and in violation of HIPAA's Administrative Simplification provisions uses a unique health identifier or obtains or discloses individually identifiable health information. See 42 U.S.C. § 1320d-6. Criminal penalties can be enhanced if the offense was committed under false pretenses, with intent to sell the information or reap other personal gain. The criminal penalties include a fine of not more than $50,000 and/or imprisonment of not more than one year for a violation. 42 U.S.C. § 1320d-6(b). If the offense was committed under false pretenses, the penalty will be a fine of not more than $100,000 and/or imprisonment of not more than five years. If the offense was committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, then the violation will incur a fine of not more than $250,000 and/or imprisonment of not more than 10 years. See also Luis J. Diaz & David N. Crapo, The Cost of a Data Breach: The Health Care Perspective, The Metropolitan Corporate Counsel, Nov. 18, 2013, http://www.metrocorpcounsel.com/articles/26260/cost-data-breach-health-care-perspective.

57 Ieuan Jolly, US Privacy and Data Security Law 27 (2014), available at Thomson Reuters Practical Law.

58 Id.

PII.[59] For example, many states have adopted laws that govern the collection, use, and disclosure of Social Security numbers, and other states such as California, New Jersey, and New York have enacted laws requiring the proper disposal of records that contain personal information.[60] Additionally, some state laws are more stringent than the protections afforded by HIPAA and are not preempted by federal regulation, so long as the state's laws are not inconsistent with the federal regulatory scheme.[61]

C. Cyber Security Compliance in Higher Education

Congress has debated comprehensive cyber security legislation since at least 2009.[62] Earlier proposals would have included a mandatory federal framework for cyber security compliance.[63] Later proposals have stressed voluntary public-private partnerships with liability protections and other incentives for compliance.[64] Comprehensive reform, however, has stalled in Congress for a variety of political and practical reasons.[65]

In February 2013, frustrated with Congress' inability to pass comprehensive cyber security reform, President Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."[66] This Order directed the National Institute of Standards and Technology (NIST) to develop a framework for cyber security compliance by owners and operators of critical infrastructure, although the Order does not impose any specific legal obligations on non-governmental entities.[67] NIST released its framework in February 2014, and it has become recognized as a "gold standard" in cyber security compliance.[68]

---

59 Nancy J. King & V.T. Raja, What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Sensitive Consumer Data, 50 Am. Bus. L.J. 413, 445-446 (2013).

60 Id.

61 Id.

62 These attempts included the Cybersecurity Act of 2009, S. 773, 111th Cong. (as introduced, Apr. 1, 2009); the Cybersecurity Act of 2010, S. 773, 111th Cong. (as reported by S. Comm. on Commerce, Sci., & Transp., Mar. 24, 2010); the Protecting Cybersecurity as a National Asset Act of 2010, S. 3480, 111th Cong. (as reported by S. Comm. on Homeland Sec. & Governmental Affairs, Dec. 15, 2010); the Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011); the Cybersecurity Act of 2012, S. 2105, 112th Cong. (as introduced, Feb. 14, 2012); the Cybersecurity Enhancement Act of 2014, S. 1353 (as introduced July 24, 2013); and the Data Security Act of 2015, S. 961 (as introduced April 15, 2015), among others. For a description of various proposals, see David W. Opderbeck, Cybersecurity and Executive Power, 89 Wash. L. Rev. 795 (2012).

63 See Opderbeck, supra, note 61, at 801-12.

64 Id.

65 Id.

66 Exec. Order No. 13,636, 78 Fed. Reg. 649 (February 19, 2013).

67 Id. at § 7.

68 See NIST Cybersecurity Framework website, available at http://www.nist.gov/cyberframework/; PWC, "Why You Should Adopt the NIST Cybersecurity Framework" (May 2014), available at http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf (stating that "the Framework comprises leading practices from various standards bodies that have proved to be successful when implemented, and it also may deliver regulatory and legal

The NIST standards are arranged around what NIST calls the "Framework Core."[69] The Framework Core identifies high-level cyber security functions, divides those functions into categories of outcomes, and relates the categories of outcomes to specific *subcategories* and *informative resources*:[70]

As the graphic from the NIST Framework illustrates, the core functions are "Identify," "Protect," "Detect," "Respond," and "Recover."[71] If these core functions seem obvious, that is because they are in a sense obvious. The NIST Framework does not break any new ground concerning the basic requirements to prepare for and respond to cyber attacks. Rather, the Framework seeks to require organizations to think systematically and carefully about cyber risk. Surprisingly, even large organizations with significant information technology assets and professional IT staff often fail to engage in this kind of deliberate risk identification and planning.

The "Identify" function requires the organization to take an inventory of all of its "systems, assets, data and capabilities."[72] The "Protect" function requires the organization to proactively develop safeguards to keep critical infrastructure services online in the event of a cyber emergency.[73] The "Detect" function requires the organization to implement procedures and technologies to identify adverse cyber security events,[74] including continuous, around-the-clock monitoring of security status and robust processes for detecting intrusions.[75] The "Respond" function focuses on containing the impact of adverse events;[76] this function recognizes that adverse cyber security events are inevitable despite robust protection and detection mechanisms, and the risk of such events cannot entirely be eliminated but often can be contained. The category responses under this function are among those most frequently overlooked in cyber security risk management. Finally, the "Recover" function requires plans to restore information capabilities lost during an attack. The category responses under this function should include restoration plans with definite timelines as well as plans to learn from the event and make improvements in the protect, detect, and respond functions.[77]

The NIST Framework includes a tier structure that enables an organization to assess

---

advantages that extend well beyond improved cybersecurity for organizations that adopt it early").

69 See NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (February 12, 2014), § 1.1, available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

70 Id. at § 2.1.

71 Id.

72 Id.

73 Id.

74 Id.

75 Id.

76 Id.

77 Id.

its current state of compliance and to move towards higher levels of compliance.[78] A vital measure of which tier an organization has reached involves the formal approval and adoption at a policy level of organization-wide cyber security risk management practices. This means that cyber security should become elevated to a top institutional priority that entails functions across all business units from the executive level down. Cyber security is no longer an afterthought for only a few information technology functions. The following graphic from the NIST Framework illustrations this dynamic:[79]

Again, there is nothing particularly novel in this structure, but it illustrates that cyber security must become an executive level issue that receives constant attention and, importantly, budgeting.

Appendix A to the NIST Framework includes a coded tool that can be used to conduct a cyber security compliance assessment[80] in a methodical, standardized fashion, providing codes for specific subcategory designators and identifying specific published standards relating to each subcategory.[81] For example, here are the cells for the first function, category, and subcategory:[82]

Obviously, with 14 pages of such detailed mappings within Appendix A to the NIST Framework (pages 20 to 34), the work involved in becoming compliant can seem impossibly daunting.[83] Moreover, some of the standards referenced in the NIST framework may not map directly onto the unique circumstances of higher education institutions. For these reasons, some universities and university trade organizations have adopted or proposed simplified models that focus on particular standards.

For example, the Higher Education Information Security Council (HEISC) has published an Information Security Guide keyed to the ISO/IEC 27002:2013 standard, which is one of the standards referenced in the NIST Guidelines.[84] The HEISC Guide incorporates 15 compliance domains, ranging from cryptography to supplier relationships.[85] As another example, the University of Ohio Information Risk Management Program condenses the NIST Framework into 30 risk areas within seven business functions, and condenses the text into eight pages.[86] The

78 Id. at § 2.2.

79 Id. at § 2.4.

80 Id. at Appendix A.

81 Id.

82 Id.

83 Id. NIST also makes the core framework and coding tool available on its website in Excel and FileMaker formats. See http://www.nist.gov/cyberframework/csf_reference_tool.cfm and http://www.nist.gov/cyberframework/upload/framework-for-improving-critical-infrastructure-cybersecurity-core.xlsx.

84 See HEIS Information Security Guide, Introduction, available at https://spaces.internet2.edu/display/2014infosecurityguide/Welcome+to+the+Guide.

85 Id.

86 See Ohio State University Information Risk Management Program website, available at https://ocio.osu.edu/itsecurity/riskmgmt.

business functions identified in the University of Ohio policy include management, legal, purchasing, human resources, facilities, and information technology.[87]

Other universities, colleges, and higher education providers similarly may benefit from information security planning that customizes the NIST Framework for application within their specific circumstances. Although cyber security compliance policies can become complex at the granular level of application, they all include some basic over-arching themes, including the following:

Cyber security compliance involves more than adherence to a specific legal requirement. It includes multiple legal requirements as well as contractual obligations and institutional risk management practices.

Cyber security compliance is an ongoing process, not a one-time project.

Cyber security compliance involves both technological measures and human resource management measures.

The risks of a cyber security incident cannot be entirely eliminated. Cyber security compliance therefore involves procedures to identify and remediate incidents as well as procedures aimed at preventing incidents.

Cyber security compliance is an executive-level concern that requires coordination across every significant operational unit in the organization.[88]

These general principles are as true for higher education institutions as they are for any other kind of enterprise. Indeed, the wide variety of sensitive data handled by higher education institutions, including sources as diverse as confidential and trade secret technological research and student health information, together with the diffuse nature of governance in many university systems, suggests that such institutions must make particular efforts to develop comprehensive, meaningful cyber security compliance programs.

Finally, in addition to these overarching compliance themes, public attention recently has focused on legislation that would facilitate information sharing about security risks between the public and private sectors. The Cyber Information Sharing Act (CISA) was signed into law by the President on December 18, 2015 as part of the omnibus spending bill.[89] The CISA allows private entities to share cyber threat information with the federal government without incurring liability under other laws – such as, for example, FERPA and HIPAA – that require certain information to be kept confidential.[90] The new law apparently would include colleges and

---

87 Id.

88 For a similar list, see Joanna Lyn Grama, Understanding IT GRC in Higher Education: IT Compliance, Educause Review, February 23, 2015, available at http://er.educause.edu/articles/2015/2/understanding-it-grc-in-higher-education-it-compliance.

89 Protecting Cyber Networks Act, H.R. 1560 (passed by House as amended April 22, 2015); Cybersecurity Act of 2015 (passed into law on December 18, 2015), available at https://www.congress.gov/114/bills/hr2029/BILLS-114hr2029enr.pdf.

90 See, e.g., Cybersecurity Act of 2015, § 104(c)(1) (stating that, with certain exceptions, "notwithstanding any other provision of law, a non-Federal entity may, for a cybersecurity purpose

universities, as well as their officers, employees, and agents.[91] Information sharing proposals have been very controversial with cyber civil liberties advocates.[92] Now that the CISA has been signed into law, colleges and universities will need to think carefully about procedures for logging potential threat information and for whether and when an employee or officer should report such information to the federal government.

However, the recent onslaught of cyber security cases does not require board members to become experts in cyber security risk. In looking to the Wyndham, supra, case for guidance, there are several actions that the board can proactively take in advance of a cyber security event, which include making data privacy and data security regular topics of discussion at board meetings; providing that a specific committee has primary oversight on data security and ensures that data protection measures are discussed regularly at committee meetings; periodically retaining third-party consultants to assess the institution's cyber security practices and remediating any deficient areas; and establishing a cross-functional incident response team that has primary responsibility for investigating and responding to a cyber security breach.[93]

III. Risk and Mitigation

Through a comprehensive risk analysis, a University's board of governors or trustees and administrators can ensure that organizational cyber risks are adequately mitigated through a combination of effective diligence, contract negotiation, and, in many instances, the purchase of cyber insurance coverage. These steps are necessary to provide effective governance and management of the university. Cloud vendor contracts are not yet associated with the typical collateral issues that are raised in outsourcing or shared control contracts. These models offer worthwhile guidance about risks created by shared responsibilities and possible liabilities, as well as ways to contract around common problems. As recent large-scale cloud failures demonstrate, a breach results not only in data recovery problems, but also in attendant unfavorable publicity and extensive remediation and legal costs.[94]

. . . share with, or receive from, any non-Federal entity or the Federal Government a cyber threat indicator or defensive measure.").

91 See, e.g., id. § 102(14)(A) (stating that " 'non-Federal entity' means any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof)."; id. § 102(15)(A) (stating that " 'private entity' means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.").

92 See, e.g., Andy Greenberg, Privacy Critics Go 0-2 With Congress' Cybersecurity Bills, Wired, March 26, 2015, available at http://www.wired.com/2015/03/privacy-critics-go-0-2-congress-cybersecurity-bills/.

93 Data Breaches Hit the Board Room: How to Address Claims Against Directors and Officers, Hogan Lovells Chronicle of Data Protection, Jan. 23, 2015, available at http://www.hldataprotection.com/2015/01/articles/cybersecurity-data-breaches/data-breaches-hit-the-board-room/. See also, In re Heartland Payment Systems, Inc. Security Litigation, Case No. 09-1043. 2009 WL 4798148 (D.N.J. Dec. 7, 2009)

94 Supra note 2.

A. Overview of Risks Associated with Cloud Computing

Cloud computing offers both benefits and risks that must be weighed. Educational institutions have employed cloud computing for a variety of needs, from hosting of simple applications to complex, enterprise-wide human resources and student information management systems.[95] Cloud computing frequently offers granular pricing that lets institutions optimize software or services utilization and tailor the same to meet the needs of students, alumni, or employees.[96] Moving system architecture to the cloud reduces the long-term costs of IT resources while increasing employees' and students' "anywhere, anytime" access to the resources the institution selects for common availability.[97] Resources hosted remotely are necessarily flexible, potentially including infrastructure, platforms, or even stacked software as a service, and these options offer cost savings through economies of scale, off-site hosting, and off-site maintenance.[98] The cloud's modular, on-demand model permits educational institutions to reduce the sunk costs of quickly outdated hardware or data storage and to easily swap out software on a global level for more recent applications.[99] By enabling faster updates, with no delay for procurement or individual installation, the institution can more efficiently serve its various stakeholders while reducing overhead costs.[100]

Against these benefits, decision-makers must educate themselves about the associated cyber risks in order to exercise sound judgment before migrating PII to the cloud. The use of cloud computing forces an institution to rely on the policies and security of a third party vendor (and any affiliated data center utilized by the vendor), which creates incremental organizational risk that must be analyzed as compared to the inherent risk of the institution managing its own data and IT resources.[101] Here, we analyze the risks associated with the most common cloud

---

95 Cloud computing allows organizations to purchase and use technology services through the internet on an as-needed basis and is a cost-effective alternative to buying and maintaining expensive hardware or software. See Timothy D. Martin, Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security and Property in Cloud Computing, 92 J. Pat. & Trademark Off. Soc'y, 283, 285 (2010).

96 Id.

97 Organizations can reduce or eliminate IT capital expenditures and decrease ongoing operating expenses by paying only for the services they use, which can result in reducing or redeploying IT staff. See Cisco, Cloud Computing in Higher Education: A Guide to Evaluation and Adoption 2 (2011). See also Steve Mutkoski, Cloud Computing, Regulatory Compliance, and Student Privacy: A Guide for School Administrators and Legal Counsel, 30 J. Marshall J. Computer & Info. L. 511, at 512 (2014).

98 Melanie J. Teplinsky, Fiddling On The Roof: Recent Developments in Cybersecurity, 2 Am. U. Bus. L. Rev. 225, 238 (2013).

99 Cisco, supra note 96, at 2.

100 Martin, supra note 94, at 294.

101 The complex nature of cloud computing services creates a "level of abstraction between the physical infrastructure and the owner of the information being stored and processed." The organization that contracts with a cloud computing vendor no longer has any visibility into the operations of the physical infrastructure where the data is being stored, and it is argued that more transparency should be provided regarding service providers' cybersecurity measures. See J. Nicholas Hoover, Compliance in the Ether: Cloud Computing, Data Security, And Business Regulation, 8 J. Bus.

service offered by vendors, that being public, multi-tenant cloud services, where remote data centers host multiple customers' data on the same servers without segregation.

As stated earlier, cloud computing creates incremental risk by outsourcing an institution's IT functions to third party vendors, which eliminates or impairs the institution's control over its data, processing, and security.[102] This increased risk and the resulting increased liability from a breach by a third party vendor are frequently borne directly by the institution itself.[103] These new risks must be analyzed in addition to the familiar vulnerabilities associated with IT functions, such as cyber security threats from networked mobile media, hardware malfunction, software installations, and malicious insiders or external cyber attacks. As a result, some institutions, particularly those with a larger volume of PII, trade secrets, or confidential data subject to high levels of regulation (i.e., under HIPAA requirements, Department of Defense procedures, or SEC oversight), may choose to avoid cloud computing because the additional risks, requirements, and potential exposures are too great.[104] Alternatively, such institutions may choose to create private, self-contained cloud computing systems to increase the level of control retained over the security of the data centers.[105]

Other educational institutions, particularly smaller schools with more limited data sets, may find it is both safer and economically efficient to rely on the more advanced security provided by larger cloud vendors.[106] However, even these schools must ensure that such vendors can comply with the "school official exception" under FERPA.[107] For these smaller institutions, the incremental risk

---

& Tech. L. 255, 260-261. See also Zacharis Enslin, Cloud Computing Adoption: Control Objectives for Information and Related Technology (COBIT) – Mapped Risks and Risk Mitigating Controls, Afr. J. Bus. Mgmt. Vol.6 (37), 10185-94 (2012).

102 Teplinsky, supra note 97, at 238 ("characteristics of cloud computing – including system complexity, the multi-tenant environment, and loss of control – pose significant challenges to corporate cybersecurity").

103 Significant concerns by cloud users about shifting liability from the cloud users to the cloud vendors are not adequately addressed in the standard contract terms offered by most cloud computing vendors. These contracts typically heavily favor the cloud vendor, and, unfortunately, most cloud users lack the leverage to sufficiently bargain for a more balanced agreement. See T. Noble Foster, Navigating Through The Fog of Cloud Computing Contracts, 30 J. Info. Tech. & Privacy L. 13, 24-25 (2013).

104 Aside from state laws, there are nine applicable sets of regulations, at least six industry-specific guidelines and requirements, and a wide array of international laws in the data security space. See James Ryan, The Uncertain Future: Privacy And Security In Cloud Computing, 54 Santa Clara L. Rev. 497, 506 (2014).

105 In a "private cloud," an organization develops or purchases its own cloud-computing environment, rather than using a multi-tenant platform that is available to the general public or a large industry group. See Cisco, supra note 96, at 3.

106 Cisco, supra note 96, at 3. By contracting with a cloud computing vendor (that may even be another, larger university), smaller colleges can adopt state-of-the-art applications and services, thereby bypassing many of the costly challenges such as lack of high levels of computerization, recruitment of qualified IT personnel, and the ability to secure and protect PII and other sensitive data.

107 U.S. Department of Education PTAC, supra note 11, at 2.

created by outsourcing the security of their student data is offset by the net benefits to overall security offered by more advanced security systems than those the smaller organizations can individually afford. Larger educational institutions with more robust security processes will have to find other benefits and methods of risk mitigation to offset the incremental risk and craft a positive net benefit bargain by switching to cloud computing.[108]

Universities may also face different risk levels depending on whether they are public or private institutions. With different appetites for risk or different security risk profiles, each institution must achieve an acceptable balance of risk against benefit by identifying the incremental risks associated with cloud computing that are germane to their programs and then finding ways to mitigate those risks.[109] Some of the risks that require consideration include:

Educational institutions remain legally liable for data breaches, even though control over security shifts to the cloud vendor. Accordingly, data breaches can leave the institution subject to different laws for each jurisdiction implicated, by the location of either the data, compromised employee, student or alumnus/a, or cloud vendor's citizenship.[110]

Any single breach may put a cloud vendor out of business or in bankruptcy, while for young or small vendors, lack of significant assets and limited applicable or available insurance coverage may preclude full recovery of losses.

PII may be compromised or commingled with third party data, including that of competitors, with respect to the university's research or intellectual property.[111]

Cloud vendors may impose unreasonable or otherwise unacceptable policies or terms of service, including: failure to provide adequate indemnity for claims resulting from security breaches; failure of transparency regarding third party data center security; limitation of liability to amounts inadequate to meaningfully remedy the loss; exclusion of consequential damages; refusal to limit future use of client data; refusal to secure client consent before transferring data overseas; refusal to provide service level agreements or damages for disruption during outage; refusal to return data in usable form to client after termination of agreement; or refusal to agree to abide by FERPA's "school official exception" as it relates to

---

108 Cisco, supra note 96, at 4.

109 See Association of Governing Boards of Universities and Colleges, supra note 9, at 1 ("While institutional focus on risk has grown[,] . . . risk appetite and tolerance are less likely to be considered in decision making. In 2013, 31 percent 'strongly agreed' that risk appetite and tolerance are part of the institution's culture, down from 47 percent in 2008.").

110 International students attending a U.S. educational institution may pose unique jurisdictional implications, especially as more and more countries adopt increasingly sophisticated data privacy laws intended to protect its citizens. See Cynthia Rich, Privacy Laws in Asia, A Special Report for Privacy & Data Security Professionals, Bloomberg BNA Vol. 13, No. 16 (2014).

111 Public cloud services are delivered online, and the internet-based nature provides hackers with a larger "attack surface" to attack in comparison to private networks. See J. Nicholas Hoover, Compliance in the Ether: Cloud Computing, Data Security and Business Regulation, 8 J. Bus. & Tech. L. 255, 261 (2013).

direct control or the use and redisclosure of PII.[112]

The physical location of cloud vendors' servers around the world may result in trans-border information flow and could subject information to the laws of multiple foreign jurisdictions.[113]

Cloud computing makes it difficult to administer enterprise-wide information security policies for risk mitigation, as well as resource mapping procedures for data forensics, preservation, and management.

Because sensitive personal, financial, and other confidential information may be stored on the cloud vendors' servers, risk of breach, loss, or liability must be analyzed in terms of publicity as well as the financial and legal consequences. Cyber attacks directed at cloud vendors may impact a large population of unrelated users and generate greater publicity.

Cloud vendors are reluctant to assume significant risks or the resulting liability because the pricing models are kept low through contractual provisions limiting liability and avoiding indemnification for breaches of data availability, security, or privacy.[114] While weighty bargaining power or competitive leverage can aid in bringing cloud vendors to the bargaining table to negotiate risk-sharing, these advantages likely will not be available to individual universities or smaller higher education nonprofits.[115] Because few institutions can individually lay claim to those bargaining advantages, universities may consider pooling resources and forming consortiums to collectively bargain with vendors, share the costs of due diligence, and secure insurance. Due diligence in determining which risks are the most vital remains the best method to shore up bargaining positions, as can be seen below.

B.Best Practices for Higher Education When Considering a Move to the Cloud

When an institution of higher education intends to make the strategic decision to move its data and information technology systems to a third party cloud provider and procure software as a service, it should first establish a team of stakeholders. The team should include the institution's general counsel; the highest ranking officials charged with overall authority to oversee information technology and security, risk management, finance, and business administration; and the head of the business unit that will utilize the technology. These stakeholders should participate in the due diligence of the software service providers and the

---

112 Cloud vendors typically exclude or restrict liability as much as possible, and it is generally difficult for large or global users to negotiate successfully for vendor liability, particularly for outages and data loss. See W. Kuan Hon, Christopher Millard & Ian Walden, Negotiating Cloud Contracts: Looking at Clouds From Both Sides Now, 16 Stan. Tech. L. Rev. 81, at 94 (2012).

113 Id. at 103. Cloud vendors may provide round-the-clock "follow the sun services" and use support staff or sub-contractors outside the U.S. who have or are given access to data or metadata.

114 Hon, supra note 111, at 94.

115 John Soma, Maury Nichols, Melodi Mosley Gates & Ana Gutierrez, Chasing The Clouds Without Getting Drenched: A Call For Fair Practices In Cloud Computing Services, 16 J. Tech. L. & Pol'y 193, 211 (2011). Given their size and commensurate bargaining power, cloud vendors are able to dictate terms that are favorable for themselves, but risky for the purchaser.

negotiation of their contracts, so that they are fully informed of and understand the nature of the risks to the institution by moving to a cloud environment. By involving key stakeholders in this manner, the institution will achieve consensus in making recommendations to its president and governing body to approve the individual contract and use of the particular technology resource, as well as to ensure that there is fully informed consent to the risks inherent in this type of transaction and that techniques have been developed by the institution to mitigate them.

The information technology stakeholder should develop a checklist soliciting information from the providers to assist in the evaluation of their security, and general counsel should also develop a form of agreement with the provider that contains the terms and conditions appropriate for the risks the institution is willing to accept. The institution should solicit a response to the checklist from those providers of software services that are appropriate for the institution's needs. Because the checklist will solicit sensitive security information, the institution should be prepared to enter into a non-disclosure agreement with the provider prior to receiving its response. The responses to the checklist should then be evaluated by the individual assigned to oversee information technology security for the institution and make a recommendation to the stakeholders. If the responses are determined to create an acceptable level of risk to the institution, the vendor should be provided the institution's form of agreement to begin negotiations.

The checklist is the first step in the institution's due diligence of the provider and should focus on the vendor's security policies and processes to maintain, monitor, and test the adequacy of security to protect data from disclosure to unauthorized parties.[116] The checklist should identify the type of institutional data to be shared with or stored by the provider and should specifically focus on whether it includes credit card information, health records, student records, and personally identifiable information, because federal and state law impose heightened obligations in the event of a breach. The checklist should inquire if the data will be stored outside of the United States so that the institution can determine if it would be subject to the laws of any foreign jurisdiction in the event of a breach.[117] The provider should also be asked to identify its methodology for exchanging the data, such as upload via a secure web interface, secure file transfer, etc., so that the institution can evaluate the security of the transfer. The checklist should solicit the policies of the provider (and any third party subcontractors of the provider) on data security, data storage and protection, network systems and applications, and disaster recovery; the procedures for review and updating of those policies; and policies that ensure compliance with laws applicable to PCI, HIPAA, and FERPA, so that the institution can verify the provider has a comprehensive plan for compliance.

---

116 Congress recently created a compilation of citations that provide many available resources to assist in the development of appropriate due diligence in order to assess the apparent risks of cloud providers. See Cybersecurity Authoritative Reports and Resources, Congressional Research Service (June 10, 2015).

117 See Privacy Laws in Asia: A Special Report for Privacy and Data Security Professionals, Bloomberg BNA, Apr. 21, 2014, available at http://www.bna.com/uploadedFiles/Content/Web_Forms/Real_Magnet_Form/Legal/Privacy_Law/11759-iapp-whitepaper.pdf (providing a comprehensive summary of privacy laws in major regions outside of the United States).

The checklist should request the provider's SOC1 and SOC2 reports and the results of recent external audits and other tests, to determine the integrity of its system and penetration vulnerabilities. In addition, the checklist should inquire about the physical security and access restrictions to the provider's data center, data storage area, and network systems; the provider's response to security incidents; and the provider's awareness training, so that the institution can evaluate the provider's preparedness for a breach and strategies for prevention.[118]

In addition to the items on the checklist, the provider should be asked to provide its most recent audited financial statements and, if publicly traded, its 10K and 10Q reports, so that the institution may examine its assets and liabilities and the risks to it as an entity and within its industry. The stakeholders should also perform an independent assessment of the provider by conducting reference checks with existing customers, verifying the size of the provider's customer base, and estimating the total amount of individual information stored within the provider's services. In doing so, stakeholders will be able to project the potential losses the provider might suffer in the event of a system-wide breach and whether there is heightened risk of an attack if data is aggregated. An examination of the checklist and the additional information solicited will provide a clear picture of the potential risk of a data breach by using the vendor's services; the vendor's ability to prevent, detect, mitigate, and respond to a breach; and the vendor's ability to withstand the financial impact of a significant breach.

If the institutional stakeholders are satisfied that the risks disclosed during due diligence of the provider may be adequately addressed through contract negotiation or other means, the provider should be forwarded the institution's form of agreement.[119] While the agreement will contain standard provisions applicable to all purchase agreements, it should include the following key provisions relevant to the heightened risks associated with data security and breaches.

Specifically:

The agreement should contain representations by the provider that service and support will meet specified levels of service, that security will be provided to prevent unauthorized access or destruction in accordance with industry standards, and that storage and backup will be maintained so that data is in retrievable form

---

118 In response to the number of cyberattacks suffered within the United States in 2014, Congress commissioned a study of the issues and challenges with cybersecurity, and the report can serve as resource to the stakeholders and institution's governing body in assessing, understanding, and appreciating the current risks to data within the United States. See Cybersecurity Issues and Challenges: In Brief, Congressional Research Service (April 14, 2015).

119 The U.S. Department of Education's Privacy Technical Assistance Center issued guidance to education institutions to assess the use of cloud computing and develop standard contract terms. See "Frequently Asked Questions – Cloud Computing," USDOE Privacy Technical Assistance Center (June 2012). See also "Protecting Student Privacy While Using On-Line Educational Services: Requirements and Best Practices," USDOE Privacy Technical Assistance Center (February 2014). In addition, guidance and contract templates issued by the United States federal government can also serve as useful resources for public education institutions. See Creating Effective Cloud Computing Contracts for the Federal Government – Best Practices for Acquiring IT as a Service, CIO Council/ Chief Acquisition Officers Council (February 24, 2012) (standard contract clauses can be found at: www.gsa.gov/graphics/staffoffices/FedRAMP_Standard_Contractual_Clauses_062712.pdf) .

to ensure the institution's continuity of use after contract termination.

The agreement should clearly state that the data is owned by the institution and may be used by the provider only to deliver the services. Data that constitutes confidential information should be clearly defined in the agreement and include, at a minimum, passwords, institutional data, personally identifiable information, student records, and health records.

The agreement should identify the actions to be taken in the event of a data breach, which should include, at a minimum, prompt notice to the institution, investigation of the cause and prevention of any reoccurrence, responsibility for all institutional losses as a result of the breach, and the granting to the institution of sole authority to determine if, when, how, and to whom notice of the breach should be sent.

Moreover, the agreement should exclude from any limitation of liability clause the provider's intentional or gross negligence and breach of data or confidential information.

To adequately protect against the risk of a data breach, the agreement should require the provider to name the institution as an additional insured on the provider's relevant insurance policies, including cyber insurance and commercial general liability insurance (which should have limits of liability of no less than $1 million per occurrence or per claim), umbrella or excess insurance, and professional liability insurance (with limits of liability of at least $10 million unless the amount of data to be stored with the provider demonstrates that a higher limit is appropriate).

Finally, the agreement should require the destruction of the institution's data after the agreement is terminated and certification that destruction has occurred.

Very often, a provider will seek to restrict its liability for data breaches through a limitation of liability and may be unwilling to agree to an absolute exclusion for a data breach. In that event, the institution should evaluate the potential costs it may incur and losses it may suffer as a result of a data breach by considering the total number of records and number of individuals related to the data that will be transferred to the provider. At a minimum, the institution should expect to incur, in the event of a breach, costs associated with providing notice to individuals, credit monitoring, undertaking forensic analysis to identify the cause of the breach, adequately and responsibly responding to media inquiries while protecting the institution's reputation, and responding to or defending third party claims. Studies that examined the losses associated with responding to data breaches over the past few years estimate these costs are approximately $200 per individual or 57 cents per record, and institutions should annually reevaluate this information to determine if costs are increasing.[120] At the present time, these studies provide a guideline

120 In 2015, Verizon commissioned a study with contributions from 70 entities around the world, and its findings are summarized in a report entitled the "Data Breach Investigation Report," Verizon Risk Team (2015). In 2014, Verizon commissioned a similar global study with 17 partners from the audit, law enforcement, and security fields, and its findings were summarized in a report entitled "Data Breach Investigation Report," Verizon Risk Team (2013). Verizon's reports are located

for institutions to negotiate secondary caps on limitation of liability clauses for claims arising out of data breaches. In the event the provider is unwilling to agree to a secondary cap that will limit its liability for data breaches in an amount that is acceptable to the institution, the purchase of cyber insurance by the institution provides an alternative for mitigating that risk.[121]

The risks inherent in storing personally identifiable information with a third party are an institutional risk, and the members of the governing body owe a fiduciary duty to the institution to be fully informed of and consent to these risks.[122] Therefore, it is recommended that the team of stakeholders present to the governing body, with participation and approval by the institution's president, their summary of the due diligence undertaken of the selected cloud provider and the terms of the agreement, along with an explanation of how the agreement or a cyber insurance policy will mitigate the risks associated with cloud data storage. Upon approval by the governing body, the stakeholders' work does not end. As we have seen in recent media associated with Rutgers University[123], Penn State University[124], and the Internal Revenue Service, the risk as to "if" a data breach will occur no longer exists; it is really a question of "when." Consequently, institutions would be well served to prepare in advance of a data breach by creating a response team; implementing a response protocol and performing practice drills; establishing compliance activities to implement, monitor, review, and update data security policies; and regularly informing the governing body so it can properly discharge its fiduciary duties.[125]

C. Insurance Coverage for Cyber Security Breaches

The importance of investing the necessary time, effort, and expense to identify and establish appropriate IT solutions for an institution's ongoing educational, research, or business operations – including cloud-based alternatives – cannot be overstated. But even after an institution completes a comprehensive due diligence process and negotiates maximum contractual protection, the vast majority of cloud-based IT opportunities will nonetheless expose the institution to additional (and potentially substantial) risk, which must be mitigated to satisfy the governors' or

---

at: www.verizonenterprise.com/DBIR. Studies with similar findings were undertaken by Zurich Insurance and The Ponemon Institute. See Data Breach: The Cloud Multiplier Effect, Ponemon Institute (June, 2014); see also Diaz and Crapo, supra note 33; Data Breach Cost: Risks, Costs, and Mitigation Strategies for Data Breaches, Zurich General Insurance (2012).

121 See discussion infra Section III.C.

122 Gallardo and Kaplan, supra note 3.

123 Ellen Wexler, Another Network Outage at Rutgers Leads to Frustration Among Professors and Students, The Chronicle of Higher Education, Sept. 30, 2015, http://chronicle.com/article/Another-Network-Outage-at/233483/. See also, David Gialanella, Universities Help Drive Need for Data-Security Advice, New Jersey Law Journal, October 3, 2014.

124 Universities 'Peculiar Creatures' in Cybersecurity World, Cyber Security Caucus, May 22, 2015, http://cybersecuritycaucus.com/universities-peculiar-creatures-in-cybersecurity-world/.

125 The U.S. Department of Commerce's National Institute of Standards and Technology issued comprehensive recommendations to identifying confidential data, implementing safeguards to prevent breaches, and developing breach response protocol in a report entitled Guide to Protecting the Confidentiality of Personally Identifiable Information, Special Publication 800-122 (April 2010).

trustees' obligations to exercise sound judgment and risk management in university governance. Accordingly, an institution must pursue an in-depth analysis of its existing insurance coverage to determine whether additional coverage is required to transfer the risk of potential loss and damage in the event of a data security breach.

At the outset, it is important to recognize that reliance on existing commercial general liability (CGL) insurance to mitigate the risk of loss and damage from cyber security breaches is simply not appropriate without careful assessment, analysis, and decision-making with respect to potential risks the institution faces as a result of its data processing and data storage solutions, and the need for alternative risk mitigation and risk transfer mechanisms.[126] Recent developments regarding the availability of insurance coverage under a CGL policy for losses resulting from a cyber security breach demonstrate that the existence of coverage is far from certain. For example, the Connecticut Supreme Court recently affirmed an intermediate appellate court decision that there was no coverage available under a CGL policy for $6 million of costs incurred as a result of the loss of 130 back-up tapes that contained employment related data of more than 500,000 past and current employees.[127] Similarly, a New York trial court concluded that the insurance company had no duty to defend under a CGL policy because it was the acts of a third party – not the policyholder – that caused the release of personal information as a result of a data security breach.[128] Other courts, however, have reached the opposite result, concluding that insurance coverage was available because the disclosure of personal information was within the scope of the terms of the relevant CGL policy at issue.[129] Separately, the insurance industry has taken affirmative steps consistent with its steadfast position that the CGL policy was not intended to provide insurance for the losses and damage that may be suffered as a result of cyber security breaches, as evidenced by the introduction of specific exclusions for general liability policies that purport to eliminate coverage for liability arising out of certain data breaches.[130] Due to this "mixed bag" regarding availability, an institution relying on a CGL policy to provide insurance coverage in the event of a data breach might be successful, but its likelihood of actual

---

126 Foster, supra note 102, at 27. Cyber insurance has been available for an extended period and has evolved to become suitable for both cloud users and cloud providers. Ideally, both the institution and the vendor will have completed appropriate due diligence and implemented comprehensive risk mitigation strategies that include cyber insurance coverage.

127 See Recall Total Info. Mgmt. v. Federal Ins. Co., 83 A.3d 664 (Conn App. 2014), aff'd, 115 A.3d 458 (Conn. 2015).

128 See Zurich American Insurance Co. v. Sony Corp. of America et al., 2014 N.Y.LEXIS 5141 (N.Y. Sup. Ct. 2014).

129 See Travelers Indem. Co. v. Portal Healthcare, 35 F.Supp 3d 765 (E.D. Va. 2014); Hartford Cas. Inc. Co. v. Corcino & Assocs., No. 13-1328, 2013 U.S. Dist LEXIS 152836 (D. Calif. Oct. 7, 2013); see also Eyeblaster, Inc. v. Federal Ins. Co., 613 F.3d 797 (8th Cir. 2010) (coverage under CGL policy was available because insurer failed to establish that the policy terms applied to preclude coverage).

130 See ISO Form Nos. CG 21 06 05 14 (Exclusion for Access or Disclosure of Confidential or Personal Information and Data-Related Liability – With Bodily Injury Exception); CG 21 07 05 14 (Exclusion for Access or Disclosure of Confidential or Personal Information and Data-Related Liability – Limited Bodily Injury Exception Not Included); CG 21 08 05 14 (Exclusion for Access or Disclosure of Confidential or Personal Information (Coverage B Only)).

success is increasingly narrow and depends on the jurisdiction and law applied to policy interpretation, the relevant facts, and the specific terms, conditions, and exclusions of the individual CGL policy.

Standalone cyber insurance policies can serve as an effective "gap filler" to cover some of the potential losses and damage that the educational institution may suffer from a data security breach that is not covered under other insurance. In general, cyber insurance provides coverage for certain losses arising out data breaches, but not all cyber insurance policies are created equal. Therefore, the terms of each policy must be carefully reviewed to verify that coverage is provided for potential losses identified in the due diligence process, including losses resulting from services of third party cloud providers. In this regard, insurance coverage is available for losses related to third party claims, notification to individuals, credit monitoring, forensic investigations, public relations and crisis management, data recovery, and government sanctions (within and outside of the United States). It is also very important to consider the appropriate geographic scope of coverage, particularly with respect to cloud computing, which, as noted above, may result in data being sent and/or stored outside a defined geographic location or area, including outside the United States. Finally, the cost of cyber insurance varies by insurer and the scope and amount of insurance desired, so focusing on the extent of necessary insurance is essential to obtaining appropriate, cost effective coverage. In addition, by keeping IT security and data policies up-to-date and ensuring that third party cloud vendors adhere to those updated policies, any requirements imposed by law, and the terms of the negotiated contracts, institutions can minimize the costs of cyber insurance coverage while also lowering potential exposure.

It should be emphasized, however, that any cyber security breach that results in wrongfully disclosed data carries hidden costs that are difficult, if not impossible, to quantify and are generally not insurable. In this regard, institutions must be concerned with damage to their endowments, enrollment, and reputations, both from those individuals directly affected and because large or sensitive breaches draw unfavorable media attention. Further, efforts directed at responding to a breach impair institutional productivity due to employee time and effort being redirected toward response instead of normal operations. Finally, a large breach erodes public trust, potentially further damaging future opportunities with prospective employees, potential students, alumni, and endowments.

In an effort to mitigate some of the risk associated with cloud-based data solutions, cyber insurance should be considered for the following categories of potential liability:

Costs of notice, reporting, investigation, and credit monitoring in the event of a data security breach;

Costs of defending third party lawsuits that may result from the loss of personally identifiable employee, alumni, or student information, in particular for public universities in the event the state attorney general's office declines to defend;

Statutory and/or regulatory investigation costs, penalties, and fees;

Public relations and crisis management fees;

Wrongful acts of outside vendors, consultants, or service providers;

Data restoration costs to replace or restore a system that suffered a data security breach;

Failure to prevent the spread of a virus or cyber attack within the institution's network;

Expenses required to respond to threats to harm or release data, as well as ransom payments; and

Impairment or loss of data as the result of a criminal or fraudulent cyber incident, including theft and transfer of funds.

When evaluating the amount of coverage and the relevant terms, conditions, and exclusions, note that a recent study estimates that costs of a data breach per lost or stolen record for an educational institution could average as high as $300 per compromised record, which would quickly exhaust a $5 million policy with a breach of only 16,700 records (well below the average records per breach in 2015).[131] Moreover, educational institutions should insist on readily understandable policy wording – e.g., some policies make distinctions between "lost" and "stolen" data that can serve to exclude coverage.[132] In addition, as noted above, for an institution that was unable to secure sufficiently favorable terms with respect to a vendor's obligations in that contract, negotiating with the insurer to include coverage for certain acts and omissions of cloud vendors may present a way to nonetheless mitigate some of that risk. Finally, since data breaches are a relatively recent phenomenon, and the costs and manner of resolving any resulting third party claims are evolving, purchasers of cloud services should reevaluate annually the limits of liability and the terms, conditions, and exclusions of their cyber insurance policy to verify that they are adequately insured.

IV. Conclusion

Optimizing an educational institution's cyber risk protection mechanisms involves a considerable commitment of resources to achieve focused preparation, analysis, and decision-making. Given the ever-increasing sophistication of cyber security threats and the expanding use of cloud-based alternatives to data processing and storage needs, educational institutions must take proactive steps to protect information and secure maximum protection against potentially crippling liability in the event of a data security breach. Even where high levels

---

131 Ponemon Institute LLC, 2015 Costs of Data Breach Study: Global Analysis, 1 (2015). The Ponemon Institute's study involved 350 companies from eleven different countries, and, while the global average per record costs of a data breach were estimated at $154, U.S. companies had the most costly per record costs at $217 per compromised record.

132 For example, under Amazon's standard contract for cloud computing services, it states that "Neither we nor any of our affiliates or licensors will be responsible for any compensation, reimbursement or damages arising in connection with…any authorized access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of your content or other data." See Foster, supra note 102 at 13.

of security controls are implemented in response to high levels of risk, many educational institutions have been victims of data breaches or experienced serious system failures within the past year.[133] Appropriate cyber insurance thus should be considered an integral part of any institution's cyber security protections. Cyber insurance is not a substitute for properly designed and implemented data security programs, but it can serve as effective supplementary protection that educational institutions and boards of trustees or governors may turn to when data security breaches occur despite best efforts at prevention.

133 Warwick Ashford, Cyber Insurance Complements Security Controls, Says Aon, ComputerWeekly.com, Jul. 14, 2014, http://www.computerweekly.com/news/2240224437/Cyber-insurance-complements-security-controls-says-Aon.