IADC COMMITTEE NEWSLETTER

PROFESSIONAL LIABILITY

MARCH 2015

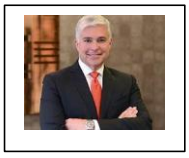
IN THIS ISSUE

This month's Newsletter discusses issues surrounding Cyber Breach, including breach notification laws, risk assessment and risk transfer, and breach management essentials and process.

The Year of the Cyber Breach

ABOUT THE AUTHORS

Elizabeth S. Fitch of Righi Fitch Law Group, is a founding and managing member of the Righi Fitch Law Group. She is a trial lawyer with 28 years of civil defense experience and has the AV Preeminent rating. Beth is the past President of Arizona Association of Defense Counsel and has been featured twice in Attorney At Law. Her practice has concentrated on representing businesses and individuals in complex civil litigation matters. She has developed expertise in risk management and assists clients with risk transfer strategies. Beth is board certified in Privacy and US Data Protection (CIPP/US). She advises clients on privacy and cyber related issues and leads her firm's data breach response team. She can be reached at beth@righilaw.com.



Theodore M. Schaer of Zarwin, Baum, Devito, Kaplan, Schaer, Toddy, P.C., is the Chairman of Zarwin, Baum, DeVito, Kaplan, Schaer & Toddy's Casualty Defense Department and is the Chairman of the firm's Cyber Liability, Privacy and Data Breach Response team. Ted has been certified by the International Association of Privacy Professionals. The CIPP/US certification is the preeminent privacy credential in the US private sector. Ted also serves as Chief Information Security Officer for his law firm. Ted counsels companies and their insureds on cyber liability and responding to a data breach. Ted regularly blogs on cyber liability issues and has been interviewed by national media on cyber security issues. He can be reached at tmschaer@zarwin.com.

ABOUT THE COMMITTEE

The Professional Liability Committee consists of lawyers who represent professionals in matters arising from their provision of professional services to their clients. Such professionals include, but are not limited to, lawyers, accountants, corporate directors and officers, insurance brokers and agents, real estate brokers and agents and appraisers. The Committee serves to: (1) update its members on the latest developments in the law and in the insurance industry; (2) publish newsletters and Journal articles regarding professional liability matters; and (3) present educational seminars to the IADC membership at large, the Committee membership, and the insurance industry. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact

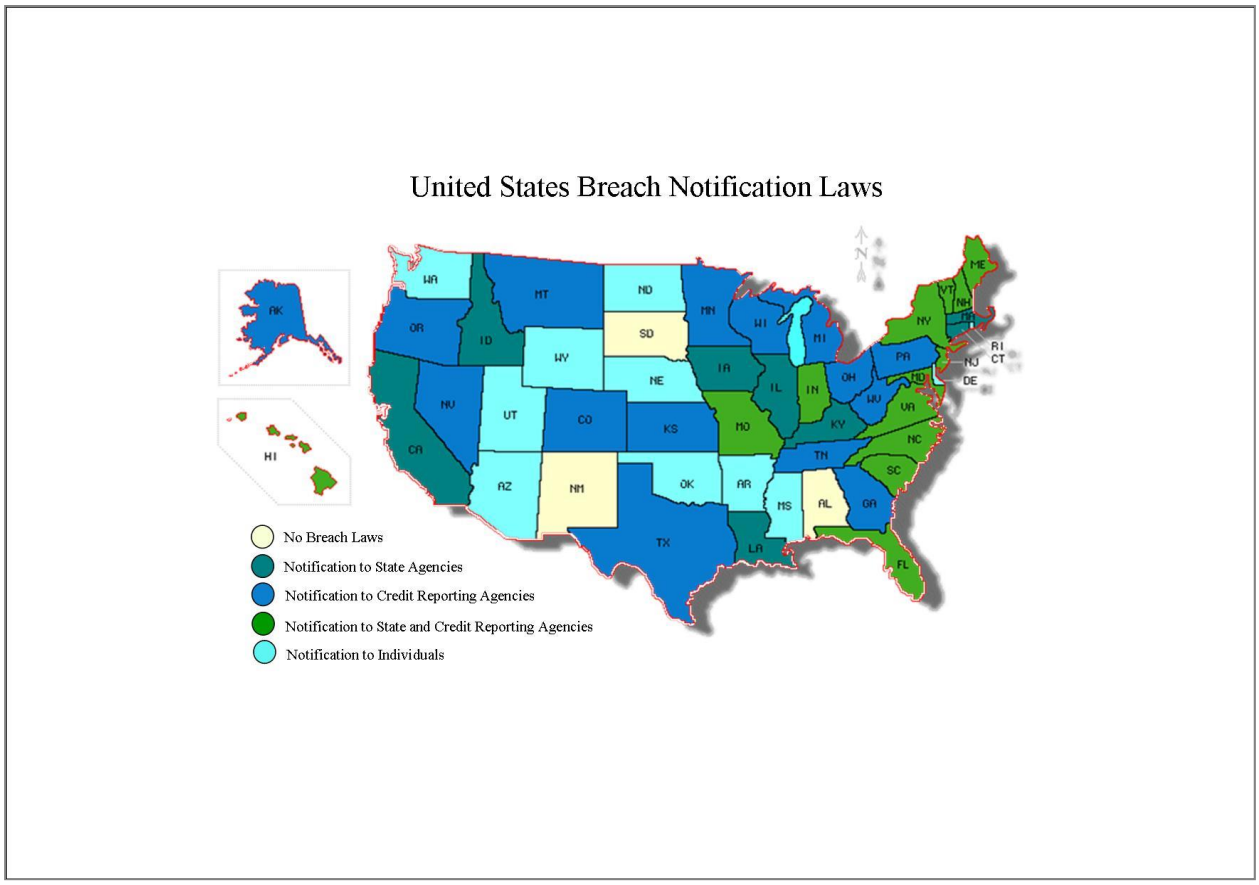
Mary G. Pryor
Vice Chair of Newsletters
Cavanagh Law Firm
mpryor@cavanaghlaw.com

Technology is rapidly changing and expanding. Unlimited sources of information are available with the quick click of a mouse. Companies often keep data, full of confidential client information, stored in internal or online databases. This facilitates efficient and quick access to customer records, but increases the risk of confidential data being compromised. The recent high profile data breaches involving Sony and Anthem are indicative of the cyber breach avalanche that is to come. A recently released cyber claims study has produced some eye-popping data for all businesses to consider, making this the "Year of The Cyber Breach." [1] The NetDiligence Cyber Claims Study for 2014,[2] which is a survey of leading cyber insurers word-wide, found that smaller organizations experienced the most cyber breach incidents.[3] The authors theorized that cyber breaches occur to smaller organizations because they are less aware of their exposure and commit fewer resources to risk and data security and assessment.[4] Most importantly, the study examined the real costs of cyber breaches to businesses and to insurance companies.[5] According to the study, the average claim payout for cyber breaches was $733,109 with the average claim payout in the Healthcare sector being $1.3 million, and for a large company, $2.9 million.[6] The average legal costs for companies and their insurers were $698,797.[7] Crisis services costs (e.g. forensics, notification, misc.) on average were $366,484.[8] So, what is the take away from this study? *All* businesses are targets for cyber-crime, no matter what their revenues. When it comes to a cyber breach, it is not a question of "if"; rather, it is a question of "when." Is your company ready?

Breach Notification Laws. Federal and State governments have enacted privacy laws to protect personal information when databases have been breached. Currently, 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted breach notification laws.[9] While key differences do exist, state breach notification laws generally contain similar provisions. The primary recipients of a breach notification are individuals who are at risk because their personal information has been compromised. For example, Texas state law requires companies that experience a data breach to notify not only its residents, but also residents of states

[1] FORBES, http://www.forbes.com/sites/danielfisher/2015/01/02/if-2014-was-the-year-of-the-data-breach-brace-for-more/ (last visited Mar. 24, 2015).
[2] NETDILIGENCE, http://www.netdiligence.com/ (last visited Mar. 24, 2015).
[3] *NetDiligence Cyber Claims Study* (2014), available online at www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf.
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES, available online at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Mar. 25, 2015).

lacking a data protection notification law.[10] Additionally, fifteen states and Puerto Rico require further notification to state governmental agencies[11] and 27 states require notification to national credit reporting agencies. [12] Three states do not have any mandatory breach notification laws.[13]



[14]

[10] Peter P. Swire, et al., U.S. Private Sector Privacy, Law and Practice for Information Privacy Professionals, 121 (2012).

[11] Idaho, Illinois, California, Louisiana, Puerto Rico, Hawaii, Missouri, South Carolina, Virginia, Maryland, New Jersey, New York, Maine, Massachusetts, New Hampshire, North Carolina. *Id.*

[12] Minnesota, Alaska, Colorado, the District of Columbia, Florida, Hawaii, Indiana, Kansas, Maine, Maryland, Michigan, Missouri, Nevada, New Jersey, Ohio, Oregon, Pennsylvania, South Carolina, Tennessee, Vermont, Virginia, West Virginia, Wisconsin, New York, Georgia, Texas, Montana. *Id.* at 121-22.

[13] Alabama, New Mexico, and South Dakota. *Id.* at 121-22.

[14] Not pictured: District of Columbia, Puerto Rico, and U.S. Virgin Islands. *See infra* notes 12-13.

RISK ASSESSMENT AND RISK TRANSFER:

Risk Assessment:

With the advent of cyber liability, it is critically important that companies take immediate steps to protect against this rapidly evolving risk. A company can best protect itself from breaches by conducting a risk assessment and then adopting technological, administrative, and physical controls that suits the company's overall objectives and corporate culture. The International Association of Privacy Professionals, the international certifying organization for privacy professionals, has adopted the following formulas as the industry standard.[15]

Risk = Threat x Vulnerability x Expected Loss

Risk: the measure of the adverse impact of a cyber breach.

Threat: any circumstance with the potential to adversely impact organization operations.

Vulnerability: weakness in the organizational information security systems and processes.

Expected Loss: financial cost from breach.

The executive management team should work closely with the internal IT team to develop an assessment methodology that identifies the risk, threats, and vulnerabilities without a disruption to company operations. Depending upon the size of the company, the more expedient and economical approach may be to retain an outside cyber consultant to perform an audit. Once the assessment is complete, the executive team should adopt and implement information security policies that protect the company and meets its short term and long term goals.

Security policies should take into account the three key security controls:

Technological controls are technical barriers put in place to prevent virtual breaches. A complete technological control system is preventive, detective, and corrective. Preventive security controls are to halt potential breaches before they actually happen. Examples include password verifiers and firewalls. Detective security controls alert the system when they identify activities that are out of the ordinary. Corrective security controls automatically respond to manage or ameliorate threats after preventive or detective systems identify a threat.[16]

Administrative controls are personnel barriers that only permit users access to information they need to know. An information classification system helps identify what information employees should be permitted to access. The three most

[15] Peter P. Swire, et al., *Foundations of Information Privacy and Data Protection*, 80 (2012) available online at https://privacyassociation.org/media/pdf/certification/foundations-ch3.pdf.

[16] *Id.*at 89.

common information classes are confidential, sensitive, and public information. Confidential information would cause a company to fail or be severely compromised if it were divulged. This information should be kept extremely secure and private. Sensitive material is important work-related information that is to be used internally. It should be kept secure. Public information can be shared with the public at large without risk of a compromise.[17]

Physical and environmental controls are physical barriers to protect the actual information-storing equipment. They prevent the actual physical invasion of premises and destruction of property. Physical controls include surveillance systems, security personnel, locked doors, and alarm systems. Environmental controls involve strategically placing critical equipment and materials away from potential hazards such as fire, wind, rain, floods or other natural emergencies.[18]

Risk Transfer:

Insurance Coverage:

Most companies seek to transfer risk through procurement of various forms of insurance. A majority of businesses purchase commercial general liability insurance ("CGL") to cover them risks of bodily injury claims, property damage, and advertising injury. Anecdotal data suggest that businesses are assuming that any damages from a data breach are covered by the CGL. This assumption is precarious. While the U.S. Court of Appeals for the Eighth, Ninth, and Tenth circuits[19] have found coverage for computer, cyber and privacy risks under traditional CGL policies, the U.S. Court of Appeals for the Sixth and Third Circuits reached the opposite result.[20]

The high profile lawsuit of *Zurich American Insurance Company v. Sony Corporation of America* (Index No. 651982/2011 (N.Y. Sup Ct., Feb 21, 2014). is the case to watch for cyber coverage under CGL policies. Sony sought coverage under its Zurich's CGL policy for theft of customer personal information by online hackers. On April 16, 2011 computer hackers unlawfully gained access to Sony's PlayStation networking, allegedly stealing personal identification and financial information for 25 million customers. Over the next three days the hacking continued and an additional 77 million customers had their personal identification and financial information stolen. When a class action lawsuit was filed, Sony sought coverage from Zurich pursuant to its CGL policy. Zurich filed a declaratory relief action requesting a ruling that the data beach did not qualify as bodily injury or property damage. Sony countered

[17] *Id*. at 91-92.
[18] *Id*. at 98-99.
[19] *See, e.g*., Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797 (8th Cir. 2010); Netscape Communications Corp. v. Fed. Ins. Co., 343 Fed. Appx. 271 (9th Cir. 2009); Park Univ. Enterprises, Inc. v. Am. Cas. Co. of Reading, PA, 442 F.3d 1239 (10th Cir. 2006).
[20] *See, e.g*., Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 691 F.3d 821 (6th Cir. 2012); St. Paul Fire & Marine Ins. Co. v. Brother Int'l Corp., 319 Fed. Appx. 121 (3d Cir. 2009).

that the breach fell within the purview of the personal and advertising injury provision of the policy. The New York Supreme Court rejected Sony's position and found that coverage was not afforded under any of the policy provisions.

Insurance companies are responding to cyber breach claims with sweeping cyber exclusions under the traditional CGL policies and developing cyber insurance products to cover the new business risks. According to Lemme Insurance Group, a major cyber liability insurance broker, the insurance industry has responded by developing Cyber Insurance policies that provide coverage to eliminate or mitigate against the following exposures.[21]

1. Reputational Risk: Reputation and trust are the cornerstone of most businesses. A company builds this reputation slowly. A publicized data breach can result in the loss of reputation in an instant.
2. Data Corruption or Loss: Data and information are businesses assets. Loss, destruction of corruption of data can interrupt not only the day to day operations of a company but also exposes the company to third party claims.
3. Cyber Crime: Cyber-criminals prey upon companies that lack sophisticated technological controls and focus on discovering the vulnerabilities. That is why smaller companies are particularly at risk for cyber crime.
4. Technology failures: Any type of cyber attack from hacking to malware can corrupt data and can cause hardware failures resulting in business disruption.
5. Regulatory Exposures: Federal Regulators and State Attorney Generals are taking an active role in ensuring that breach notifications laws are followed. Costs associated with defending a regulatory action and the assessment of fines and penalties can be in the millions.
6. Crisis Management: Due to the timing requirements of date breach notification laws, a data breach of any kind is a true crisis which requires an immediate commitment of financial and human resources. The cost of notifying customers, regulatory compliance, cooperating with law enforcement investigations and coordinating with credit reporting agencies result are significant.
7. Website Exposure: Sources of potential liability for websites include defamation, intellectual property infringement, and negligent misrepresentation. Social media engineering could expose a company to invasion of privacy claims.

[21] Kelly S. Geary, *Cyber Related Business Risks and the Cyber Insurance* Solution, 2014, http://www.lemme.com/assets/1/13/Cyber_Related_Business_Risks_and_the_Cyber_Insurance_Solutions.pdf.

8. Third Party privacy claims: The inadvertent loss or dissemination of personal information data subjects companies to third party claims. Individual and class action lawsuits may very well be the next wave of civil litigation.

The cyber insurance products vary greatly so it is critical to carefully review the insurance policy language.

Contractual Indemnification and Additional Insurance Provisions

Many companies elect to outsource IT functions to outside vendors. Outsourcing does provide the opportunity to shift the risk of cyber breach to outside vendors. While engaging outside vendors, it is important to gain an understanding of what data protection they employ. Furthermore, ensure that all vendors follow industry specific best practices.

Requiring the vendor to procure cyber insurance and name the company as an additional insured provides another avenue of potential coverage. The service contract should include an insurance provision that not only requires the service provider to procure cyber liability insurance but also requires that the company be named as an additional insured.

Contractual indemnification provisions are common in many industries and typically have been enforceable. A well drafted contractual indemnification provision that imposes the duty to defend and indemnify on the service provider shifts the cost of defending a third party claim from the company to the service provider. Each jurisdiction has unique laws governing the interpretation and enforcement of these provisions. To ensure the company is fully protected from third party claims, it is imperative that legal counsel review each of the state's breach notification laws and statutory and case law governing the interpretation of risk shifting contract provisions.

The flip side is that IT vendors will include boiler plate reverse indemnification and limitation of liability provisions in their service contracts. These boilerplate provisions are enforceable in most jurisdictions so a careful review of an IT service provider agreement is critical to risk assessment and risk transfer. Careful evaluation and negotiation of service agreements will go a long way towards protecting company and shifting risk.

Breach Management Essentials:

Early Response Team:

With technological, administrative, and physical controls in place, a company has the foundation to protect against data breaches. Despite these controls, companies are still at risk for cyber breach and should have in place an Early Response Team ("ERT"). Swift action is required for timely compliance with regulatory breach notification requirements. This team, at a minimum should consist of a member of the company's executive

management team, Chief Information Officer, Chief Security Officer, public relations specialist, legal team, and forensic cyber expert. While large companies may employ the necessary forensic and legal experts, smaller companies can be equally prepared with the selection of outside service providers. For example, the authors head up the Early Response Team for Themis Advocacy Group.[22] Themis is a national network of preeminent law firms that provides innovative, cost-efficient legal services to clients by sharing best practices and technology. If a Themis client experiences a cyber breach, the Themis early response team can leap into action. The Themis lawyers serve as the quarterback who with the help of carefully vetted forensic and public relations experts manage the crisis.

Breach Management Process:

The first step is to evaluate whether a breach has actually occurred and what data was compromised. Because the breach notification laws for each state are unique what may constitute a breach in one state will not be a breach in another. Since the cost of breach notification can be significant, the forensic technical team should work closely with the legal team to assess whether a cyber breach has occurred and nature and magnitude of the breach. The legal team should have the final determination as to whether a breach requires compliance with notification laws. Regardless of whether an actual breach occurred requiring compliance with the notification laws, the company's reputation is at risk. As the CEOs of Sony, Target, and Anthem can attest, a privacy breach can become a public relations nightmare. Involving a public relations/social media expert to control and craft the media message will help to minimize the reputational damage.

Once the ERT determines that a breach has occurred the next step is containment. The IT and forensic experts not only need to identify the source of the breach but also need to perform a full system audit so that the companies vulnerabilities are identified and remedied. The third step is to comply with the applicable notification laws. Again, these vary from state to state and may require notification to customers, regulatory agencies, law enforcement and national credit reporting agencies.

Conclusion. As technology continues to expand, the need to adopt detailed data privacy practices will become increasingly important. A company can minimize risk by procuring insurance and negotiating contracts that shifts risk to outside vendors. Not only are these practices vital to protecting confidential information, but also a vital for company's survival. These best practices serve as the foundation to securing confidential data, increasing client or customer trust, and maintaining a successful business.

[22] THEMIS ADVOCATES GROUP, http://www.themisadvocatesgroup.com (last visited Mar. 24, 2015).

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

FEBRUARY 2015
The Tide Has Turned:
An Update Regarding the Evolution of the Intra-Firm Attorney-Client Privilege
Charles Lundberg and Aram Desteian

JANUARY 2015
Cybersecurity: The Continuing Evolution of Insurance and Ethics
Dan Zureich and William Graebe

OCTOBER 2014
An Attorneys Duty to Disclose Evidence to Opposing Counsel
Michael E. Brown

SEPTEMBER 2014
Defending the Outside Referral Case
Michelle M. Lore

AUGUST 2014
Third Party Litigation Funding – The Perils to Attorneys
Margaret Fonshell Ward

JULY 2014
Where is the Locality Rule?
Brian A. Homza

JUNE 2014
Liability of Insurance Agents and Brokers to Third-Party Non-Clients and Recent Developments
Brad Jones and Anthony Alt

MAY 2014
Who's the Boss? Professional Liability Risks for Insurance Defense Attorneys
Daniel E. Ashmore and Jana Smoot White

APRIL 2014
Recent Professional Liability Cases
Richard L. Neumeier

FEBRUARY 2014
Consumer Protection Laws: Liability and Coverage Implications for Licensed Professionals and Their Insurers
Matthew Marrone

JANUARY 2014
Recent Developments in Legal Malpractice
Richard L. Neumeier

OCTOBER 2013
Property Managers that Are Collecting Assessments Are Not Debt Collectors under the FDCPA
Debora Verdier