

Information Malpractice Assurance

Higher education institutions are self insuring for information breaches.

Colleges and universities are very high risks for incidents of information loss. According to The Privacy Rights Clearing House, over 8.6 million records have been reported breached from 553 educational institutions since 2005 which is more than any other industry. Notably, one hundred percent of them had compliance policies and some form of prevention measures in place. Are higher education institutions and administrators prepared for this kind of liability?

Undeniable Liability - “Several recent events have set precedents that will greatly impact the information management practices of colleges and universities.”

1) The Case of Ohio State University (2010) – “Could a breach really cost that much?”

In a breach reported by Ohio State University they had to notify current and former faculty, students, applicants, and other university affiliates that hackers had accessed Social Security Numbers, dates of birth, and addresses. Though the university stated that there is no concrete evidence that this information was actually stolen, there is always the risk of the exposed individuals becoming victims of identity theft.

“The breach will cost the university \$4 million in expenses related to investigative consulting, notification of the breach, credit security, and a call center for anyone with questions or concerns,” reported Atty Marotti, a writer for The Lantern, a news website for Ohio State University. This financial burden does not include other damages associated with these types of breaches such as class action lawsuits and regulatory actions.

2) The Case of FTC Regulatory Actions Against Ceridian Corporation (2011) – “We have policies for compliance regulations and industry standards so why such a harsh settlement?”

The Federal Trade Commission (FTC) enforces certain legislation to ensure that organizations secure the sensitive consumer information that they maintain. According to an FTC complaint against the Ceridian Corporation, the company claimed, among other things, that it maintained “Worry-free Safety and Reliability . . . Our comprehensive security program is designed in accordance with ISO 27000 series standards, industry best practices and federal, state and local regulatory requirements.”

However, after a breach of approximately 28,000 individual’s Social Security numbers and direct deposit information, the complaint alleges that Ceridian’s security was inadequate. The FTC challenged the companies’ security practices as unfair and deceptive. This settlement orders Ceridian to bar misrepresentations, including misleading claims about the privacy, confidentiality, or integrity of any personal information collected from or about consumers. They require the company to implement a comprehensive information security program and to obtain independent, third party security audits every other year for 20 years.

Other Federal Trade Commission settlements involving unfair and deceptive practices look similar to the requirements imposed upon the Ceridian Corporation below:

“It is further ordered that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device shall no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to the respondent’s size and complexity, the nature and scope of the respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. *the designation of an employee or employees to coordinate and be accountable for the information security program;*
- B. *the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, (2) information systems, including network and software design, information processing, storage, transmission, disposal, and (3) prevention, detection, and response to attacks, intrusions, or other systems failure;*
- C. *the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing and monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;*
- D. *the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent and requiring service providers by contract to implement and maintain appropriate safeguards; and*
- E. *the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program."*

(Federal Trade Commission Docket No. C-4325: Ceridian Corporation, Decision and Order)

3) The Case of FTC Regulatory Actions Against Lookout Services, Inc. (2011) – “Our information is protected with policies and the appropriate safeguards – not the case.”

In another Federal Trade Commission announcement on May 3, 2011, Lookout Services, Inc. claimed it would take reasonable measures to secure the consumer data it maintained, including Social Security numbers, but failed to do so. The FTC's complaint charges that despite the company's claims that its system kept data reasonably secure from unauthorized access, “respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on Lookout's networks. (Federal Trade Commission, Docket No. C-2346)” Among the discrepancies found between what was advertised and actual practice, Lookout failed to require strong user passwords, failed to require periodic changes of such passwords, and failed to provide adequate employee training.

The outcome is similar to that of the Ceridian Corporation. In fact, both companies are required to make available for FTC inspection all materials relied upon for the mandated Assessments for a period of three years. All advertising materials prepared for or by the respondents must be made available for a five year period.

4) The Case of the Michaels Stores Breach (2011) – “We comply with Payment Card Industry Data Security Standards. How could this happen?”

Michaels Stores, one of the largest retailers in America recently had an incident involving the loss of card holder data. Officials say that thieves tampered with credit card PIN pads affecting consumers from stores in twenty states. Credit card, debit card, and PIN codes have already been misused creating damages for the exposed individuals. One consumer has already filed a federal lawsuit against Michaels to recover \$1300 that was illegally taken from her checking account shortly after she made a purchase for less than a \$20 at one of their stores.

In spite of Michaels Stores' claims of 100% compliance with Payment Card Industry Data Security Standards, such standards are required as a security baseline that does not transfer liability to credit card processors or carriers. The merchant is responsible for protecting consumer data that they collect. They must now replace over 7200 pin pads across their stores nationally. Additional damages may include monitoring services for all potential victims, legal expenses and settlements, loss of customers, consequential and statutory concerns. Michaels may face replacement costs of all credit and debit cards affected by the breach.

5) The Case of Epsilon (2011) – “The information lost wasn’t considered Personally Identifiable Information (PII). Why do we have to report this incident to the world?”

Epsilon, the world’s largest permission-based email marketing provider, had a breach of contact information which included names and email addresses. They provide services to some of the most well known companies across the globe. This breach is estimated to cost Epsilon \$4 billion by the time the dust settles.

However, there are a couple twists in this case. First of all, even though Epsilon had the incident, the companies that have contracted them had to send notifications to their affected client base. What will this do for their brand reputation? According to the Ponemon Institute, in the event of a breach . . . **31% percent of your affected customers will terminate their relationship**, 57% percent will lose trust and confidence in the company, 8% will file formal complaints (lawyers), 72% said there is a great chance they will become victims of Identity Theft.

Second, why did companies notify their customer base when the information that was stolen is not considered PII? Studies show that such contact information may be used as a tool to extract other Confidential and Sensitive Information from individuals as well as companies. The hundreds of affected companies are hedging the potential liability bet by taking immediate post breach actions. As of now the damages are unknown. More than likely lawsuits will be filed by the companies that have contracted Epsilon for services but it will be a long, time extensive, and costly road.

Breaches of this nature have a profound impact on new legislation. The Commercial Privacy Bill of Rights Act, introduced this year by Senators John McCain and John Kerry, cites that email addresses found with an individuals name are included within the scope of this legislation. When Acts like these are passed organizations have to re-think their entire security strategy.

The Definition of Insanity – “Doing the same thing and expecting different results.”

The “Rule of Thumb” in higher education for information compliance and prevention programs has been to put everything you can in writing and buy insurance to cover the rest. Creating these programs typically involves audit survey questions that lead to very general policy statements. Employees are trained by being asked to read the policy and sign it. The results of these measures are simply not broad enough in scope to address all of the information at risk and are not focusing on the practices that leave the institution exposed.

Unfortunately, these policies are out-of-compliance at the point they are approved by the Board because they do not address the full scope of risk to the operation as seen in the above listed cases. More importantly, it leaves the organization without a Defensible Position. Technology administrators typically have done a good job with hardware and software controls with only 29% of information breaches annually related to computer hackings. The true challenge for program auditors and administrators is proving the level of expertise necessary to address the other 71% of institutional risk for information loss or breach.

Preparing for information exposure should not involve expending resources on an event that may never take place. In fact, every college and university is already exposed. Managing the risks for information

loss or breach must become a top priority for higher education institutions considering the fact that every administrative and most academic operations involve the management of confidential and sensitive information. Unauthorized access to student, employee, faculty, and vendor information in any of these areas will damage the institution's finances, operations, and reputation. Be forewarned, the probably of exposure is the highest it has ever been and regulators are taking action with very serious consequences.

Lawsuits and Personal Liability – “*Is your prevention program leaving your organization and you exposed?*”

Administrators at higher education institutions have become very familiar with writing, or borrowing, policies to comply with laws that protect consumer information such as the Family Education Rights and Privacy Act, the Health Insurance Portability and Accountability Act, and the Red Flags Rule. When exposed individuals become victims of identity theft, they look for restitution from the organization that lost their information. The courts, and the regulators for that matter, judge an institution based upon its actions (the practices that take place when information was exposed), and not its intentions (policies written to satisfy regulations that do not address actual operations).

Perhaps the most overlooked liability in preparing for information exposure is the notion of Vicarious Liability. Vicarious Liability is a legal doctrine that imposes tort liability, or legal responsibility on one person for the negligence or actions of another. Under this doctrine, Board members, executives, administrators, faculty, and employees can be held civilly and criminally responsible for damages that individuals incur based upon how breached information is misused.

In other words, there is a shared liability between the institution and the employee for prudent information management programs and practices. Dr. John White, the Criminal Justice Coordinator at Martin Methodist College states, “Therefore the question, as it regards vicarious liability as courts have defined it, is not what the administrator knew but what the administrator should have known to execute the proper level of care in relation to the injury or harm caused.” The administrator's level of expertise related to assessing information exposure risks and the employee's adherence to prudent practices comes into question in these types of cases.

Every higher education institution has well-trained staff in their departments such as technology, public safety, risk management, human resources, and financial aid. Each of these professionals has experience in their own area of practice. However, it is only when their experience with the institution's operations is combined with outside industry expertise in providing guidance and exposing the “unknown unknowns” that a defensible position can be created. In fact, when collaborating with colleges and universities nationally to assess practices, create infrastructure, implement solutions, and maintain prevention programs, Identity Theft Loss Prevention practitioners find an average of 150 areas of information exposure. These areas of concern translate to non-compliance and a high probability that there will be a loss or breach.

Information Malpractice Assurance – “*Standing the test of time*”

A relatively new concept for managing information exposure risk is “Information Malpractice Assurance.” Introduced by Identity Theft Loss Prevention, LLC (IDTLP), this approach offers a positive declaration against reprehensible ignorance, negligence, and criminal intent allowing institutions to self-insure themselves through a system of prudent actions. This is not an insurance policy, but rather a necessary assurance action.

Insurance policies are a necessary evil that triggers after an unfortunate event. Often they only cover a fraction of financial damages incurred. Compliance policies are written to satisfy certain pieces of legislation, but rarely translate into the daily practices of the institutions that adopt them. Information Malpractice Assurance is a preventative action encompassing professional expertise, assessment, training, infrastructure, design, implementation, and maintenance.

Identity Theft Loss Prevention's Industry Experts facilitate a collaborative effort including executives, administrators, department heads, employees, faculty, and staff to build a defensible position for information exposure, lawsuits, regulators, insurance claims, vicarious liability, and consumer confidence. This proven revolutionary system helps to establish, implement, and thereafter maintain, a comprehensive identity theft prevention program reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Information Malpractice Assurance includes:

- establishing and training an Identity Theft Prevention Team;
- information risk and breach preparedness assessment;
- Identity Theft Prevention Program design;
- employee behavior modification;
- implementation strategy;
- service provider oversight;
- and periodic evaluation and updates.

Since the world of Information Protection is so complex, it takes a joint effort that includes both IDTLP's Industry Experts and your organization to create a solid system. As soon as a consultant makes a recommendation that might not fit the operational flow or the culture of an organization is the minute a program becomes a potential disaster.

Conclusion – “It's time for action.”

Information exposure is a risk that involves almost every aspect of a higher educational institution's operations. One breach can be very costly and even extend personal liability to individuals within the organization. Collaborative action and expertise is the only assurance of a defensible position for information exposure, lawsuits, regulators, insurance claims, vicarious liability, and consumer confidence. Where is your assurance for information malpractice?

Contact Identity Theft Loss Prevention, LLC at 419.902.0102 or info@idtlp.com for more information, to set up a webinar for your organization, or for inquiries about our program that assists with creating a Defensible Position.

About the Authors

Frank R. Mitchell is the Director of Research and Development, and a driving force behind the innovative practice management strategies Identity Theft Loss Prevention, LLC uses to identify and remediate information exposure for organizations and individuals. He is a practitioner in the fight for a culture of safety for social and business interaction.

Tom Glanville is the Founder and CEO of Identity Theft Loss Prevention, LLC. His military and military contractor background, higher education experience, and his relationship with Infragard as well as with the FBI has assisted hundreds of organizations to a better path for information protection and creating a Defensible Position.