LATHAM&WATKINS

Client Alert White Paper

Latham & Watkins Insurance Coverage Litigation Practice April 15, 2014 | Number 1675

Cyber Insurance: A Last Line of Defense When Technology Fails

As cyber risks increase, specialized insurance policies can protect companies, but only if those policies are appropriately tailored and negotiated.

I. INTRODUCTION

Daily news headlines reveal the escalating, and costly, problem of data breaches for companies today. All companies store assets digitally — from consumer personal data, to B2B customer data, to trade secrets, to confidential information relating to mergers and acquisitions. E-commerce sites, financial institutions, social media outlets, and many other businesses depend upon the integrity and availability of their websites and computer networks to operate. Corporate directors and officers have fiduciary obligations to safeguard these assets, and when a breach happens, reputational, regulatory, financial and legal risks abound. Companies are required to comply with explicit security standards or requirements for these types of data, such as the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX), the Payment Card Industry (PCI) Data Security Standard, and the Health Insurance Portability and Accountability Act (HIPAA), to say nothing of non-US data breach notification laws for global enterprises. Legal risk may be associated with government investigations or private party civil challenges on due care and due diligence issues. Against the backdrop of these diverse threats and vulnerabilities, this white paper evaluates an important method of managing cyber risk: the purchase of a cyber liability insurance policy.

This white paper will explain that:

- Cyber risk is increasingly prevalent and costly, and it cannot be eliminated through available security measures (Section II).
- The market for cyber insurance is maturing, with over 20 carriers now offering robust first-party and liability policies. Growth is a result of increased attack activity, increased awareness of the risk, and heightened regulatory enforcement and oversight activities — which typically involve costly notification and remediation obligations as well as the potential for increased oversight in the event of cyber breach (Section III).
- A traditional Commercial General Liability (CGL) policy is unlikely to cover the expenses related to a cyber attack and breaches on a company's data (Section IV).
- Companies should negotiate a policy to include provisions that address their particular cyber threats and data sets and avoid exclusions that could limit coverage (Section V). In particular, Section V discusses:

- The importance of the application and coverage negotiations and tips for navigating the process
- A summary of key policy provisions, including first- and third-party expenses and losses
- A comparison of some coverage provisions specific to cyber insurance: event management, network interruption and third-party damages
- The importance and impact of the definitions of Confidential Information and Personally Identifiable Information (PII)
- Typical exclusions to look out for, such as an exclusion for costs or expenses incurred to replace, upgrade, update, improve, or maintain a computer system; contractual liability; or criminal conduct
- Common considerations in setting policy premiums, such as industry and geographic spread of operations

II. CYBERSECURITY AND THE PREVALENCE OF CYBER RISK

For the past decade, increasingly prominent and frequent security and data breaches have amplified the risk of financial and data loss in cyberspace. To illustrate:

- In April 2011, Sony Corporation suffered a "hacktivist" attack allegedly exposing information from nearly 77 million user accounts.[1]
- In March 2013, a Schnucks Markets breach compromised 2.4 million credit and debit cards.[2]
- In late 2013, Target Corporation's Black Friday attack exposed the personal information of as many as 110 million customers, including information on 40 million credit and debit card accounts.[3]

Not only are breaches increasing in number, but the volume of data involved in each breach is increasing as well. Threats resulting from state-sponsored espionage attacks, malicious insiders, "Bring Your Own Device" policies, and cloud computing escalate the complexity of safeguarding a company's data.

A data security breach is an incident in which the confidentiality, integrity or availability of data (often stored electronically) is compromised, such that the data is vulnerable to access or acquisition by unauthorized persons. Not all data breaches are caused purposefully by hackers or malevolent individuals; some are caused by individual carelessness, such as leaving an unsecured laptop somewhere and exposing the data to an unsecured environment. With personally identifiable information — such as Social Security numbers, financial account numbers or access credentials — the loss of confidentiality potentially can lead to identity theft, unauthorized credit or debit card charges, and bank account fraud. Consumer brands or retailers experience direct and indirect losses, including fines and penalties imposed by the card associations. Companies may also face third-party liability in the form of lawsuits and claims, regulatory fines, and, in some cases, even civil and criminal penalties.

Security Technology Is Limited, and the "Dark Market" Is Growing

Security threats to electronic information are as old as the technologies involved and have been evolving since the early 1940s. Firewalls, anti-virus software, "defense-in-depth" strategies, intrusion detection/prevention systems and newer activity/event correlation systems all provide significant protection against even advanced persistent attacks.[4] But no security technology available today offers a "silver bullet," and almost certainly no technological solution ever could.[5] To a large extent, security

technology is reactive — either to patterns of code or to activity. When new threats appear that cannot be detected by current configurations, the products are updated to detect those new threats. But the deck is stacked against the defender, because the cyber attacker only needs to find one vulnerability — often the humans rather than the computer systems — and exploit it, while the security vendor must try to anticipate every attack and block them all.

In the battle between the attackers and protectors of computer systems, the attackers seem to be gaining ground.[6] The growing economic value of Internet-based information has made the market more attractive for criminals by offering larger targets as compared to past computer systems. Cybersecurity at the enterprise level increasingly involves an expensive arms race. Corporate IT departments evaluate and procure increasingly advanced (and very expensive) hardening, monitoring, surveillance and logging capabilities (tuned to increasingly precise threat indicators), while hactivitists, nation-states and identity-theft rings turn to an active "Dark Market" where the equally advanced tools, services and information needed to conduct cyber attacks can be shared or acquired.[7] This growing Dark Market also provides "turnkey" services for use in launching cyber attacks.[8] Underground service providers will install malicious software on vulnerable computers for a price of US$100-US$150 per 1,000 downloads.[9] A week-long distributed denial-of-service attack can be purchased for as little as US$150.[10] The Dark Market for hacking products allows even unsophisticated criminals to acquire the tools they need at modest cost to run massive cyber-criminal attacks from the comfort and safety of their bedrooms, in some cases using functions of publicly accessible servers to amplify their attacks.[11] And in many countries, these attackers need not fear that US law enforcement will be able to bring them to justice.

Very commonly, cyber attacks that involve sophisticated or advanced means to conceal the identity or methods of attackers, in fact involved only simple means to gain initial access to the sensitive corporate or consumer financial data. The most recent Verizon Data Breach Investigations Report (DBIR) reported that 78 percent of initial intrusions were rated as low difficulty, consistent with enforcement experience.[12] Whether a phishing email — tricking users into opening attachments containing malicious code — a failure to change default passwords, or failing to prevent a reasonably foreseeable "Structured Query Language" (SQL) injection attack, cyber attacks most often involve an attacker exploiting a known vulnerability.

Equally or even more commonly, negligent or malicious actions by trusted computer users or administrators cause the loss of confidentiality of key data. Sometimes the threat comes from insiders or "bad leavers" who intentionally steal or leak information, but more often the threat stems from well meaning workers. Vendor access to corporate data and systems is another vulnerable area for many corporations, as was apparently the case in the Target Corporation attack. That attack now appears to have exploited a combination of common sources of cyber vulnerability and, according to some reporting, was even detected by advanced systems before any data exfiltration occurred, but was not stopped – apparently because either the alarms were not recognized (or were misunderstood), or there was no plan for response.[13] In hindsight, critics can easily fault Target's planning and response at this point, but at the end of the day the real lesson may be a reminder that even a well prepared, well financed defense against a cyber attack can fail.

Notably, Target had demonstrated the foresight to obtain cyber insurance coverage, with an aggregate limit of US$100 million. Even with the best people, processes and technology, some attacks succeed. For businesses such as Target, a cyber insurance policy can provide an important "last line of defense" to remediate the damage and cover the losses that result from a successful cyber attack.

Cyber Attacks Are Increasingly Costly

Companies lose as much as US$500 billion per year to cyber attacks and data breaches.[14] The cost of a data breach involving the compromise of personal or financial account data is commonly determined using the cost of the breach per individual record. In 2013, the average record compromised cost US$188 in remediation, and the average number of records compromised in an individual breach was 28,765, resulting in an average cost per breach of approximately US$5.4 million.[15] Overall, the financial impact for a breach averages US$9.4 million, and companies estimate their maximum public exposure in the next 24 months will be an average of US$163 million.[16] According to reports, the Target breach will cost the mega-retailer at least US$500 million just to replace the impacted credit cards.[17] Daniel Binder, a Wall Street analyst at Jeffries, says that 10-15 percent of Target's stolen cards are turning up on the black market, totaling about 5 million cards, and industry fines for Target for this number of stolen cards could reach US$400 million to upwards of US$1 billion.[18]

III. THE EVOLUTION OF DATA BREACH LIABILITY AND CYBER INSURANCE

Cyber liability insurance products first appeared in the market during the late 1990s and addressed issues concerning the use of the Internet. These policies bore little resemblance to the cyber policies we see today, and they were both expensive and limited in scope. By the "DotCom" bust of the early 2000s, insurers had begun to target the larger DotComs such as Google, Amazon and eBay with cyber policies that included both property and liability coverage. But cyber insurance still did not take off, largely because identifying cyber liability lawsuits and lax data security as a potential "unfair or deceptive" trade practice was almost unheard of, and the insurance product itself was extremely expensive, requiring intense security audits. In addition, many companies assumed they had adequate coverage under existing CGL policies. In 2003, California passed the country's first breach notification law covering the compromise of certain unencrypted personally identifiable information.[19] In 2004, the data broker Choice Point discovered that some of its small-business customers in Los Angeles were engaged in suspicious activity. Eventually, the company notified more than 150,000 small businesses and individuals of the data breach, and more than 5,000 cases of identity theft were reported as the result of the breach. The incident became public because of the then-new California notification law. ChoicePoint paid a US$10 million fine to the Federal Trade Commission (FTC) and defended and settled dozens of state investigations as well.

The new reporting obligations and ensuing federal and state investigations into whether the corporate data owners had taken reasonable measures to live up to privacy policy promises of security, or to otherwise reasonably secure personal data, became not only routinized, but increasingly expensive to defend and resolve. Private class actions soon followed, claiming that credit monitoring was required to mitigate actual or sometimes merely anticipated damage or loss to affected individuals.

In recent years, cybersecurity reporting laws and regulatory requirements have undergone a sea change, partly in response to the growing problem of data breaches. The Securities and Exchange Commission (SEC), the FTC, the Department of Health and Human Services (HHS), President Barack Obama and state governments have all stepped up notification requirements in the event of a data breach, adding to the costs and seriousness of a cyber attack. While definitions vary, "personal data" generally covers first name or first initial, plus last name, plus any of the following:

- Social Security number
- Driver's license or state identification (ID) number
- Credit or debit card number or bank account information

- Passwords, security codes, personal identification numbers (PINs) and login information
- Unique biometric data (fingerprint, voice print, retina or iris image)[20]

In the case of medical information, definitions under both state and federal law tend to be quite broad, encompassing all identifiable information. As discussed more fully below, these state law definitions of personal data interplay with policy definitions to affect coverage, and the policyholder should be cognizant of both definitions when evaluating policies.

State Laws: 46 states, plus Guam, Puerto Rico, the Virgin Islands and the District of Columbia all have specific reporting laws for data breaches that can add to a company's cost and liability after a breach occurs.[21] Fines can be steep if companies do not give proper notification. For instance, in Virginia, the attorney general may impose a civil penalty for failure to notify of up to US$150,000 per breach.[22] In Texas, the failure to notify can cost US$100 per person to whom notification is due per day, capping at US$250,000 per breach.[23] In Florida, a breach may cost as much as US$500,000 per breach for a failure to notify.[24] Michigan fines violators US$250 for each failure to notify with a maximum penalty of US$750,000 per breach.[25]

In recent years the federal government has implemented stricter oversight and enacted specific cyber risk management and disclosure requirements for healthcare, defense, energy and other critical infrastructure industry sectors.

SEC Guidance: In 2011, the SEC issued, through their Division of Corporation Finance, "CF Disclosure Guidance: Topic No. 2 – Cybersecurity."[26] This Guidance requires publicly traded companies to disclose "material information" regarding cyber attacks and their costs to shareholders. Companies must disclose risk factors relating to a potential cyber incident. Whether a company carries cyber insurance coverage is a factor that can be used to assess the company's potential cyber-liability risk and, by extension, whether the company's cyber-security risk is significant and requires a special risk disclosure. The SEC Guidance's calculation of risk for Item 503(c) for Regulation S-K states that the less the probability of future harm and likelihood of cyber incidents, the less a company must disclose. One of the important factors in this risk calculation is whether the company owns cybersecurity insurance. While cybersecurity insurance is not required or even encouraged in the Guidance, such a calculation implies that if a company has cybersecurity insurance, that company would have a lower risk factor for cybersecurity issues. The SEC also requires that a company disclose a "description of relevant [cyber] insurance coverage."[27]

FTC Regulations: To promote data security, the FTC enforces several statutes and rules that impose obligations upon businesses that collect and maintain consumer data. These include the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act, the GLBA, the Fair Credit Reporting Act, and the Children's Online Privacy Protection Act. Under the GLBA, the FTC has issued stricter identity protection regulations that apply to financial institutions and "creditors" with "covered accounts." With what has colloquially become known as the "Red Flags Rule," the regulations require these financial institutions to implement Identity Theft Protection Programs that identify "red flags" alerting to the risk of identity theft, and to detect, mitigate, and deal with identity thefts when they occur.[28] The FTC has settled 50 Section 5 unfair/deceptive trade practice enforcement cases against companies who suffered data breaches and has investigated many more.

HHS Notification Requirements: For healthcare providers and other "covered entities," along with their "business associates," the HHS has strengthened notification requirements under HIPAA as it relates to cyber breaches pertaining to patients' electronic protected health information (ePHI). On January 17,

2013, HHS released the HIPAA Omnibus Rule, under which companies that "perform services on behalf of the covered entity, such as claims processing, data analysis, utilization review, and billing, or provide services to the covered entity, such as legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services" and deal directly with the use or disclosure of protected health information, are required to comply with HIPAA. This requirement is especially significant because of the extremely high cost of complying with notification requirements for breached health care records (US$240 per record) and because under the new HIPAA, penalties for noncompliance can be up to US$1.5 million per breach. Moreover, the obligations "flow down" through the supply chain to all vendors who can access ePHI. Specifics on the new requirements for breach notification under HIPAA can be found at the HHS website. In the three or four years before the passage of the new rules which impose direct liability on business associates, HHS received 571 reports of breaches involving more than 500 individuals, and nearly 80,000 breaches involving less than 500 individuals. HHS actively and deeply investigates large breaches in order to identify perceived systemic or significant compliance problems to address through corrective action and resolution agreements. Multi-million dollar response, investigation and resolution agreements are not uncommon.

Executive Order 13636: On February 12, 2013, President Barack Obama signed Executive Order 13636, Critical Infrastructure Cybersecurity (the Cybersecurity Order), which mandated the development of a national "Cybersecurity Framework."[29] EO 13636 subjects several sectors to federal data breach notification requirements (chemical, transportation, financial and electricity industries), but most such notification is voluntary.[30] However, political pressure is mounting for greater federal regulatory action regarding data breaches, especially after the massive breaches at Target and the Edward Snowden security leaks highlighted cyber vulnerabilities in critical data banks. The 112th Congress considered numerous cybersecurity bills, including several specifically related to data notification.

International Reporting Requirements. The EU has a data breach notification directive for companies in the telecommunications industry[31] and, through the Article 29 Working Party, has recently issued general guidance on breach notification.[32] Some member states impose broader requirements. Moreover, the EU's proposed data protection regulation (which would update the current approach under the EU data protection directive) [33] would impose specific breach notification obligations with fines reaching five percent of gross revenue.[34] Asia, South America and the Middle East also have legal reporting issues that global enterprises should analyze. Thus, when a cyber attack impacts a global enterprise with non-US data centers and affected parties, the enterprise must quickly assess notification obligations worldwide, an undertaking few companies are prepared to handle quickly.

IV. COVERAGE FOR CYBER RISKS UNDER CGL POLICIES

Going forward, in light of recent court rulings and amendments to policy forms, a traditional CGL policy is unlikely to cover the expenses related to a cyber attack on a company's data. Many CGL policies have specific exclusions for electronic data. Insurance Services Office, Inc. (ISO), an industry organization that develops standard insurance forms, recently filed a number of data breach exclusionary endorsements for use with its standard-form, excess and umbrella liability policies, which are set to take effect in May of 2014.[35] Even without such exclusions, however, CGL policies generally only cover "tangible" property, and as the below cases demonstrate, courts have been reluctant to find that software and data constitute tangible property.

Consider the following examples:

AOL:[36] Users sued AOL for damages when, after a data breach, AOL software damaged other software, data and computer hard drives. AOL sought coverage under their CGL policy. When the carrier refused to

pay the claim, AOL sued. The court held in favor of the carrier, finding that the damaged software and data were not "tangible" under the plain meaning of the term (since "tangible" had not been defined in the policy) and thus, the software and data were subject to the exclusion in the CGL policy that limited coverage to tangible property.

Ex Log:[37] In a similar case, some data tapes belonging to IBM were lost from the back of a truck belonging to a company called Executive Logistics (Ex Log), which had subcontracted the transportation of the tapes. The tapes contained 500,000 personal records of IBM employees, including Social Security numbers, birth dates and other information. The costs of employee notification, call centers and credit monitoring totaled more than US$6 million for IBM. Through a negotiated settlement, the subcontractor paid IBM for the loss, then sought coverage under Ex Log's CGL policies, which named the subcontractor as an additional insured. When the carrier denied the claim, Ex Log and the subcontractor sued, arguing the loss should have been covered under the "personal injury" section of the policy. However, the court found that absent any evidence the tapes had actually been accessed, the "publication" required to show a personal injury did not exist, and the claim was not covered. In January of 2014, a Connecticut appellate court upheld the verdict.

Sony: In one of the larger data breaches in recent memory, Sony Corporation's popular PlayStation network was hacked in June of 2011, exposing the personal information of 77 million user accounts in an incident which appears to have cost Sony US$2 billion.[38] Sony filed for a declaratory judgment that its CGL policy covered costs of the breach. The carrier took the position that the CGL policy only covered "property damage" and "bodily injury," neither of which, the carrier contended, had occurred as a result of the breach.[39] On February 21, 2014, in what may be a very influential decision, New York Supreme Court Justice Jeffrey K. Oing issued a bench ruling that the policy did not cover breach costs because the provision only covered confidential material published directly by Sony, not by the hackers who stole the information. This decision underscores the reason that many more companies are seeking out policies specifically written to cover cyber business interruption, notification, crisis management and liability-related losses.

Schnucks Market: In case echoing the Sony matter, Schnucks Market experienced a cyber attack between December 2012 and March 2013 that exposed 2.4 million credit and debit cards used at 79 of its 100 stores.[40] Schnucks sought coverage under its CGL policy with Liberty Mutual, but Liberty Mutual filed for a declaratory judgment to deny coverage, arguing that electronic data is not tangible property, and Schnucks had not made a claim based on "bodily damage" or "property damage," nor was the breach an "occurrence" per the policy.[41] The parties eventually settled out of court.

Compounding the CGL issue, neither Directors and Officers Liability (D&O) nor Errors and Omissions Liability (E&O) coverage address the most common categories of expense and liability experienced in the wake of a cyber attack or other loss of data security. For public companies, D&O policies may only cover the insured organization's liability for a *securities claim* related to a cyber incident. While a private company's D&O may provide coverage for wrongful actions of directors and officers that led to the data breach, this still leaves coverage holes in the areas of business interruption, notification, crisis management, credit monitoring for affected individuals and so forth. E&O coverage for a cyber incident requires that the insured be able to show some sort of nexus between the cyber issue and the professional services in which the insured is engaged. To illustrate, in *Eyeblaster Inc. v. Fed. Ins. Co.,* the court found that the E&O policy Eyeblaster had purchased did indeed cover the damages caused by Eyeblaster's online advertising software scripts, because Eyeblaster had disclosed to Federal Insurance that Eyeblaster's main business activity was interactive advertising — which was the very activity that had caused the damages to the plaintiff in the underlying lawsuit.[42] Showing such a nexus presents a significant obstacle to coverage for most businesses, however.

V. CYBER INSURANCE POLICIES

Since cyber insurance policies first were issued in the late 1990s, the market for cyber insurance has become robust and varied. Not only has the number of carriers offering cyber coverage increased significantly, the variety of coverage options has increased as well. Currently, more than 20 carriers write cyber insurance policies.[43] Most of these carriers offer multiple coverages, and coverage must be crafted to each individual client. Some carriers impose minimum revenue requirements, but as the market gains maturity, these carriers are bringing in more small to mid-sized insureds. Some carriers limit their coverage to non-technology companies or prohibit certain types of insured, such as universities or payment processors. Other carriers avoid stated restrictions such as this but specifically target specific industries, such as retail, healthcare, or financial institutions. Available capacity is generally within the US$10 to US$25 million range, with some carriers offering excess coverage with capacity of around US$10 million.

Cyber insurance policies typically cover both first-party and third-party losses suffered as a result of a cybersecurity breach. However, the scope of coverage is increasingly refined and can be tailored to a variety of risk scenarios. Furthermore, carriers now offer a variety of additional coverage options and services to assist companies in responding to a cyber breach. Policies are generally offered both as stand-alone policies and as components of larger suites of coverage.

The biggest difference in coverage between carriers is in breach remediation coverage, and with many carriers the extent of that coverage is negotiable. Most carriers do not require the insured to utilize designated service providers, but almost all provide discounted rates through their own providers. Of those carriers who have a time limit for remediation coverage, the most common time period is one year after the breach. Almost all of the available policies cover losses caused by a failure to secure data, loss caused by an employee, acts of third parties, and loss resulting from theft or loss of property.[44] Carriers also offer policy extensions, such as for media liability.

The discussion below is intended to provide a general introduction to some of the coverage options currently available and to hit on some key issues to consider when negotiating policies. A more detailed discussion of some of the areas covered summarily below falls beyond the scope of this white paper. Therefore, we have restrained our analysis to a high-level review. Any comparisons made between policies are based on form policies that are subject to change. In fact, with the assistance of a knowledgeable broker and the advice of experienced counsel, many companies successfully negotiate policy terms that are better suited to their particular risk profile than the form policies.

Purchasing and Negotiating a Cyber Insurance Policy

Like any insurance procurement process, purchasing cyber insurance is fraught with important decisions and requires careful consideration and negotiation of key policy points. As a first step in this process, an insured should always analyze potential exposure, which will dictate specific coverage requirements. For example, is the policyholder a data vendor or a data owner? A data vendor is the custodian of third-party information and is exposed to risk that third-party information will be accessed and disseminated, triggering obligations under privacy and other regulations and potentially resulting in third-party claims related to the improper dissemination. A data vendor may have contracts in place with third parties that address confidential information, and the contractual liability exclusion discussed below may come into play. A data owner, on the other hand, does not control third-party data but is exposed to the risk that its own confidential information will be improperly accessed and disseminated. Other key considerations include whether the company has overseas operations, whether the company has call centers, the extent of the company's internet operations and the company's reliance on cloud computing.

After coverage requirements are established, the insured can evaluate the various form offerings presented by carriers and identify the desired coverage options. Once the insured chooses options, underwriters will be informed about the scope of coverage and will begin the review process. In the past, companies were sometimes subject to audits of their network systems in order to evaluate risk levels. Now smaller companies more commonly submit an application containing information relevant to a cyber risk analysis. Policy purchasers should take the application process very seriously and ensure that their legal counsel and IT department work closely with risk management during this time. Errors and omissions in applications can compromise coverage, so care should be taken to provide complete and accurate information.

The application process for larger companies can be intense and will vary depending on the magnitude of potential risk. While the use of third-party audits is no longer ubiquitous, an application may involve identifying any existing third-party audits that have been conducted by the company outside of the application process. Large companies generally will be required to participate in a lengthy call or in-person briefing, with key individuals in the company who are responsible for cybersecurity presenting to the carrier. The underwriters are able to ask questions and obtain additional information during these briefings, so these presentations should be well researched and the presenters prepared to answer questions. While underwriters will focus on security technology implemented by the company, they have not identified any specific preferred technology in this process. Rather, they will evaluate technology in combination with the policies and procedures in place for protecting confidential information and the people responsible for implementing those policies and managing the technology.

After the underwriters have evaluated the application, the parties will negotiate key policy provisions and definitions. When seeking coverage, policyholders should pull from a reasonably wide pool of carriers, because some carriers refuse to negotiate on certain provisions. In the process of obtaining coverage, one or more coverages or exclusions may emerge that disproportionately impact the value of the policy for a particular company. In such cases, policyholders benefit from negotiating with several carriers on these items.

Typical Cyber Coverage Options

Notwithstanding the increasingly varied provisions of these policies, the following types of losses are commonly covered under cyber insurance policies:

First-party Losses:

- *Direct or extra expense of responding to the breach.* Covered expenses typically include:
  - Hiring an independent information security forensics firm
  - Public relations
  - Notification of affected parties (*i.e.*, business customers and/or individuals whose data was accessed or acquired in the data breach)
  - Credit monitoring for individuals
  - Identity theft resolution services
  - Call centers
  - Costs to re-secure, re-create and/or restore data or systems

- Legal services/advice
- Crisis management services
- E-extortion costs (company is forced to pay hacker in order to get data/access back)

- *Fines/penalties.* While civil fines themselves are usually covered, some carriers may not offer coverage for costs to investigate, defend and settle fines.

- *Denial of service costs to business.* These costs include loss of use and resulting business interruption. Coverage can be set as a per day amount or can be tailored to a company's specific loss. For example, losses to an online retailer would likely be higher on Cyber Monday than on Memorial Day.

- *Losses resulting from misappropriation of the insured's information assets or confidential business information.* Under some policies, losses related to misappropriation of intellectual property, trade secrets, company records, customer lists, company credit card numbers, budgets, proposals, work papers, and any other proprietary or sensitive company data that results from a data breach are covered.

- *Damage to systems.* This could include losses resulting from damage to the insured's computer systems resulting from the breach. Some policies include coverage for the cost of restoring lost or compromised data.

- *Disclosure of information.* Some policies include coverage for damages in connection with the disclosure of information to a competitor.

- *Intellectual property.* Coverage could include expenses related to the restoration or recreation of intellectual property, including trademarks, copyrighted material and proprietary business information, up to amortized value.

Third-party Losses:

- *Third-party claims*. This includes claims for damages brought by customers, consumers or outside business entities for damages they incurred as a result of the insured company's breach of security, namely *their* losses from the inability to transact business, including punitive and exemplary damages, settlements and costs.

- *Defense costs.* These costs include attorney fees and expert fees for outside claims made against an insured related to a data breach.

- *Media liability.* This provides coverage for losses related to libel, slander, defamation and other media torts, as well as copyright, trademark and patent infringement. This can include losses resulting from information posted to social networking sites, such as Facebook and LinkedIn.

- *Data and PII loss.* This covers losses or breach of a third party's data, including dissemination of PII. One example would be if confidential third-party information, such as Social Security numbers or passwords, was used to breach the third party's data. Policies define PII differently in the absence of an industry-standard definition.

- *Fines and penalties*. These include fines that may be assessed under state privacy statutes as well as under federal privacy regulations.

The above lists are not exhaustive, but they do cover the primary offerings under policies currently in the market. Carriers may offer additional coverage, especially for companies with specialized risks.

Comparison of Coverage Offered by Cyber Insurance Providers

Many carriers offer both standalone policies and policies that can be wrapped into a more comprehensive program of coverage. While the majority of the available coverage overlaps, companies should consider some important differences. The charts provided in Attachment 1 analyze three key components of any cyber insurance policy: first-party coverage for costs incurred responding to the event; first-party coverage for lost business income; and third-party coverage, including potential media liability. This comparison is based on a review of form policies available on various carriers' websites and is not intended to reflect the entire scope of coverage that may be available through add-on policies or negotiated changes in the policy wording. The comparison provides an introduction to prospective insureds as to what types of coverage options they might see when they begin to investigate coverage.

First-party Coverage: Event Management. As the chart in Attachment 1 illustrates, while both carriers advertise that they offer event management coverage, the scope of the offering is quite different. While neither hypothetical policy is per se "better" than the other, the comparison demonstrates that policies offer a "menu" of options — not all of which may be beneficial to the policyholder. For example, Policy A is time-limited to losses (one year), and requires insurer agreement to an outside firm hired to advise the policyholder on breach response. Policy B is not time-limited and does require some prior approval for lawyer, investigator and public relations costs. Additionally, Policy A specifically offers coverage for call centers, which can be a significant portion of the policyholder's total response costs. For example, in response to the "Black Friday" holiday breach at Target, the retailer had to triple its already robust call center staffing and keep the call centers open around the clock as well as on Christmas Day, which greatly increased the total costs of the breach.[45] Of course, policies often cover "reasonable and necessary" costs of notifying persons who are affected, and a call center may qualify for coverage under that provision in some situations. While coverage for call centers is not specified, Policy B does cover the cost of changing account numbers or codes. A policyholder's willingness to cover such costs might avoid reputational damage, class action lawsuits, or third-party litigation by credit card companies. However, Policy B does not cover the cost of restoring, recreating or recollecting the data as part of event management coverage — the cost of which could vary considerably depending on the manner in which the policyholder uses the data in its business operations.

First-party Coverage: Network Interruption. Both policies offer comparable coverage for loss of business income due to a breach that results in an actual interruption or impairment of the insured's business operations. The important distinction is the duration of such coverage. Policy A covers loss of business income from the time the network interruption begins until 120 days after the interruption ends. Not included in the form policy is a "waiting hours" period that could be written into an individual policy, requiring a specified number of hours to elapse once a material interruption has begun. Policy B's coverage does not kick in until 24 hours after the interruption begins, and it continues only until business operations are back to normal or 60 days after the insured's system is restored, whichever comes earlier. A policyholder may want to consider this provision carefully. Depending on the nature of a company's operations, the first 24 hours of network interruption may significantly impact operations and could cause a substantial business loss. Again, each policyholder will need to assess its own potential exposure to determine the appropriate time span for coverage of business losses.

Third-party Coverage: Defense Costs and Third-party Damages. Both policies offer coverage for third-party claims based on a failure to protect confidential information. However, Policy A also offers coverage for the insured's failure to disclose a breach in accordance with privacy laws and in violation of privacy statutes. Given the proliferation of statutes and regulations governing data privacy, such coverage may be increasingly valuable. Policy B covers injury incurred by a third party due to loss of use of its own system that was a result of the cyber attack on the insured, as well as injury to the third party caused by an inability to access the insured's system. Depending on the nature of the insured's business, third-party system losses could be considerable. For instance, if a retailer could not access the database of its third-party email marketing provider, and the retailer was unable to send out advertising to its customer base in advance of an important sale, the resulting losses could be significant. Both policies include a duty to defend. While the Policy B form policy includes coverage for losses resulting from reputational injury, for Policy A, that coverage would require an additional coverage section to be purchased.

Definitions of Confidential Information and (PII). Perhaps the most fundamental definition in a cyber insurance policy is that of the information — often referred to as Confidential Information or Personally Identifiable Information (PII) — that has been breached or misappropriated. Some policies define "Confidential Information" broadly as any

> information from which an individual may be uniquely and reliably identified or contacted, including, without limitation, an individual's name, address, telephone number, social security number, account relationships, account numbers, account balances, account histories and passwords.[46]

Under this definition, an individual's name, on its own, could be considered Confidential Information. The definition gives policyholders room to argue that pieces of information not listed specifically in the definition (or combinations of pieces of information) qualify as Confidential Information. For example, in some circumstances, an individual's employer's name, along with date and place of birth, might constitute information from which they could be "uniquely and reliably identified." Because of the relative youth of the cyber insurance market, policyholders do not have the benefit of judicial interpretation of the applicability of such broad definitions.

In contrast, other policies may identify very specific items that are considered Confidential Information. For example, some policies may mirror state definitions of PII and use a definition such as:

A natural person's first name or first initial, and last name, in combination with any of the following:

A. Their Social Security number, driver's license number or other personal identification number (including an employee identification number or student identification number)

B. Their financial account number (including a bank account number, retirement account number or healthcare spending account number)

C. Their credit, debit or payment card number

D. Any information related to their employment by an Insured Organization

E. Any individually identifiable health information, pursuant to HIPAA, held by an Insured Organization[47]

when any of the information in "A" through "E" above is intended by an Insured Organization to be accessible only by persons it has specifically authorized to have such access.

This definition is consistent with many state privacy laws. This has the interesting — and perhaps intentional — effect of limiting coverage for breach response to those responses required by law. If the policyholder does not experience a breach of PII as defined under the relevant privacy law, but voluntarily undertakes breach response, the PII may not be considered to trigger coverage under the policy.

Cyber Policy Exclusions

As with CGL policies, cyber policies often contain a host of exclusions. Agreement on the wording of many of these exclusions — and therefore their scope — are an important part of the negotiation process. Possible exclusions from cyber policies should be carefully noted and, if feasible, negotiated around. Because many of these exclusions have not been the subject of litigation, policyholders lack the benefit of judicial interpretation when assessing the boundaries of coverage. The relative lack of analysis cautions towards careful and creative evaluation of the scenarios in which exclusions may apply.

Examples of some exclusions to keep in mind during negotiations include:

- *Contractual liability exclusion.* This exclusion typically functions to exclude coverage for any liability assumed by an insured under a contract or agreement. To the extent a third-party claim can be styled as breach of contract, this exclusion may come into play. In some cases, this exclusion can be limited to situations where, but for the contract, the policyholder would not be liable for losses. As discussed more fully below, data vendors who have contracts in place with third parties that address confidential information should pay close attention to the language of the contractual liability exclusion during the negotiation process.

- *Criminal conduct exclusion.* Many policies contain exclusions for criminal or fraudulent acts by the insured. Companies with call centers should carefully negotiate this exclusion, given the abundance of criminal eavesdropping statutes that could apply.

- *Exclusion for terrorism, hostilities, and claims arising from "acts of foreign enemies."* This exclusion could bar coverage where a cyber attack or breach originates in a foreign country and arguably occurred at the direction of a hostile foreign government. Companies in certain industries, such as energy or defense, may be more likely to face this type of cyber threat and should be cognizant of the potential applicability of this exclusion. For example, the exclusion may apply if a foreign government targets a specific entity, such as a search engine or social network. Some brokers remove this exclusion as a matter of course, but potential policyholders should be aware of its inclusion in form policies, especially if they are not working with brokers familiar with the industry.

- *Exclusion for unauthorized collection of customer data.* Some policies contain exclusions for losses related to data whose collection was not authorized. Companies engaged in online activities, especially activities in which consumer financial data is collected, could find this exclusion at play. Indeed, for some companies, the collection of data is central to their business, and this exclusion could present a significant bar to coverage.

Cyber Insurance Premiums

In many insurance markets, ballpark estimates of the cost of a given level of coverage can be provided to prospective policyholders. This is not so in the cyber insurance market. For some time, observers attributed the lack of standardized pricing to the newness of the market and the lack of available data points for creating an "average" price. However, the market is now more developed and suffers from no lack of data points. The more likely reason for a lack of standardized pricing is the specificity of each policy to the policyholder's individual situation and the lack of uniformity in the risks carriers assume. At

the outset, and as discussed more fully above, important differences that can impact pricing exist between the base policies different carriers offer. Those differences are compounded by the reality that — if tailored correctly — the cyber insurance policies are intensely specific to the needs of individual companies. However, some key factors drive pricing of cyber insurance policies. The following considerations may carry different weight depending on the policy being written and the underwriter conducting the analysis.

- *The insured's industry*. Some industries have more significant exposure to PHI or PII. For example, companies in the healthcare industry are likely to have PHI. In the retail industry, companies might be further subcategorized based on characteristics such as the number of credit card transactions processed yearly.[48]

- *Geographic spread of operations*. Companies with a global footprint face different risks in different jurisdictions. The US is a fairly litigious environment with significant privacy laws and regulations, creating significant exposure. Other jurisdictions may not have robust regulation or enforcement, reducing the risk of exposure from a breach.

- *Limits sought by insured*. The aggregate limit of coverage will certainly impact price, but limits in other key areas such as notification costs will also affect premiums. For example, many policies limit coverage for notifications to a set number of persons.

- *Deductible/retention*. A higher deductible or retention will generally operate to reduce premiums.

- *Security and privacy controls*. Companies that can demonstrate high quality controls will generally see lower premiums. Notably, quality is not based solely on the technology a company uses to protect data. Rather, quality is the combination of people, processes and technology that a company uses to safeguard PHI and PII. While some carriers continue to inflict lengthy applications on applicants, much more commonly carriers ask the company to participate in a briefing at which individuals with responsibility for management and security of PHI and/or PII provide information and respond to questions.

- *Claims and loss experience*. A company's history of loss will inform decisions on the likelihood of future losses.

- *Data breach team choice*. If the insured wants to utilize its own data breach team rather than using the carrier's team, the premium will likely increase. Policies requiring the insured to use the carrier's data breach team reflect the savings a carrier is able to realize as a result of providing high volume business to chosen experts. Some carriers will not write a policy that permits the insured to choose its own data breach team.

This non-exhaustive list of factors illustrates why the pricing spectrum of cyber insurance is so broad and so unpredictable. Even two similar companies in the retail industry could face significantly different pricing because of loss history and security and privacy controls. Rather than asking whether a premium is standard for the market, prospective policyholders may be best served by focusing on the premium cost in light of their own particular risk of loss.

VI. CONCLUSION

Cyber attacks are not going away. While improving security technologies will play an important and necessary role in defending against these attacks, the very nature of computer and network technology means that security technologies cannot detect or block every threat. Even where technology is effective, trusted individuals can undermine technology if they fail to follow proper procedures, are tricked into dangerous actions, or themselves harbor malicious intent. Absent any silver bullets to solve this problem, organizations that face cyber risks must develop serious, well thought out strategies, combining effective technology, careful security practices, and qualified and diligent people. Organizations must also carefully plan for how to respond when the inevitable attacks do occur.

Insurance offers an important tool for businesses as part of an integrated approach to managing risks that involves business procedures and technical defenses. For the reasons explained above, traditional business insurance products are unlikely to cover losses from cyber attacks. Instead, businesses must turn to specialized cyber insurance products to protect themselves. Companies at risk for financial losses from cyber attacks should carefully examine the available cyber insurance products and consider whether such policies can play a role in their plans for managing cyber risks.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Peter K. Rosen
peter.rosen@lw.com
T+1.213.891.8778
Los Angeles

Bob Steinberg
bob.steinberg@lw.com
+1.213.891.8989
Los Angeles
+1.650.463.2642
Silicon Valley

Margrethe K. Kearney
margrethe.kearney@lw.com
+1.312.777.7040
Chicago

Martha L. O'Connor
martha.o'connor@lw.com
+1.312.876.7640
Chicago

Neil A. Rubin
neil.rubin@lw.com
+1.213.891.8841
Los Angeles

Endnotes

[1] Martyn Williams, *PlayStation Network Hack Timeline,* PC WORLD (2011), *available at* http://www.pcworld.com/article/226802/playstation_network_hack_timeline.html (last visited Mar. 13, 2014).

[2] St. Louis Public Radio, *Data Breach at Schnucks Could Affect More Than Two Million Cards,* ST. LOUIS PUBLIC RADIO (Apr. 15, 2013), *available at* http://news.stlpublicradio.org/post/data-breach-schnucks-could-affect-more-two-million-cards (last visited Mar. 13, 2014).

[3] Don Reisinger, *Yikes! Target's Data Breach Now Could Affect 110M People,* CNET (Jan. 10, 2014), *available at* http://news.cnet.com/8301-1009_3-57617034-83/yikes-targets-data-breach-now-could-affect-110m-people/ (last visited Mar. 13, 2014).

[4] Jennifer Kent and Kate Steiner, *Ten Ways to Improve the Security of a New Computer* at 2-3 (2012), *available at* https://www.us-cert.gov/sites/default/files/publications/TenWaystoImproveNewComputerSecurity.pdf (last visited Mar. 13, 2014).

[5] Indeed, a famous result in computer science means that it is impossible to write a computer program that can determine, with 100 percent reliability, whether another computer program is capable of doing a particular thing. Alan Turing, *On computable numbers, with an application to the Entscheidungsproblem*, 42 PROC. LONDON MATH. SOC'Y 230–65 (1936), *available at* http://www.turingarchive.org/browse.php/B/12 (last visited Mar. 23, 2014); Henry Gordon Rice, *Classes of Recursively Enumerable Sets and Their Decision Problems*, 74 TRANS. AMER. MATH. SOC. 358-366 (1953), *available at* http://www.jstor.org/discover/10.2307/1990888 (last visited Mar. 23, 2014). This makes writing a perfectly reliable anti-malware program impossible. Fred Cohen, *Computer Viruses – Theory and Experiments*, 6 COMPUTERS & SECURITY 22-35 (1987), *available at* http://security.dsi.unimi.it/~roberto/teaching/vigorelli/0607/malware/material/cohen.pdf (last visited Mar. 23, 2014).

[6] *See* Kamala Harris, GANGS BEYOND BORDERS: CALIFORNIA AND THE FIGHT AGAINST TRANSNATIONAL ORGANIZED CRIME at 53 (Mar. 20, 2014), available at https://oag.ca.gov/transnational-organized-crime (last visited Mar. 23, 2014).

[7] *Id.* at 59 –61.

[8] Max Goncharov, *Russian Underground 101*, Trend Micro Incorporated (2012), *available at* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf (last visited Mar. 23, 2014).

[9] *Id.* at 6.

[10] *Id.* at 8.

[11] Adam Greenberg, *DDoS attacks against NATO likely DNS amplification or NTP reflection, expert suggests*, SC MAGAZINE (March 17, 2014), *available at* http://www.scmagazine.com/ddos-attacks-against-nato-likely-dns-amplification-or-ntp-reflection-expert-suggests/article/338524/(last visited April 2, 2014).

[12] http://www.verizonenterprise.com/DBIR/2013/ *See* 2013 Verizon Data Breach Investigations Report.

[13] Michael Riley, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUSINESSWEEK (March 13, 2014), *available at* http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data?campaign_id=DN031314#p1 (last viewed April 2, 2014).

[14] Center for Strategic and international Studies, *The Economic Impact of Cyber Crime and Cyber Espionage* at 18*,* MCAFEE (July 2013), *available at* http://mcaf.ee/1xk9a (last visited March 12, 2014).

[15] Ponemon Institute, *2013 Cost of Data Breach Study: Global Analysis* at 1, 4*,* PONEMON INSTITUTE LLC (May 2013), *available at* https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf (last visited Mar. 14, 2014).

[16] *Id.*

[17] Brian Acohido, *Experts Testify on True Cost of Target Breach,* USA TODAY (Feb. 4, 2014), *available at* http://www.usatoday.com/story/cybertruth/2014/02/04/experts-testify-on-true-cost-of-target-breach/5205365/ (last visited Mar. 13, 2014).

[18] Tom Webb, *Analyst Sees Target Data Breach Costs Topping $1 Billion,* ST. PAUL PIONEER PRESS (Jan. 30, 2014), *available at* http://www.twincities.com/business/ci_25029900/analyst-sees-target-data-breach-costs-topping-1 (last visited Mar. 13, 2014).

[19] SB1386, Cal. Civ. Code 1798.82 and 1798.29, effective July 1, 2003.

[20] Commercial Law League of America, *State Data Security/Breach Notification Laws Spreadsheet* (Dec. 2011), COMMERCIAL LAW LEAGUE OF AMERICA, *available at* http://www.clla.org/documents/breach.xls (last visited Mar. 13, 2014).

[21] National Conference of State Legislatures, "State Security Breach Notification Laws," http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (Jan. 21, 2014) (last visited March 12, 2014).

[22] Va. Code § 18.2-86.6 (2012)

[23] Tex. Bus. & Com. Code § 521.151 (2012).

[24] Fla. Stat. § 817.5681 (2012).

[25] Mich. Comp. Laws § 445.74 (2012).

[26] SECURITIES & EXCHANGE COMM'N, DIV. OF CORP. FIN, CF DISCLOSURE GUIDANCE: TOPIC NO. 2 – CYBERSECURITY (OCT. 11, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (last visited Mar. 14, 2014); Latham & Watkins Client Alert, *SEC Staff Issues Disclosure Guidance on Cybersecurity Risks and Cyber Incidents*, October 24, 2011.

[27] *Id.*

[28] 16 C.F.R. 681 (2014).

[29] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

[30] *Id.*

[31] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002. The directive has not been implemented by all member states. Some have issued only voluntary guidance by the data protection authorities and others are still considering whether and how to introduce breach notification obligations.

[32] Article 29 Data Protection Working Party, *Opinion 03/2014 on Personal Data Breach Notification* (Mar. 25, 2014) *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf (last visited April 5, 2014).

[33] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive), 1995 O.J.

[34] Peter Waterhouse, *Snowden, Bitcoin, and Data Breaches Foretell New Regulations,* INFORMATION WEEK (Mar. 12, 2014), *available at* http://www.informationweek.com/security/risk-management/snowden-bitcoin-data-breaches-foretell-new-regulations/d/d-id/1127648 (last visited Apr. 11, 2014).

[35] Randy J. Maniloff, More On ISO's Just-Filed CGL Data Breach Exclusions, LEXISNEXIS LEGAL NEWSROOM (Sept. 18, 2013), *available at* http://www.lexisnexis.com/legalnewsroom/insurance/b/cyberinsurance/archive/2013/09/18/more-on-iso-s-just-filed-cgl-data-breach-exclusions.aspx (last visited Apr. 11, 2014).

[36] *America Online, Inc. v. St. Paul Mercury Insurance Co.,* 207 F.Supp.2d 459, 462 (E.D. Va. 2002).

[37] *Recall Total Info. Mgmt., Inc., et al. v Fed. Ins. Co., et al.,* 147 Conn. App. 450, 463-4 (Conn. App. 2014).

[38] Judy Greenwald, *Zurich Owes No Defense in Sony PlayStation Hacking: Court,* BUSINESS INSURANCE (Feb. 25, 2014), *available at* http://www.businessinsurance.com/article/20140225/NEWS07/140229914/zurich-owes-no-defense-in-sony-playstation-hacking-court?tags=%7C68%7C299%7C76%7C329%7C303%7C335 (last visited Apr. 11, 2014).

[39] Complaint for Declaratory Judgment at ¶¶ 71, 73, 76,80, 85, 87, *Zurich Am. Ins. Co. & Zurich Ins. Co. Ltd. v. Sony Corp. of Am., et al,* Case No. 651982/2011 (N.Y. Sup. Ct. July 20, 2011).

[40] Jaikumar Vijayan, *Schnucks Supermarket Chain Struggled To Find Breach That Exposed 2.4 Million Cards,* COMPUTERWORLD (Apr. 15, 2013), *available at* http://www.computerworld.com/s/article/9238402/Schnucks_supermarket_chain_struggled_to_find_breach_that_exposed_2.4M_cards (last visited Apr. 11, 2014).

[41] Complaint for Declaratory Judgment at ¶ 84, *Liberty Mutual Ins. Co. v. Schnuck Mkts., Inc.*, Case No. 4:13-CV-1574 NAB (E.D. Mo. Aug. 14, 2013).

[42] *Eyeblaster, Inc. v. Fed. Ins. Co.,* 613 F.3d 797 (8th Cir. 2010).

[43] The Betterley Report, Cyber/Privacy Insurance Market Survey, June 2013, at p. 6 et. seq.

[44] *Id*. at 8.

[45] Megan Stewart, *Target Call Centers open through Christmas Day in Response to Data Breach,* KSTP.COM (Dec. 25, 2013), *available at* http://kstp.com/article/stories/s3259578.shtml (last visited Apr. 11, 2014). See *also* TARGET TWITTER FEED, *We Want You To Know,* TWITTER.COM (Dec. 26, 2013), *available at* https://twitter.com/Target/statuses/416250152018378752 (last visited Apr. 11, 2014) (announcing tripling of call centers).

[46] NATIONAL UNION FIRE INSURANCE COMPANY OF PITTSBURGH, PA ("AIG"), *PORTFOLIO SELECT FOR PUBLIC COMPANIES SPECIMEN POLICY* AT EVENT MANAGEMENT COVERAGE SECTION 1-2, SECURITY AND PRIVACY COVERAGE SECTION AT 9-10*,* AIG.COM, *available at* http://www.aig.com/Chartis/internet/US/en/PortfolioSelect_for_Public_Companies_Specimen_Policy_tcm3171-533001.pdf (last visited Mar. 19, 2014).

[47] "Individually identifiable health information" is, as the title suggests, limited to information related to physical or mental health conditions or the provision of health care to an individual. This information can include demographic information. *See* The Privacy Rule, 45 CFR Part 160 and Subparts A and E of Part 164 (2014).

[48] The Payment Card Industry Data Security Standard (PCI DSS) is an example of a subcategorization of retail companies. PCI DSS classifies merchants into one of four merchant levels based on yearly credit card transaction. A merchant that processes over six million transactions per year would be classified as a Level One, and may be perceived as a higher risk to insure. *See PCI FAQS, available at* http://www.pcicomplianceguide.org/pcifaqs.php#1, (last visited Apr. 11, 2014).

Attachment 1

First Party Coverage: Event Management	
Policy A	**Policy B**
Definition of "Loss" includes reasonable and necessary expenses, incurred within one year of the discovery of the event to: • conduct an investigation to determine the cause of the event; • hire a public relations firm, crisis management firm, law firm or breach coach agreed to by the insurer to advise on minimizing harm to the insured (including maintaining and restoring public confidence) • notify those whose Confidential Information is subject of the breach and advise of any available remedy • provide call centers, credit monitoring, victim reimbursement insurance to those notified • provide other services approved by Insurer • restore, recreate, or recollect the electronic data (or to determine that it cannot be restored).	Covered "Crisis Management Expense" includes the reasonable and necessary cost of either: (a) retaining, for a stipulated period of time with prior approval (1) an independent attorney, (2) information security forensic investigator, (3) public relations consultant **OR** (b) advertising and public relations media and activities. Covered "Privacy Notification Expenses" include the reasonable and necessary expense of • notifying potentially affected persons, • changing their account and other ID numbers, and • providing (for a stipulated period of time and with prior approval) credit monitoring or other protective services. The expenses must result from a "Disclosure Injury," which is an injury resulting from unauthorized use of confidential information that occurs during the policy period and results from a cyber attack or a hacker.

First Party Coverage: Network Interruption	
Policy A	**Policy B**
Covers loss of business income caused by a failure or violation of the security of a computer system that results in an actual and measurable interruption or suspension of the insured's business. • Only covers losses that are incurred within 120 days after the actual and measurable interruption ends. • Business income means the sum of net income that would have been earned and normal operating expenses incurred, including payroll • Does not cover losses resulting from general failure to protect confidential information (including phishing, other social engineering technique or otherwise).	Covers loss of business income caused by fraudulent and unauthorized access of the insured's system, or a cyber attack on the insured's system. • Only covers losses that are incurred during the time period that starts twenty-four (24) hours after the actual impairment and ends the earlier of (1) when business operations are back to normal, or (2) sixty (60) days after the insured's computer system is fully restored • Business income means net profit that would have been earned before taxes and continuing normal operating and payroll expenses. • Also covers extra expenses incurred in an attempt to continue operations that are over and above expenses that would normally be incurred.

Third Party Coverage: Defense Costs and Third Party Damages	
Policy A	**Policy B**
Covers damages, judgments, settlements, and interest that the insured is legally obligated to pay, resulting from a written demand, lawsuit, or regulatory action, alleging • a failure or violation of the security of a computer system or a failure to protect confidential information, • failure to disclose a failure to protect confidential information in violation of disclosure laws, or • violation of any privacy statute. Available Media Policy covers damages and defense costs where insurable by the applicable law for any act, error, omission, negligent supervision of an employee (including the broadcast or distribution) of media content (TV/internet broadcasts, publications) by the insured that results in: • Copyright, trademark, domain name infringement • Plagarism, theft, misappropriation • Invasion of rights of privacy or publicity • Defamation/libel/slander • Trespass, eavesdropping • Infliction of emotional distress • Loss because a third party acts upon or makes a decision based upon the disseminated materials	Covers damages, judgments, settlements, and interest that the insured is legally obligated to pay, resulting from a written demand, lawsuit, alleging: • **Disclosure Injury** (an injury resulting from unauthorized use of confidential information that occurs during the policy period and results from a cyber attack or a hacker). • **Reputational Injury** (injury sustained for disparagement of an organizations products or services, libel, slander, violation of rights of privacy or publicity as a result of the electronic display, transmission, or dissemination of information through the insured's system.) • **Content Injury** (infringement of a trademark, copyright, name of product, service or organization, or the title of an artistic or literary work) • **Conduit Injury** (third party's loss of use of its own system caused by cyber attack) • **Impaired Access Injury** (injury from third party's inability to access the insured's system)