



# Cyber Liability & Higher Education Aon Professional Risk Solutions White Paper

*December 2008*

**Authors:**

**Sarah Stephens**

Aon Financial Services Group - Professional Risk Solutions

**Shannan Fort**

Aon Financial Services Group - Professional Risk Solutions

# Table of Contents

<b>Risk Profile &amp; Exposure Channels.....</b>	<b>02</b>
Scope of Network Operations .....	02
Internet Usage.....	02
Outsourcing .....	02
IT Implementation.....	02
Miscellaneous.....	03
<b>Liability and the Regulatory Environment .....</b>	<b>03</b>
Regulatory Actions .....	04
Civil Litigation .....	04
<b>Education Incidents .....</b>	<b>06</b>
Causes of Security Incidents.....	07
<b>Risk Management Strategies.....</b>	<b>08</b>
Technology & Strategy .....	08
Contractual Allocation of Risk .....	08
<b>Insurance Solutions .....</b>	<b>09</b>
Coverage under Existing Policies.....	09
Available Coverage Overview .....	09
Coverage Features and Exclusions .....	10
Insurance Marketplace & Benchmarking .....	11
<b>Underwriting Process .....</b>	<b>11</b>
Policies in Action .....	13
<b>Notes.....</b>	<b>14</b>

## Risk Profile & Exposure Channels

Due 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. An overriding challenge that educational institutions face when dealing with privacy and security risks continues to be the fundamental conflict between a culture that values an unfettered exchange of ideas, and the security and privacy of sensitive or private information.<sup>i</sup>

### Scope of Network Operations

In order to facilitate the open access described above, network systems are configured to allow for multiple points of access. Outsourced IT entities and other service providers may also have direct access to the education organization's network, thus increasing exposures. Additionally, some larger universities may have multiple departments not managed by central IT that have little connectivity to the master network, operate proprietary systems, and abide by loosely defined privacy and security practices, which increases the risk of the parent organization.

### Internet Usage

Nowhere is the paradox of openness and expectation of privacy more evident than in social networking sites, which are used extensively by students<sup>ii</sup>. Sites like Facebook and MySpace allow students to share personal information in a more publicly accessible way than ever before. Many universities have incorporated the use of social networking websites into their student code of conduct, with some even monitoring students' postings<sup>iii</sup>. Institutions walk a fine line when they begin monitoring online behavior, since doing so may create a duty of care to protect students from dangerous or criminal behavior. Recent controversy surrounding JuicyCampus.com, a website that allows anonymous gossip specific to a particular college campus, has led to a consumer fraud investigation by the New Jersey attorney general after a student claimed that she was terrorized after explicit postings that included her address. In a step that some believe may begin to infringe on first amendment rights, the New Jersey Attorney General issued a letter to all New Jersey universities asking them to "incorporate...cyber-harassment...into your school's code of conduct, with consequences for those who engage in these activities<sup>iv</sup>."

### Outsourcing

Educational institutions are increasingly embracing outsourcing in some manner. The nature of operations outsourced may range in scale from student email systems, which almost 43% of universities have outsourced or plan to do so, to the management of student ID cards used to make purchases and gain access to buildings and resources, to a university's financial aid disbursement system. The cost savings of outsourcing can be very attractive, but these arrangements also worsen the organization's risk profile because of the increase in number of users and probable inconsistencies in network operations. The outsourced service provider's information security protocols should be given the highest level of attention.

## IT Implementation

Much like outsourcing, the modernization of operations and implementation of the latest technologies can result in tremendous cost savings if performed effectively. The downside, however, can be system integration problems, employee training hurdles, and unknown bugs or system glitches that can facilitate a breach of confidential information. Educational institutions are often faced with the task of securing networks with limited resources, leading to the widespread use of free or open source security software that may be less effective than a customized solution.

## Miscellaneous

Nearly all universities have custody of student health information in the context of on campus health clinics, which means they must ensure compliance with Health Information Portability and Accessibility Act (HIPAA) privacy and security rules. Universities with associated hospitals, those that host clinical trials, and even those that conduct any human subject research, may have additional exposure and resultant liability.

## Liability and the Regulatory Environment

The protection and disclosure of confidential consumer information - both personally identifiable information (PII) and protected health information (PHI) - is currently governed by a patchwork of state and federal laws that target different exposures and different entities. Some of these statutes include Family Educational Rights Privacy Act (FERPA), HIPAA, Gramm Leach Bliley Act (GLBA), Fair Credit Reporting Act, Sarbanes-Oxley (SOX), Federal Privacy Act, and others. The regulations most applicable to the education industry include:

### Family Educational Rights Privacy Act (FERPA)

FERPA mandates protection of the privacy of education records and affords students the right to view and correct the information contained therein. FERPA also allows certain information that would not be harmful if made public, known as “directory information,” to be disclosed without consent. Directory information can include name, address, telephone number, date of birth, honors and awards, and dates of attendance, but it is unclear about whether or not student ID numbers and Social Security Numbers are included.<sup>v</sup> This is particularly concerning considering that as recently as 2004, half of all universities used Social Security Numbers as student ID numbers.<sup>vi</sup> Only recently (March 2008) did the Department of Education propose FERPA rule changes to ensure that SSNs were not considered directory information.<sup>vii</sup>

### Fair and Accurate Credit Transactions Act (FACTA)

FACTA added sections to the Fair Credit Reporting Act (FCRA) intended to help protect consumers from identity theft. It also contains a “Red Flag” provision that requires any entity with a covered account to adopt a written plan to detect “red flag” events related to consumer accounts that could indicate identity theft.<sup>viii</sup> The Department of Education issued guidance confirming that educational institutions participating in the Federal Perkins Loan program are subject to the red flag rules, and

any other institution that can be considered a creditor should look into becoming compliant by the May 1, 2009 deadline.<sup>ix</sup>

### Health Information Portability and Accessibility Act (HIPAA)

Passed in 1996, this was one of the very first statutes that specifically concerned any form of confidential or personal information. The HIPAA framework contains both a security and a privacy rule that loosely dictate protocols for the protection of health information, as well as provisions for penalties in the event of non-compliance. In July of 2008, the Office of Civil Rights entered into a settlement agreement with Providence Health System, which suffered a major privacy breach in 2006, in which the system agreed to pay a “resolution amount” of \$100,000.<sup>x</sup> Many are calling this the first HIPAA fine and expect more to follow. Educational and research institutions that run health clinics, or hospitals, and those whose research involves collecting any PHI of human subjects may need to pay special attention to HIPAA compliance.

### Notification Framework

FERPA, FACTA, and HIPAA do not contain any specific provisions mandating consumer notification in the even of a data breach, but educational institutions are subject to the framework of 44+ state breach notification statutes. While some states allow exceptions for breaches involving encrypted data, most require swift public disclosure of any potential breach of personally identifiable information.

### Minnesota Plastic Card Security Act

Minnesota recently amended its data breach notification law to hold entities responsible for the costs of re-issuing credit cards in the event of a data breach. The law, which was passed in the wake of the TJX security breach, can certainly pertain to educational institutions as it applies to any entity accepting credit cards, debit cards, or other stored value cards. The statute requires companies to reimburse card-issuing financial institutions for the “costs of reasonable actions” to both protect its cardholders’ information and to provide post-breach services to its cardholders. More specifically, reimbursement covers costs related to providing cardholders with notification of the breach, cancellation and reissuance of cards, closing or reopening of accounts, stop payments and cardholder refunds for unauthorized transactions charged to their accounts. A financial institution may also bring an action to recover for the costs of damages it pays to cardholders resulting from a breach.<sup>xi</sup> Currently, Minnesota is the only state with such a law, but other states have tried to pass similar statutes, so far without success.

### Regulatory Actions

In the aftermath of some incidents, it is not uncommon for the Federal Trade Commission (FTC), Federal Communications Commission (FCC) or State Attorneys General to launch investigations and levy penalties. In 2006, ChoicePoint, a consumer data provider, paid a \$15 million fine to the FTC after thieves hacked the company’s database.<sup>xii</sup> In 2008, Hannaford Bros., an east coast grocery store chain, suffered a data breach that exposed over four million credit card numbers and resulted in 1,800 cases of fraud. Four class action suits were quickly filed against the company, and lawyers subsequently filed 12 additional complaints. Not only has the incident led to Hannaford defending litigation across the east coast, but the Secret Service has also launched an investigation into the breach.<sup>xiii</sup>

## Civil Litigation

Although there is no statutorily recognized foundation for launching lawsuits over data breaches, lawsuits charging negligence must show that accepted standards of performance were not met.<sup>xiv</sup> Historically, the plaintiff must show that he/she suffered some sort of direct harm as a result of the negligence. One publicly disclosed case involved San Diego-based Ligand Pharmaceuticals Inc. According to the San Diego district attorney's office and the plaintiffs' attorney in the case, a lab assistant found a box with 38 former employees' personnel records. The assistant used the information to acquire at least 75 credit cards and \$100,000 in merchandise, open 20 cellular telephone accounts and rent three apartments. The assistant was subsequently convicted and imprisoned, and fourteen of the former employees filed suit, charging Ligand with negligence. A confidential "significant six-figure" settlement was approved by the court.<sup>xv</sup>

Conversely, a 2006 case involving a stolen laptop containing 550,000 people's full credit information sheds some light on what "reasonable" protections an entity must provide in order to avoid damages. Stacy Guin had a student loan with Brazos Higher Education Service Corporation. Brazos employed a financial analyst to review its loan portfolio and decide which loans to buy and sell. The financial analyst worked from his house in Maryland, and had files related to as many as 550,000 of these loans on his laptop at home. The analyst's house was burglarized, and the unencrypted files were stolen. Ms. Guin sued Brazos for breach of contract, breach of fiduciary duty, and negligence.

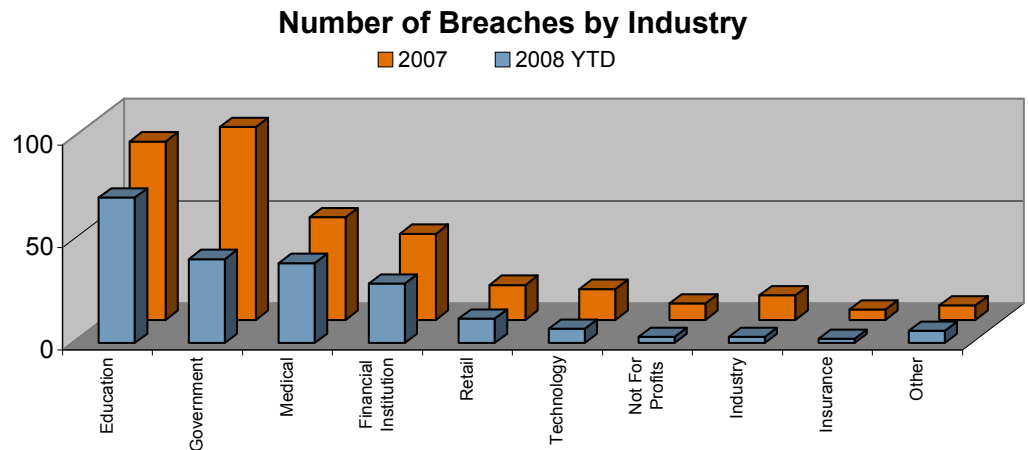
The court granted summary judgment for the defendant mortgage company, finding that it was not negligent and that the victims who lost data could not demonstrate any "damages" as a result of the conduct. The court concluded that the defendant had complied with the statutory provisions of GLBA because it had written security policies, had current risk assessment reports, and had "proper safeguards for its customers' personal information."<sup>xvi</sup>

Courts in other data breach cases in 2006, such as those in *Forbes v. Wells Fargo Bank*, *Bell v. Acxiom Corporation* and *Key v. DSW*, have dismissed similar litigation based on plaintiffs' lack of ability to demonstrate damages stemming from the theft or loss of their PII.<sup>xvii</sup> <sup>xviii</sup> <sup>xix</sup> Most recently, the United States Court of Appeals for the Seventh Circuit has held that plaintiffs who only sought damages for future credit monitoring and emotional distress did not suffer a "compensable damage" under Indiana law for negligence and breach of contract actions.<sup>xx</sup>

While civil lawsuits generally contend that a plaintiff must have suffered harm in order to recover from the offending firm, regulatory proceedings can focus on merely the offending firm's actions or inactions. For instance, in March 2008, ValueClick settled with the FTC for \$2.9 million dollars regarding a lawsuit that alleged negligence in protecting sensitive data.<sup>xxi</sup> The lawsuit stated that ValueClick violated their own privacy policy by neglecting to encrypt consumers' private information, as well as failing to fix vulnerabilities to hacker attacks.

## Education Incidents

In 2007, educational institutions were responsible for 25% of all reported data breaches, and to date in 2008, an astonishing 33%. From January 1, 2007 until November 19, 2008, approximately 158 educational institutions experienced data breaches involving 3,716,209 records. Combine that statistic with a study conducted by the Ponemon Institute that found the average cost of a data breach was \$197 per record, and the potential costs are astounding. Below are details of several security incidents in the education industry within the last few years, including the two largest breaches suffered by an educational institution to date.



### UCLA Hacked

In December 2006, the University of California, Los Angeles (UCLA) reported a breach that may have compromised more than 800,000 records (including names, birthdates and social security numbers of current and former students). By taking advantage of a flaw in software used by a UCLA vendor, hackers, specifically seeking social security numbers, were attempting to access information since October 2005. UCLA established an informational website, Identity Alert Hotline and sent notices to all affected individuals in the wake of the breach. The website remains active to date. As of April 2007, the investigation into the breach confirmed social security numbers for approximately 28,600 people were illegally retrieved by the hackers. At the time, this breach was the largest ever reported by a U.S. university.<sup>22</sup>

### Chicago Public Schools

Chicago Public Schools (CPS) suffered two significant breaches in the past three years. In November 2006, a contractor sent mailings regarding benefits to more than 1700 former CPS employees. Included in these mailings was a 125 page packet that included the names, addresses and social security numbers of the former employees receiving the packets. A former teacher that received the mailing subsequently filed a lawsuit against CPS seeking compensation and punitive damages.<sup>23</sup> In April 2007, more than 40,000 records were breached when two laptops belonging to an accounting

firm hired to audit the CPS pension fund were stolen from the CPS central office. A \$10,000 reward was offered for information leading to arrests of the perpetrators.<sup>24</sup>

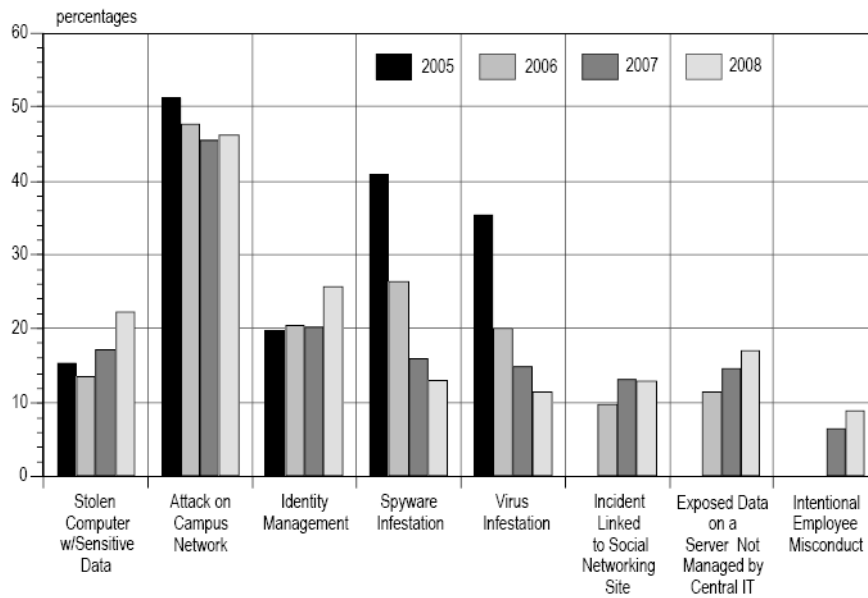
### University of Miami

Likely the most devastating breach involving an educational institution to date was revealed in April 2008. In this incident, the University of Miami announced a container carrying back-up tapes on which nearly 2,100,000 medical records were stored, was stolen from the truck of the off-site storage firm used by the University. University of Miami was praised by the Wall Street Journal for its immediate and efficient response, which included hiring an information technology forensics expert to determine if the encrypted information kept on the tapes could be accessed, notifying 47,000 individuals whose financial information was exposed, establishing a website and an informational call center.<sup>25</sup>

### Causes of Security Incidents

The information displayed in the graph below was gathered from data provided by senior campus IT officials representing 531 two and four year colleges and universities across the United States. The graph shows the percentage of security incidents suffered by the colleges and universities that were attributable to each type of breach and the variance year over year. Each security incident may involve multiple breach types thus accounting for the variance in the percentage amount. The graph is also an important illustration of changing technologies. For example, in 2005, spyware and virus infestation contributed to at least 40% of all breaches where as they contributed to less than 15% of breaches in 2008. Additionally, between 2006 and 2008 there has been a rise in breaches linked to social networking sites, which generated little to no breach activity in 2005.

## IT Security Incidents, 2005-2008



Source: The Campus Computing Project 2008 National Survey of Information Technology in U.S. Higher Education

## Risk Management Strategies

### Technology & Strategy

It is critical that the technologies educational institutions use conform to their security policies and protocols. Unfortunately, highly secure applications often have lesser utility given the need to freely exchange information within the collaborative workings of the academic community. This dynamic, combined with the decentralized nature of most large educational institutions, makes enforcement of effective security close to impossible. Those responsible for central IT in an educational environment should make every effort to be cognizant of how different departments are sharing information, and what steps, if any, they are taking to secure it.

### Contractual Allocation of Risk

As 30 percent of all reported breaches are attributed to external partners, consultants, outsourcers and contractors, it is critical to determine the boundaries of liability when any confidential information is shared for business purposes. The failure to do so can result in confusion and disarray when a breach occurs. Even standard outsourcing arrangements can cause complicated chains of liability when multiple layers of subcontractors become involved. Appropriate contractual provisions in business agreements and outsourced services arrangements can mitigate the effect of these situations by clearly defining responsibility, ensuring the proper precautions are taken when the information is out of the control of the educational institution, and limiting the liability of the organization in the unfortunate event of a data breach. Institutions should work closely with legal counsel and insurance advisors to ensure that insurance requirements, contractual indemnities, and the institution's own insurance policies all work in concert.

# Insurance Solutions

## Coverage under Existing Policies

### General Liability and Property Policies

All insureds should review their traditional insurance policies to determine the exact scope of coverage for data breaches. Changes in 2004 to the Insurance Service Organization (“ISO”) forms, as well as some insurance litigation have limited the coverage available under traditional general liability and property forms, and exclusions are becoming more common as general liability carriers offer standalone network security and privacy policies.

### Other Insurance Policies

Depending upon the facts of the data breach and the particular wording of the policies, some coverage could exist in various other policies, including Commercial Crime Policies, Employment Related Practices Policies, Data Processing Policies, Computer Fraud Policies, Advertising or Kidnap and Ransom Policies. For instance, if a hacker claims that confidential information will be distributed on the Internet unless the insured pays some type of extortion fee, some Kidnap and Ransom policies may provide defense and indemnity coverage. In general, such policies were not intended to cover privacy and data breaches and there are significant coverage gaps in each.

### Available Coverage Overview

Security & Privacy Liability insurance (also called Cyber Liability or Network Risk) can be designed to respond to third party liability and related defense costs and/or the insured’s own costs following a data breach. The available coverage parts are as follows:

1 <sup>st</sup> Party Coverage Part	Covers:
Information Asset	Damage to or theft of the insured’s information assets from its computer system.
Business Interruption	Lost income suffered as the result of a system outage or extended downtime due to negligence.
Cyber Extortion	Extortion threats to commit an intentional computer attack against you.
Crisis Management/ Identity Theft Expenses	Various costs resulting from a security/privacy breach.
3 <sup>rd</sup> Party Coverage Part	Covers:
Professional Services Coverage	Acts, errors, or omissions in the course of providing professional services.
Content/Media Liability	Personal and advertising injury and some intellectual property infringement arising out of media content created, produced or disseminated by the insured.
Network Security Liability	Breaches in network security or unauthorized access events
Privacy Liability	Wrongful disclosure of confidential information.

Educational institutions considering this coverage should note that the Information Asset and Business Interruption coverage parts have not been especially relevant to the Education industry. There are exceptions, however, and one example is an entity whose primary revenue stream is from network/internet activities, such as online universities. Additionally, there have been few first party claims paid by any insurer, and significant hurdles to coverage exist, such as waiting periods of 6-18 hours before coverage applies, and no coverage for an organization's internal information technology expenses.

### **Coverage Features and Exclusions**

Each carrier addresses the risks in a different manner, so it is essential that the insured review the policy form and work with their broker to customize it to their specific exposures. The following areas should be carefully reviewed:

#### **Policy Trigger**

Early versions of network risk policies were tied to "network security" breaches and were meant to respond to breaches of the insured's computer network security only. Today's network risk coverage responds to breaches of the security and/or privacy of information by online or offline means; arising from electronic devices not connected to a network like laptops, PDAs, data tapes, or external hard drives, or from non-electronic incidents like dumpster diving or the theft of paper files or log books.

#### **Media Liability**

Media liability, which responds to personal and advertising injury claims arising from online or print media and advertising content, is often included in the same policy. This serves a dual purpose of expanding the Advertising Injury/Personal Injury coverage in the insured's General Liability policy, and ensuring that data breach-related claims, like invasion of privacy and/or publication of private facts, are covered when they arise from content. One example would be the unintentional publication of a database of student names and social security numbers on the insured's website.

#### **Insider Acts Coverage**

Security and privacy policies generally exclude coverage for intentional wrongful acts, and some states prohibit such coverage on public policy grounds. A broad policy should include a severability provision that maintains coverage for the entity even if the wrongful act was committed maliciously by an employee. Policies should also provide for coverage and defense of insureds facing allegations of intentional wrongful acts until such conduct is established by a final adjudication.

#### **Employee Claimants**

As with most third party liability policies, there is an insured vs. insured exclusion in all security and privacy policies. The broadest policies now include a carveback to cover the entity for claims made by employees in the event that a breach involves employee information.

#### **Independent Contractors**

Many educational institutions outsource functions like billing and data storage to third party vendors. Policies should respond on a blanket basis whether the breach is caused by an employee of the insured or by an independent contractor operating on behalf of the insured.

### **Regulatory Claims**

Proceedings related to state disclosure laws, and other government initiated actions can result in both defense costs and fines or penalties. Defense cost coverage is readily available at a sublimit of \$250,000 or less, but some carriers offer full policy limits. Coverage for fines/penalties is less available and the coverage is only provided to the extent allowable under law (many state laws prohibit coverage for statutory or regulatory fines and penalties as against public policy). More recently, some carriers have agreed to cover the portion of a penalty that is paid into a consumer redress fund from which affected individuals can recover.

### **Identity Theft Mitigation/Crisis Management Expenses**

Coverage is available for a number of the costs that can result from a data breach event. It is important for an entity to clarify its priorities in this area, since the available limit and scope of coverage differs by carrier. Covered costs can include consumer notification, provision of credit monitoring, operation of call centers and related ID theft services, or the services of a public relations, law, or crisis management firm. Carriers impose a variety of sublimits, different retentions, and/or coinsurance provisions to this coverage.

### **Additional Terms and Conditions**

There are many other terms to consider that are not unique to Network Risk policies, such as Choice of Counsel, Extended Reporting Period options, "hammer clause," and prior acts coverage.

### **Insurance Marketplace & Benchmarking**

The market for Security and Privacy Liability is rather competitive at this time, with favorable risks renewing at substantial rate decreases and carriers actively soliciting new insureds. However, educational institutions are a difficult class of business for underwriters due to a perception of higher risk. Benchmarking in this area is difficult to categorize and not particularly valuable because each underwriting situation is based on many different factors, such as revenues, student statistics, loss history, information security posture, contractual allocation of liability, and number/accessibility of data records.

## **Underwriting Process**

The first step in the underwriting process is the completion of an application and/or self-assessment. It is essential that the risk management team engage the appropriate information security and privacy personnel in the application process to provide complete and accurate information. The assessment and application process also provides an opportunity to critically examine an entity's information risk management strategies. Implementation of best practices and due diligence with respect to information security and privacy are paramount to obtaining this insurance coverage and to maintaining sound risk mitigation practices.

In conjunction with the base application, a potential insured should be prepared to provide the following:

- Copies of privacy policies
- Standard contracts
- Outsourced service arrangements
- Results of any external or internal audits or assessments that illustrate the information security posture - examples include SAS 70, PCI, or ISO 27001 (formerly 17-799).
- Details of any security breach incidents and the response to them; any new protocols put in place to prevent similar incidents.
- Financial information and student statistics

In addition to an analysis of the standard application materials, underwriters will ask targeted questions in response to the current environment and the latest breach incidents.

## Policies in Action

Neither Aon nor the ten insurance carriers surveyed for this paper have seen significant losses covered by the purchase of Network Risk and Security Insurance by educational institutions. However, it is still important to determine where and how the policies would likely respond in the event coverage is purchased and available. Using the University of Miami breach (described in more detail under “Breach Incidents”), application of the coverage sections previously discussed is indicated below. It is important to note the description below is merely **an indication**, not a factual discussion, of how coverage, if purchased, would **likely** respond.

### Example:

Prior to its April 2008 breach, a hypothetical university purchases a policy that includes both first and third party elements, with a limit of \$10,000,000 (certain applicable sublimits would apply) and a retention of \$500,000; the elements of coverage would only respond after the applicable retention is exhausted:

1 <sup>st</sup> Party Coverage Part	Breach Component:
Information Asset	Coverage would likely respond allowing the University to gather and recreate the information stored on the lost back-up tapes containing the 2.1M records. (Sublimit)
Crisis Management/ Identity Theft Expenses	Coverage would likely respond with the costs of notifying the 47,000 individuals whose financial records were exposed, setting up the informational call center and even providing credit monitoring if the University deemed it necessary to the extent the sublimit would allow.
3 <sup>rd</sup> Party Coverage Part	Covers:
Network Security Liability	If a lawsuit were to be filed by the affected individuals because of the breach, coverage would likely respond with the defense costs and indemnity if assessed.
Privacy Liability	

### For more information contact:

**Sarah Stephens**  
sarah\_stephens@aon.com  
312.381.4470

**Shannan Fort**  
shannan\_fort@aon.com  
312.381.4109

## Notes

- <sup>i</sup> Anderson, Alicia. "Effective Management of Information Security and Privacy" *Educause Quarterly*. Number 1 2006.
- <sup>ii</sup> Jannasch-Pennell, Angel et al. "Crafting a Campus Identity: First-Year Students, Residential Life, and Social Networking" Presented at EDUCAUSE Annual Conferences 29 October 2008.
- <sup>iii</sup> Steinbach, Sheldon and Lynn Deavers. "The Brave New World of MySpace and Facebook." *Inside Higher Ed*. 3 April 2007.
- <sup>iv</sup> <http://www.nj.gov/oag/newsreleases08/082608-college-internet-letter.pdf>
- <sup>v</sup> "When FERPA Affects IT" *Inside Higher Ed*. May 8, 2008.  
<http://www.insidehighered.com/news/2008/05/08/ferpa>
- <sup>vi</sup> <http://www.usnews.com/usnews/biztech/articles/040906/6theft.htm>
- <sup>vii</sup> <http://www.ed.gov/legislation/FedRegister/proprule/2008-1/032408a.html>
- <sup>viii</sup> <http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>
- <sup>ix</sup> <http://www.ifap.ed.gov/eannouncements/1014FTCRedFlagRules.html>
- <sup>x</sup> "Feds finally put teeth into HIPAA enforcement,"  
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=325376&taxonomyId=17&pageNumber=2>
- <sup>xi</sup> "In response to TJX data breach, one state enacts legislation imposing new security and liability obligations," <http://privacylaw.proskauer.com/2007/05/articles/security-breach-notification-l/in-response-to-tjx-data-breach-one-state-enacts-legislation-imposing-new-security-and-liability-obligations-similar-bills-pending-in-five-other-states/>
- <sup>xii</sup> "State fines Kaiser Permanente for Privacy Breach,"  
<http://www.californiahealthline.org/articles/2005/6/21/State-Fines-Kaiser-Permanente-for-Privacy-Breach.aspx?topicId=40>
- <sup>xiii</sup> "Breach exposes 4.2 million credit, debit cards," <http://www.msnbc.msn.com/id/23678909/>
- <sup>xiv</sup> John Soma, professor at the University of Denver College of Law and the executive director of its Privacy Foundation. See also: *Doe v. Dartmouth-Hitchcock Media Center*, No. CIV. 00-100-M (D.N.H. July 19, 2001), *Nexans Wires S.A. v. Sark-USA Inc.*, 319 F.Supp.2d 468 (S.D. N.Y. 2004); But see: *Theofel v. Farey-Jones*, 359 F.3<sup>rd</sup> 1066 (2004); *Charles Schwab & Co. Inc. v. Carter*, No. 04 C 7071 (N.D. Ill. Sept. 27, 2005)
- <sup>xv</sup> Dan Bacalski, attorney with San Diego-based Bacalski, Byrne and Koska.
- <sup>xvi</sup> *Guin v. Brazos Higher Education Service Corporation*, No. Civ. 05-668 RHK/JSM, Feb. 7, 2006, D. Minn. (Not Reported in F.Supp.2<sup>nd</sup>)
- <sup>xvii</sup> *Forbes v. Wells Fargo Bank*, 420 F.Supp.2<sup>nd</sup> 1018 (D. Minn. March 16, 2006).
- <sup>xviii</sup> *Bell v. Acxiom Corporation*, 2006 WL 2850042 (E.D.Ark).
- <sup>xix</sup> *Key v. DSW*, No. 2:06-cv-459 (S.D. Ohio, Sept. 27, 2006).
- <sup>xx</sup> "Court limits damages for data security breach,"  
[http://blawg.scottandscottllp.com/businessandtechnologylaw/2007/09/court\\_limits\\_damages\\_for\\_data.html](http://blawg.scottandscottllp.com/businessandtechnologylaw/2007/09/court_limits_damages_for_data.html)
- <sup>xxi</sup> "FTC deal suggests enterprises could be liable for poor security,"  
[http://www.darkreading.com/document.asp?doc\\_id=148572](http://www.darkreading.com/document.asp?doc_id=148572)
- <sup>22</sup> "Breach at UCLA Exposes Data on 800,000," Vijayan, Jaikumar,  
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005925&pageNumber=2>
- <sup>23</sup> "Former Teacher Sues Over Release of Social Security Numbers,"  
[http://news.lp.findlaw.com/andrews/bt/prv/20061208/20061208\\_cohen.html](http://news.lp.findlaw.com/andrews/bt/prv/20061208/20061208_cohen.html)
- <sup>24</sup> "Laptop Theft Hits Chicago Public Schools," <http://www.networkworld.com/news/2007/040907-laptop-theft-chicago-schools.html>
- <sup>25</sup> "How to Respond to a Data Breach," Worthen, Ben, <http://blogs.wsj.com/biztech/?s=University+of+Miami>