The John Marshall Journal of Information Technology & Privacy Law

Volume 33 | Issue 2 Article 3

2017

Protecting Colleges & Universities Against Real Losses in a Virtual World, 33 J. Marshall J. Info. Tech. & Privacy L. 101 (2017)

Gregory Demers

Seth Harrington

Mark Cianci

Nicholas Green

ARTICLE

PROTECTING COLLEGES & UNIVERSITIES AGAINST REAL LOSSES IN A VIRTUAL WORLD

GREGORY L. DEMERS, SETH C. HARRINGTON, MARK A. CIANCI, AND NICHOLAS R. GREEN,

– ROPES & GRAY LLP *

SUMMARY:

Colleges and universities are prime targets for cyberattacks. Authors Gregory L. Demers, Seth C. Harrington, Mark A. Cianci, and Nicholas R. Green explore emerging data security risks and litigation trends on college campuses, and offer ways to manage these risks through a comprehensive insurance plan. Given the increasing variety and complexity of plans available, it is incumbent upon universities to regularly reassess the coverage afforded by their existing policies.

* Gregory L. Demers (gregory.demers@ropesgray.com or 617-951-7015) is an associate in Ropes & Gray's business & securities litigation practice, Seth C. Harrington (seth.harrington@ropesgray.com or 617-951-7226) is a partner in Ropes & Gray's privacy & data security practice, Mark A. Cianci (mark.cianci@ropesgray.com or 617-951-7122) is an associate in Ropes & Gray's business & securities litigation practice, and Nicholas R. Green is a student at Boston College Law School.

I. INTRODUCTION[1]

One of the institutions to benefit most from rapid advancements in computer technology is the university. Colleges and universities have long been a hub of innovation in a variety of fields, but over the last two decades, the entire system of higher education itself has been transformed by innovation, both internal and external.

At its core, a university facilitates the transfer of knowledge between faculty, students, administration, and the broader community. Advances in information technology, and, specifically, computer technology, have fundamentally changed the way in which this process takes place. Today, professors teach their classes with the aid of computer simulations and iPads, students takes notes on laptops, study groups form after class in chat rooms, and entire courses occur online. But as the educational process moves further and further into a virtual world, real risks remain.

One cyber security analyst has opined that "[n]o more fertile ground for security breaches exists in the United States than our colleges and universities."[2] A 2015 forecast published by the credit reporting agency Experian identifies insider breaches, both inadvertent and malicious, as one of the largest data security threats in the coming years.[3] The existence of vast amounts of valuable personal data, combined with the presence of thousands of sometimes gullible, sometimes malicious, young students places colleges and universities at particular risk of targeting. For example, in 2014, thirty educational institutions reported having experienced data security incidents, five of which each potentially implicated over 50,000 unique records.[4] This article explores certain emerging risks and litigation trends on college campuses, and offers ways to manage these risks through a comprehensive insurance plan.

II. EMERGING RISKS & LITIGATION TRENDS

Just before stepping down in March 2012, Shawn Henry, the FBI's top cyber security expert, gave a sobering view of America's war on

---

1. Peter L. Welsh, a partner in the business and securities litigation practice group at Ropes & Gray, and J. William Piereson, a student at Harvard Law School, also contributed to the authorship of this article.

2. Alan Wlasuk, *Higher Education – The Perfect Security Storm*, SECURITYWEEK (June 29, 2012), http://www.securityweek.com/higher-education-perfect-security-storm.

3. Experian Data Breach Resolution, *2015 Second Annual Data Breach Industry Forecast*, 6 (2015), https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf.

4. Kyle McCarthy, *5 Colleges With Data Breaches Larger Than Sony's in 2014*, THE HUFFINGTON POST (Mar. 17, 2015), http://www.huffingtonpost.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html.

cyber crime: "We're not winning."[5] Another cyber security expert was even less optimistic, opining that there is not a single secure, unclassified computer network in the United States.[6] In a remarkable testament to these statements, the United States Office of Personnel Management announced a massive data security breach in 2015 that allegedly put at risk the personal information of at least 18 million former and current federal employees.[7] The breach also reportedly included detailed information on approximately 4 million Americans who had applied for or received a security clearance.[8]

Colleges and universities are prime targets for these attacks. More than any other demographic, college students spend massive amounts of time on the internet, engaging in various forms of information-sharing.[9] Consequently, on college campuses, "[m]alicious software (malware), phishing, infrastructure attacks, social network targeting, and peer-to-peer (P2P) information leakage are not potential threats; they're actual, daily issues."[10] The expanded scope of university network operations, including the use of outsourced service providers, further compounds these issues[11]—not to mention the ever-present risk of students or employees stealing or misplacing laptops containing sensitive information.

Recent studies prove these fears well-founded. According to the Privacy Rights Clearinghouse, the education sector had the second most reported breaches over the 9 year period between 2005 and 2014 out of all the industry sectors tracked by the non-profit privacy group.[12] In addition McAfee, one of the world's leading computer security companies,

---

5. Devlin Barrett, *U.S. Outgunned in Hacker War*, THE WALL STREET JOURNAL (Mar. 28, 2010), http://online.wsj.com/article/SB10001424052702304177104577307773326180032; *see also* Juliette Fairley, *Insurance Industry Responds to Cyber Attack Increase*, INSURANCE NETWORKING NEWS (Apr. 20, 2012), https://www.dig-in.com/news/insurance-industry-responds-to-cyber-attack-increase (quoting one cyber insurance broker as stating that data breaches are "a threat that's here to stay. We're sure to see even more of an increase going forward.").

6. Barrett, *supra* note 5.

7. L. Gordon Crovitz, *We're Losing the Cyber War*, THE WALL STREET JOURNAL (Jun. 28, 2015), http://www.wsj.com/articles/were-losing-the-cyber-war-1435508565.

8. *Id*.

9. Rod Rasmussen, *The College Cyber Security Tightrope: Higher Education Institutions Face Greater Risks*, Security Week (Apr. 28, 2011), http://www.securityweek.com/college-cyber-security-tightrope-higher-education-institutions-face-greater-risks.

10. *Id*. Furthermore, "[d]ue to the nature and complexity of operations and the academic culture of open access, educational institutions, and in particular, large research-oriented universities, face unique exposures related to the internet and information security and privacy." Sarah Stephens & Shannan Fort, *Cyber Liability & Higher Education*, Aon Professional Risk Solutions White Paper 2 (Dec. 2008).

11. Stephens & Fort, *supra* note 10 at 2.

12. Joanna Grama, *Just In Time Research: Data Breaches in Higher Education*, 2, EDUCAUSE (2014), https://net.educause.edu/ir/library/pdf/ECP1402.pdf.

ranked universities as the most dangerous place for an individual to give out sensitive personal information.[13]

Recent data suggest that colleges and universities have made progress enhancing data security protocols, with the educational sector accounting for 7.4% of total known breaches in 2015, down from a 10-year high of 47.8% in 2005.[14] Nevertheless, educational institutions have suffered at least 53 known breaches in 2016 alone, potentially placing at risk more than 360,000 records, outpacing both the government and banking industries in terms of total number of breaches in the first six months of the year.[15] This data confirms that colleges and universities continue to face significant data security risks.

In recent years, university data breaches have received wide publicity. Since January 1, 2016, at least five major universities disclosed events that potentially exposed a significant amount of individuals' personal data.[16] In January, the University of Virginia disclosed a phishing email scam that involved the W-2 information for approximately 1,400 employees.[17] In February, the University of California at Berkeley acknowledged that a hacker gained access to a database containing the information concerning more than 80,000 students and staff.[18]

An April 2015 article in USA Today further documented a series of university breaches in 2014 and 2015, including those at Auburn, Butler, University of Chicago, Iowa State, and the University of Maine.[19]

---

13. Robert Siciliano, *Top Ten Most Dangerous Places to Leave Your Social Security Number,* MCAFEE: SECURING TOMORROW (Oct. 18, 2010), http://blogs.mcafee.com/consumer/identity-theft/top-ten-most-dangerous-places-to-leave-your-social-security-number.

14. Identity Theft Resource Center, *ITRC Breach Statistics 2005-2015* (2016), http://www.idtheftcenter.org/images/breach/2005to2015_20160828.pdf.

15. Identity Theft Resource Center, *2016 Data Breach Category Summary* (Dec. 13 2016), http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2016.pdf.

16. *January 22, 2016 Incident: UVA Notifies Some Employees of Illegal Access to Personally Identifiable Information*, UNIV. OF VA.: INFORMATION SECURITY, (Jan. 22, 2016)(hereinafter *UVA Notification*), http://www.virginia.edu/informationsecurity/Jan-22-incident-FAQs (announcing breach at University of Virginia); Janet Gilmore; *Campus alerting 80,000 individuals to cyber attack*, BERKELEY NEWS (Feb. 26, 2016), http://news.berkeley.edu/2016/02/26/campus-alerting-80000-individuals-to-cyberattack/ (reporting on data breach at University of California at Berkeley); *Intrusion into UCF Network Involves Personal Data*, UNIV. CENT. FL. (May 19, 2016), https://www.ucf.edu/datasecurity/ (announcing breach at University of Central Florida); *Information on Data Security Incident*, MICH. STATE. UNIV. (accessed March 28, 2017), https://msu.edu/datasecurity/ (announcing November 2016 data breach at Michigan State University); Michelle Ricciardi, *Arizona Man Arrested for Hacking More Than 1,000 Pace Email Accounts*, THE PACE CHRONICLE (Nov. 8, 2016), http://pacechronicle.com/news/2016/11/08/man-arrested-for-hacking-more-than-1000-pace-email-accounts/ (reporting November data breach at Pace University).

17. *UVA NOTIFICATION*, *SUPRA* NOTE 16.

18. GILMORE, *SUPRA* NOTE 16.

19. Lauren Coffey, *College security breaches: Where they've happened and how to*

The Butler breach allegedly exposed nearly 200,000 records, including Social Security numbers and banking details.[20]

Worse than the recent uptick of these attacks is the potential liability posed by each event. In short, it is massive. In June 2016, IBM and the Ponemon Institute released their annual study on the costs to a business of a data breach, concluding that they continue to rise.[21] Breaches in the United States cost an average of $221 per record and $7.01 million per breach.[22] Particularly troubling for colleges and universities, the average cost per record within the education sector can be as high as $246.[23]

Colleges and universities may feel the effects of breaches for a number of years, as the costs are not only steep but varied.[24] Contributing factors include the costs of credit monitoring for affected individuals,[25] computer forensics investigations, audit and consulting services, public relations services, loss of business, loss of property,[26] and loss of reputation, which could result in a number of consequential damages including lower enrollment and a decrease in donations.[27]

The foregoing list does not even include two of the most significant costs: regulatory penalties and the costs of litigation. The government has many means of seeking to penalize institutions for the negligent

---

prevent them, USA TODAY COLLEGE (Apr. 16, 2015), http://college.usatoday.com/2015/04/16/college-security-breaches-where-theyve-happened-and-how-to-prevent-them/.

20. *Data Breach at Butler University Exposes Personal Data of Nearly 200,000*, UNIV. HERALD (Jun. 30, 2014), http://www.universityherald.com/articles/10157/20140630/personal-data-butler-breach-name-driver-license.htm.

21. *Ponemon Institute,* 2016 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS, 10 (June 2016), *available at* http://www-03.ibm.com/security/data-breach/.

22. *Id*.

23. *Id*.

24. Sherrie Negrea, *Hard Costs of a Data Breach*, UNIV. BUS. (May 28, 2015), https://www.universitybusiness.com/article/hard-costs-data-breach (listing five principal expenses for colleges after discovering data breaches).

25. *UH Settles Data Breach Class Action Lawsuit*, KITV NEWS (Jan. 26, 2012), http://www.kitv.com/UH-Settles-Data-Breach-Class-Action-Lawsuit/-/8906042/9658894/-/ucebfsz/-/index.html. According to one plaintiffs' attorney, "[w]e have researched more than 40 data breaches at colleges and universities across the country [and in] almost every instance, two years of credit monitoring and fraud restoration were offered to data breach victims."

26. Brian Krebs, *Cyber Thieves Steal Nearly $1,000,000 from University of Virginia College*, KREBS ON SECURITY (Sept. 2009), http://krebsonsecurity.(Sept. 2009), http://krebsonsecurity.from University of Virginia Collegeia-college/. One compelling example occurred in 2010, when hackers compromised a computer owned by the comptroller of a University of Virginia satellite campus and attempted to transfer $996,000 from the university to the Agricultural Bank of China. The university ultimately recovered the funds..

27. *Ponemon Institute, supra* note 21 at 21; *see also* Rasmussen, *supra* note 9 (describing the potential fallout as "a public relations nightmare, real financial losses, far-reaching legal issues and regulatory non-compliance penalties").

disclosure of personal information, such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Computer Fraud and Abuse Act (CFAA), the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), the Fair and Accurate Credit Transactions Act (FACTA), and the Federal Trade Commission's Red Flags Rule, 6 C.F.R. Section 681.2, along with numerous overlapping state and local laws.

Each of these statutes empowers the government with broad authority to punish wrongful disclosures. For instance, the 2009 enactment of the HITECH Act significantly expanded HIPAA liability, creating a tiered penalty structure with larger payouts ranging from $100 to $50,000 per violation, with an annual cap of $1.5 million.[28] The FTC's Red Flags Rule provides for up to $2,500 in civil penalties per violation,[29] the CFAA provides for a fine of $200,000 to $500,000 for organizations,[30] and FERPA violations can result in the loss of millions of dollars in federal funding.[31]

The remedies available to private plaintiffs are just as broad. As evidenced by a recent empirical analysis of data breach lawsuits in the United States, plaintiffs bring a number of claims under both common law (e.g., negligence, invasion of privacy, and breach of contract) and statutory law (e.g., state consumer protection acts, the CFAA, the Electronic Communications Privacy Act, and the Fair Credit Reporting Act).[32]

Unsurprisingly, the study found that a strong predictor of whether the breach will result in litigation is the perceived culpability of the institution.[33] If the breach is perceived to have been caused by the institution's own careless or negligent disclosure of personal information, as opposed to cyber attacks or theft, then a lawsuit is more likely to follow.[34] In addition, the likelihood of litigation varies considerably depending on the amount and perceived sensitivity of the compromised data.[35] For instance, the mean number of compromised records in data breach cases that did not result in litigation in federal court was 98,000, whereas litigated cases averaged 5.3 million records.[36] The study also

28. Pub. L. 111-5, div. A, title XIII, subtitle D, § 13410(d)(3) (123 Stat. 273) (2009).
29. 15 U.S.C. § 1681s(a)(2) (2012).
30. 18 U.S.C. § 1030(c)(2)(B).
31. 20 U.S.C. § 1232g(b) (2012).
32. Sasha Romanosky, David Hoffman, & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL L. STUD. 90, app. Figure 7 (June 1, 2012), http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf.
33. *Id*. at Table 2.
34. *Id*. at Figure 7.
35. *Id*.
36. *Id*. It is important to keep in mind that the study focused only on federal litiga tion, so the filtered data may include some cases that resulted in state court litigation.

found a positive correlation between compromised data requiring a heightened level of protection, such as Social Security numbers, medical information, and financial data, and the probability of a subsequent lawsuit being filed.[37]

Class action lawsuits against universities following data breaches are becoming increasingly common. In February 2016, a former student body president and a member of the University of Central Florida's board of trustees sued the University in federal court, as class representatives, after the school acknowledged the theft of 63,000 Social Security numbers.[38] In August 2014, the University of Miami settled class action claims stemming from a patient records hack at its medical school.[39]

One of the most highly publicized data breach lawsuits in the higher education context involved the exposure of sensitive information at the University of Hawaii between 2009 and 2011.[40] In Gross v. University of Hawaii,[41] a student filed a class-action lawsuit against the university after discovering that a retired professor had posted personal financial information, including Social Security numbers, of more than 40,000 alumni on a public internet server. The case settled in January 2012, with the university agreeing to provide two years of credit monitoring and fraud restoration services, at a cost of an estimated $550,000.[42]

Academic medical centers should be an area of particular concern for risk managers, as they serve as repositories of vast amounts of sensitive personal information, including personal health information. For this reason, academic medical centers account for a disproportionate number of data breach lawsuits affecting colleges and universities.

For example, on July 17, 2015, the University of California at Los Angeles Health System announced a major data breach that potentially exposed the medical and financial information of up to 4.5 million patients.[43] Though UCLA allegedly observed suspicious activity on one of its servers as early as October 2014, the university did not notify pa-

---

37. *Id*.

38. Sean Lavin, *UCF hit with class action lawsuit in Social Security Hack*, WKMG NEWS (Feb. 8, 2016), http://www.clickorlando.com/top-stories/ucf-hit-with-class-action-lawsuit-in-social-security-hack.

39. Kelly Knaub, *University Of Miami Reaches Deal In Health Records Suit*, LAW360 (Aug. 11, 2014), http://www.law360.com/articles/565805/university-of-miami-reaches-deal-in-health-records-suit. The case settled for a relatively modest $100,000, plus $90,000 in attorney's fees.

40. *UH Settles Data Breach Class Action Lawsuit*, supra note 25.

41. Complaint, *Gross v. University of Hawaii*, No. 10-00684-ACK (D. Haw. Nov. 18, 2010).

42. *UH Settles Data Breach Class Action Lawsuit*, *supra* note 25.

43. Chad Terhune, *UCLA Health Systems Data Breach Affects 4.5 Million Patients*, THE L.A. TIMES (July 17, 2015), http://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html

tients until seven months later.[44] The resultant class action lawsuit, currently pending in California state court, alleges that UCLA failed to take basic security steps, including encryption of the sensitive data.[45]

This most recent suit against the UCLA health system follows two lawsuits in 2011 related to alleged improper storage of patient records.[46] In December 2011, plaintiffs filed a class-action lawsuit against UCLA after burglars stole medical records and other personal information belonging to approximately 16,000 patients from a physician's home.[47] Underscoring the potential liability involved, the suit sought $1,000 for each affected individual, totaling more than $16 million in damages, under a California statute that prohibits the disclosure of patient medical information.[48] Five months before that case was filed, in July 2011, UCLA agreed to pay $865,500 to settle an investigation by the U.S. Department of Health and Human Services into prior security and privacy violations.[49]

The class action complaint in the 2015 case alleges that several large data breaches from the last decade put UCLA on sufficient notice of its data protection obligations.[50]

In November 2015, Indiana University Health Arnett Hospital notified roughly 30,000 patients that their names, dates of birth, home phone numbers, and medical diagnoses were potentially compromised after an unencrypted USB storage device containing emergency room medical records went missing.[51] Indiana University's hospital had previously announced another data incident in 2013, involving the theft of an employee laptop with sensitive data for 10,000 patients.[52]

Similarly, in September 2015, Louisiana State University's New Orleans School of Medicine informed patients that a doctor's laptop was stolen from inside his car while it was parked in front of his home, placing at risk at least 5,000 patients' data.[53] The university health system

---

44. *Id.*

45. Complaint, *Adlouni v. UCLA Health Systems Aux.*, Docket No. BC589243, July 24, 2015 (Cal. Sup.)

46. Joseph Conn, *Suit Against UCLA Health System Filed for Breach*, MODERN HEALTHCARE (Dec. 21 2011), http://www.modernhealthcare.com/article/20111221/NEWS/312219988.

47. Complaint, *Oganyan v. Regents of Univ. of Cal.*, Docket No. BC475171, Dec. 14, 2011 (Cal. Sup.)

48. *Id.* at 9, ¶ 41.

49. Amanda Bronstad, *UCLA Hospitals Sued over Patient Data Breach*, THE NATIONAL LAW JOURNAL (Dec. 20, 2011), http://www.doc1solutions.com/resources/other/ucla-hospitals-sued/.

50. Class Action Complaint at 6-7, *Miguel Ortiz v. UCLA Health System, et. al.*, No. BC589327 (Cal. Super. Ct. L.A. Cnty. 2015).

51. Chris Morisse Vizza, *Purdue IT Security Expert: Don't Panic About 30,000 Com promised Health Records*, WBAA.org (Jan. 8, 2016), http://wbaa.org/post/purdue-it-security-expert-dont-panic-about-30000-compromised-health-records.

52. *Id.*

53. WGNO.com, *LSU doc's stolen laptop brings offer for free credit protection for*

offered all affected patients one year of free credit monitoring.[54]

III. RISK MANAGEMENT THROUGH INSURANCE

A. EVOLVING RISK MANAGEMENT STRATEGIES

In the last two or three decades, risk management at colleges and universities has become an increasingly sophisticated affair. This is likely the foreseeable byproduct of the increasing size and scope of universities themselves, which now operate on the same plane as the largest companies in the United States—supervising hundreds of employees, providing food and housing to thousands of students, bringing in and doling out hundreds of millions of dollars each year, managing multi-billion-dollar endowments, undertaking massive construction projects, engaging in countless non-profit endeavors, and sustaining world-class research programs.

Even today, however, the most fundamental of all risk-management tools remains a comprehensive insurance plan. But insurance has evolved a great deal in recent years, as insurers attempt to satisfy shifting consumer demands by producing new policies and modifying or drafting new coverage provisions. Colleges and universities, like all consumers, need insurance products that will cover the broad array of risks spawned from their expanding operations. In years past, universities could survive with a standard general liability policy and perhaps one or two supplemental policies. Such is not the case today.

Now, it is common for the largest universities to maintain some or all of the following: Comprehensive General Liability Insurance (CGL), Directors and Officers Insurance (D&O), Educators Legal Liability Insurance (ELL), Employment Practices Liability Insurance (EPL), First-Party Property Insurance, Automobile Liability Insurance, Sexual Abuse and Molestation Insurance, Disaster Insurance, Athletic Insurance, and Medical Malpractice Insurance.[55] Some even purchase endorsements or separate policies that cover aircraft, water craft, ROTC, kidnap and ransom, and rare books, to name a few.

In many cases, these policies are supplemented by numerous excess insurance policies, third-party insurance policies required by contract (e.g., professional liability policies, event coverage policies), and self-insurance plans.[56] Given the increasing variety and complexity of plans available, it is incumbent upon universities to regularly reassess the

---

NOLA area patients, WGNO ABC (Sept. 16, 2015), http://wgno.com/2015/09/15/lsu-docs-stolen-laptop-brings-offer-for-free-credit-protection-for-nola-area-patients/.

54. *Id.*

55. *See, e.g., How the University Insures Itself*: *Self Insurance Programs* UNIV. OF CAL. AT BERKELEY, http://riskservices.berkeley.edu/insurance-programs (describing a broad array of self insurance and third party coverage for a variety of risk types).

56. *Id.*

coverage afforded by their existing policies. This is especially true in an age in which the scope of university operations and rapid technological advances give rise to new risks almost daily.

B. CONTRACTUAL PROTECTIONS

Before turning to insurance, risk managers should revisit (and perhaps revise) the protections afforded by their existing contracts. In particular, universities should carefully examine the allocation of risk and scrutinize indemnification provisions within vendor contracts and contracts with other external partners such as data storage companies, internet service providers, and IT consultants. Some of these third parties will have their own insurance policies, and some will not. As in other contexts, universities should demand that these companies not only have an insurance policy in place, but also that the policy names the university as an additional insured.

Determining how contractual risk-allocation terms interact with the university's insurance plan and the vendor's insurance plan is not always an easy task—and it should be done well before a major loss occurs. Moreover, the use of multiple vendors or subcontractors brings added layers of complexity, compounded by the existence of more indemnification provisions and more insurance policies. But clearly defining the scope of the university's exposure is worth the time and effort, especially given the rising costs of data breaches and the fact that roughly thirty percent of all reported breaches result from action or inaction by third party vendors.[57]

C. UNCERTAINTY SURROUNDING TRADITIONAL & SPECIALIZED POLICIES

Today, many universities still do not have specialized policies in place that provide comprehensive coverage for losses resulting from data breaches. For those that do, much ambiguity remains under these policies, given that they are a relatively new product being offered by the insurance industry.

For instance, Colorado Casualty Ins. Co. v. Perpetual Storage, Inc.[58] arose out of a 2008 data breach, which occurred when thieves stole back-up tapes containing confidential information on 1.7 million of the University of Utah's hospital's patients. The back-up tapes were being held by Perpetual Storage, Inc., a data storage company retained by the University to warehouse its electronic data.[59] Although the tapes

57. Stephens & Fort, *supra* note 10 at 8.

58. Complaint for Declaratory Judgment, No. 2:10-cv-00316 (D. Utah Apr. 9, 2010), ECF No. 1.

59. Memorandum Decision and Order, No. 2:10-cv-00316, Mar. 30, 2011 (D. Utah).

were later recovered, the university spent $3.3 million on credit monitoring services and related expenses.[60]

In 2010, Perpetual Storage sought coverage for these losses from its insurer, Colorado Casualty Insurance Company, which in turn filed a lawsuit against Perpetual Storage and the university, arguing that the losses were not covered under a commercial package policy and a commercial liability umbrella policy issued by the company.[61] The University filed counterclaims seeking a declaratory judgment that the $3.3 million it incurred constituted covered losses.[62]

Colorado Casualty is just one example offered to highlight the fact that a great deal of uncertainty remains under traditional policies with respect to the emerging litigation risks discussed in this article. A growing body of case law outside of the education context makes this even more apparent.[63]

In addition, insurers are now drafting endorsements that cover only specific internet-related risks, offering coverage that is far from comprehensive, and many CGL policies limit the scope of coverage by adding express exclusions for such losses. One potential pitfall is the fact that CGL policies generally apply to "tangible property." To more expressly limit coverage in these instances, some insurers are adding provisions that exclude "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access or inability to manipulate electronic data."[64] Consequently, insureds are often left with considerable exposure in the event of a data breach.

The uncertainty surrounding the application of CGL policies to electronic data has led many policyholders to seek out new insurance solutions that offer more specialized coverage. In an effort to bridge these coverage gaps and satisfy a growing consumer demand, insurers have begun drafting social media policies, privacy and network security policies, and a hybrid often referred to as "cyber liability" policies.[65]

---

60. Complaint for Declaratory Judgment, *supra* note 58.

61. Memorandum Decision and Order, *supra* note 59.

62. *Id.*

63. *See, e.g.*, *Travelers Indem. Co. of America v. Portal Healthcare Solutions*, LLC, No. 14–1944, 2016 WL 1399517 (4th Cir. Apr. 11, 2016) (per curiam) (unpublished appendix decision affirming district court's finding that publication of patient data provision in an insurance policy issued to data storage company applied to data breach case and that insurer had a duty to defend); *but see Eyeblaster Inc. v. Federal Ins. Co.*, 613 F.3d 797 (8th Cir. 2010) (affirming denial of coverage in part due to policy's exclusion of losses relating to the distribution of electronic data); *America Online Inc. v. St. Paul Mercury Ins. Co.*, 347 F. 3d 89 (4th Cir. 2003) (holding that loss sustained in relation to the installation of computer software did not constitute property damage under CGL policy).

64. *See ISO Comments on CGL Endorsements for Data Breach Liability Exclusions*, INSURANCE J. (July 18, 2014), http://www.insurancejournal.com/news/east/2014/07/18/332655.htm. The Insurance Services Offices, an industry producer of form CGL policy language, published an endorsement in 2013 containing this limiting language which insurers have widely adopted.

65. *See* Rick Betterly, *Advances in Cyber Insurance Risk Management Services Help*

Demand for cyber insurance has increased significantly in recent years,[66] and a 2016 PricewaterhouseCoopers survey found that 59.36% of corporations polled have cybersecurity insurance.[67] PricewaterhouseCoopers research also forecasts £4.8 billion in increased global demand by the year 2020.[68] Despite the increase in demand, the insurance industry has yet to embrace a standard set of policy terms for data security coverage.[69] Nonetheless, as in the rest of the market, interest in cyber liability insurance among institutions of higher education appears to be surging in recent years.[70]

It may take years before the policies reach some level of uniformity, as litigation and subsequent case law gradually clear up the ambiguities inherent in newly drafted policies and establish bright-line rules for insurance companies and consumers to follow. This is not to say such policies are worthless at present—it simply means that they deserve greater scrutiny. The final section of this article examines some key coverage provisions in cyber liability policies, with a particular focus on the higher education context, and offers suggestions to ensure that universities receive the broadest coverage possible.

Protect Against Data Loss – But More Can Be Done, EXPERIAN (Jun. 18, 2013), http://www.experian.com/blogs/data-breach/2013/06/18/advances-in-cyber-insurance-risk-management-services-help-protect-against-data-loss-but-more-can-be-done/.

66. *See* Deirdre Fernandes, *More Firms Buying Insurance for Data Breaches*, THE BOSTON GLOBE (Feb. 17, 2014), https://www.bostonglobe.com/business/2014/02/17/more-companies-buying-insurance-against-hackers-and-privacy-breaches/9qYrvlhskcoPEs5b4ch3PP/story.html.

67. PricewaterhouseCoopers, *The Global State of Information Security Survey 2016*, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html.

68. *See* Danielle Correa, *Global Cyber-Insurance Market Predicted to Growth to £4.8b by 2020*, SC MAGAZINE (Sept. 18, 2015), http://www.scmagazine.com/global-cyber-insurance-market-predicted-to-growth-to-48bn-by-2020/article/439369/.

69. *See* Lynda Bennett, *Cyber Insurance Policies: Are They Worth the Money?*, CFO (March 30, 2015), http://ww2.cfo.com/risk-management/2015/03/cyber-insurance-policies-worth-money/.

70. Mike Smith, *Why Educational Institutions Are Buying Cyber Liability Insur ance*, LINKEDIN (March 16, 2015), https://www.linkedin.com/pulse/why-educational-institutions-buying-cyber-liability-insurance-smith (citing insurance industry statistics suggesting that there has been a 58% increase from 2013 to 2014 in the number of colleges buying cyber liability insurance). *Contrast* Neal Morton, *College Officials Wary of 'Cyber Insurance' for Private Data*, THE MONITOR (Aug. 9, 2010), http://www.themonitor.com/articles/officials-41652-insurance-college.html (reporting that representatives from the University of Texas-Pan American and South Texas College preferred to put funds towards preventive security measures rather than cyber liability insurance); *Information Security & Cyber Liability Risk Management: The Fifth Annual Survey on the Current State of and Trends in Information Security and Cyber Liability Risk Management*, ADVISEN, 3, (Oct. 2015), available at http://www.advisenltd.com/wp-content/uploads/2015/10/information-security-cyber-liability-risk-management-report-2015-10-16.pdf

D. KEY COVERAGE PROVISIONS

Given the relative novelty of this field, the coverage afforded by cyber liability policies inevitably will vary, often significantly, from insurer to insurer. Thus, whether internet-related losses may be covered by these specialized policies or by endorsements to traditional policies, a regular and thorough review of key policy features by experienced professionals must be a priority for any university risk manager. Such review is critical to mitigating future losses, as it ensures that the university is not reliant upon a court's interpretation in a situation not expressly contemplated by the terms of the policy.

Fortunately, larger insurance companies now offer a variety of cyber liability products for consumers to choose from, allowing them to adopt the coverage that they find to be most meaningful in their field. The losses commonly covered by these policies can be segregated into two categories: third-party losses and first-party losses. The former provides coverage for liability involving claims by third parties because of alleged wrongful acts or omissions by the university, while the latter provides coverage for costs incurred directly by the university.

Some examples of third-party claims for which universities can seek coverage are invasion of privacy resulting from the disclosure of confidential information; identity theft; property damage due to the transmission of a computer virus or other malicious code; and social media liability, including defamation, slander, libel, copyright and trademark infringement. A well-drafted policy will cover all litigation costs incurred in connection with the above claims, including defense costs, settlements, and judgments.

Coverage is also available for first-party losses including the loss or corruption of the university's electronic data; the fraudulent electronic transfer of monies out of the university; security breach notification expenses and credit monitoring services; investigation expenses; contributions to criminal reward funds in order to aid in the identification of the perpetrator; lost income due to business interruption; crisis management expenses; and extortion payments to prevent a future cyber attack or the disclosure of confidential information.

For some universities, especially smaller institutions with less reserves budgeted for insurance, the above coverage may be financially unattainable. However, for most universities, the question is not whether they are willing to pay the premiums for cyber liability coverage, but how can they minimize exposure and maximize value under their policies. The following are a few examples of key provisions that universities should demand in a cyber liability policy:

- "Breach" or "data breach" should be defined broadly to include not just the unlawful dissemination of confidential electronic data, but any alleged failure to protect such information and

unauthorized access to such information. Some of the most costly breaches do not involve the actual disclosure or fraudulent use of the information, as in Colorado Casualty,[71] but such events will still trigger coverage if an "access" provision is included. The policy should cover losses resulting from access to or the disclosure of confidential information, whether resulting from a breach of a university network, the theft of a student's laptop, or an employee's unauthorized distribution of confidential information.

- The policy should apply to all data security incidents, not simply attacks from outside sources, but should include coverage for situations involving a negligent or intentional breach caused by IT professionals performing network maintenance, human resource managers failing to secure sensitive information, or faculty members leaving student data exposed on publicly accessible websites. Relatedly, a severability or non-imputation clause should prohibit the knowledge or conduct of one insured from being imputed to another, such that intentional wrongful acts by an employee would not be viewed as an intentional wrongful act by the university.
- If the policy contains an insured-versus-insured exclusion, it should also contain a carve-out for data breach suits brought by insured employees against the institution.
- The "extortion" clause should broadly include all costs incurred in responding to extortion threats, not simply payments themselves. In many cases involving extortion, the victimized institution never actually pays the amount demanded. However, significant related expenses might include the costs of obtaining legal and public relations counseling, depending on the nature of the extortion threat. For instance, in May 2012, the University of Pittsburgh was faced with an extortion attempt by two men who demanded that the university publicly apologize for a series of recent bomb scares on the campus.[72] The men asserted that they had hacked into the university's system and threatened to release personal data of students and employees if the school did not comply with their demands.[73] The university did not give in to these demands, and the perpetrators were later apprehended and charged.[74]

---

71. Complaint for Declaratory Judgment, *supra* note 58.

72. Sadie Gurman, *Ohio Pair Charged in Threats Claim Ties to 'Hacktivists'*, Pitts burgh Post-Gazette (Aug. 8, 2012), http://www.post-gazette.com/stories/local/neighborhoods-city/ohio-pair-charged-in-threats-claim-ties-to-hacktivists-649175/.

73. *Id.*

74. *Id.*

- A university risk manager should take care to provide an exhaustive list of affiliated entities and subsidiaries that require coverage. Hackers might find it easier to breach the firewall of an out-of-state or overseas affiliate, for example, and could obtain sensitive university data without ever entering the university's network. As a result, it is critical that these covered entities are listed in the policy.
- The unauthorized withdrawal of funds from an institution through electronic means may be considered to constitute computer fraud, potentially covered under a fidelity bond or crime policy, although only to the extent that the withdrawal was caused by external access. Where funds are transferred pursuant to social engineering schemes (such as "phishing scams"), insurers have denied coverage. Thus, risk managers should push for explicit coverage for losses resulting from social engineering schemes, or, if insurers balk, ensure that the university is self-insured against the risk of such losses.
- The policy must cover all costs expended in the "investigation or remediation" of the breach, including the costs of determining the precise records lost and the persons affected; all notification costs, including mailings or other communications; up to two years of credit monitoring services; costs incurred to establish call centers; business interruption; and data restoration. Additionally, universities often draw upon the resources of various professionals, such as IT forensics experts and outside counsel, when responding to a data breach. Outside auditor and public relations firms are also sometimes used. A well-drafted policy should cover all such consulting services and should be broadly drafted to include any consulting services utilized in the "investigation or remediation" process.
- Often the insurer will demand that the costs incurred shall only be covered if the insured provides prior written consent. Universities have to act fast when they are notified of a potential breach and generally incur many thousands of dollars in expenses in a very short period. Wherever these consent provisions appear, they should be followed, at minimum, by the caveat that "consent may not be unreasonably withheld," but a risk manager may also consider obtaining pre-approval for outside counsel and preferred forensics and crisis management firms.
- "Network" should include university networks, shared networks, and any other network in which the university is involved in the transmission of data. Significantly, some universities are already at the forefront of the cloud computing trend, which, among other things, involves pooling data with other users outside the university's network. A broad definition of "network"

will cover breaches of the cloud that compromise university data.

- "Data loss" should include the corruption or decrease in value of electronically stored information, whether temporary or permanent. It is particularly important for large research universities to define such loss to include the loss of proprietary material, such as trade secrets, which may be exposed during a cyber attack. Moreover, the "data" or "information" exposed by the breach should include a comprehensive list of personal data. Significantly, colleges and universities should demand that personal medical information is expressly included in this list, as academic medical centers remain one of the most vulnerable targets on campus to cyber threats.
- In addition to the costs of litigation (e.g., defense, judgment, and settlement), the policy should cover civil fines and regulatory expenses. The government is cracking down on cyber crime, and part of this process includes seeking to hold organizations accountable for the failure to protect confidential personal information. Regulators can also seek to impose penalties for the failure to timely disclose a breach. A university should not only ensure that these costs are covered, but should also seek out carriers that provide coverage for such regulatory losses up to the full policy limit, as many impose a much lower sublimit.
- Just the cost of responding to a federal probe, which often requires the help of outside counsel, can be steep. Consequently, a risk manager must ensure that regulatory investigations are fully covered, whether initiated by a formal request, or as is more common, informal inquiry and access letters. Given that this is an evolving and controversial area of insurance law,[75] it is important to craft a provision that includes any "formal or informal administrative or regulatory proceeding or inquiry" or a similarly comprehensive description. In addition, a risk manager should carefully review exclusionary provisions to ensure that claims under the FTC Act, state consumer protection acts,

---

75. *See, e.g.*, *Millennium Laboratories, Inc. v. Allied World Assurance Company (U.S.), Inc.*, 165 F.Supp.3d 931, 935 (S.D. Cal. Feb. 25, 2016) (granting insurer's motion for reconsideration and motion for summary judgment on grounds that DOJ investigation fell within the scope of D&O policy's specific claims exclusion); *see also Employers' Fire Ins. Co. v. ProMedica Health Systems, Inc.*, 524 Fed. Appx. 241 (6th Cir. 2013) (vacating district court decision that beginning of FTC investigation initiated time period for properly reporting a claim under policy); *see also MBIA, Inc. v. Fed. Ins. Co.*, 652 F.3d 152 (2d Cir. 2011) (holding that insured's D&O policies covered costs incurred in responding to informal investigations conducted by the New York Attorney General's office and the SEC); *Office Depot, Inc. v. National Union Fire Ins. Co.*, No. 9:09-cv-80554, 2011 WL 4840951 (11th Cir. Oct. 13, 2011) (holding that D&O policy did not provide coverage for SEC investigation or internal investigation performed as a result of a whistleblower's letter).

and other similar statutes and regulations are not excluded.

- Ideally, the policy will also cover the cost of responding to related government inquiries after the formal investigation has ended. For instance, it should include the cost of complying with any subsequent government audits for a designated period of time following the breach. It should also cover all expenses relating to security upgrades mandated by the government and the formation or reformation of a comprehensive security policy, which, again, may require the aid of outside counsel.[76]
- If the policy requires the use of pre-approved vendors, the university should carefully negotiate these terms before signing. A failure to do so could force the university to retain, for example, a credit monitoring service not favored by consumers, or worse, expend large amounts of money on a vendor that the insurer subsequently refuses to cover.

E. Cost-Saving Measures

A well-drafted cyber liability policy comes at a cost—often one that is not insubstantial. For a policy with a $5,000,000 liability limit, the premiums will often exceed $50,000. Unsurprisingly, insurance premiums, especially new premiums, often do not top the list of an institution's budgetary priorities. However, many university executives will find that a comprehensive insurance coverage plan is a prerequisite to the institution's success and longevity. Thus, the principal question is how a university can get the most value from its various insurance policies.

There are many options available, but one thing is certain: the answer is most certainly not to skimp on coverage. Given the massive potential liability involved, sacrificing better coverage for lower premiums is simply not a prudent trade-off.

Some universities engage in "self insurance" by setting aside a cer-

---

76. For example, the FTC entered into four consent decrees related to data breaches in 2013. "Each settlement required that settling companies: (1) designate dedicated personnel to be responsible for an 'information security program'; (2) identify 'material internal and external risks' to data security, particularly in connection with employee training and management, information systems, and threat detection; (3) implement 'reasonable safeguards' to control and prevent such risks; (4) develop 'reasonable steps' to select secure vendors who will have access to company data; and (5) evaluate, monitor, and adjust such measures regularly (over a twenty-year period)." Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 No. 1 Competition: J. Anti. & Unfair Comp. L. Sec. St. B. Cal. 229, 236-37 (2015); *see also* Liam M. D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J.L. & Cyber Warfare 1, 13 (2014) (noting that "FTC consent decrees have sought to impose a higher standard of information security compliance upon firms," thereby "increasing costs of data breach liability" and spurring insurers to begin offering products tailored to the specific risks of data breach liability).

tain amount of resources for particular risk scenarios.[77] While self insurance may be a reasonable solution when the probability of an occurrence or the potential liability involved is slight, such is not the case when the risk is substantial and the potential payout is huge.

A middle ground for financially strapped institutions is to agree to a large self-insured retention ("SIR"). Premiums decrease as SIRs increase, making it easy for a university to choose an SIR that aligns with its risk threshold and to benefit from the correspondingly lower premiums.

Another option is to devise creative alternatives to traditional insurance models. For instance, the University of California system employed a "reverse underwriting" approach when most insurers, following a massive data breach (one of the most significant up to that point) in 2006, deemed the university uninsurable.[78] The university subsequently entered into an agreement with a syndicate at Lloyd's of London in which the syndicate would provide coverage contingent upon a claims handling expert proving that the university had met previously agreed-upon risk-management standards. Unquestionably, this arrangement allowed the university to benefit from more affordable premiums than were available through the few U.S. insurers that would consider providing coverage.

Finally, developing thorough, proactive risk management policies and procedures can help achieve these ends. On the one hand, a thoughtful and heavily vetted cyber liability policy and crisis management plan will prevent many potential losses from ever coming to fruition. Additionally, in many instances, such policies have the added benefit of coaxing insurers into reducing premiums.

IV. CONCLUSION

Rapid advancements in information technology have transformed day-to-day university operations and, in doing so, have altered the landscape of risk management. On every campus, students, faculty, and administrators exchange massive amounts of data while Tweeting, Facebooking, Skyping, blogging, file-sharing, and emailing on a daily basis. These interactions give rise to new risks that standard university insurance policies simply do not contemplate or, worse, specifically exclude.

But insurance is not cheap, and today universities are facing significant budgetary constraints. Higher education faces increased scrutiny

---

77. *See, e.g., How the University Insures Itself*, *supra* note 55 (outlining self-insurance programs for a wide variety of risk types, including cyber security issues).

78. Patricia-Anne Tom, *How to Find Cyber Insurance for the Uninsurable*, INSURANCE J. (May 2, 2011), http://www.insurancejournal.com/magazines/features/2011/05/02/196901.htm.

and regulation from the federal government, combined with the lasting effects of the recession, which include sharp decreases in government funding and massive blows to university endowments. While there may be a need to take a hard look at expenditures and make some sacrifices, it is not a time to cut corners when it comes to liability insurance coverage. As this article illustrates, the risks and costs associated with litigation are steep—far steeper than the premiums that are necessitated by a comprehensive coverage plan.