



CONVERGING RISKS IN A DIGITAL ECONOMY: EDUCATIONAL INSTITUTIONS

This is one installment in a series of “White Papers” prepared by ThinkRisk Underwriting Agency discussing the converging risks faced by various industry segments as a result of the digital economy. The white papers provide real-world examples of such risks, and explore the insurance ramifications of these emerging exposures. This installment of the series discusses risks faced by educational institutions.

Introduction to the convergence phenomenon: Digital technology is a powerful tool that has changed the way businesses and other organizations operate. Digital technology has unleashed corporate creativity, leading to new products, new ways to manage and store data, and new ways to interact and communicate with constituencies. At the same time, digitization and the way it permits companies to gather, create, distribute and store information and media content has altered the risks of doing business in a fundamental way and exposes inadequacies in the current insurance response to these new risks. Here’s how this phenomenon affects educational institutions.

Content: Educational institutions have always (whether recognized or not) been all about creating informational or expressive content. Campus publications and broadcast stations are obvious sources of media content, but other sources abound. Universities are constantly creating music, art, theater, lectures, academic writings and other content that carries media exposures such as defamation and copyright infringement. Often these media activities are driven by student contributions, and may or may not be subject to the same rigorous controls that professional media organizations generally employ to manage such exposure.

School websites are also often rich in content, frequently employing chat rooms and other social networking tools that are popular with the student population. In addition, schools often provide email and internet capabilities to students, often with limited ability to monitor the usage of these platforms. Moreover, educational institutions are very active marketers, creating logos, mascots, slogans, merchandise and other aspects of a branding identity. This intellectual property can become a large

part of a school's identity, and can take on significant value. At the same time, these marketing and branding activities present significant exposures for copyright and trademark infringement.

There are many examples of media and intellectual property claims involving educational institutions:

- Several book publishers have sued Georgia State University for making digital portions of their publications available to students in the university web-based library reserve system. As of May 2010, both parties' motions for summary judgment were pending after two years of aggressive litigation.
- The University of Wisconsin sued Washburn University of Topeka KS over Washburn's use of a "Motion W" logo, similar to Wisconsin's.
- In 2010, Lake Mary High School in Florida, whose nickname is the Rams, was threatened with trademark litigation by the Chrysler Corp. over the use of a design that, according to Chrysler, looked too much like its Dodge Ram logo. After considering the costs of defending the case, the school complied with the cease and desist demand, which involved removing the logo from shirts, books, walls, and even the gymnasium floor.
- In March 2010, a University of Michigan student accused by fellow student newspaper employees of plagiarism took the newspaper, her former colleagues and the University to court, suing for defamation and emotional distress
- The rock band Metallica filed suit against Yale University, Indiana University and the University of Southern California, along with five additional unnamed universities as well as other defendants, alleging that the universities' failure to block access to a (then) relatively new Internet search software called "Napster" make them liable for contributory and vicarious copyright infringement
- Trinity University in San Antonio sued Trinity College & University in Louisiana for trademark infringement. Trinity University alleged that the use of "Trinity" by Trinity College & University caused confusion in the higher education community, and that the confusion diminished the value of a degree from Trinity University.
- The University of South Carolina and the University of Southern California became embroiled in trademark litigation over the rights to the mark "SC." South Carolina had used the design "SC" in the 1950s. When the school tried to bring the mark back for use on "throwback" jerseys, Southern Cal, which by then had registered the "SC" mark, brought a challenge. The case went all the way to the U.S. Court of Appeals for the Federal Circuit, which ultimately ruled in 2010 in favor of Southern Cal.
- In June, 2008, burglars stole back-up tapes containing sensitive data on 1.7 million patients at the University of Utah's hospitals and clinics. The tapes were on their way to a storage facility when they were stolen from a car belonging to an employee at a based data storage company used by the University. The disks were recovered untouched a few days later, but the University ended up spending more than \$3.3 million in breach notification costs, credit monitoring fees, phone bank costs and other expenses.

Network security and data privacy

Because of state and federal laws, schools have a duty to protect the privacy of student data. While that duty hasn't changed, digital technology puts that information in increased peril. Also, digital technology makes gathering and storing data easier, creating opportunities for educational institutions to collect and store vast amounts of data, including student information but also data concerning applicants, parents, alumni, faculty, employees, vendors and others. For instance, applicants for admission submit a lot of private information through the college's website and schools encourage applicants to monitor the application process through the website. Often, however, university data security practices are not state-of-the-art. The school's infrastructure may be comprised of a patchwork of legacy systems, and the university may lack the resources to upgrade to commercially sound practices. In the event of a potential breach of security, state laws in most jurisdictions require the institution to notify all potentially impacted persons of the breach, the cost of which can be astronomical. If the information is used in a way that is damaging, the institution could face liability claims as well.

There are dozens of examples of data breaches involving educational institutions, including:

-In 2009, the University of North Carolina at Chapel Hill disclosed a data breach of one of its servers that exposed the identities of 163,000 women. The women were participating in a mammography study conducted by the UNC School of Medicine. UNC officials sent out breach notification letters to all impacted persons.

-Names, photos, and Social Security numbers of 32,000 students and staff at George Mason University were compromised because of a hacker attack in 2005 on the university's main ID server.

-In 2009, it was disclosed that Binghamton University kept payment information for every student, possibly dating back at least ten years, in a storage area next to one of the most trafficked lecture halls on campus, behind a door that was not only unlocked but taped open. The information contained Social Security numbers, credit card numbers, scans of tax forms, business information, asylum records and more, in unlocked filing cabinets and shelving units. Because the information goes back at least ten years, if not more, the potential number of people affected lies well in the hundred thousands

Coverages in the standard insurance marketplace

Although most educational institutions purchase Commercial General Liability ("CGL") coverage, typical CGL policies provide limited coverage for media and network security claims. Libel and invasion of privacy in publications may be covered, but that leaves much media activity unprotected. For instance, intellectual property is excluded, except for copyright in "advertisements", which is largely not relevant to higher ed. This means that the litany of trademark and related intellectual property claims discussed above would likely not be covered. Similarly, website content is generally not covered, unless the content is considered "advertising," which is construed narrowly. Chat rooms, bulletin boards and other interactive media are excluded. Data breaches are outside the scope of the GCL.

Similarly, although D&O policies often include personal and advertising injury coverage similar to the CGL policies, those coverages are often not offered to colleges, universities and other educational institutions with heavy media activities. Likewise, many D&O policies have intellectual property and other similar exclusions that would defeat coverage in many of the high-exposure areas discussed in this paper. Even when such coverage is provided, it is generally not robust, and the carrier may not have the necessary legal expertise to deal with highly specialized or technical claims.

ThinkRisk's Converging Risk Liability Policy: The Converging Risk Liability Policy from ThinkRisk addresses these unique and emerging exposures, and fills the gaps left by traditional policies. The policy is "modular" and can therefore be customized to meet the needs of the particular institution. Coverage Part A of the Policy provides comprehensive coverage for claims arising out of the distribution of content, whether by print, electronic or any other means. To the extent that the institution provides any type of professional service, Coverage Part B provides coverage for claims alleging errors and omissions in the course of providing such services. Coverage Parts C and D provide network security coverage, both for liability claims brought against the institution (Part C) and for certain costs incurred by the institution in responding to a breach (Part D), such as the cost of notifying impacted persons.

To obtain a quote, please contact your insurance agent. For more information, contact us at info@thinkriskins.com or (816) 994-6400.