Network Security & Privacy Risk Insurance

2012 Update

Kevin P. Kalinich, J.D.
Aon Global Practice Leader: Network Risk – Cyber
kevin.kalinich@aon.com

© 2012 – Aon plc
I. Introduction

This past year was full of reminders that change – both good and bad – never stops. From the proliferation of mobile devices & applications, expansion of cloud computing, growth of “big data” and evolution of social media, to international regulations, U.S. SEC guidelines, customer contract requirements and new cyber threats; commercial entities are faced with balancing the implementation of emerging technologies and global business demands with risk management best practices. Insurance trends indicate that 2012 may end up being remembered as the year that a majority of mainstream entities considered network risk insurance as a crucial part of their comprehensive risk management strategy.

The network risk insurance marketplace is one of the most specialized in the world of commercial liability. Few privacy and security risks are alike, and many entities have unique needs, which vary greatly depending on the scope of business, number and type of personally identifiable information records at issue, use of third-party contractors, applicable regulatory rules and regulations, and the use of technology. For this reason, it is critical to continue to stay educated regarding dynamic developments in the world of privacy and security exposures and solutions. The key is to balance each company’s unique network risk exposures and risk tolerance with cost effective risk management. This White Paper provides a road map to coordinate an entity’s network risk management strategy with the world’s emerging cyber trends.

Early 2012 also saw Aon lose a treasured colleague to cancer. Shelva Holmes died on January 25, 2012. Shelva, who worked with our group for seven years, had a saying when tackling difficult problems. She would just smile and say, “It’s a beautiful thing.” Shelva seemed to have achieved an internal equilibrium as she balanced work demands, our clients’ needs, and later her illness, all with a positive outlook. So, with a hat tip to Shelva, we turn to this annual update and encourage you to stay positive, no matter how daunting the evolving challenges of cyber-related risk, and seek a state of equilibrium. “It’s a beautiful thing.”

A. The Concept of Equilibrium

Equilibrium is defined as the condition in which competing considerations are balanced, such that some level of stability is obtained. The term is used in a variety of contexts, such as economics, where equilibrium refers to the balance in economic (supply and demand) forces. It is used in mathematics, specifically game theory, where a concept known as the “Nash equilibrium” describes the state of a game in which the players make the best decisions they can, taking into account the other players’ strategies. Nash, who is still living, now 83 years old, has been in the news again in 2012. The National Security Agency recently declassified a series of unsolicited letters Nash wrote to the NSA in 1955 in which he proposed a new encryption-decryption machine. In January 2012, NSA made these letters available online. Nash’s letters, which the NSA apparently disregarded at the time, reveal that Nash anticipated many of the concepts used in modern-day computational complexity theory and cryptography, and we now know that he proposed these to the NSA a decade or two before the rest of the world caught on. He distinguished polynomial time (“feasible” or “efficient” complexity) from exponential time (“computational
hardness” complexity), and theorized that a system’s encryption could be based on problems that could not be solved faster than in exponential time. 

While scientists and theorists continue to struggle with the larger question of whether it is even mathematically possible to create truly secure cryptosystems, industries that use this technology have had to face the challenge of trying to ensure both the privacy and authenticity of transmitted information in a world of constantly-changing technology, increasingly more sophisticated third-party eavesdroppers, and a shifting legal landscape. Finding the optimal balance among competing business considerations, including the need for privacy and security, remains a constant challenge.

B. Achieving Equilibrium in the Context of Network Risk Management

To reach equilibrium – that state of stability in which competing considerations are balanced – requires decision makers to disregard the hype surrounding network security risks and engage in a deliberative process. This requires a constant analysis and reevaluation of external and internal factors such as evolving technology, dynamic exposures, and legal developments. Each entity must thoroughly analyze its internal and external risk management measures, including insurance coverage – both its existing policies and the potential purchase of cyber-insurance to address coverage gaps and new exposures.

II. 2012 Technology Developments and Trends

2012 has brought forth important developments in a number of areas. As an initial matter, the sheer volume of data transmitted electronically continues to grow exponentially. It is estimated that one-third of all households worldwide now have Internet access. Much of this increased usage is occurring in the developing world, which now comprises 62% of the world’s total number of Internet users.

At the same time, the use of mobile devices continues to increase. In 2011, there were 5.9 billion mobile cellular subscriptions worldwide, and for the first time ever, more smartphones were sold than PCs. As a consequence, the availability of mobile applications has also increased dramatically. For instance, Apple and Google alone have over a million mobile applications for sale, and these have been downloaded an estimated 35 billion times. According to the International Telecommunications Union (ITU), there were almost 1.2 billion mobile Web users in the world. An important trend is for mobile application providers to be held to the same standards as Internet companies in terms of privacy issues such as consumer notice, tracking, and targeted marketing.

The increase in the number of users and amount of data being transmitted has only heightened the attention from hackers and cybercriminals. The environment is riskier than ever before. Public concern over privacy matters is on the upswing, and privacy advocates are gaining strength.

As a result of these changes, governments worldwide are increasing the regulatory pressure upon businesses. Privacy rights continue to be formalized into laws, enforceable through agency action and private litigation.
A. Increasing Threats to Security of Corporate Data

The emergence of new technologies and dramatic changes to existing technologies necessarily alters the types and severity of threats to security. In particular, companies’ control over their information technology is weakened due to increased reliance on cloud computing and mobile device technology. Businesses’ reliance on “big data” applications creates additional exposure. Whether these threats are in the form of cybercrime, privacy breaches, theft of intellectual property, or business interruption, they imperil the competitiveness of a business.

In 2011 and early 2012, we saw a number of security breaches making the news. What was most surprising about these reports were that the targets appeared to be very sophisticated entities, yet the attackers were nonetheless able to penetrate their systems. Cybercriminals are increasingly sophisticated in terms of high-value target selection, meticulous planning, and data collection capabilities. Each breach we have seen this past year confirms the need for companies to find the balance – the equilibrium – among competing considerations.

What is not clear is whether cyberattacks are happening more frequently, or whether they are simply being reported at a higher rate due to statutorily mandated disclosure obligations. In any event, businesses should stay abreast of technological changes and their associated risks.

1. Mobile Devices and Applications

The dramatic increase in use of mobile devices by company employees presents new security threats to corporate networks. Data breaches caused by smartphones are becoming more common than lost or stolen laptops. Though companies have learned to protect their employees’ laptops through the use of full-disk encryption, mobile devices are softer targets because they are smaller, making them more vulnerable to loss or theft. And because they are generally turned “on,” they are constantly vulnerable. Mobile devices are also far less likely to be subject to tight, centralized IT control. A decade ago, firms routinely banned the use of devices that had not been company-issued, but today employees often purchase their own devices (a phenomenon referred to as the “consumerization of IT”).

Many of the risks associated with the use of mobile devices are the same types of risks that threaten desktops or laptop computers, such as spyware, Trojans, and insecure applications. For instance, a user unknowingly installs an application that carries hidden spyware that monitors activity and intercepts data from the device or even from the cloud applications used by the device. However, mobile devices carry even greater exposure because, since they are designed for communication, malicious applications can easily penetrate the mobile device’s many communication vectors (e.g., telephone dialing, SMS text messaging, Bluetooth) to send data to eavesdropping cyber-criminals.

Moreover, mobile device users are constantly being tempted with countless new applications, which have only been superficially tested for malware. Furthermore, only a tiny fraction of smartphones are shipped with pre-installed security software. Think about these issues in the context of our transformation to mobile payments from our smartphones in lieu of credit/debit cards.

Recent concerns over the Carrier IQ smartphone application illustrate the problem. Carrier IQ, which cell carriers choose to have configured into their phones, has been criticized as being a “rootkit” or keylogger...
that spies on users by recording SMS messages, passwords, or other information. Others who have examined Carrier IQ deny that it is capable of such actions, but it is clear that this application can collect pieces of raw data from users and send them back to the carrier for analysis. It is possible that Carrier IQ’s software, as initially designed, simply performs the legitimate diagnosis and repair tasks its vendor claims, but then modifications to the code by the phone manufacturers leads to the transmission of private information.\textsuperscript{12} It is clear that mobile devices carry new and different risks.
2. Cloud Computing

Companies are more frequently outsourcing their computer services (platform, infrastructure, software) to third-party service providers – cloud computing – as a cost-effective approach for centralized computing and to meet growing data storage demands. The users are generally geographically separated (sometimes in different legal jurisdictions) from the cloud providers, so the services are accessed via the Internet.

Centralization of information technology carries increased risk, and the loss of control over sensitive data raises security concerns, particularly in the context of cloud systems housing data from multiple unrelated users. The initial sharing of private data between the customer and the cloud host companies is seen as creating potential exposure, since the cloud provider may freely access the private data. Each company must thoughtfully assess its own unique risk in terms of privacy, data security, and pertinent legal issues. Companies should obtain detailed information from cloud providers concerning their security programs, including who can access the data, where it will be located (country of jurisdiction for evaluation of legal obligations), technical aspects of the infrastructure, and what steps the provider has taken to protect the integrity and security of the data. Both contractual protections and cyberliability insurance should be utilized to mitigate financial risks associated with security breaches.

Some suggest that the centralization of data that is the essence of cloud computing will allow security resources to be more focused, thus enhancing security. While this may be true, a comprehensive and thoughtful analysis is required to determine whether cloud computing is a safe and cost-effective option for a company. Companies should evaluate a range of information, including how the cloud provider erects security walls between data from different customers, who will have access to the information, whether customers must be notified that their information will be stored in a cloud, whether the cloud provider has its own adequate insurance coverage, and whether some information is simply too sensitive to turn over to a third party.

3. Big Data

Companies using datasets that exceed the capabilities of traditional database tools (“big data”) must find ways to address the unique compliance and security concerns that accompany these enormous accumulations of mostly unstructured data. The “big data” industry is expected to grow considerably as more companies analyze large stores of information to plan and make predictions.

Again, because big data applications are generally housed outside a company’s information technology department, the lack of control may lead to the loss of security.

4. Social Media

The continued popularity of social networking brings a host of security issues. Facebook, Twitter, Yelp, YouTube, and other such sites are increasing in popularity. Notwithstanding the potential value of social media for companies seeking to amass followers, to recruit employees, to communicate with customers or to compile data for marketing purposes, social networking sites are a source of significant exposure.
Not only does employee use of social media lead to potential human relations problems (e.g., harassment claims, National Labor Relations Board), the most obvious legal concerns are potential liability for disclosure of private information, consumer fraud, false advertising, defamation, trade libel, copyright infringement, and the like. Social media communications are held to the same standard as any other corporate publication, such as formal marketing materials, but the use of social media tends to be much more “freewheeling and informal.” A recent report by the Altimeter Group reveals that companies are not managing their corporate use of social media as well as they should. Businesses tend to take on too many accounts to manage properly and the employees responsible often lack adequate education or oversight.

It is also unclear whether the business or an individual employee “owns” the contacts made through social media. Two recent cases addressed this issue. In July 2011, PhoneDog.com sued a former employee, claiming that 17,000 Twitter followers constituted a company-owned customer list. In December 2011, a company and its former employee sued each other over ownership of the former employee’s LinkedIn account. Issues such as these can be avoided if companies adopt appropriate social media policies addressing ownership rights.

The U.S. Federal Trade Commission is monitoring companies who mislead consumers by having their agents pretend to be independent consumers and say favorable things about products and services, without disclosing this affiliation. Posting fake reviews and creating “flogs” (fake blogs) are actions that may subject a business to an FTC investigation, consumer fraud actions by state attorneys general, or even class action consumer lawsuits.

Companies that are too aggressive in monitoring their employees’ use of social media risk liability for invasion of privacy and other torts. Discrimination cases may result if employers use social media to learn of applicants’ and employees’ status in protected classes (e.g., religion, disability, pregnancy, etc.) and then are accused of improperly using that information against them in making employment decisions. Moreover, federal labor laws protect employees’ speech about working conditions, so adverse actions based on employees’ expression of criticism online could result in liability.

Lawsuits continue to increase. Cyberliability insurance is a valuable tool to protect against the risks associated with social media.

B. Adequacy of the Response to Growing Threats

The CEO of Heartland Payment Systems – a victim of one of the largest security breaches in history – cautioned businesses in the spring of 2012 that “…anyone that thinks they’re not going to be breached is being naive.” Despite this warning, and although the risks seem to be at their highest point in history, some businesses may be neglecting to undertake the crucial analysis required to protect themselves against breaches or to mitigate their financial losses.

The February 23, 2012, preliminary report from Carnegie Mellon University’s CyLab evaluated results from a 2011 survey and compared them to earlier results in 2008 and 2010, and identified ongoing gaps in corporate governance. Despite new Securities and Exchange Commission guidelines requiring public companies to disclose material cyber risks, these survey results show that corporate leaders still neglect oversight responsibilities, fail to set necessary policies, and deny adequate budgets for protecting companies from security breaches or for damage mitigation. While “corporate data is at a higher risk of
theft or misuse than ever before” a survey of the Forbes Global 2000 list of key leaders (CEOs, CFOs, CROs, and board members) indicates that senior management and corporate boards are still not devoting sufficient attention or budgets to security and privacy issues. CyLab specifically recommended that each company “[e]valuate the adequacy of cyber insurance coverage against the organization’s risk profile.”

One recent survey indicated that only 1 out of 4 companies are buying cyberinsurance.19 Specifically, 72% of the 153 risk managers surveyed indicated that they had not purchased specific coverage for privacy and data breaches.20 Aon’s experience has been that companies are, in fact, increasingly heeding the warnings and taking appropriate cautionary measures. Aon Risk Solutions estimates that, prior to 2008, it sold 1.5 policies for every 10 prospects interested in insurance covering cyberattacks. By 2012, the data reflects that 4.5 privacy and security policies are sold for every 10 prospects.21 The rate of purchase trend increase is much higher (over 75% in some cases) for certain industries such as hospitality, entertainment, retail, technology, healthcare, and financial institutions.

C. The Cost of Security Breaches

Security breaches cause companies to suffer embarrassment, public relations problems, loss of business, exposure to litigation, government investigations, and other substantial harm. Losses range from difficult-to-insure damages, such as lost future business and reputation, to insurable damages, such as customer class action litigation, notification costs, and credit card issuer cancellation and reissuance costs. And the breaches are common. In fact, 79 to 83 percent of entities acknowledge having experienced a breach, and the true number is believed to be even higher, since companies are known to “pick and choose” whether to report breaches. New security challenges, such as the spread of cloud computing and increased use of mobile devices, create exposures with no historical benchmarking. Class action lawsuits relating to security breaches continue to increase, with severe financial consequences for companies in nearly every industry.

While security breaches are very costly to an organization, companies may be learning to handle them better than in previous years. Ponemon Institute’s study, “US Cost of a Data Breach in 2011,” released in March 2012, showed a slight decline in the average cost of a data breach, partly due to organizations’ increasing sophistication about preventing and responding to breaches.22 The average cost of a breach decreased from $214 per compromised record in 2010 to $194 per record for 2011. On an organization basis, the average cost of a breach declined from $7.2 million in 2010 to $5.5 million in 2011. The report examined 49 data breach cases from 14 different industries and evaluated both direct and indirect costs. Negligent insiders account for the largest proportion of breaches and criminal attacks are the most costly. Security breaches also involve costs that are difficult to quantify, such as the lost business based on customers’ perception of a lack of security. Edelman’s consumer research indicates that consumers are more worried now about the security of their personal information than in the past and, as a result, these customers avoid purchases due to these security concerns and abandon even trusted merchants if they experience a breach.23
Source: http://www.ponemon.org/data-security

Average Organizational Cost per Data Breach Event
Average Cost per Compromised Record
Aon’s own benchmarking indicates that approximately 80 percent of reported breaches result in total defense and indemnity costs of less than $1 million, approximately 15 percent of breaches result in insurable damages between $1 million and $20 million, and approximately 5 percent result in total costs above $20 million.

In 2011-2012, we have seen a number of security breaches make the news, as hackers continue to break into retailers (Amazon$^{24}$, Zappos$^{25}$), marketing firms (Epsilon Interactive$^{26}$), online gaming (Sony$^{27}$), health care providers (Massachusetts General Hospital$^{28}$, Sutter Health$^{29}$), health insurers (BlueCross BlueShield of Tennessee), banks (Citigroup$^{30}$, Ocean Bank$^{31}$, Bank of America$^{32}$), law firms$^{33}$, government departments (Pentagon, Canadian government, California Department of Child Support Services, Utah Department of Health), defense contractors (Lockheed Martin$^{34}$), social networking sites (RockYou$^{35}$), cloud providers (Google’s Gmail$^{36}$), online brokers (T.D. Ameritrade$^{37}$), credit card processors (Global Payments) and even sophisticated security firms (EMC’s RSA$^{38}$, Stratfor$^{39}$, Symantec). Associated costs, including breach response and exposure to class action lawsuits, can be astronomical. Cybercriminals are increasingly sophisticated in terms of high-value target selection, meticulous planning, and data collection capabilities.

Credit card processors remain a prime target. Sometime in late January or February 2012, a security breach occurred at Global Payments, the seventh-largest “merchant acquirer” in the US.$^{40}$ A blogger first broke the story of the breach on March 30, and subsequently, Global Payments publicly acknowledged the occurrence. Initially, it was reported that 50,000 accounts had been exposed, but that number was subsequently increased to 10 million cards, and then changed again to 1.5 million Visa and Mastercard account numbers. According to Global Payments, no fraudulent charges have been made on the stolen credit card numbers. However, the event clearly jeopardized the company’s relationships and compliance records with credit card companies. Global Payments serviced $120.6 billion in payments for Visa and Mastercard in 2011, but as a result of the breach, Visa removed Global from its list of approved service providers (PCI-Compliant List) and Mastercard is currently evaluating the situation. In addition, on the day the breach was first reported, Global Payments’ stock dropped 9%, until trading was halted midday.

BlueCross BlueShield of Tennessee has agreed to pay $1.5 million to resolve potential HIPAA claims resulting from the theft of 57 unencrypted computer hard drives from one of its facilities. The stolen drives contained personal health information for over a million BCBS members. On March 13, 2012, the US Department of Health and Human Services announced the settlement between BCBS and the Office for Civil Rights.$^{41}$ This was in addition to the $17 million in breach response costs incurred by BCBS.

In California, where a unique state law provides for damages of $1,000 per person per violation of the Confidentiality of Medical Information Act of 1981, plaintiff law firms are lining up to file privacy data breach class-action lawsuits against hospitals, medical service providers and health insurers that, if successful, could easily yield payouts in the multiple millions.

The biggest cost so far is the liability to banks that must cancel and reissue credit and debit cards. Javelin Strategy and Research estimates credit and debit card issuers spent $252.7 million last year replacing more than 70 million cards compromised by data breaches. Although some early cases did not hold the breached entity liable because there was no privity of contract with the issuing banks, more recent cases have found liability. Some state statutes (Minnesota, Nevada, and Washington) specifically impose such liability. The fallout from the recent Sony, Epsilon, and Citigroup breaches could exceed the Heartland
Payment System’s reported $145 million credit card breach and TJX Company’s record breach of $256 million in liability.

The largest uncertainty is not whether a breached entity is liable to its patients, customers, employees, and third parties – but whether and to what extent the victims can prove damages. Some companies have been more adept at responding to breaches, thus minimizing their losses. A recent example of “risk management best practices” involved Motorola’s response after learning that it had inadvertently sold uncleanse d, refurbished Xoom tablets through Woot.com. Motorola estimated that approximately 100 of the 6,200 tablets sold between October and December 2011 had not been put through the company’s factory reset and data wipe procedure, resulting in the possibility that these 100 tablets may have contained a prior customer’s data. Motorola received positive response to its remediation efforts, which included prompt and thorough notification, efficient return and repair, and the award of a $100 gift card to affected customers.

III. Insurance Coverage Trends

A. Recent Insurance Coverage Cases of Note

A number of cases were decided in the past year, providing companies with guidance as they consider insurance coverage options. It is becoming clear, for instance, that companies should not rely on their base (no customized enhancements) Commercial General Liability (CGL) policies to provide complete coverage for the many costs associated with privacy and security breaches. Rather, companies should review their CGL and other existing policies to determine the exact nature of their coverage for network-related risks and consider more specialized forms of insurance to guard against such exposures. In the past, some courts held insurers liable under the “personal injury” provisions of CGL policies. But even where coverage has been held to exist, it is limited, and typically does not cover the breached entity’s own expenses, such as investigation expenses, notification costs, credit monitoring costs, or increased public relations costs, which are often the greatest expenses incurred after a breach.

Recent cases illustrate the need for careful attention to insurance policies, as businesses battle with their insurers over coverage for network-related losses. Following hackers’ attack on Sony’s PlayStation Network (77 million records exposed) in April 2011, Sony has been engaged in litigation with its insurer, Zurich American Insurance Company, over whether its primary and excess commercial general liability (CGL) policy covered such a breach, requiring Zurich to defend or indemnify Sony.42 The remediation actions alone for the Sony breach are estimated to cost at least $171 million, and this legal battle illustrates why companies should consider separate privacy and security insurance to address these types of exposures. To be clear, the Zurich policies at issue were not “cyberliability” policies, but rather only CGL policies, which are generally not intended to cover security breaches.43 Similar declaratory judgment general liability insurance litigation denials have been filed against Michaels Stores (by Arch Insurance), Crate and Barrel (by Hartford), The Children’s Place (by Hartford), and seeking enforcement of coverage by University of Utah/Perpetual Storage (against Colorado Casualty).

For example, in the Arch Ins. Co. v. Michaels Stores, Inc.44 coverage litigation, filed in February 2012, Arch alleges that the comprehensive general liability policy excludes electronic data from the definition of tangible property, for purposes of determining whether “property damage” has been alleged. Furthermore, the policy excludes damages arising out of the loss of, loss of use of, damages to,
corruption of, inability to access, or inability to manipulate electronic data. In that case, Michaels Stores allegedly failed to safeguard PIN pad terminals, which allowed criminals to fraudulently access and use customers’ credit card and debit card information.

Retailers Crate & Barrel and The Children’s Place were sued by their insurer, The Hartford, seeking declaratory judgments that the insurer has no duty to defend the stores against statutory claims resulting from store associates asking customers for their ZIP codes. Hartford asserts that its CGL policies with these two retailers excluded them from defending any action “arising out of the violation of a person’s right of privacy created by any state or federal act.” These cases, once again, clarify why CGL coverage is inadequate to insure against customer privacy suits.

Another case illustrates the risks businesses assume when they rely on third-party service providers to have adequate insurance coverage for security and privacy breaches. In 2010, Perpetual Storage’s General Liability insurer, Colorado Casualty, denied coverage when this third-party service provider lost confidential data on 1.7 million University of Utah hospital patients. Perpetual Storage was transporting the backup tapes containing sensitive personal and medical data on patients at the University of Utah when the tapes were stolen from a Perpetual employee’s car in 2008. The university incurred $3.3 million in remediation (notification, credit monitoring, call center, etc.) costs related to the breach. Colorado Casualty had sold Perpetual Storage a commercial package policy and commercial liability umbrella policy, which it claims does not cover the losses related to the stolen tapes. Those policies appear to define “property damage” as relating only to “tangible property,” from which electronic data (including tapes) is excluded. Colorado Casualty argued that the university, by selecting the lowest-rate storage option, expressly agreed to limit Perpetual Storage’s liability for loss or damage to $20 per tape, and therefore cannot recover damages for a greater amount. Colorado Casualty also argued that the university lacked standing to assert claims directly against the insurer because it was not a party to the insurance policies, was not in privity, was not named as an “additional insured” in the policies, and was not named as an intended beneficiary of the policies. The judge is allowing the university some additional discovery, but has already expressed skepticism that the university may assert claims directly against the insurer. Note that there are accusations of insurance broker negligence for not recommending the purchase of a privacy and security insurance policy.

The standard CGL policy is insufficient to cover the range of network-related risks or damages from breaches. CGL policies often exclude damages arising from criminal actions committed by the insured or even third parties, such as hackers or cybercriminals. Furthermore, the “property damage” coverage in the CGL policies may not cover lost computer data. Earlier legal precedents cut both ways, and as a result, most insurers now use specific language to exclude data loss under “property damage” coverage. In fact, most CGL policies now exclude lost computer data or software from “property damage” claims. Precise drafting is required to ensure that a company’s unique needs are addressed. These more recent cases continue to illustrate the need for specific privacy and security policies. Another provision of standard CGL policies that may offer some coverage is the “personal and advertising injury” provisions, but even that coverage is subject to dispute. Such injuries are typically defined as arising out of specific offenses, which requires “oral or written publication, in any manner, of material that violates a person’s right of privacy.” However, a data breach may not be considered a “publication” of private material, and insurers might argue that unless a communication is intentional and widespread, it is not a “publication” so no coverage exists. The cases are split on this issue. Moreover, whether a data breach constitutes a privacy violation for purposes of a CGL policy may depend on the type of information disclosed.
B. Increased Regulatory and Legal Obligations

1. Sources of Privacy Obligations

A business’s obligation to maintain the privacy of its data arises from a variety of sources. Laws in 46 U.S. states and in foreign countries throughout the world require companies to disclose incidents of lost or stolen information of various types. Businesses may also promulgate policies or enter into contracts which contain privacy obligations, and some industries have adopted standards.

2. United States Legal Developments

Each year brings new laws and regulations that increase companies’ network security obligations and this past year was no exception. In fact, there have been some milestone events, including the Securities & Exchange Commission’s (SEC) new disclosure guidelines for public companies in their SEC filings. On October 13, 2011, the SEC issued guidelines that recommend public companies disclose cyber risks that “materially affect products, relationships, services, relationships with customers or suppliers...” Under these new SEC guidelines, directors and officers now have a specific fiduciary directive to exercise an acceptable level of corporate governance over their systems’ security. They should disclose security breaches, denial of service attacks, or any other cyber security event or risk that could have material adverse effects. Importantly, the SEC guidelines specifically include appropriate network risk insurance as an item to be addressed and disclosed, raising network risk insurance to a board of directors issue.

While not mandatory, the guidance is helpful for public companies with SEC filings and is a useful overview for private companies interested in properly addressing their network risk exposures.

The Obama Administration’s issuance of an aggressive report proposing comprehensive privacy legislation may change the legal landscape in the near future as well. Most notably, the report favors a single, unified federal standard that would minimize compliance costs by preempting the burdensome patchwork of state data breach laws and provide “greater certainty for companies.”

At the state level, we continue to see a patchwork of different laws. Many govern privacy, but vary widely in their definition of what constitutes protectable personally identifying information. Some laws are directed at technical aspects of encryption and disposal of data. Other laws specify measures required in the event of a security breach. Because the laws vary so widely, they provide no comprehensive guidance for businesses. In addition, the laws change frequently, as privacy concerns are elevated, technology advances, and cybercrime increases.

A few of the more significant recent state developments:

On February 22, 2012, the California Attorney General announced that all mobile applications are required to post sufficiently clear and conspicuous privacy announcements that comply with California’s Online Privacy Protection Act (“OPPA”). The Attorney General unveiled its recent agreement with a group of mobile application providers (Amazon, Apple, Google, Hewlett Packard, Microsoft, and Research in Motion/Blackberry) in which they agree to a set of privacy principles, and published a “Mobile Applications and Mobile Privacy Fact Sheet” detailing the clarified expectations. The Attorney General
emphasized that violations of the OPPA would be pursued under California’s Unfair Competition Law, which seems likely to provoke class action litigation on the issue.

Businesses which access or maintain the personal information of Massachusetts residents must comply with state security regulation as of March 1, 2012. This regulation requires businesses to adopt and follow a Written Information Security Plan (WISP) to protect the privacy of personal information about employees, customers, prospects, business contacts, and other third parties. Companies were required to promulgate WISPs by March 1, 2010, and to ensure their service providers had adopted WISPs by March 1, 2012.

3. International

Since 1995, data privacy issues in Europe have been governed by the Data Protection Directive 95/46/EC. The Directive is outdated and inconsistent in scope, interpretation, and enforcement from one member state to another (27 different laws), making compliance difficult and costly.

On January 25, 2012, the European Commission proposed a new EU-wide Data Protection Regulation to reform European privacy law. Among the most noteworthy aspects of the proposal is its extra-territorial application to businesses outside the European Union if they offer goods or services to individuals in the EU or monitor their behavior. Non-EU companies would be required to appoint a representative based in the EU to facilitate enforcement. Following US criticism, the European Commission proposed to exempt small- and medium-sized companies and companies with only occasional European customers, but the regulation’s terms would still apply to many companies. While the proposed EU regulation may provide uniformity and predictability, international businesses are concerned that it creates substantial new rights for employees, consumers, and users throughout the EU countries, and are critical of the proposed law’s onerous breach notification provisions (within 24 hours “where feasible”) and high fines (up to 2% of a company’s global turnover).

While the proposed regulation is still in draft form, and it is unclear how long the process might take, it is clear that the EU intends to more tightly regulate this area to address privacy concerns. Some legal experts are concerned that the EU laws will conflict with US laws, making it difficult for companies doing business globally to comply with laws in both jurisdictions.

On February 12, 2012, the EU’s largest mobile provider industry group, the GSM Association, announced a set of global Privacy Design Guidelines for Mobile Application Development. The comprehensive privacy guidance requires mobile applications to include adequate privacy policies and offer mobile users control over the use of their personal information.

Canada has also been grappling with these issues. In December 2011, Canada’s Office of the Privacy Commission (OPC) issued its guidance on online behavioral advertising (OBA) and tracking, taking the position that OBA “generally” constitutes personal information. It condemned the collection of data from children and recommended that if declining cookies made a service unusable, the technology should not be used.
III. Roadmap for Achieving Equilibrium

The process for achieving the right balance requires evaluating and quantifying (where possible) these competing considerations and making a series of mutual adjustments until the optimal balance – equilibrium – is reached. However, equilibrium is not static. As a business’ circumstances change and as external conditions (technology, legal considerations) evolve, the point of balance will shift, so this deliberative process must be an ongoing, almost constant, practice.

Among the competing considerations which risk management professionals must balance cost versus benefit of each risk mitigation strategy. For example, requiring every employee to change her password on a weekly basis would greatly diminish production beyond the value of increased security. Risk managers must involve relevant managers from throughout the organization at each step of the decision making process to ensure buy-in from each business unit. Working together, a cross-functional Network Risk Management team can more accurately and comprehensively quantify risks, evaluate options and develop a cost-benefit analysis to determine if cyber insurance is a prudent investment.

A. Evaluate privacy and security risks and other network exposures in the context of Enterprise Risk Management;

B. Create a Corporate-wide Network Risk Management Committee, which should include leaders from Risk Management, Information Technology Security, Privacy, Compliance, Chief Information Officer, Legal, Human Resources, Procurement, Sales, Research and Development and Public Relations to address the following:

1. Has the entity taken inventory and thoroughly qualified and quantified its information assets, including classification of confidential information?

2. Does the entity understand and comply with the constantly evolving applicable state, local, and industry association statutory and contractual compliance regulations, including international legal requirements, if applicable?

3. Has the entity implemented risk management best practices with respect to the protection of information assets, including, but not limited to the following?
   a. Information Technology Security (insurance underwriters desire to measure IT security assessments against standards, such as ISO/IEC 27000 series, SAS 70, Type II, etc. – including same requirements for outsourced operations of third party IT vendors). Note that this process in and of itself is a benefit to the insured even if network risk insurance is not purchased. A third-party certification can often lower the premium and allow for more robust coverage.
   b. Limit access to confidential information, including control of software, hardware, and system access.
c. Develop data protection and privacy policies and procedures for all employees, partners, customers, suppliers and independent contractors.

d. Appropriate training, awareness and monitoring, which must be updated regularly.

e. Third-party vendor network risk management, including appropriate contractual allocation of liability.

f. Implementation of data breach response plan. Insurers now realize that every entity will suffer some type of breach and the underwriters are increasingly conducting due diligence regarding breach response plans to determine the scope of insurability and pricing costs.

g. Integration of insurance claims process with internal breach response. Entities must understand how and when to involve their carrier if a data breach occurs. This may include updating documented procedures, such as the data breach incident response plan with new roles and responsibilities, revised timeline, and current contact information.

C. Assist Management with Global Privacy Risks (see pyramid below)
Achieving and maintaining equilibrium will require constant analysis of risks and frequent reevaluation of protective measures. No entity is safe, as risks evolve and increase, and preventative security measures are obviously an essential component of a balanced program. Just as essential, however, is a comprehensive analysis of existing coverage by risk management professionals who can ignore the hype surrounding these issues and who are thoroughly knowledgeable about evolving technology, each entity’s unique exposures, applicable legal considerations, and available coverage options.

A. Analyzing Existing Policies for Gaps in Coverage

A number of different insurance products may be responsive to part of the losses resulting from privacy or security breaches, including Crime, General Liability, Professional Liability, Employment Practices Liability (e.g., for social media exposures), Kidnap and Ransom (e.g., cyber extortion), Internet Media Liability (libel, plagiarism, defamation, or invasion of privacy), and Property Business Interruption and Data Loss policies (e.g., losses for company’s “downtime”). Each of these various types of existing coverage should be thoroughly examined to ascertain the potential coverage for network risks.

By way of example, professional service companies (e.g., law firms, accounting firms, architectural firms, engineering firms, consultants, financial institutions, payment processors, brokers and agents, and health care providers) typically have some type of professional liability (aka “Errors & Omissions”) insurance coverage. A broad-based professional liability policy is intended to cover defense costs and indemnity liability for economic/financial loss of third parties due to the alleged errors, omissions or negligent acts of the insured in the provision of its services or products. Do professional liability insurance policies extend to address first- and third-party network risk exposures? Does the firm’s property policy address business interruption due to inaccessibility of systems because of an “intangible property peril,” such as a computer hack where there has been no tangible property damage? The answer to these questions is far from clear.

We recommend that companies ask the following questions to determine the protection provided by existing policies and to identify gaps in coverage that may need to be addressed through network risk insurance:

a. Does the policy specifically describe “intangible information assets?”

b. Does the policy address wrongful dissemination of data?

c. Does the policy address wrongful collection of data?

d. Does the policy address dissemination of a computer virus, worm, or Trojan horse?

e. Does the policy cover claims against the entity that are due to a third-party IT or security vendor?
f. Does the policy cover advertising injury and personal injury claims that could arise from social media usage, such as defamation, libel, invasion of privacy, copyright, trademark, and service mark infringement?

g. Does the professional liability policy cover employee claims (as opposed to client claims) regarding breach of personally identifiable information?

h. Do the existing property or professional liability policies cover first-party costs, such as forensic and investigation expenses, data breach notification disclosure costs, credit monitoring, business interruption (due to the entity’s systems), contingent business interruption (due to a third-party vendor) or the lost value of business assets?

i. Common exclusions that may (or may not, depending upon the insurer) be addressed via customized enhancement include:

   i. Unencrypted laptops and devices
   ii. Loss if regular software patch updates are not downloaded
   iii. Loss if employee passwords are not changed periodically
   iv. Devalued intellectual property
   v. Security upgrades after a system attack
   vi. Restoration of damaged reputation
   vii. Cost of written information security program required by an enforcing regulatory body
   viii. Cost of periodic audits required by an enforcing regulatory body
   ix. Network downtime

B. Developments in the Network Risk Insurance Market

Changes continue to occur in the insurance markets. Coverage is becoming more differentiated, as insurance companies accumulate actuarial data enabling them to establish different pricing for different industries and based upon their insured customers’ level of security vigilance. For example, insurers will add exclusions to policy coverage for risky practices, such as the use of unencrypted laptops. Businesses which are common targets for cyber attacks, such as social networking sites, pornography sites, and online gaming sites, will be charged more for coverage based on actuarial data.

In 2001, in the wake of *American Guaranty & Liability Insurance Co. v. Ingram Micro, Inc.*, No. 99-185 TUC ACM, 2000 U.S. Dist. LEXIS 7299 (April 18, 2000), many insurance companies revised their standard CGL and Property insuring agreements to state specifically that electronic data is not considered tangible property. Since that time, additional court decisions and CGL policy revisions have made it even more apparent that specific network risk insurance should be explored to obtain adequate protection.

The following are some important threat protections to consider when looking for a cyber insurance policy or adding onto an existing policy:
Privacy and Security Liability: Any business that keeps sensitive data on employees, customers, patients, students, partners, or other third parties can be liable for damages if that information is breached, regardless of the reason. If a breach happens and a third party sues, privacy and security liability insurance is intended to cover the business for defense and indemnity costs. Privacy Regulatory Proceeding Coverage is generally provided as a sub-limited part of the coverage and covers costs resulting from a governmental, civil, administrative, or regulatory proceeding that alleges the violation of a privacy law.

Data Breach Crisis Management: In the event of a data breach, a business needs to immediately hire a forensic team to find out what happened, plug the hole, and comply with federal, state and international notification requirements. Sub-limited coverage is available to address extortion threats for intentional computer attacks against the insured.

Business Interruption or Data Loss: If a hacker breaks into a company’s computer network and launches a virus or denial of service attack, data and software may be damaged and the system may need to be shut down to make repairs. Coverage may be customized to address online events that destroy intangible property such as data or software applications.

Internet Media Liability: As more companies rely on their websites and social media to advertise to consumers or other businesses, they may want coverage to protect against possible libel, plagiarism, defamation and false light, invasion of privacy, and copyright or trademark infringement of content posted on their site.

Specific Policy Enhancements: Since the policy forms vary so dramatically, the insured should verify that the following are covered, among other coverage grants: third-party contractor breaches; offline or non-technical breaches, including hard copy paper breaches; breaches from mobile devices, including flash drives, laptops, tablets, and smartphones; choice of vendors to respond to a breach, including legal counsel, breach notification response, forensics, investigations, credit monitoring and call centers. Pre-approved vendors can save a lot of time and money post breach.

Policy forms are claims-made and reported, and coverage is available on a worldwide basis. Most insureds purchase $5 million to $20 million in limits, although some larger companies buy $100 million to $200+ million in limits.

Premium rates vary dramatically with a competitive environment and plenty of carrier capacity ($300+ million). For small insureds, premiums range from $5,000 to $25,000 per $1 million, with retentions of $10,000 to $100,000. For large insureds, retentions start at $500,000 to well over $1 million, and the price could be $10,000 to $50,000 per $1 million. The number of markets that can be accessed for excess layers has increased to 27, and the abundant competition allows brokers to bargain for favorable pricing on excess coverage.

Entities that can educate the underwriters as to implementation of risk management best practices can enjoy comprehensive coverage and aggressively low premiums. Companies that do not meet industry standards for IT security will see significant retentions, higher prices, and exclusions introduced. Some network risk policies include services to help reduce breach-related risks, such as consulting, legal advice, access to a proprietary portal with privacy and security resources, educational webinars, and data breach incident response services (note that some of these services and specific vendors are mandated by certain carriers in the policy in the event of a breach).

Based primarily on the fact that few privacy and security risks are alike, it is extremely difficult to compile overall marketplace statistics that track limits purchased, retentions, premiums, and specific coverage...
elections. Rather, it is critical to consider the unique exposures of each entity and customize a responsive program.

Conclusion

Due to the dynamic nature of Network Risk exposures and solutions, entities are well-advised to assemble a privacy and security team comprised of participants from administration, risk management, information technology, legal, security and human relations to collaborate on these issues on a regular basis. Evolving developments such as the SEC Cyber Guidelines, increasing privacy enforcement actions, enhanced focus on contractual allocation of liability, reconciliation of U.S. civil discovery obligations with international privacy and “blocking” laws are sure to change the legal landscape in the near future. Under these new SEC guidelines, directors and officers have a fiduciary obligation to exercise an acceptable level of corporate governance over their systems’ security. They are advised to disclose security breaches, denial-of-service attacks, or any other cyber security event or risk that could have material adverse effects. And internationally, on January 25, 2012, the European Commission proposed a new EU-Wide Data Protection Regulation to reform European privacy that has been governed for nearly two decades by the Data Privacy Directive 95/46/EC. Asian and Latin America countries are likely to introduce enhanced disclosure obligations as well, which should correspondingly increase litigation and liability as it did in the United States.

A company that engages in this balancing of competing considerations by undertaking a thorough evaluation of existing exposures and insurance coverage and purchasing additional insurance to cover identified gaps, will achieve the desired equilibrium. And for those who succeed, “It’s a beautiful thing.”
How to cite this publication

Individuals are encouraged to cite this report and any accompanying graphics in printed matter, publications, or any other medium, as long as the information is attributed to the cited source or to Aon plc.

About Aon

Aon plc (NYSE: AON) is the leading global provider of risk management, insurance and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 61,000 colleagues worldwide, Aon unites to empower results for clients in over 120 countries via innovative and effective risk and people solutions and through industry-leading global resources and technical expertise. Aon has been named repeatedly as the world’s best broker, best insurance intermediary, reinsurance intermediary, captives manager and best employee benefits consulting firm by multiple industry sources. Visit www.aon.com for more information on Aon and www.aon.com/manchesterunited to learn about Aon’s global partnership and shirt sponsorship with Manchester United.

1 The Nash equilibrium is named after the mathematician who proposed it, John Nash. Nash was the subject of a best-selling biography, later made into a movie, called “A Beautiful Mind.” That movie traces Nash’s battle with schizophrenia and his mathematical achievements, culminating in his being awarded the Nobel Prize in Economics in 1994. Nash’s work in mathematics has had wide implications, including significant applications in economics, biology, politics, military strategy, computing, and artificial intelligence, among others.


4 Of course, Nash could not prove the conjecture at the heart of his proposal—whether P (“quickly solved by computer”) does or not equal NP (“quickly verified by computer”)—as that is the elusive million-dollar question which continues to confound mathematicians to this day (“The P vs NP Problem.” The Millennium Prize Problems. Clay Mathematics Institute, announced 24 May 2000. Online at http://www.claymath.org/millennium/P_vs_NP/). But we see that Nash did articulate the conjecture, that P does not equal NP, at least 16 years before that famous problem was defined by Stephen Cook (Cook, Stephen. The Complexity of Theorem-Proving Procedures. In Conference Record of Third Annual ACM Symposium on Theory of Computing, 1971. Online at http://www.cs.toronto.edu/~sacook/homepage/1971.pdf).

5 ICT

6 ICT


24 Despite the heightened focus on cloud availability and uptime caused by Amazon’s prolonged service outage in April 2011 (Amazon Web Services EC2), security remains the bigger long-term concern for enterprises, analysts say.

25 In January 2012, the online retailer Zappos announced that a data breach involving the information of an estimated 24 million customers. While it appears that the hackers only obtained the last four digits of the credit card numbers, some estimate that the breach could cost Zappos over $500 million.

26 In April 2011, the email marketing firm, Epsilon Interactive, was the target of a massive attack that resulted in the theft of customer email addresses from over 50 clients. Damages from the Epsilon Interactive data breach are estimated to be as high as $1 billion.
27 In April 2011, Sony revealed that hackers into its PlayStation Network and other Sony networks had caused massive data security breaches resulting in the theft of more than 12 million credit and debit cards and nearly 100 million users. These breaches have already led to over 55 class action lawsuits seeking billions in damages. Sony estimated that breach remediation actions alone would cost at least $171 million. Sony continues to battle with one of its insurers, Zurich American, over Zurich’s obligation to defend or indemnify Sony under its primary and excess commercial general liability policies. The Sony-Zurich legal dispute demonstrates why companies should consider separate privacy and security insurance to cover such security breaches as the one Sony experienced in 2011.

28 Massachusetts General Hospital was recently fined $1 million for a 2009 data breach (the Department of Health and Human Services fined Cignet Health $4.3 million for a HIPAA violation).

29 In October 2011, a computer was stolen from the Sacramento, California offices of Sutter Medical Foundation. Although the computer was password protected, the data (3.3 million patients’ names, addresses, birthdates, medical record numbers and health insurance providers, and health information for 943,000 patients) was not encrypted. Eleven class-action lawsuits have been filed, with eventual damages estimated to be as much as $944 million to $4.25 billion, plus attorneys fees. See “11 Class Action Suits Combined as Single Case Over Sutter Data Breach.” iHealthBeat, 1 Mar. 2012. www.ihealthbeat.org/articles/2012/2/1/11-class-action-lawsuits-over-sutter-data-breach

30 In May 2011, Citigroup discovered, through routine monitoring, that its network had been attacked by hackers who accessed the data (customers’ names, account numbers, contact information) of about 200,000 bank cardholders in North America.

31 In June 2011, a Maine judge ruled that Ocean Bank was not liable to its customer, Patco Construction, after cybercriminals broke into the company’s online account and siphoned out nearly $589,000 via unauthorized Automated Clearing House (“ACH”) transfers. In the lawsuit, Patco charged Ocean Bank with negligence and breach of contract for failing to spot and stop the unauthorized ACH transfers.

32 Bank of America’s stock dropped by 3% on the mere rumor that its internal documents had been disclosed to WikiLeaks.

33 Law firms are increasingly considered valuable targets because they serve as repositories of the most highly sensitive information about their clients’ corporate acquisitions, products, and intellectual property. In February 2012, attackers based in China hacked into the networks of seven Canadian law firms in an effort to sabotage a corporate deal. The hackers destroyed data and stole sensitive client information. See Riley, Michael A., and Sophia Pearson. “China-Based Hackers Target Law Firms to Get Secret Deal Data.” Bloomberg (31 January 2012). Online at http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html With the increase in use of electronic information assets, and hackers more clever than ever, it is possible that attacks on law firms will increase. Law firms attract particular attention if they advocate positions or represent clients who are unpopular with the hacktivist community, such as Anonymous and LulzSec. In February 2012, hackers broke into the network of Puckett Faraj, the law firm representing a Marine Staff Sergeant who was involved in a raid resulting in the death of Iraqi civilians. The hackers stole client record content, evidence, lawyers’ personal email correspondence and other information, and have published it online. Last year, UK-based ACS, an anti-piracy law firm affiliated with the entertainment industry, was the victim of a coordinated attack intended to punish the firm for bringing a large number of copyright infringement actions involving peer-to-peer file-sharing. The hacker group, 4chan, leaked confidential firm information, including attorneys’ private emails and protected information (including records of downloading pornographic videos) about more than 5000 individuals targeted by ACS, subjecting the law firm to fines and lawsuits. Within a year, the firm closed and the targeted attorney went bankrupt. Law firms are also vulnerable to breaches caused by former employees, including departing attorneys eager to retain access to client files. In February 2012, a Pennsylvania law firm, Elliott Greenleaf & Siedzikowski, sued a former partner and his new firm for allegedly installing Dropbox software onto the Elliott firm’s computers that provided ongoing remote access to client files through a third-party cloud site. Law firms are also unique in that they have obligations to preserve evidence in litigation, and network outages and breaches can result in disrupted chain of custody and accusations of spoliation, for which their clients may be severely penalized. Failure to maintain security could result in waiver of a privilege, and lawyers have an ethical duty to protect clients from inadvertent disclosure. Indeed, the most sophisticated business clients are asking their outside law firms to demonstrate that they have adequate security measures in place.

34 Hackers broke into Lockheed Martin’s network in 2011 after its data storage firm, EMC’s RSA, was hacked. The hackers had obtained information about SecurID from RSA. SecurID is the authentication token provided by Lockheed Martin and other RSA clients.

In 2011, Google suffered a major attack on its Gmail accounts, including the accounts of senior U.S. government officials. The attack, which appeared to originate in China, raises questions about the security of online data abroad. Federal officials scrambled to assess whether security had been compromised by the raid on Google’s Gmail system, reflecting increasing concerns among global policymakers about cyber security.

In January 2011, the court finally approved the T.D. Ameritrade settlement for between $2.5 million and $6.5 million. T.D. Ameritrade’s initial settlement was not approved by the court because there was “insufficient compensation to the harmed consumers.”

In March 2011, EMC Ltd, the data storage firm, was the target of hackers based in China. The hackers infiltrated RSA’s network and stole critical information about SecurID, an authentication token used by RSA’s customers to protect their networks. The hackers then used data from RSA to break into Lockheed Martin’s network. EMC offered to replace millions of electronic keys as a result of this breach.

In December 2011, the security firm Strategic Forecasting (Stratfor) acknowledged that hackers had breached its website and collected information (passwords, credit card details, home addresses) on 4,000 of Stratfor’s clients.


42 A copy of the Complaint for Declaratory Judgment can be found online at https://apps.courts.state.ny.us/fibm/DocumentDisplayServlet?documentId=irVQewp3WujFno1EgNuTA==&system=prod

43 Direct costs to companies impacted by cyber breaches, such as forensics, notification, credit monitoring, and public relations costs, “are basic costs we would cover under our Zurich Security and Privacy Protection policy,” says Zurich. Then if a claim is filed, “we have a liability coverage part that would cover the affected entity for defense costs and indemnity they have to pay out as a result.”


45 Case filings in Colorado Casualty Ins. Co. v. Perpetual Storage, Inc., et al., Case No. 2:10-cv-00316 (D. Utah, 2010) may be obtained from Electronic Filing System/Pacer, at https://ecf.utd.uscourts.gov/cgi-bin/DktRpt.pl?1712945444616052-L_1_0-1


48 See, e.g., Valley Forge Ins. Co. v. Swidersky Elect. Inc., 223 Ill.2d 352 (2006) (holding that CGL policy definition of “right of privacy” requires “both an interest in seclusion and an interest in the secrecy of personal information”). While social security and credit card numbers, as well as health information, would undoubtedly be sufficiently personal, it is less clear whether an employee’s compensation history or a customer’s purchasing history would suffice.

49 Although only 46 states have adopted breach notification laws, Texas recently amended its own breach notification law to require notification to not only Texas residents, but to residents of states which have not enacted their own laws (Alabama, Kentucky, New Mexico and South Dakota). Online at http://www.legis.state.tx.us/lodocs/82R/billtext/pdf/HB00300F.pdf


57 Massachusetts’ “Standards for the Protection of Personal Information of Residents of the Commonwealth,” 201 CMR 17.00.


60 GSMA’s Privacy Design Guidelines are available online at http://www.gsma.com/Mobile-Privacy-Design-Guidelines
