What Every Insurance Professional Must Know About Network Security and Privacy Liability

Peter R. Taffae
M. Damien Magnuson

AUTHORED BY:
ExecutivePerils
EXECUTIVEPERILS

About the Authors of this whitepaper

ExecutivePerils

Since 2000, ExecutivePerils has been uncompromising in its business model of bringing value to its clients. We are an independent wholesale broker whose sole purpose is to bring product expertise, enhanced underwriter relationships and excellent service to our retail agent clients across the country in the desire to make them more successful.

From our past careers in underwriting and retail brokerage, we approach wholesaling from a unique prospective. Our emphasis has been on creativity, proactive risk management and direct involvement with claims solutions. Our entrepreneurial spirit has developed into doing business in over 40 states; being recognized by Risk & Insurance magazine as a 2011 Risk Innovator® and as a PowerBroker® in 2009 and 2012. Members of the firm have been published and quoted in over 25 periodicals including the Wall Street Journal.

From the beginning, the goal was simple, and we have tirelessly stuck to our original business plan to bring value to retailers. We created “Super Continuity” shortly before the 2008 subprime melt down to allow our insureds extra protection when the future financial stability of their Insurers was unknown. Many competitors followed us and offered a similar product. In 2011, we introduced “Trilateral Coverage” which has forever changed the post-merger “tail” (run off) coverage in D&O liability. In the late 1990’s we wrote one of the insurance industry’s first cyber policies and were a lead contributor in drafting a major carrier’s cyber policy (still utilized today). We hire the industry’s brightest, hardest working and creative people, and give them an environment that allows them to blossom. Our Insureds range from the best of class, Fortune 500, IPO, high claims frequency, to new nonprofits.

We focus on a limited number of insurance products. This allows us to develop a true understanding of the insurance marketplace as well as the legislative and judicial environments. This approach also facilitates developing deep relationships with the underwriters, many we have known for decades.


Learn more at www.eperils.com; Telephone: 310-444-9333; Fax: 310-444-9355
Executive Summary

This white paper discusses the most relevant laws and regulations that impact data security and privacy liability exposure. It presents statistics on data breaches, as well as discusses different types of breaches. Finally, it analyzes the current insurance market for cyber liability, particularly focusing on network security and privacy liability coverages. As the insurance market for privacy liability is rapidly changing, a broker focused on these perils and the insurance products available is compulsory in securing the state of the market protection for insureds. We are available to assist.

This is the second annual publication of ExecutivePerils’ What Every Insurance Professional Should Know About Network Security and Privacy Liability whitepaper. In the year since the first release of this report, there have been a number of developments, as well as continuation of certain trends and the revision of others. This second edition includes updates to loss and exposure data, coverage changes and market developments. Actuarial data is still limited, fragmented and often contradictory. We have consulted numerous sources and tried to gather what we consider the most reliable based on our over a decade of experience in cyber insurance. What we do know is that data breach frequency and severity have increased.

The following are some of the highlights since the first edition:
- 2012 included several large breaches including Zappos (24 million records), South Carolina Department of Revenue (6.4 million record), Texas Attorney General’s Office (3.5 million records) Global Payments (1.5 million records), LinkedIn (6.5 million passwords), eHarmony (1.5 million passwords), and more
- For the first time in seven years, Ponemon Institute reported a decline in the cost of a data breach, however,
- NetDiligence reported the average cost per breach climbed to $3.7 million in 2012 from $2.4 million in 2011
- Cloud storage, mobile devices and social media maintain their growth and present challenges
- “Hactivists” and state sponsored breaches increase in 2012
- Breach of privacy lawsuits continue to increase
- Over 30 large carriers now offer some cyber liability coverage
- More organizations are purchasing cyber liability coverage - the adoption of coverage in most industry segments grew at about a 25% rate in 2012
- Past buyers are purchasing higher limits
- The average cost of insurance continues to soften with rate reduction of roughly 5%
- Gross written premium increased to approximately $1 billion in 2012
- Insurance companies are continuing to expand the value-added services they offer, such as risk audits, and discounted forensic and response services (see Chapter 3)
# Table of Contents

**Background** ........................................................................................................... 5  
**Chapter 1: Laws and Regulations** ................................................................. 7  
  Federal .................................................................................................................. 7  
  States .................................................................................................................... 9  
  Private .................................................................................................................. 12  
  International ......................................................................................................... 12  
**Chapter 2: Statistics and Claim Examples** ....................................................... 13  
  Healthcare ........................................................................................................... 17  
  Financial Services ............................................................................................... 19  
  Hospitality ........................................................................................................... 20  
  Large Loss Timeline ............................................................................................. 21  
**Chapter 3: Insurance** ....................................................................................... 23  
  Approach & Structure ......................................................................................... 24  
  Markets / Carriers ............................................................................................... 30  
  Additional Sources of Information ........................................................................ 32
Background

In the early days of Cyber Liability, intellectual property (media liability) exposures such as trademark and copyright infringement were the driving decision maker for most companies who purchased coverage. For larger technology and e-commerce companies, business interruption coverage was another major reason behind the decision to purchase the insurance. As the technology and infrastructure of the World Wide Web matured and network reliability increased, and as redundancies and backups reduced downtime, business interruption became less and less of a threat except for the largest ecommerce companies. Recently, the related issue of lost business resulting from a data breach has come to the fore. As legislation passed, such as the Digital Millennium Copyright Act, the uncertainty of trademark and copyright infringement on the web subsided. This is not to say that “media” exposures are not still a concern. In fact, with the explosion of social media and interactive websites that include user generated content, personal injury litigation has risen. However, coverage in these “traditional” cyber liabilities has matured as actuarial data and case law has developed.

The newest and fastest growing exposure in the cyber world is now Privacy Liability.

Privacy in the United States has a long and storied history. Although some contend that the Constitution does not include a right to privacy, the general consensus is that there is at least a limited right to privacy in the country’s founding documents dating back to 1791, at least from intrusion from government. Americans have always placed a high importance on privacy compared to other parts of the world.

The Right to Privacy, 4 Harvard L.R. 193 (1890), by Warren and Brandeis, is generally considered to be first publication advocating privacy, though the codification of the principles of privacy law did not occur until 1960 with William Prosser’s Privacy, 48 Cal.L.Rev. 383, which he subsequently entered into the Second Restatement of Torts at §§ 652A-652I (1977).

In the 1990’s, as more and more personal information was collected by employers, credit card companies, marketing firms, educational entities, health care providers, and others, and as these entities stored the date in electronic databases that were then joined to a public (and global) internet / World Wide Web, it became easier for mass amounts of personal information to be accessed by those for whom it was not intended. Misuse of such personal information as well as identity theft subsequently began to increase. Personal information is valuable, and nefarious parties have taken the opportunity to profit; an extensive black market evolved.

<table>
<thead>
<tr>
<th>Overall Rank</th>
<th>Item</th>
<th>Percentage 2010</th>
<th>Percentage 2009</th>
<th>2010 Price Ranges</th>
<th>2010 Price Ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Credit card information</td>
<td>22%</td>
<td>19%</td>
<td>$0.07–$100</td>
<td>$0.07–$100</td>
</tr>
<tr>
<td>2</td>
<td>Bank account credentials</td>
<td>16%</td>
<td>19%</td>
<td>$10–$900</td>
<td>$10–$900</td>
</tr>
<tr>
<td>3</td>
<td>Email accounts</td>
<td>10%</td>
<td>7%</td>
<td>$1–$18</td>
<td>$1–$18</td>
</tr>
<tr>
<td>4</td>
<td>Attack tools</td>
<td>7%</td>
<td>2%</td>
<td>$5–$650</td>
<td>$5–$650</td>
</tr>
<tr>
<td>5</td>
<td>Email addresses</td>
<td>5%</td>
<td>7%</td>
<td>$1/MB–$20/MB</td>
<td>$1/MB–$20/MB</td>
</tr>
<tr>
<td>6</td>
<td>Credit card dumps</td>
<td>5%</td>
<td>5%</td>
<td>$0.50–$120</td>
<td>$0.50–$120</td>
</tr>
<tr>
<td>7</td>
<td>Full identities</td>
<td>5%</td>
<td>5%</td>
<td>$0.50–$20</td>
<td>$0.50–$20</td>
</tr>
<tr>
<td>8</td>
<td>Scam hosting</td>
<td>4%</td>
<td>2%</td>
<td>$10–$150</td>
<td>$10–$150</td>
</tr>
<tr>
<td>9</td>
<td>Shell scripts</td>
<td>4%</td>
<td>6%</td>
<td>$2–$7</td>
<td>$2–$7</td>
</tr>
<tr>
<td>10</td>
<td>Cash-out services</td>
<td>3%</td>
<td>4%</td>
<td>$200–$500 or 50%-70% of total v.</td>
<td>$200–$500 or 50%-70% of total v.</td>
</tr>
</tbody>
</table>

Source: Symantec Corporation
Businesses have no right to privacy, however, they are granted property rights such as protection of trade secrets, formulas, etc. which are analogous to personal property rights.

The exposure to Privacy Liability risk varies for every entity, nevertheless, all entities of every size and structure face Privacy risks. The fast pace and complexity of business today do not allow for many companies, particularly smaller companies, to fully develop data management and security procedures with proper legal and technical review. They simply lack the economic ability, legal and technical expertise to keep constantly up to date. In addition to strong risk management with regards to information technology (IT) such as network security (i.e. intrusion prevention, encryption) and data retention policy, insurance policies exist that can transfer certain risks. The newness of the risk and varying appetite of insurance companies has lead each carrier to take its own and differing approach. One should be aware that the scope of coverage afforded can be drastically dissimilar from carrier to carrier. Having an insurance policy and insurance company’s resources as part of an insured’s risk management program is invaluable. When a data breach occurs, legal, technical, financial and business consequences arise. The insurance industry has evolved to address all of these.

The Ponemon Institute’s 2011 Cost of a Data Breach Study: United States, estimated the average cost per compromised record at $194, down from $214 in 2010. 2011 was the first time in seven years that the per capita cost of a data breach decreased. In their 2008 survey, the Ponemon Institute, noted that most breaches occur from lost or stolen laptops or other portable data-bearing device, followed by software systems failures, loss of paper records and hacker attacks. In 2011 negligent insiders and malicious attacks were the leading causes of data breaches. Even at the lower $194 per record, the cost of a data breach is more than all but the largest organizations can bear. Moreover, a policy covering only one’s network is not broad enough to cover two of the three most prolific causes of a data privacy breach – loss of a portable data-bearing device and loss of paper records.
Chapter 1: Laws and Regulations

The number of laws, regulations and rules that touch upon privacy rights and disclosure rules are too numerous to recount herein, however, we will address some of the most important. As of year-end 2012, 46 states, the District of Columbia, the U.S. Virgin Islands and Puerto Rico have enacted legislation requiring notification of breaches, or potential breaches of personally identifiable information (PII). Additionally, there are several relevant federal statutes that pertain to privacy. Clearly, this patchwork of laws and regulation make it nearly impossible for most business owners, c-suite executives and risk managers to keep current, particularly for those who do business in multiple states. The jurisdiction of the state laws is based on both the consumer’s state of residence as well as the home state of the business. Compliance, especially for those in highly regulated industries such as healthcare, legal, educational and financial services, is no easy task. Following are some noteworthy laws on the federal and state levels.

It is interesting to note how many of the legal issues arise from laws enacted before the internet because an everyday part of our lives:

Federal

Governmental Agencies

The Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579, (Dec. 31, 1974), which precedes the World Wide Web by over 15 year, established “a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.” The act prohibits the disclosure of PII without the written consent of the subject individual except under twelve statutory exceptions.

In October 2011, the SEC started to require publicly traded companies to disclose “material” cyber-attacks and their costs to shareholders. Public companies must also disclose a “description of relevant insurance coverage.”

Healthcare

In 1996 Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPPA contains two relevant parts; first, HIPPA Privacy Rule, which protects the privacy of individually identifiable health information, and second, HIPAA Security Rule, which sets national standards for the security of electronic protected health information. HIPPA was followed with The Patient Safety and Quality Improvement Act of 2005 (PSQIA). This includes the Patient Safety Rule, in particular the confidentiality provisions, which protect identifiable information that is being used to analyze patient safety events and improve patient safety. Originally, HIPPA does not require an organization to report a breach of individually identifiable health information, however, 2009 saw the addition of the Health Information Technology for Economic and Clinical Health Act (HITECH) with was included as part of the stimulus bill (American Recovery and Reinvestment Act of 2009, Title XII). HITECH includes a national breach notification requirement and extends HIPPA to business associates. Moreover, HITECH requires periodic audits to ensure compliance with security and privacy requirement and exposes organizations to civil as well as criminal penalties. In January of 2010, Connecticut Attorney General, Richard Blumenthal, was the first AG to utilize the law when he filed suit against Health Net for, “failing to secure private patient medical records and financial information involving 446,000 Connecticut enrollees and (for failing to) promptly notify consumers endangered by the security breach.” In July of that year, Health Net consented to a stipulated judgment, whereby they agreed to pay the State of Connecticut a $250,000 fine and enter into a “Corrective Action Plan.” Additional, Health Net reported that it incurred costs in excess of $7,000,000 to investigate circumstances surrounding a missing portable disk drive, notify Members and to offer credit monitoring services and identity theft insurance.
Financial Services

The Financial Modernization Act of 1999, commonly called the Gramm-Leach Billey Act (GLB) includes provisions to protect personal financial information (PFI) collected and/or held by financial institutions, including smaller FI entities such as individual tax preparers, credit counseling organizations and debt collectors. GLB furnishes administration and enforcement authority for the Financial Privacy Rule and the Safeguard Rule to eight federal agencies and the states.

The Financial Privacy Rule governs the collection and disclosure of PFI. This rule applies to any company, whether they are financial institutions or not, who received PFI. The Privacy Rule requires FI's to provide privacy notices to their customers. By their very nature, data breaches violate the collection and sharing practices stated in these privacy notices.

The Safeguard Rule requires FI’s to implement and maintain safeguards to protect PFI. Again, these safeguards are typically violated when a data breach occurs. Plaintiffs contend that the breach could not have occurred if proper safeguards were implemented and maintainedv.

GLB also contains a pretexting provision (Subtitle B - Fraudulent Access to Financial Information) that precludes the use of false pretenses to obtain PFI.

The Fair and Accurate Credit Transactions Act of 2003 included the Red Flag Rule primarily aimed at FI's and other “creditors” who maintain “covered accounts” such as credit cards or loans. The definition of “creditor,” as originally written, included anyone who provides a product of service for later payment. Originally set to become effective on November 1, 2008, outcry from small businesses prompted enforcement of the Red Flag Rule to be delayed numerous times, while Congress considered legislation to determine the types of businesses to be covered by the Red Flag Rule and possible provide exemptions. In December of 2010, Congress passed and President Obama signed the Red Flags Clarification Act (RFCA) of 2010 into law. RFCA redefined “creditor” to remove businesses that merely bill customers for services previously provided. Act now specifies that the terms “creditor” applies only to entities ““that regularly and in the ordinary course of business— (i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction; (ii) furnishes information to consumer reporting agencies, as described in section 623, in connection with a credit transaction; or (iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person.” Professionals such as doctors, lawyers and insurance agents and brokers no longer fall under the purview of the Red Flag Rule.

Numerous other bills have been introduced in Congress and are in various stages of progressing though one or both chambers.

Other Noteworthy Federal Privacy Laws:
- The Computer Security Act
- The Driver's Privacy Protection Act
- The eGovernment Act of 2002
- The Electronic Communications Privacy Act
- The Family Educational Rights and Privacy Act
- The Freedom of Information Act
- The Paperwork Reduction Act
- The Privacy Protection Act of 1980
- The Right to Financial Privacy Act
TOP FEDERAL LAWS RELATING TO PRIVACY/CYBER BREACH

Fair Credit Reporting Act of 1970

This Act regulates credit bureaus, entities or individuals who use credit reports, and businesses that furnish information to credit bureaus. A major purpose of the Act is the privacy of a consumer’s credit-related data. The Act also requires that consumer reports are supplied only to those with permissible purposes, and for correcting information in a consumer’s report that may be incorrect or the result of fraud. There are various monetary penalties, injunctive penalties and punitive damages for violation of the Act.

Sarbanes – Oxley (SOX)

This Act came into effect in July 2002 and has regulation governing the management of sensitive financial data. It holds CEOs and CFOs directly responsible for the accuracy of financial reports. Although not expressly, the law requires entities conduct risk assessments, either across the entire company, or by a summation of narrower risk assessments on individual transactions and operations within the company. It also imposes requirements related to information storage and retention.

FTC’s Red Flag Rule

Part of Fair and Accurate Credit Transaction Act ("FACTA") which amended the FCRA, these rules require financial institutions and creditors to implement written identity theft protection programs designed to detect the warning signs of identity theft, to prevent the crime, and to anticipate the damage caused. Prior to the enforcement effective date, President Obama issued a clarification related to the definition of "creditor" for purposes of Red Flags Rule enforcement. The law now states that the rule should only apply to businesses that obtain or use consumer reports, directly or indirectly, in connection with a credit transaction; and advance funds to or on behalf of a person based on an obligation to repay the funds or repayable from specific pledged property. However, the new law also gives the FTC the authority to apply the rule to businesses whose accounts the FTC decides are subject to a reasonably foreseeable risk of identity theft.

Identity Theft Enforcement and Restitution Act

Identity theft offenders must “pay an amount equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense.” 18 U.S.C.A. § 3663(b)(6).

Payment Card Industry Date Security Standards

These are standards for the payment card industry that is an industry regulation developed by VISA, MasterCard and other bank card distributors. It requires organizations that handle bank cards to conform to security standards and follow certain requirements for testing and reporting.

Pending Legislation

There were over 100 bills introduced in the 112th Congress dealing with computer security and identity theft, and over 160 bills relating to right of privacy.

The House passed the Cyber Intelligence Sharing and Protection Act in April 2013. President Obama has threatened to veto.

© ExecutivePerils, Inc. 2013

States

In 2001, California became the first state to have an agency dedicated to promoting the protection of consumer privacy rights when the Office of Privacy Protection, which was created by legislation in 2000, opened. A year later, California became the first state to pass privacy breach notification requirements with the passage of A.B. 70013 and S.B. 138614 which became operative on July 1, 2003. 2004 saw the introduction of legislation in at least six states. Many, but not all, used California as a model. In 2005, 22 additional states enacted some form of privacy protection legislation. However, legislation was considered in at least 32 states that year. The following year, legislation was introduced in 32 states and D.C. and adopted in 11. In 2007, four additional states added breach notification laws to their books. In 2008, three more. In 2009, four more, and one additional state (MS) in 2010. As noted earlier, to date, 46 states, D.C., the U.S. Virgin Islands and Puerto Rico have breach notification laws on the books. The only four states that do not have data loss / breach notification laws are Alabama, Kentucky, New Mexico and South Dakota. It is important to note that new legislation is constantly being proposed. Of the 46 states that have notification legislation, 35 do not have a centralized reporting authority such as a Consumer Protection Division or Attorney General. In 2012, at least 13 states introduced security breach notification legislation.

California Office of Privacy Protection has a whitepaper titled “Recommended Practices on notice of Security Breach Involving Personal Information” that we recommend reading.”15

© ExecutivePerils, Inc. 2013
Some Other State Laws of Special Note:

Massachusetts’ law (Massachusetts General Law Chapter 93H / 201 CMR 17.00) requires notification of any breach that involves one or more Massachusetts resident regardless of where the breach takes place or from where the entity who held the private information is domiciled and/or operating.

In NJ, breaches must be reported to the Division of State Police for investigation.

Nevada passed the first law incorporating all of PCI as a state requirement. More on PCI is found in the next section.

Texas: Effective September 1, 2012, notice must be provided to any individual who is either a resident of Texas, or a resident of a state that does not require notification of a security breach.

Connecticut: Of particular interest to insurance brokers, on August 18, 2010, the State of Connecticut Insurance Department issued Bulletin IC-25 wherein all licensees and registrants are required to notify the Department of any “information security incident” which affects any state resident as soon as the incident is identified, but not later than five calendar days. One note of concern is the broad definition of “information security incident” that includes even encrypted information.
U.S. Legal History to 2013

Key

- State Breach Disclosure and Security Laws
  - Influential Data Incident
  - Federal Law
  - HIPAA Enforcement Action
  - Card Industry Regulation
  - State Breach Revision/Additions

© ExecutivePerils, Inc. 2013
Private
In 2007 the PCI Security Standards Council, founded a year earlier by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, released the Payment Card Industry Data Security Standard (PCI DSS). The PCI Security Standards Council also developed and manages Payment Application Data Security Standard (PA-DSS), and Pin-Entry Device (PED) Requirements. The various payment card companies require all merchants, no matter how small or large, to be PCI compliant.

PCI DSS is a comprehensive set of security standards that include security management requirements, policies and procedures, software and hardware design specifications and more. The PCI Security Standards Council periodically updates these standards so merchants must constantly keep abreast of the latest requirements. Current specification may be downloaded from the PCI Security Councils website at https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html.

PCI Compliance consists of four merchant provider levels– Level 1 is the most secure and Level 4 is the most lacks. Although the PCI Security Standards Council redeveloped the levels, each payment card brand has its own definitions and requirements for compliance levels. Therefore it is tough for many merchants to determine what level they must be compliant with, however, generally level requirements are based on total transactional volume with higher requirements for e-commerce transactions then traditional brick and mortar transactions. Once an entity suffers a breach they are usually required to move up the compliance level ladder. Similarly, there are three levels for service providers.

Failure to comply with the PCI requirements could result in fines and loss of one’s contract with the card brands. Additionally, contracts with payment card companies include requirements for reimbursement of charge-backs and cost of reissuing cards. The Insurance Industry section of this whitepaper contains more on these contractual requirements. The PCI Security Standards Council also has Security Standards known as PIN Transaction Security (PTS) Requirements for manufactures to follow in the design, manufacture and transport of a device to the entity that implements it. Additionally, PCI has the Payment Application Data Security Standards (PA-DSS) for software developers and integrators of payment applications.

In March 2013, Genesco (GCO), the parent company of over 2,440 retail stores and a footwear wholesaler, filed suit for $13 million against Visa for breach of contract, failing to follow its own rules and procedures for levying penalties and engaging in unfair business practices under California law. The suit steamed from a December 2010 announcement by Genesco that it had been hacked. Genesco states in court filings that “packet sniffer” malware was inserted onto its computer network, however, “…the thieves did not target, nor did the thieves access any stored payment card account information located on Genesco’s computer network.” This marks the first time a merchant has sued a card company over PCI DSS.

International
The European Union Data Protection Directive was implemented in 1995 by the European Commission. The EU Data Protection Directive was in part a result of the 1981 Convention for the Protection of Individuals with regard to Automatic Procession of Personal Data that requires signatories to enact legislation protecting right of privacy. The EU Data Protection Directive has a broad definition of “personal data” that applies when the data may be linked to a specific person, even if indirectly, and the directive applies even when the “controller” does not reside in the EU, but even if the “controller” merely uses equipment located within the EU.

In addition to the EU Data Protection Directive, many European countries has criminal laws protecting privacy rights. One well publicized example of this was the sentencing of Google’s (former) Chief Financial Officer, Chief Legal Officer and Chief Privacy Counsel to six months in prison by the Criminal Court of Milan, February 24, 2010 for violating Italy’s privacy laws.

Canada has its own PIPA – Alberta’s Personal Information Protection Act that became law on January 1, 2004. “The Act protects individual privacy by requiring, in most cases, private-sector organizations to obtain consent for the collection, use and disclosure of personal information and providing individuals with a right of access to their own personal information.”
According to Javelin Strategy & Research’s 2013 Identity Fraud Report, 12,600,000 Americans were victims of identity fraud in 2011, a more than 23% increase in two years. 12.6 million equates to one victim of identity fraud every three seconds. Additionally, the report found that nearly 25% of consumers that received a breach notification letter became a victim of ID fraud. Of particular importance to smaller retailers, fraud victims are more selective where they shop after such fraud, with smaller business most deeply affected. In 2012, Javelin reported that from 2010 to 2011, 67% more Americans were impacted by data breaches. Data breach victims are near ten times more likely to be a victim of ID fraud. The clearly indicated that if a breach occurs, individuals whose data is compromised will become a victim and are likely to seek redress.

Norton reports that over two-thirds of online adults worldwide have been a victim of cybercrime at a remarkable rate of nearly three out of four in the U.S. with 18 adults becoming a victim of cybercrime every second. Norton calculated the global cost of cybercrime to be $110 billion annually with an average cost over nearly $200 per victim. Clearly, cyber privacy breaches are all too real for far too many. This section lays out some statistics and claim examples to help one better understand the breadth of this peril.

As we noted in last year’s report, total data breach disclosures fell in 2009 and 2010. DataLossDB, the Identity Theft Research Center, Privacy Rights Clearinghouse, the United States Secret Service and Verizon reported total losses well below 2008 (see figure 3). We wrote at the time that the reason for this decline was uncertain, and hypothesized that could have been a result of high profile cases, such as the prosecutions on Albert Gonzalez of TJX and Hartland Payment Systems fame, or be simply a result of falling prices for personal information, such as bank account credentials and credit card information, on the black-market (see figure 1 & 2). Other possible reasons included a simple lack of reporting - even with strict breach reporting laws, many breaches are still not reported - or that cyber criminals were becoming more adept at hiding their tracks, and breaches were just not being detected. Fraud alerts are the most common method of breach discovery. The marked increases in 2011 and 2012 give credence to the theory that criminals were holding back for reasons such as depressed pricing and fear of being caught.

2011 also saw some large breaches of large, well-known companies such as Sony and Alliance Data Systems’ Epsilon unit. Some of Epsilon’s clients include, Capital One, Citigroup, Kroger, TiVo, Verizon, Walgreen, and more. In all, Epsilon sends more than 40 billion permission-based e-mails annually on behalf of its over 600 clients. Sony also saw a significant breach in early 2011 that at last count consisted of an estimated 100 million compromised customer accounts and a cost of over $300 million. The totals for past year continue to be revised upward as over half of all breaches take weeks or months from the date of first compromise to discovery, so there is always a delay in breach statistics.

2012 started with the theft of some of Symantec’s Norton anti-virus source code. Also in January major online retailer Amazon’s Zappos and 6PM were breached, compromising account information of 24 million customers. Global Payments was hacked possibly exposing 1.5 million credit and debit card owners, and costing the firm over $93 million. 6.46 million LinkedIn user passwords were breached. Total cost to the company is estimated at over $3 million. Even high-profile individuals were exposed. Vice President Joe Biden and first lady Michelle Obama had their PII exposed, and in March of 2013 Chief Justice Jon Roberts was hit by credit card fraud.

Last year also brought a marked increase in “hackivist” activity as well as state sponsored hacking. Anonymous increased its activity, and in February 2013, computer firm Mandiant identified the People’s Liberation Army’s Unit 61398 based in Shanghai as the party most likely responsible for hacking over 140 organizations from 2006-2013.
While the total number breaches declined in 2009 and 2010, the overall cost of breaches was rising. According to the Ponemon Institute, the estimated cost of a data breach on a per capita basis in 2010 was $214, up from $204 in 2009 and $138 in 2005. The average organizational cost of a data breach this year increased to $7.2 million, up seven percent from $6.8 million in 2009. Total breach costs had grown every year from 2006 to 2010. One reason for the increase cost was that data breaches from malicious attacks and botnets, which cost more than breaches caused by human negligence or system errors, doubled from 2008 to 2009 to nearly one quarter of all data breaches. Another reason may have been the increased reporting requirements. Companies that notified victims within one month of discovering a data breach paid nearly 55% more than companies that took longer to notify.

In 2012 the world witnessed the largest breach ever with Shanghai Roadway D&B Marketing Services Co. exposing over 150 million records. Some breaches already in 2013 include, Midwest BankCentre, Kirkwood Community College, Erlanger Hospital, Olive Garden, OP Productions, Schnucks and more.

Although some of these factors still push costs up – malicious or criminal attacks accounted for more than a third of reported breaches, companies that were too quick to notify customer paid an average of $33 more per record, and notification costs increased nearly 10% over 2010 – the overall trend reversed in 2011. Organizational cost declined to $5.5M and the cost per record edged down to $194. It appears that organizations are becoming better prepared to respond to a breach. Factors such as if the organization has a CISO or equivalent (up to $80/record), or utilized an outside consultant (up to $41/record) reduce overall cost. Detection and escalation costs declined by roughly 6%, suggesting that better processes were in place to handle such activities. The growth of insurance products providing additional value added services is certainly aiding insureds to reduce cost.
More statistics from Ponemon Institute’s 2011 Annual Study

- Lost business costs declined from $4.54 million in 2010 to $3.01 million in 2011.

- Organizations with a first time breach spent an average of $37 more per record.

- Average size of breach, per capita cost, churn and average total cost all declined from 2010 to 2011.

- Viruses, malware, worms, Trojans are the leading cause of a malicious attack.

- 41% of data was lost or stolen due to a third party error.

- 39% of breached involved lost or stolen devises.

- 43% of organizations have a CISO or equivalent person with overall responsibility.

- 41% of organizations notified potential victims within 30 days.

- 37% hired outside consultants to assist in the breach response and remediation.

### Average Cost Per-Record, 2005-2011

![Average Cost Per-Record, 2005-2011](chart)

### Per capita cost by industry classification

![Per capita cost by industry classification](chart)

### Distribution by Root Cause of Breach

![Distribution by Root Cause of Breach](chart)

Compiled by ExecutivePerils
Social Networking and Mobile Devises

In 2011, nearly 20% of all web traffic was on social networking sites, and it's estimated that roughly 25% of all web traffic in the U.S. starts from a social networking website. That's up from only about 2% in 2009. Facebook alone has over 1 billion active users, and nearly 50% of the top 10,000 websites worldwide link to Facebook. As the number of individuals and organizations using these social networking services has grown, they have become a much more attractive target for cyber criminals. Additionally, attempts by these social networking organizations to monetize their user base, along with their rapid growth, has caused the entities themselves to violate privacy laws.

We noted last year that according to IT security and data protection firm Sophos, 67% of social networking users reported being spammed in December 2010, up from just over 33% a year and a half earlier, and 40% reported social network based malware attacks. Even with this startling fact, 49% of U.S. businesses allow their employees unfettered access to Facebook at work. Sophos’ report states that 72% of firms believe that employees’ behavior on social networking sites could endanger their business’ security.
In addition to direct threats, the use of social networks and blogs by company employees exposes companies to inadvertent privacy and media violations such as trademark infringement, copyright infringement, and personal injury (defamation, cyber-bullying). Users often post messages on Facebook, LinkedIn, Twitter or blogs without giving much thought to the potential universal audience of these services. Moreover, once something is posted online, it is impossible for it to be completely erased. Private information as well as defamatory and damaging statements are routinely posted online. Javelin Strategy & Research reported, “68 percent of people with public social media profiles shared their birthday information (with 45 percent sharing month, date and year); 63 percent shared their high school name; 18 percent shared their phone number; and 12 percent shared their pet’s name - all are prime examples of personal information a company would use to verify your identity.”

The use of mobile devices expanded in 2012. According to Cisco, Global mobile data traffic grew 70 percent, and average smartphone usage grew by over 80% in 2012. By the end of 2013, there will be more mobile devices on Earth than people. IDC forecasts tablet sales to exceed 172 million units in 2013. Email open rates on smartphones increased by 300% From October 2010 to October 2012. Unfortunately, mobile security has not kept pace. Javelin found that seven percent of smartphone users were victims of ID fraud, a rate 33% higher than the general public. 62% do not use a home screen password, and nearly a third save login information on their device. Norton’s 2012 Cybercrime Report states that two-thirds of adults use a mobile device to access the internet. Meanwhile, mobile vulnerabilities doubled from 2010 to 2011. 35% of adults have lost their device or had it stolen, and two-thirds of users do not utilize a security solution on the device. Still, 31% shop online, and 24% access their bank account. Norton estimates that more than one in five online adults has been a victim of either social or mobile cybercrime.

- 15 percent of social network users reported someone had hacked into their profile and pretended to be them.
- 1 in 10 social network users said they’d fallen victim to a scam or fake link on social network platforms.
- While 75 percent believe that cybercriminals are setting their sights on social networks, less than half (44 percent) actually use a security solution which protects them from social network threats and only 49 percent use the privacy settings to control what information they share, and with whom.
- Nearly one-third (31 percent) of mobile users received a text message from someone they didn’t know requesting that they click on an embedded link or dial an unknown number to retrieve a “voicemail”.

All companies, but especially those with Bring Your Own Devise (BYOD) policies should be aware of the risks associated with mobile devices and set their security policy accordingly. Not all insurance policies cover BOYD.

**Healthcare**

Since enactment of the Interim Final Breach Notification Rule in September 2009, nearly 22 million patients have been affected by data breaches, including over 300,000 in the Q1, 2013. In the Ponemon Institute’s 2012 Third Annual Benchmark Study on Patient Privacy and Data Security, 94% of participating healthcare organizations had at least one breach, and 45% had more than five. The total annual economic impact of data breaches could be as high as $7 billion. NetDiligence reported an increase from 500,000 records exposed in its 2011 report to 6.4 million records in 2012, and increase of nearly 13 times. In addition to the high regulatory scrutiny that the healthcare sector carries, perhaps nowhere more than healthcare organizations is Personal Identifying Information (PII) of groups such as minors, the elderly and the deceased more at risk. Protected Health Information (PHI) must be open enough for physicians and other health professionals to access it, but at the same time, proper safeguards must exist to protect it. With the increase in online health records and the vast amount of outsourced services within the healthcare industry, the risk of privacy breaches is amplified. Significantly, medical information fraud is could result in bodily injury if medical records are altered or misinformation is included in a patient’s file. The good news is, according to the 2012/2013 Kroll Global Fraud Report Survey, the healthcare, pharmaceuticals and biotechnology industry reported the second lowest percentage of companies hit by fraud (only travel, leisure and transportation was lower). The bad news is that this sector had the highest percentage of fraud involving external partners. More good news / bad news was reported by Redspin – while the total number of health data breaches affecting more 500 plus individuals increased from 121 in 2011 to 146 in 2012, the total number of patient affected declined strikingly from 10.6 million in 2011 to only 2.4 million in 2012.
Kroll Advisory Solutions 2012 HIMSS Analytics Report: Security of Patient Data:
- 27% of respondents had a security breach within the past year. Up from 19% in 2010
- 69% of organizations who reported a breach had more than one
- 56% reported that the source of the breach was by an employee of the organization
- Only 56% of respondents indicated they ensure that their third-party vendors conduct a periodic risk analysis
- Theft was the most commonly reported cause of large breaches
- 99 incidents involved theft of paper records or electronic media, together affecting approximately 2,979,121 individuals.
- Loss of electronic media or paper records affected approximately 1,156,847 individuals.
- Unauthorized access to, or uses or disclosures of, protected health information affected approximately 1,006,393 individuals.
- Human or technological errors, or other failures to take adequate care of protected health information, affected approximately 78,663 individuals.
- Improper disposal of paper affected approximately 70,279 individuals.

Ponemon Institute, Third Annual Benchmark Study on Patient Privacy and Data Security:
- 57% of data breaches cost more the $500,000. Up from 48% in 2010
- Insider negligence continues to be at the root of the data breach
- 81% of healthcare organizations allow employees and medical staff to use their own mobile devices. 51% are bringing their own devices.
- 21% of respondents say that employee records are most at risk of data loss or theft
- Two-thirds of respondents were unsure of the security and privacy of Health Information Exchanges
- Less than half (40%) said they had confidence in preventing and detecting data loss or theft

Identity Force Spring 2010 National Survey of Hospital Compliance Executives:
- Nearly 85% of hospitals are NOT in compliance with the HITECH Act which went into effect in February 2010
- Only 30.5% are only at the “evaluating options” stage.
- 61% of hospitals say they do not have a formal process in place to verify that vendors or business associates are in compliance with the HITECH Act
- 36% report they have business associate that are not in compliance with the HITECH Act.
- 41% of hospitals now have 10 or more data breaches annually this is up over 120% from the 2009 survey
- 34% of hospitals keep inadequate photo ID records and 70% investigate less than one case per week
- 56% of hospitals expect new Healthcare Reform Law to either make no difference or to increase medical identity theft
- 83.6% of hospitals investigate are least one data breach every year
- 41.5% investigate 10 or more each year
- 20.3% investigate 20 or more each year

2011 HIMSS Security Survey:
- 22% of respondents reported at least one known security breach at their organization within the last year
- 64% reported that their organization conducted an IT security plan audit
- Less than half reported testing their data breach response plan

HIPAA violation penalty tiers under HITECH

<table>
<thead>
<tr>
<th>Tiers</th>
<th>Per Violation</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without knowledge/intent</td>
<td>$100</td>
<td>$25,000</td>
</tr>
<tr>
<td>Due to reasonable cause</td>
<td>$1,000</td>
<td>$100,000</td>
</tr>
<tr>
<td>Willful neglect</td>
<td>$10,000</td>
<td>$250,000</td>
</tr>
<tr>
<td>Willful neglect, not corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Financial Services

While the financial services industry is often thought to be one of the most commonly breached sectors, the data do not bear this out. Although financial data, particularly credit card data, is frequently stolen, the source where the data is compromised is usually nonfinancial organizations. Financial services firms were some of the first to address the issue of network security and privacy. This attention to exposure has paid off. Verizon reported that the financial and insurance industry dropped from 22% of breaches in 2010 to only about 10% in 2011.44

Privacy & Data Protection Practices Benchmark Study of the Financial Services Industry45

- 83% of companies use real customer of employee information in development and testing phases. 51% of these companies admit they do not take appropriate steps to protect these data
- 25% of companies do not use authentication to determine who has access to PII.
- Less than half of companies use intrusion detection systems
- Data loss prevention solutions are used by only 41% of companies
- Less than half of companies vet business partners before sending sensitive data
- Less than one-third of companies review security systems and possibly modify them to ensure compliance with the Red Flag Rule
- Half of all companies report they do not have sufficient resources to accomplish their security goals and objectives
- Only 41% say they have sufficient procedures in place to know and understand the root cause of most privacy violations or data breaches

Internet Crime Complaint Center46

- The number of fraud complaints increased 3.4% from 2010 to 2011 to 314,246
- Total losses linked to online fraud was over $485 million
- For victims reporting financial losses, the average was $4,187
- Of the top five categories of offenses reported to law enforcement during 2011;
  - FBI-related Scams
  - Identity Theft
  - Advance Fee Fraud
  - Non-Auction/Non-Delivery of Merchandise
  - credit card fraud, 10.4%;
  - Overpayment Fraud

Yearly Comparison of Complaints
Trustwave SpiderLabs, a provider of information security and payment card industry compliance management solutions, reports that the food and beverage industry made up nearly 44 percent of data breaches in 2011. "Industries with franchise models are the new cyber targets: more than a third of 2011 forensic and security incident investigations conducted by Trustwave SpiderLabs occurred in a franchise business."

<table>
<thead>
<tr>
<th>Rank</th>
<th>State</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>California</td>
<td>11.95%</td>
</tr>
<tr>
<td>2</td>
<td>Florida</td>
<td>7.01%</td>
</tr>
<tr>
<td>3</td>
<td>Texas</td>
<td>6.46%</td>
</tr>
<tr>
<td>4</td>
<td>New York</td>
<td>5.27%</td>
</tr>
<tr>
<td>5</td>
<td>Ohio</td>
<td>4.43%</td>
</tr>
<tr>
<td>6</td>
<td>New Jersey</td>
<td>4.02%</td>
</tr>
<tr>
<td>7</td>
<td>Pennsylvania</td>
<td>3.34%</td>
</tr>
<tr>
<td>8</td>
<td>Illinois</td>
<td>3.07%</td>
</tr>
<tr>
<td>9</td>
<td>Virginia</td>
<td>2.96%</td>
</tr>
<tr>
<td>10</td>
<td>Washington</td>
<td>2.44%</td>
</tr>
</tbody>
</table>

Why is the hospitality sector a natural target?

First, hotels, restaurants, travel agencies, and other types of hospitality companies collect and store large amounts of personal data, most notably financial information.

The U.S. Bureau of Economic Analysis reports that in the fourth quarter of 2012, total current-dollar direct tourism spending was $865.3 billion.

Second, most of these companies lack robust security systems. Whereas large banks, hospitals and major online retailers have invested significantly in security, many companies in the hospitality industry are smaller companies, with even smaller IT budgets.

Moreover, they are not technology-forward companies. They provide rooms, meals, transportation and entertainment, not technology services.

Recently, franchised businesses have been a major target because of consistency from business to business. If a cyber-criminal breaches one franchisee, the doors to the other franchisees often have the same key and are simple targets.

Third, they typically have multiple points of entry and multiple systems of data collection and storage to exploit. Nearly 60 percent of travel reservations are now made online. Hotels often store customer information on electronic key cards. Rewards/loyalty programs are more and more common. Third-party affiliates store and share information between multiple networks. Wireless devices such as PDAs with credit card payment hardware and software are becoming more ubiquitous. All of these leave potential vulnerabilities for hackers to exploit.

Fourth, staff has access to customer’s data. Many of these employees are paid low wages and are not properly vetted through background checks. Workers at Tropicana Casino and Resort in Atlantic City, N.J., were indicted for stealing a list with 20,300 top gamblers’ names, addresses, phone numbers and gambling losses.

Fifth, value-added services such as wireless access points / Wi-Fi or common “business center” computers expose customers to potentially corrupted systems.

This sector has been investing in data security measures and their efforts seem to be paying off, at least somewhat. In Trustwave’s 2013 report, retail over took hospitality including food and beverage, to take the number one spot at 45%. Hospitality/food & beverage still accounted for one third of breaches, however.

<table>
<thead>
<tr>
<th>Rank</th>
<th>State</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alaska</td>
<td>196</td>
</tr>
<tr>
<td>2</td>
<td>District of Columbia</td>
<td>137</td>
</tr>
<tr>
<td>3</td>
<td>New Jersey</td>
<td>131</td>
</tr>
<tr>
<td>4</td>
<td>Nevada</td>
<td>130</td>
</tr>
<tr>
<td>5</td>
<td>Colorado</td>
<td>123</td>
</tr>
<tr>
<td>6</td>
<td>Ohio</td>
<td>110</td>
</tr>
<tr>
<td>7</td>
<td>Maryland</td>
<td>109</td>
</tr>
<tr>
<td>8</td>
<td>Florida</td>
<td>107</td>
</tr>
<tr>
<td>9</td>
<td>Virginia</td>
<td>106</td>
</tr>
<tr>
<td>10</td>
<td>Washington</td>
<td>104</td>
</tr>
</tbody>
</table>
ExecutivePeril’s Large Loss Timeline

Following is a list of large data breaches that occurred in the last five years. The list is not exhaustive, but represents some of the most publicized.

**February 18, 2005** – Bank of America claimed that it had lost more than 1.2 million customer records. It said there was no evidence that the data had fallen into the hands of criminals.

**April, 2005** – Hackers accessed a total of 1.4 million records, including highly sensitive credit card security codes stored on DSW’s in-store computer network. As part of the Consent Agreement with the FTC, DSW is required to obtain a biannual security audit by an outside firm for the next 20 years.

**June 16, 2005** – a series of class action cases against CardSystems, a merchant payment-processing provider, alleging that it failed to adequately protect the PII of 40 million customers. VISA and American Express cut their ties with the company, prohibiting it from processing their card data. Nearing collapse, CardSystems was subsequently acquired by another company.

**January, 2006** – Boston Globe and The Worcester Telegram & Gazette unwittingly exposed 240,000 credit and debit card records along with routing information for personal checks printed on recycled paper used in wrapping newspaper bundles for distribution.

**February, 2006** – 200,000 debit card accounts (estimated) were disclosed by unknown retail merchants, apparently OfficeMax and others. These included accounts related to banks and credit unions nationwide including CitiBank and Wells Fargo.

**January, 2007** – MoneyGram, a payment service provider, reported that a company server containing information on about 79,000 bill payment customers, including names, addresses, phone numbers, and in some cases, bank account numbers was unlawfully accessed over the Internet.

**January, 2007** – TJX Companies Inc. (T.J. Maxx) disclosed that they had experienced an unauthorized intrusion into the electronic credit/debit card processing system. In what is considered the most glamorous security breaches to date, as much as 94,000,000 credit/debit card account numbers and over 455,000 merchandise return records (containing customer names and driver’s license numbers) were stolen from the company’s IT system.

**March, 2008** – Hannaford Brother, a Maine based grocery, reported that hackers had breached their system and stole ‘track 2’ data as it was transmitted from the stores (300) to card processors. 4.2 million card numbers, expiration dates and security codes were stolen. Hannaford had received PCI certification on February 27th of that year. This breach lead to a class action suite, Anderson v. Hannaford Brothers, Co., wherein the First Circuit held that plaintiff's claims for negligence and implied contract should survive Hannaford’s motion to dismiss because plaintiffs’ reasonably foreseeable mitigation costs constitute a cognizable claim for damages under Maine law (Oct. 11, 2011).

**September, 2008** - GS Caltex, one of the nation’s largest oil refineries, lost two discs containing PII of 11.1 million customers.

**January, 2009** - Heartland Payment System, a payment card processor, announced that 130 million transactions were potentially compromised. 31 suits were filed in two weeks.

  $60 million set aside to reimburse Visa  
  $3.6 million to settle with American Express  
  $41 million to reimburse MasterCard  
  $5 million to settle with Discover  
  $4 million to settle a consolidated consumer class action  
  More than $26 million in legal costs  
  $? in reputation damage and lost customers

March, 2011 – RSA SecurID, the Security Division of EMC, a major two-factor authentication system, was breached. The breach cost EMC over $66 million and left many SecurID users vulnerable.

April, 2011 – Sony’s PlayStation network and Sony online.
   - 100 million customer accounts
   - 75 class action lawsuits
   - $300 million anticipated cost
   - Pending coverage dispute with Zurich American Insurance Company

April, 2011 – Alliance Data Systems’ Epsilon Interactive, an email service provider with clients such as Capital One, Citigroup, JPMorgan Chase, Kroger, Scottrade, TiVo, Verizon and Walgreen. Unknown number of names and email addresses.

April, 2011 – Texas Comptroller’s Office. 3.5 million records

September, 2011 - TRICARE Management Activity, the military’s health insurance carrier. Backup tapes storing records of 4.9 million people from a military electronic health record system in use from 1992 through Sept. 7, 2011 were reportedly taken from the car of an SAIC employee. $4.9 billion lawsuit filed.

November, 2011 – Steam (Valve, Inc.), and online digital store, game library and multiplayer network was hacked. 35 million records exposed.

January, 2012 – Zappos, an online shoe retailer owned by Amazon. 24 million email addresses, billing and shipping addresses, phone numbers, password and the last four digits of customers’ credit cards. Dozens of class actions suits were filed. In Oct, 2012 a federal court denied Zappos’ request for arbitration striking down Zappos.com’s user agreement.

January, 2012 – New York State Gas and Electric – 1.8 million customers. PII included SSN, DOB, and some bank account numbers.

April, 2012 – Global Payments, an Atlanta, GA based payment processor discovered it had been hacked exposing between 1.5 million and 7 million payment cards. The breach may have dated back as far as June 2011. $94 million estimates cost to date (see below) with another $25 to $35 million expected in 2013
   - $60 million for professional fees and costs associated with the investigation and remediation, incentive payments to certain business partners and costs associated with credit monitoring and identity protection insurance;
   - $36 million estimated fraud losses, fines and other charges that will be imposed by the card networks;
   - $2 million received for insurance recoveries, based on claims submitted to date.

October, 2012 - South Carolina Department of Revenue. 6.4 million Social Security numbers exposed and over 3.8 million bank account and credit cards.

March, 2013 – Schnucks, a St. Louis based 100 store supermarket chain that include 96 in-store pharmacies. Breach occurred from December 2012 to March 2013 exposing 2.4 million payment cards used at 79 stores. At least three class action suits have been filed to date.
Chapter 3: Insurance

For the last two years, over forty percent of all data breaches are a result of an error by a third party. Moreover, in its 2012 Breach Report, Verizon reported that of the attacks investigated, "96% were not highly difficult" and "97% of breaches were avoidable through simple or intermediate controls" both percentages higher than the year before. This continues to demonstrate just how vulnerable many businesses are, particularly small and middle market companies. However, not all breaches occur at poorly protected small and middle market companies. Large organizations with vast IT budgets such as Google, Sony and the Departments of Defense and Homeland Security have experienced failures in their ability to fully protect their systems. Even network security companies such as Symantec/VeriSign have been victims of data breaches. Certainly, insurance should not be considered a substitute for good risk control. Most companies will need coverage for losses that occur in spite of the controls they have put in place. Insurance may be effective in protecting an entity's balance sheet in the face of a security failure. Insurance should be a part of any complete risk management program.

When a privacy breach occurs there are two victims – the individual whose personal information is exposed, and the entity who was breached. The individual seeks recompense from the entity, but many times the entity has nowhere to turn and is forced to absorb the expense internally. Fortunately, the insurance industry has recognized the vulnerabilities companies have and has developed specialized insurance products to address this growing exposure. Although we have seen double-digit increases in the number of entities purchasing cyber liability insurance in each of the past three years, far too few companies still recognize their exposure and purchase the insurance coverage. For example, a 2010 survey of senior executives at middle market companies conducted by Betterley Risk Consultants revealed that only about one third of these companies purchased specialized cyber insurance policies. This percentage has been corroborated in reports issued since by Advisen. The potential number of insureds has the industry excited.

Limitations in Standard Insurance Portfolios

A surprising number of respondents to the 2010 Betterley survey indicated they believed their standard insurance portfolio adequately protected their companies from cyber risks. While limited coverage for some privacy, media, or data breach exposures may be included in “traditional” insurance programs comprised of commercial general liability, umbrella liability, fidelity/crime, and kidnap, ransom and extortion policies, there will inevitably be substantial gaps and plenty of room for coverage disputes. Most underwriters of traditional types of insurance contend that it is not the intent of these policies to pick up cyber exposures. Changes have been made, and are continuing to be made, to these forms to clarify the intent not to cover cyber exposures.

For example, the following limitations have been added to the standard ISO commercial general liability policy in the past decade or so:

- An exclusion for damage arising from damage to or the loss of electronic data.
- A clarification that electronic data is not tangible property (thus, damage to electronic data is not covered property damage)
- An exclusion for liability arising from violation of statutes, regulations, or ordinances related to sending, distributing, transmitting information.
- An exclusion for personal or advertising liability arising from chat rooms or bulletin boards owned, managed, or controlled by the insured

Additionally, the standard CGL policy covers copyright infringement only if the infringement is in an “advertisement,” which is strictly defined and narrowly construed. Of course, the cost to notify others that their personal information has been breached – as required by the laws discussed in chapter 1 – would not be covered under standard CGL or umbrella policies. Some insurers go further than the limitations in the standard policy, adding their own restrictive endorsements. These exclusions and limitations make coverage under a CGL for liability arising from privacy claims, social media activities, copyright infringement in websites, and e-mail marketing nonexistent.
Sony’s massive data breach and resulting class actions claims in early 2011 resulted in a denial of coverage by Zurich American Insurance Company. On July 20, 2011 Zurich filed suit against Sony contending that the CGL and excess liability policies purchased by Sony do not cover these claims.\textsuperscript{51} Even should Sony prevail in this case, consider the cost of the litigation, the disruption incurred from the necessity of litigating coverage while defending the underlying actions, and the cost of the litigation. The very survival of most companies would be imperiled.

Questions such as these arise with commercial property insurance too. Loss from damage to or destruction of data is typically subject to a low sublimit, if covered at all, in both direct damage and business income policies.

In summary, using specialized policy forms developed specifically to cover data breach, media liability, business interruption and loss of business, cyber extortion, notification and crisis management, and other risks arising from Internet activities has become mandatory. Agents and brokers are well advised to review their clients’ exposures to potential losses, and recommend appropriate cyber insurance where warranted.

### Cyber Defenses Eroding

<table>
<thead>
<tr>
<th>Peril</th>
<th>Damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Theft</td>
<td>Stollenwerk vs. Tri West: plaintiffs with damages survived summary judgment</td>
</tr>
<tr>
<td>Fear of Identity Theft</td>
<td>Krottner vs. Starbucks Corp: increased risk of identity theft constitutes an injury-in-fact (class plaintiffs survived summary judgment)</td>
</tr>
<tr>
<td>Lost Time</td>
<td>ITRA (Identity Theft Enforcement and Restoration Act) pay an amount equal to the value of the time reasonably spent to remediate intended harm</td>
</tr>
<tr>
<td>Lost Time</td>
<td>ChoicePoint/FTC Data Breach Settlement: paid for “time victims may have spent monitoring their credit&quot; $18.17 x 14,000 = $254,000</td>
</tr>
</tbody>
</table>

TJX: $10 hour (up to $60 hour)   Countrywide: $10 hour (up to $60 hour)   Heartland: $10 hour (up to $50)

© ExecutivePerils, Inc. 2013

### Coverage Approach and Structure

The insurance industry began offering cyber liability coverage in the 1990's. In the early days, however, coverage was limited, premiums were high and only technology and e-commerce companies purchased it. Recently the marketplace has evolved, and broader cyber liability policies, including privacy liability coverage, have come on the market. Overall, premiums are lower, and a broader cross section of industries are including the coverage in their insurance portfolios. Our research has estimated gross written premium for cyber liability insurance as follows:

<table>
<thead>
<tr>
<th>Year</th>
<th>Premium Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>$300,000,000 to $350,000,000</td>
</tr>
<tr>
<td>2007</td>
<td>$400,000,000 to $450,000,000</td>
</tr>
<tr>
<td>2008</td>
<td>$450,000,000 to $500,000,000</td>
</tr>
<tr>
<td>2009</td>
<td>$500,000,000 to $550,000,000</td>
</tr>
<tr>
<td>2010</td>
<td>$600,000,000 to $650,000,000</td>
</tr>
<tr>
<td>2011</td>
<td>$750,000,000 to $850,000,000</td>
</tr>
<tr>
<td>2013</td>
<td>Over $1,000,000,000</td>
</tr>
</tbody>
</table>

© ExecutivePerils, Inc. 2013
Though cyber perils in some form have been around for nearly a quarter century, the actuarial data is still scant. Laws affecting coverage are new and there is not enough case law to confidently evaluate the exposure. Breach disclosure laws have pushed data into the public sphere, and more and more courts are deciding cases and setting precedence. As the legal environment matures and reduces uncertainty, and as insurers gain experience, expect to see a more homogeneous market approach. We think it will be at least five to 10 years before we see standardization. Today, however, the market is far from uniform. Though Insurance Services Office, Inc. (ISO) has developed a form called the Internet Liability and Network Protection Policy, it is rarely used (and already outdated), and it can be said that there is no standard cyber liability form. In fact, there is not even agreed upon nomenclature. Coverage and terminology is as disparate as the number of insurers in the market. As a result, insurance buyers or their brokers must carefully review and compare policy forms in determining which insurer’s policy form best matches up with an organization’s loss exposures. Product expertise is paramount.

Simplistically, cyber policies may be broken into two coverage types, Third Party Liability (liability to others), and First Party Liability (coverage for the insured’s own losses). Each is discussed in general terms below.

**Third Party Cyber Liability Insurance**

The main focus of this coverage is to cover liability arising from violations of privacy and data breach notification laws. These exposures also result in the need for first party coverage (discussed subsequently). Third party cyber liability policies also can include coverage for a number of other types of liability, such as liability from transmitting a computer virus to another party or from copyright infringement included in the insured’s website.

Policies are typically written on a claims made and reported basis. It is important to pay attention to the Prior Acts Date included in the policy, keeping it as far in the past as possible. As noted earlier, over half of all breaches take weeks to months from the date of first compromise to discovery.

**Type of information covered under some policies.**

A key to coverage is the types of information the policy specifies as being covered, and there are substantial variations between forms.

Coverage should be provided for both electronic and physical (paper, laptop, portable disk, PDA, etc.) breaches. As noted in Chapter 2, laptops are lost or stolen at a rate of nearly 300 per day in the largest U.S. airports. PDAs, smartphones, jump drives, and even traditional hard copy (paper) records are lost, stolen or improperly disposed of on a regular basis, and all of these media are subject to breach notification statutes.

Coverage should include both personal and corporate information. Although most privacy laws refer only to personal information, the loss of corporate information can be costly, and some insurers will extend coverage to apply to breaches involving this type of information.

Coverage should apply to employee data as well as customer information. There are policies that cover only employee data. Conversely some policies only cover customer data. Since most entities collect and hold information on both groups the broadest coverage should be secured.

Information in the “care, custody or control” of the insured’s vendors should be covered. Some policies limit coverage to information in the “care custody, or control” of the insured. Exactly what this includes is not clear. For example, is data on “cloud” servers considered to be in the insured’s “care, custody or control?” What about medical records being transported to a long term storage facility by a vendor? These could be argued either way. For this reason, it is important to either avoid the “care, custody, or control” limitation or clarify it with respect to the insured’s exposures. One approach is to ask for explicit coverage for “cloud” systems or data transferred by the insured to a third party. Knowing what to ask for is an important part of securing the broadest coverage.
Coverage may apply to accidental losses/leaks or just breaches perpetrated by criminals. We think the policy should address both. Here again the lost laptop example comes into play. Accidents happen and there is insurance coverage in the market that will cover these types of incidents.

Requirements to be “PCI compliant” should be avoided. Compliance is an ongoing state. Many companies are “PCI validated” at one point in time, but when a breach occurs, almost by definition, the company is not “compliant.” Perhaps an update was missed, or new processes opened a security hole. These inadvertent security failures are one reason entities look to insurance. There are ways for insurers to avoid moral hazards without putting onerous requirements on the insured. Here too, beware of warranties outside the policy form. Several insurers’ applications contain PCI warranties.

Avoid encryption requirements. Some policies require all data to be encrypted for coverage to apply. Password protection is not considered encryption, and most laptops, PDA’s and smart phones contain unencrypted data. Paper files are never encrypted.

Don’t accept an “insider” exclusion. Although the exact proportion of identity crimes that involve insiders is uncertain, estimates are that it is about half. Coverage should apply to breaches perpetrated by employees, ex-employees, as well as outsiders.

**Virus / Malware / Hacking Coverage.**
Coverage should apply to liability to others for unintentionally sending them a virus or malware. This should apply if the transmission is by e-mail or through malicious code placed on the insured's website.

Some policies limit the coverage for viruses and hacking to direct intentional attacks that target the insured specifically. Look for coverage that includes “wild” viruses that are not specifically targeting the insured.

Beware of anti-stacking clauses. A large scale attack could hit multiple policyholders. If the policy includes an aggregate limit for all policies issued by the particular insurer, a system wide attack could leave a substantially reduced limit for individual insureds. This has become more relevant in the last five plus years as more companies are buying cyber insurance and companies are partially outsourcing data services.

**Media Liability / Content Injury - Intellectual Property Infringement and Personal Injury.**
The exposure to intellectual property infringement (e.g., copyright and trademark, patents are not covered) libel, and disparagement suits resulting from websites, e-mail newsletters, blogs, and social network marketing activities is underestimated by many companies. Cyber insurance policies can provide valuable coverage for these exposures.

Beware of policy language that limits coverage to only claims made in the United States and its territories. The World Wide Web is just that, worldwide, and these types of claims can emanate from anywhere. The policy should cover claims made anywhere in the world even if the insured target audience is U.S. based. It should also cover violations of foreign laws.

Look for coverage that extends beyond the insured's website to also include social networking sites (e.g., LinkedIn, Facebook, and Badoo) as well as e-mail and other messaging services like Twitter. Trademark and copyright violations, as well as libelous comments occur in e-mails and even over instant messaging services. Sometimes these documents are intended for internal use only, but leak out to third parties.

Coverage for user-generated content is particularly important because user posts are oftentimes opinionated and inflammatory. Additionally, third parties often pay little or no attention to intellectual property rights. Although limited protection exists via the Digital Millennium Copyright Act’s safe harbor provision, costs of defense can still be crippling to small and mid-sized companies.

Some insurers will extend trademark and copyright coverage beyond the insured's website content to the insured's products. This can be a very valuable coverage extension.
Errors and Omissions or Professional Liability.
There are policies tailored to address the specific needs of entities operating in various industry classes such as technology services providers, healthcare providers, and vendors. These policies may include a professional or errors and omissions liability module in addition to the coverage sections noted above. Some E&O carriers will only write E&O coverage for certain classes of business if cyber liability is included.

First Party Cyber Coverage
A number of first party exposures arise from the risks of data breach and a cyber-attack against the insured organization. Most cyber policies include (or can be endorsed to include) some of these first party coverages alongside the liability coverage.

Fines, Penalties, Contract Obligations.
Regulatory fines and penalties should be covered, as well as contractual obligations such as charge-backs from credit card companies and the cost of replacing customers’ credit cards. Card replacement costs can run between $10 and $20 per card. In some cases, such as DSW’s 2005 breach, Consent Agreements with the FTC require that the insured obtain a security audit from a qualified, independent, third-party every two years for some period of time (20 years in DSW’s case). Will the policy cover the future cost of these biannual audits?

Crisis Management.
Although insurers include different coverages under this header and some break the coverages into multiple sections, generally Crisis Management includes data breach notification expenses, public relations expenses and costs associated with brand protection.

When a breach occurs, a timely response is vital. Certain laws dictate when and how disclosures must transpire. Multiple jurisdictions with varying laws and regulations often apply. Unreasonable delay may result in increased fines and penalties as well as damage to one’s reputation. For this reason the history and reputation of the insurer in dealing with cyber liability claims is vital. Some questions to consider are:

• May the insured use any service provider/resource, or only select providers (similar to panel counsel), or must they use a specific provider assigned by the carrier? If they are allowed to select, must the selection be pre-approved?
• What expenses are included within the breach notification expenses? Does the policy just cover attorney fees to draft various letters to comply with relevant jurisdictions or does it include the cost of printing, postage, etc? Will the policy cover the cost of staffing a call center for victims?
• Is credit monitoring included for individual victims? If so, does it cover all three major credit reporting companies, or only one? For how long will the policy cover monitoring costs? Some insurers offer a policy with a limit of liability based upon the number of records breached rather than a dollar limit. Although this is an innovative approach that seems to be catching on, and it could potentially offer a much high limit of liability, a question remains as to how this would work practically if more than the allotted number of records were compromised (e.g. would the x-number of records be figured alphabetically, or could the insured select which records to choose such as only those that selected credit monitoring?). If electing this style of coverage, one should purchase a limit large enough to coverage the largest possible breach.
• Will the policy cover more than just the minimum legal requirements for notification? For example, some state laws only require that a notification must be published. An insured may wish to notify effected individuals in a more personal manner, such as with a letter. Will the insurer cover this additional elective expense?
• When is coverage triggered? Does the policy start to respond when the insured suspects a breach or does the clock start ticking when the breach is confirmed? Some insurers will allow expenses incurred prior to a claim being filed, such as forensic costs, to erode the deductible. Additionally, one should look for the ability to notify “when appropriate” not just “when required.”
• Does a deductible apply?
• Are pre-loss or loss prevention services offered? Does the policy include any security or process analysis?
Example Crisis Management Policy Language

**A. Crisis Management Expenses** means those reasonable and necessary legal expenses, public relations expenses, and related compensatory expenses (including, but not limited to, the costs of credit monitoring services provided to affected individuals) approved by the Insurer and incurred by the Insured as a result of any actual or potential violation of any Privacy Regulations.

**Definitions:**

**Network Breach** means:
1. the alleged or actual unauthorized access to a computer system that results in:
   a. the destruction, deletion, or corruption of electronic data on a computer system;
   b. a data breach from a computer system; and
   c. denial of service attacks against Internet sites or computers; and
2. transmission of malicious code from a computer system to third party computers and systems.

**Privacy Wrongful Act** means:
1. the theft or unintentional disclosure or mishandling of personally identifiable information that is in the care, custody, or control of the Insured; or
2. the Insured's unintentional failure to timely disclose a network breach in violation of any breach notification law.
3. Solely with respect to Insuring Agreement I.C.2., privacy wrongful act also means the Insured's unintentional failure to comply with that part of a privacy policy that expressly:
   a. requires notification to a person of the Insured’s obtaining, acquisition, compilation or use of their personally identifiable information;
   b. requires the Insured to disclose personally identifiable information or correct inaccurate personally identifiable information after a proper request has been made by an authorized person;
   c. requires the Insured to prevent the loss of personally identifiable information;
   d. prohibits, prevents, restricts, or limits the improper or intrusive obtaining, acquisition, compilation or use of personally identifiable information; and
   e. allows a person to opt-in or opt-out of the Insured’s obtaining, acquisition, compilation or use of their personally identifiable information.

Business Interruption Coverage.
Roughly 55% of cost of a breach was attributable to lost business. Organizations with revenue streams tied to their websites have an exposure to business interruption should their systems fail, and coverage for this exposure can be provided by cyber policies. The policy should respond not only when interruption occurs as a result of the insured's own systems, but also because of a failure on a third party system, including large scale internet failure.

If traffic or revenues are seasonal, limits should adjust accordingly. This is particularly important for e-commerce companies that do a bulk of their business during a limited few weeks of the year. For example, a computer e-tailer that sees a spike in sales on Cyber Monday (the Monday following Thanksgiving) will need higher limits on that day than at other times during the year.

Watch out for waiting periods and time restrictions limiting the duration of coverage. Most insurers’ policy forms impose at least a 12 hour waiting period prior to coverage being triggered. Nowadays, only the most catastrophic events will keep a network down for more than a few hours. Additionally, some policies (or applications) include back-up and/or redundancy warranties that all but preclude any event that would last more than 12 hours. These clauses substantially reduce the value of this coverage.
Example Business Interruption Policy Language

A

The Company will indemnify the Named Insured all sums in excess of the deductible for
The reduction in business income the Named Insured sustains during the period of restoration of an actual interruption of the use of the computer system of the Named Insured provided the claim results from a network breach to the Named Insured's computer system.

B

D. E-BUSINESS INTERRUPTION AND EXTRA EXPENSES
The Company shall pay:
1. The loss of Business Income an Insured incurs during the Period of Recovery of Services due to the actual impairment or denial of Operations resulting directly from Fraudulent Access or Transmission, and
2. Extra Expenses an Insured incurs during the Period of Recovery of Services due to the actual or potential impairment or denial of Operations resulting directly from Fraudulent Access or Transmission, when the Fraudulent Access or Transmission causes an actual or potential impairment or denial of Operations during the Policy Period.

Business Income means:
A. net profit or loss that would have been earned or incurred before income taxes; and
B. an Insured's continuing normal operating and payroll expenses.
Business Income does not mean bank interest or investment income.

Crime Coverage.
This coverage may apply to the perils of theft, fraudulent communication, extortion and vandalism. Beware of “other insurance” clauses. This coverage often overlaps with traditional fidelity policies that cover employee theft, computer fraud and wire transfer fraud. Extortion coverage for demands of payment to prevent a criminal from taking down the insured's network or exposing PII can also be provided. Coverage for this exposure may also be found in a Kidnap, Ransom and Extortion policy. Some policies only cover first party expenses while others offer third party coverage as well.

Determining Limits
Determining the appropriate limits of liability that a company should purchase is more of an art than a science. As noted previously, historical data is limited, even well reported losses do not usually divulge internal costs. The cumulative average cost per breach is over $3,700,000, however, costs can soar into the tens of millions and even higher. Risk managers should conduct a thorough internal audit of their collected and stored data in order to determine the total value of these data as well as the aggregate cost should a breach occur. Consultation with outside data security experts may prove valuable. Lastly, a knowledgeable insurance broker can provide guidance and benchmarking as to what limits similar companies are purchasing and what is available given a company's exposure and budget.
As previously noted, the growing demand for cyber liability insurance has drawn several new insurers into the market. In June, 2012, The Betterley Report published its annual “Cyber Risk and Privacy Market Survey 2012.” The 2012 issue discussed insurance available from 31 sources - two more than the previous year. Some carriers, such as Admiral Insurance Company, do not write stand-alone cyber liability coverage, however, will include cyber coverage extensions to their E&O policies. Although the increase in capacity has continued to pushed rates downward and expand available coverage, one must pay attention not only to the coverage sections outlined above, but also to the insurer’s experience handling claims, the value added services provided, and its consistency in the market. The history of insurance is littered with insurers who enter into a new “hot” coverage only to be hit with claims and exit as suddenly as they appeared. Some of the prevalent markets are listed below.

Insurance Markets
Cyber Liability Insurance Markets Include, but are certainly not limited to:

ACE – $25 million in primary capacity
AIG - $25 million in primary capacity
Allied World Assurance Company – $5 million in primary capacity
Arch – $10 million in primary capacity
Argo Pro - $5 million in primary capacity
Axis – $10 million in primary capacity
Beazley - $25 million in primary capacity
Chubb - $25 million in primary capacity
CNA - $10 million in primary capacity
Crum & Forster - $5 million in primary capacity
Hudson - $10 million in primary capacity
Ironshore – $15 million in primary capacity
Liberty International - $10 million in primary capacity
London - various syndicates with different capacities
Navigators – $10 million in primary capacity
OneBeacon – $10 million in primary capacity
Philadelphia – $5 million in primary capacity
The Hartford - $10 million in primary capacity
Travelers – $10 million in primary capacity
XL - $10 million in primary capacity
Zurich – $5 million in primary capacity

Please note that this document was written solely as a broad overview of the then current marketplace. It should be noted that events are occurring almost daily that will cause some information provided within to be out of date post publishing.
Appendix A
Websites Providing Useful Cyber Risk and Insurance Information

http://advisen.com
http://betterley.com
http://bna.com
http://bostoncomputing.net
http://datalossdb.org
http://ftc.gov
http://idtheftcenter.org
http://www.IRMI.com
http://privacycg.com
http://privacyinternational.org
http://privacyrights.org
http://rbs2.com/privacy
http://www.eperils.com
http://www.ic3.gov
http://www.ponemon.org
http://www.privacy.ca.gov
http://www.sophos.com
http://www.symantec.com
http://www.verizonbusiness.com
https://www.javelinstrategy.com
https://www.pcisecuritystandards.org
About the Authors

Peter R. Taffae
Managing Director
ExecutivePerils, Inc.

Prior to starting ExecutivePerils, Inc., Mr. Taffae was Senior Vice President and Manager of Minet’s (AON) Financial Services Department for four years and served for 8 years as Senior Vice President and Manager of Marsh & McLennan’s FINPRO Division and Pacific South FINPRO Regional Coordinator and five years underwriting at Chubb in their Philadelphia, Wall Street and Los Angeles offices. All positions had Mr. Taffae specializing in D&O, E&O, EPLI, and Kidnap/Ransom insurance.

Mr. Taffae is on the editorial board of Employment Practices Liability Consultant (EPLiC), board member of the Digital Risk Underwriting Society (DRUMS), a member of the National Association of Corporate Directors (NACD), Professional Liability Underwriter Society (PLUS), and a chartered member of Aetna/ERMA National Advisory Committee. He has lectured on D&O, EPLI and Cyber topics for various RIMS Chapters, ACI, IIR, Mealey’s, PLUS®, the Practicing Law Institution (PLI), Tillinghast – Towers Perrin, and Insurance Educational Association (IEA). He has published over 100 articles on D&O, EPL, Fiduciary Liability, Intellectual Property and Cyber related subjects.

Mr. Taffae is a board member of the International Montessori Institute, Entrepreneurs’ Organization (EO), Stop Cancer, and Meals on Wheels West. He was a 2009 and 2012 Risk & Insurance Power Broker ® and recipient of 2011 Risk Innovator® award.

M. Damien Magnuson
Senior Vice President
ExecutivePerils, Inc.

Since joining ExecutivePerils in 2004, Mr. Magnuson has developed a national reputation for his superior product knowledge with an emphasis in Media Liability, Privacy, A&E and Intellectual Property. He is regularly quoted in trade publications about current state of affairs and market conditions. Mr. Magnuson is a frequent author of articles pertaining to recent legislative, judicial and market changes appearing in industry publications including, but not limited to, Wall Street Journal, Business Insurance, and Insurance Journal.

Graduating with honors from the University of Southern California and earning his MBA degree, Mr. Magnuson spent time in the entertainment industry and online world. After wearing many hats and learning the inner workings, he decided to enter the insurance industry.

Mr. Magnuson’s insureds range from Fortune 500, NASDAQ, foreign domicile companies, famous production companies, to startups. With clients in over 40 states, Mr. Magnuson has his fingers on the pulse of the D&O/E&O/EPL marketplace.

Mr. Magnuson is an active member in PLUS, USC Alumni Association, including the Wrestling Club, which he coached for over 11 years, and various charitable organizations. The proud father of three, Damien and his wife live in Los Angeles. His Kansas roots bring a strong work ethic and importance on integrity.
ABOUT ADVISEN FOR CYBER RISK

Advisen’s Loss Insight database (160,000 cases / $6.7 trillion in loss value) includes over 6,000 Cyber / Identity Risk case entries. Underwriters and Actuaries use Advisen’s Loss Insight Cyber data to design and test primary and excess insurance and reinsurance program underwriting and pricing plans. Brokers use this data to pinpoint actual examples of loss events for their clients. For additional information, contact support@advisen.com

Advisen’s Policy Wordings archive contains over 350 Cyber Liability and Technology E&O insurance policy forms. Each is distilled down to individual provisions and clauses, so clicking a button to see a side-by-side comparison is fast & easy. Brokers use this tool to illustrate policy differences to their clients. Carriers use this tool for product development and to help accentuate the unique attributes of their own forms. For additional information, contact support@advisen.com

Advisen also publishes several editions of our email newsletter called Front Page News. Our Cyber Liability edition is distributed at 7am Eastern time on Mondays and Thursdays. Subscribe via http://corner.advisen.com/insurance_news_home.html

ADVISEN CONTRIBUTED CONTENT

This report titled, “What Every Insurance Professional Must Know about Network Security and Privacy Liability” is a collaboration between Peter Taffae & Damien Magnuson of ExecutivePerils and Advisen. As the authors of the report, Peter Taffae & Damien Magnuson are responsible for all content.

As the publisher and distributor of this report, Advisen has created the presentation and made it available to Advisen’s audience of 150,000 commercial insurance underwriters, brokers, risk managers and other insurance professionals.

In our view, this combination effort represents an exemplary marriage of original and high-impact content together with an effective mass-distribution pathway that puts this material into the maximum of hands. We hope you agree.

If you would like to see your Contributed Content appear in Advisen’s Front Page News or be published by Advisen, send your submission in Word format to editors@advisen.com for consideration. In addition to our main Front Page News edition, we have dedicated FPN editions for Europe, Healthcare, Environmental, Property, Management Liability, and Cyber.

Jeff Cohen
EVP & Chief Marketing Officer
Advisen
jcohen@advisen.com
NOTES:
1 Executive Perils wrote one of the first cyber liability policies in 1997 and consulted on a major carrier’s cyber policy still in use.
2 Three bills currently under debate, that have the potential to drastically change the online environment are Stop Online Privacy Act (SOPA), the PROTECT IP Act (PIPA), and the Online Protection and Digital Enforcement Act (OPEN).
3 Privacy Law in the USA. by Ronald B. Standler http://www.rbs2.com/privacy.htm
5 Alabama, Kentucky, New Mexico and South Dakota currently have no legislation specifically pertaining to security breach notification.
6 For a list of state laws, please visit the National Conference of State Legislatures website at http://www.ncsl.org/Default.aspx?TabId=13489
7 There is no universal definition of PII, however, PII typically includes Social Security Numbers, bank account or credit card numbers, date and place of birth, address, driver’s license number, fingerprints, passwords and more. In CA zip codes are even considered protected PII.
8 There is no universal definition of PII, however, PII typically includes Social Security Numbers, bank account or credit card numbers, date and place of birth, address, driver’s license number, fingerprints, passwords and more. In CA zip codes are even considered protected PII.
11 Civ. No. 3:2010CV-00057 (PCD)
13 http://www.leginfo.ca.gov/pub/01-02/bill/asm/ab_0651-0700/ab_700_bill_20020929_chaptered.html
14 http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020928_chaptered.html
17 http://www.pcisecuritystandards.org/
18 http://servicealberta.ca/pipa/
19 Damien Magnuson
22 Norton Cybercrime Report 2011
23 These statistics are not without their critics. See Peter Mass and Megha Rajagopalan’s Aug. 1, 2012 ProPublica article titled, Does Cybercrime Really Cost $1 Trillion? http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion?
24 http://datalossdb.org
25 http://idtheftcenter.org
26 http://privacyrights.org
27 Verizon, 2010 Data Breach Investigations Report
29 Verizon, 2011 Data Breach Investigations Report
30 Verizon, 2011 Data Breach Investigations Report
31 Ponemon Institute, LLC, 2009 Annual Study: Cost of a Data Breach
32 Ponemon Institute, LLC, 2010 Annual Study: U.S. Cost of a Data Breach
33 Ponemon Institute, LLC, 2011 Cost of a Data Breach Study: United States
35 Royal Ppingsom. May, 2012
37 Identity Fraud Rose 13 Percent in 2011 According to New Javelin Strategy & Research Report
39 http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02
40 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
41 Ponemon Institute, Third Annual Benchmark Study on Patient Privacy and Data Security, December, 2010,
47 http://www.trustwave.com/
48 Trustwave 2013 Global Security Report
50 Understanding the Cyber Risk Insurance and Remediation Services Marketplace: A Report on the Experiences and Opinions of Middle Market CFOs, Betterley Risk Research
51 Zurich stated in an Advisen paper “[g]provisions in CGL policies may provide coverage for some types of lawsuits triggered by a data security breaches.” Data security: A growing liability threat. August 2009
52 Verizon 2010 Data Breach Investigations Report
54 Ponemon Institute, LLC, 2011 Cost of a Data Breach Study: United States