ALERT
JUNE 29, 2011

GLOBAL INSURANCE GROUP
News Concerning
Recent Professional Liability Issues

COZEN O'CONNOR
www.cozen.com

CYBER LIABILITY INSURANCE FOR UNIVERSITIES: INCENTIVIZING BEST PRACTICES AS A CONDITION TO COVERAGE (A/K/A "REVERSE UNDERWRITING")

Richard J. Bortnick • 610.832.8357 • *rbortnick@cozen.com*
Matthew N. Klebanoff • 215.665.5575 • *mklebanoff@cozen.com*

Computer hacking is a constantly evolving and growing threat. While recent high-profile network security breaches at companies such as Epsilon and Sony (with crisis management and other costs estimated to range from $1 billion to multiples thereof in the case of Sony) have helped raise awareness about the need to adequately protect personal identifiable information, the problem has existed for decades. Yet, the situation has only recently begun to receive proper attention from the media, government officials, businesses, and certain segments of the insurance industry. Of course, the cost of a security breach may have something to do with that. According to a study from Marsh and the Ponemon Institute, the typical data breach in FY 2010 resulted in companies and their insurers having to pay an average of $7.2 million to deal with and remedy the situation.

One particularly alluring target for hackers has been educational institutions. While schools and universities may not immediately appear to be obvious targets, the statistics confirm that attacks against educational institutions are on the rise.

In 2007, educational institutions accounted for 25 percent of all reported data breaches. This number jumped to 33 percent in 2008. *See* Sarah Stephens & Shannan Fort, *Cyber Liability & Higher Education*, Aon Professional Risk Solutions White Paper (December 2008). Indeed, some of the most devastating and costly security breaches have occurred at institutions such as UCLA (more than 800,000 records were compromised and approximately 28,600 Social Security numbers were obtained), the University of Miami (2,100,000 medical records were stolen and 47,000 potential victims were notified), and the Chicago Public School system (two different breaches occurred, including one involving 40,000 records as the result of the theft of two accounting laptops).

Perhaps most problematic for institutions of higher learning, insurers are less willing to underwrite cyber and network coverage because of the inherent difficulty in determining risk due to a lack of uniformity in the operation and management of computer systems throughout a university. Large research-based universities often operate on a decentralized network system – each department maintains and utilizes its own network. Thus, a college of liberal arts may operate on its own network separate and apart from a college of engineering. This problem was best exemplified when Grace Crickette, chief risk officer of the University of California, attempted to obtain tech and cyber liability coverage. Crickette found that she could not even complete the necessary insurance applications due to the university's largely decentralized computer system (400 departments multiplied by 10 campuses, as well as five medical centers, bookstores, etc.) and various other factors unique to a large, research-based institution. Moreover, because of the nature of funding for large research institutions, Crickette could not simply side-step the issue by pushing for all systems to be centralized.

Two years and countless unsuccessful meetings later, Crickette finally was able to obtain the coverage she sought from Aspen, a Lloyds syndicate, by adopting an outside-of-the box approach that she referred to as "reverse underwriting." The reverse-underwriting approach allows an insurer to cover losses only if best practices for securing information are implemented and followed. Analogizing such coverage to the more familiar practice of lowering deductibles and premiums for safe drivers in the context of automobile insurance, Crickette explained that the University would be covered *only* if forensic computer analysts could prove that the breached computer system met the minimum security standards developed by the

university's chief information officers and approved by Aspen. In short, the coverage incentivizes best practices for protecting information.

The terms of the Aspen policy also function to generally raise awareness amongst the university's various departments about the importance of adequately securing information. Ms. Crickette noted that some departments even agreed to centralize their systems when it was feasible to do so. Thus, the university not only obtained the tech and cyber coverages that it sought, it also was able to increase institutional awareness of cybersecurity risks, thereby reportedly lowering the risk of future breaches.

Notwithstanding the fact that large educational institutions and universities often contain decentralized network systems that make assessing risk difficult for underwriters, the fact remains that tech and cyber coverage may be available through the reverse underwriting method. As such, underwriters should not instinctively turn their backs on the potentially lucrative premiums that large universities may be willing to pay simply because their risks are difficult to gauge. Rather, it is reasonable for underwriters to demand that certain base-line levels of protection be put in place, and condition coverage on the university forensically proving that the data at issue was fully protected at the time the breach occurred. Of course, the level of protection required must be negotiated, and the security systems must be regularly updated as the state of the art evolves. So long as universities are willing to implement protocols and enforce internal compliance with the latest information-protection best practices, underwriters should be willing to meet universities half-way by conditioning coverage on compliance with the protocols agreed upon by the parties.

Finally, some universities have taken other approaches to minimize the risks associated with cyberattacks. For instance, the University of Texas-Pan American opted to forego obtaining cyberinsurance and instead invested its premium dollars into developing and adding new layers of security protection. In our view, however, the most prudent course of conduct would be for all prospective policyholders (whether institutions of higher learning or not) to develop and implement added layers of security, which will enable them to: (1) better protect against network intrusions, and (2) use such added protection as leverage in negotiating lower premiums based upon diminished risk of breach.

As the old saying goes, you can pay me now or pay me later.

To discuss any questions you may have regarding this Alert, please contact Richard J. Bortnick, a member in the West Conshohocken office and co-publisher of the industry blog cyberinquirer.com, at rbortnick@cozen.com or 610.832.8357 or Matthew N. Klebanoff in the Philadelphia office at mklebanoff@cozen.com or 215.665.5575.