Network Security and Privacy:

Risk Management and Insurance to address Legal Exposures and Financial Statement Protection

2013 Update

by Kevin P. Kalinich
Gobal Practice Leader, Cyber Insurance
Aon Risk Solutions, Aon plc
312.381.4203
kevin.kalinich@aon.com

Contents

Shifting Legal and Regulatory Landscape

> "We ignore the risks that are hardest to measure, even when they pose the greatest threats to our well-being"[1]

Successful businesses increasingly use technology to increase sales, maximize efficiency and reduce expenses. Evolving technologies such as cloud computing, social media, mobile devices and big data analytics have helped entities achieve profits and lift the U.S. stock markets to record heights in the first half of 2013. However, these same businesses face an increasingly diverse and sophisticated array of threats to the security of their information management systems. Cyber theft, fraud, sabotage, espionage, and hacking (including from governments[2]) are more frequent in the social media age and the associated costs with information security breaches are increasing for entities in every industry sector—from Retail, Financial Institutions, Healthcare, Hospitality, Media, Communications, Technology, Consulting and Professional Services to Manufacturing and Transportation[3]. The legal exposure, reputational harm and business interruptions that may result can wreak havoc on a company's bottom line.

The digital revolution raises new cyber risk concerns that can significantly affect an entity's financial statements[4]. Because corporate directors and officers have a fiduciary duty to protect their company's assets—including digital assets themselves as well as the stock prices that may be affected should a breach occur—they have a legal obligation to focus on IT security and risk mitigation matters[5]. Corporate counsel, therefore, are becoming more focused on how to advise their clients' boards on matters relating to data security and other IT-related risks[6]. The next wave of shareholder class action litigation is predicted to be against boards of directors that have not satisfied their duty of care to manage such exposures[7]. As a matter of judicious corporate governance, boards of directors must maintain a reasonable level of oversight[8] since latency, jurisdiction, privacy, data and security obligations can remain the legal burden of the board's entity—even though caused by a third-party outsourced service provider or anonymous hacker.

Paying attention to cyber risks is good business. Responsible corporate leaders will focus on, and devote resources to, effective programs to manage information security matters. They will mitigate their risk by engaging experts to place specialized cyber insurance coverage, with language tailored to address their specific needs and exposures.

New Technologies and Emerging Threats

Corporate leaders continuously seek new technological tools to make their organizations more automated, responsive, and profitable. Technological developments in recent years, such as increased reliance on cloud computing, mobile devices, and social networking, have contributed to the dramatic increase in security risks. Such developments necessitate that each entity develop consistent corporate policies and contractual allocation of liability guidelines as primary risk mitigation measures to the extent possible.

Mobile Devices, Cloud Computing, Big Data and Social Media

Among the technological advances that have contributed to the increased security risks are the countless types of personal tools—USB/thumbdrives, smartphones, tablets, and other devices—that your clients' employees use in connection with their work. These tools were initially developed and enjoyed widespread use before employers focused on the security implications that accompany them. Often, the devices are purchased by the employees themselves, used for both personal and work-related matters, and

1 Nate Silver, "The Signal And The Noise: Why So Many Predictions Fail – But Some Don't," 2012

2 The United States Federal Bureau of Investigation and the U.S. National Security Agency are reportedly tapping directly into servers at major Internet companies to keep track of the communications and interactions of known and suspected foreign terrorists. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html and http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.

3 Breaches spanned multiple countries across a wide variety of industries (March 2013) (http://www2.trustwave.com/rs/trustwave/images/Trustwave_GSR_ExecutiveSummary_4page_Final_Digital.pdf)

4 KPMG Data Loss Barometer 2012 (January 2013) (http://www.kpmg.com/EE/et/IssuesAndInsights/ArticlesPublications/Documents/Data-Loss-Barometer.pdf)

5 Carnegie Mellon University, Governance of Enterprise Security: Cylab 2012 Report: How Boards & Senior Executives Are Managing Cyber Risks, J. Westby, Author, May 16, 2012. http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf

6 Law in the Boardroom: Corporate Board Member/FTI Consulting May 2013 Survey: http://www.fticonsulting.com/global2/media/collateral/united-states/law-in-the-boardroom.pdf. Only a third of corporate general counsel surveyed reported that they felt "very confident" in their clients' ability to respond to a security breach.

7 P. Bessette, M. Biles and T. Highful, King & Spalding LLP, "The Next Big Thing In Securities Litigation," Law360 New York, Feb. 26, 2013: http://www.kslaw.com/imageserver/KSPublic/library/publication/2013articles/2-13Law360BessetteBilesHighful.pdf

8 Steps the C-Suite and Board Can Take to Guard Against Cyber threats: http://deloitte.wsj.com/riskandcompliance/2013/05/07/steps-the-c-suite-and-board-can-take-to-guard-against-cyber-threats/

are not encrypted or tracked in any fashion by the employer's IT department. The security implications are endless—as varied as the seemingly infinite choice of brands, models, and applications available. And because of their widespread use, these devices are considered indispensable by many workers and bringing their use under control can be challenging.

In addition, companies are more frequently outsourcing their computer services to third parties—such as "cloud providers"—as a cost-effective approach for centralized computing and to meet growing data storage demands. Because the users are generally geographically separated (sometimes in different legal jurisdictions) from the cloud providers, the services are accessed via the Internet in the case of a public cloud. The 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. And the cloud providers themselves are vulnerable: a class action lawsuit was filed against cloud provider Dropbox regarding alleged data security issues and failure to notify of a breach.[9] However, a superior cloud provider could actually reduce the overall privacy and security risk of its individual customers due to the implementation of continuously updated state of the art IT security and mitigation procedures (compared to the customer's attempt to maintain its IT security as a non-primary part of its core business). A key consideration with cloud providers may be severity as opposed to frequency due to the aggregation of risk where one breach could affect many customers.

Big data is another technological trend that carries additional risk due to the potential severity of a breach (more data breached = greater potential severity). These enormous accumulations of often unstructured data, sometimes hosted outside a company's IT department, are potentially less secure because they are outside the company's usual controls. The outsourcing contract should ideally include an indemnity clause triggered by the negligence, privacy breach or security incident of the outsourced provider and specifically request evidence of insurance from the outsourced provider in favor of your client to back the indemnity. An added benefit of obtaining evidence of insurance from your client's outsourced provider is that obtaining such insurance would have required that the outsourced provider was scrutinized by an insurance underwriting expert.

The continued popularity of social media brings additional security concerns. While these tools are valuable for recruiting employees, communicating with customers, and compiling marketing data, they also expose companies to potential human relations problems (e.g., harassment claims), privacy violations, false advertising and consumer fraud issues, defamation actions, copyright infringement claims, and the like. By their very nature, social media communications are less formal, and companies tend not to manage these outlets as well as they should.[10] Therefore, lawyers can help clients review their Employee Handbooks and implement a Social Media Policy to ensure employee use of social media is clearly aligned with acceptable company policy and ultimately in accordance with the law.

Cyber Crime, Hacktivism, Cyber Espionage and Cyber Warfare

Attacks upon companies' networks continue to occur with such frequency that no business should consider itself immune. Increasingly creative, invasive, and costly, these attacks can cripple an organization's activities and devastate profits. Businesses in some industries are particularly vulnerable to hacktivism due to the unpopularity of their products or actions with certain groups. For instance, recent hacktivist attacks have targeted energy companies, agribusiness, political parties, media outlets, educational institutions, religious groups, governmental entities, and, ironically, even organizations devoted to cybersecurity.[11] Foreign governments and groups engage in espionage and destruction through electronic means. Cybercriminals continue to enrich themselves through exploiting security weaknesses.

The hacking of The Associated Press' Twitter account in April 2013 caused a fake tweet about the White House being the target of a bomb that injured President Obama, causing the stock market to plunge—a $136 billion drop in the Standard & Poor's 500 Index.[12] A group of international cybercriminals hacked into two credit card processors, India-based EnStage and ElectraCard Services, and withdrew $45 million from two Middle Eastern banks through ATMs in 24 countries in just over 10 hours.[13] Global Payments, Inc., a payments processor, suffered a security breach in the spring of 2012, exposing an estimated 1.5 million Visa and Mastercard accounts and losses in excess of $84 million. Similar reported payment processor breaches include Heartland

9 Wong et al. v. Dropbox Inc., No. 11-CV-3092-LB, complaint filed (N.D. Cal. June 22, 2011).

10 http://www.slideshare.net/jeremiah_owyang/smms-report-010412finaldraft.

11 Verizon 2013 Data Breach Investigations Report: http://www.verizonenterprise.com/DBIR/2013/

12 J. Weisenthal and S. Ro, "AP Just Got Hacked And A Fake Tweet Caused The Stock Market To Tank," Business Insider, 23 Apr 2013. http://www.businessinsider.com/ap-tweet-on-white-house-2013-4#ixzz2WJq7OhFk

13 B. Browdie, "Card Processors Attacked in 45 Million Bank Heist Identified," American Banker, May 13, 2013. http://www.americanbanker.com/issues/178_91/card-processors-attacked-in-45-million-dollar-bank-heist-identified-1059040-1.html?zkPrintable=1&nopagination=1

14 Cyber Liability & Data Breach Insurance Claims: A 2012 Study of Actual Payouts for Covered Data Breaches http://www.netdiligence.com/files/CyberClaimsStudy-2012sh.pdf

Payment Systems ($143 million) and RBS Worldpay. Losses are not limited to payment processors. According to publicly filed documents, TJX suffered a $256 million breach and SONY suffered a breach estimated to cost a total of between $171 million—$280 million and counting. Some prudent businesses purchased specific insurance to address these types of privacy and security incidents.[14] However, many entities have ended up in litigation with their insurer with respect to whether traditional legacy policies are intended to cover losses from evovling intangible network security and privacy exposures.[15]

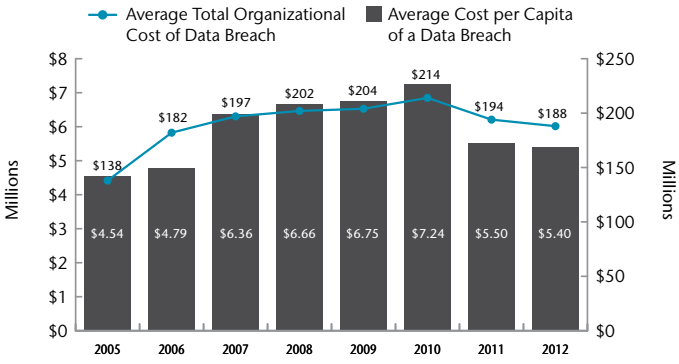
A great deal of attention has recently been devoted to the existence of programs allowing the US government, specifically the National Security Administration (NSA), to access certain data for national security purposes through its PRISM program. Many questions remain about what information was shared, how it was shared, and how it may have been used, but it is no longer a secret that information about individuals' internet and phone use is being requested, gathered, used, and shared. Leading Internet related entities seek more government transparency, but deny that officials were given unfettered access to their systems. As governments' tools become more and more sophisticated, the potential for overreach seems greater. Companies will continue to grapple with their competing obligations to their governments versus their customers and employees.

Several large technology firms, as well as financial institutions and even defense contractors, have acknowledged that their source code has been stolen, presumably to expedite future attacks by those same hackers. It is suspected that hackers based in China have engaged in widespread cyberespionage for both political and economic gain, and to determine whether their own spies have been discovered. And Google was recently able to stop what appeared to be a series of attempts to hack Iranians' Google accounts to initiate a phishing campaign designed to influence the Presidential election in favor of current President Mahmoud Ahmadenejad.[16] Similar technology-enhanced cyber exposure issues are developing in Turkey, Egypt and Brazil.

Costs of Security Breaches Continue to Increase

Year after year, the costs incurred by companies experiencing data breaches continues to climb.[17] The most recent analysis, the 2013 Ponemon Cost of Data Breach Study,[18] released in May 2013, evaluated a range of business costs relating to data breaches. Globally, the average cost of a single data breach is estimated to be $136 per record in 2012 (up from $130 per record in 2011). In the United States, the cost per record compromised dropped only slightly, from $194 in 2011 to $188 in 2012. Moreover, the annualized cost of cybercrime increased by 6% per year for the 56 companies in an analogous study, with each spending from $1.4 million to $46 million annually.[19]

Financial Statement Impact of a Data Breach[20]



*A portion of the "cost" in this study - abornomal churn post-breach - uninsurable in Cyber policies

*Study excludes data breaches in excess of 100,000 records

15 State National Insurance claims no responsibility to pay for Global Payments' breach costs: http://www.databreaches.net/?p=27378; Zurich American Insurance Co. vs. Sony Corp. of America Case: http://zra.com/attachments/article/73/zurich.pdf;

16 "Google finds Iranians hacked on election eve :Web giant calls attacks 'email-based phishing' attempts as election campaign is wound up," Aljazeera, 13 June 2013. http://www.aljazeera.com/news/middleeast/2013/06/201361310354844266 6.html

17 Empirical Analysis of Data Breach Litigation: http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf

18 Ponemon Institute, 2013 Cost of Data Breach Study, May 2013, http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-global-report-2013.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach

19 Ponemon Institute, 2012 Cost of Cyber Crime Study: United States, October 2012, http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

20 2013 Cost of a Data Breach Study: Ponemon Institute Research Report, May 2013.

21 SEC and CFTC Adopt Identity Theft Red Flag Rules: http://www.stroock.com/SiteFiles/Pub1339.pdf

Impact of Recent Legal and Regulatory Developments

Lawmakers, regulators, and courts throughout the US and abroad continue to try to keep pace with both technological advances and rapidly evolving security hazards.[21] These governmental leaders then must balance the need to protect their individual constituents from privacy violations and other harms while not placing such extraordinary burdens on businesses that it hampers technological progress. What results from these disjointed efforts is a patchwork of laws, regulations, and industry standards establishing rules that vary dramatically from country to country, from one state to the next, between industries, and often depends upon the precise type of information involved. Businesses are challenged with having to stay abreast of the data security requirements for not only the jurisdictions in which they are located, but virtually anywhere in the world where they do business, have customers, or even where their data may be transmitted by third parties.

A few recent developments are worth mentioning. New privacy bills being introduced around the globe, such as Europe's proposed updated data privacy protection directive could give consumers the right to withhold basic information while using the Internet, stalling the marketing efforts of social media savvy entities. Penalties for violations of the proposed EU law are high, potentially reaching as much as 2% of an entity's worldwide revenue.[22] The UK, Australia, Canada, India, Russia and China, as well as many other nations, are also in an ongoing process of developing information security laws and regulations.[23]

In September 2011, the U.S. Securities and Exchange Commission issued disclosure guidance advising public companies to disclose "material" cybersecurity risks.[24] As a result, many of the largest public corporations now include data security information in their Form 10-K risk factor disclosures. In some instances, SEC Comment Letters have noted companies' failure to include adequate risk factors related to cybersecurity matters. Without question, inadequate disclosures can lead to expensive and time-consuming legal or administrative actions. The costs of legal fees in such cases can far exceed the costs of disclosure. Corporate communications relating to cybersecurity should be vetted carefully, with information reported accurately, factually, and only by those authorized to do so in the appropriate manner. While the SEC will not require companies to disclose details that could hinder an entity's cybersecurity efforts, material breaches must be reported. It is likely that the SEC will eventually chose to initiate formal investigations, using the agency's subpoena power to obtain breach records from third party providers. Even more troubling is the prospect of securities class action litigation relating to security breaches or the possibility of derivative lawsuits by shareholders alleging that the corporate directors failed to take adequate security measures.[25]

The U.S. Federal Trade Commission (FTC) is also getting into the action. The FTC, in recent years, has asserted its power to enforce companies' obligations to adequately protect consumer information from hackers. While most companies settle with the FTC, Wyndham is fighting back by challenging whether the FTC can sue an entity for lax data security practices. The FTC's lawsuit against Wyndham alleges that the hotel chain failed to protect customer credit card information in three breaches between 2008 and 2010, which resulted in $10.6 million in losses, including fraudulent charges on the stolen credit card accounts. The case will test whether the FTC has the power to compel companies to provide a minimal level of security to protect consumers' personal information.

22 Hacking threat, tougher data laws promise insurance boom: http://www.businessinsurance.com/article/20130620/NEWS07/130629989?tags=%7C299%7C76%7C303%7C335

23 2013 International Compendium of Data Privacy Laws: http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf

24 Division of Corporate Finance, SEC, CF Disclosure Guidance: Topic No. 2: Cybersecurity, 13 Oct. 2011. http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

25 P. Bessette, M. Biles and T. Highful, King & Spalding LLP, "The Next Big Thing In Securities Litigation," Law360 New York, Feb. 26, 2013: http://www.kslaw.com/imageserver/KSPublic/library/publication/2013articles/2-13Law360BessetteBilesHighful.pdf

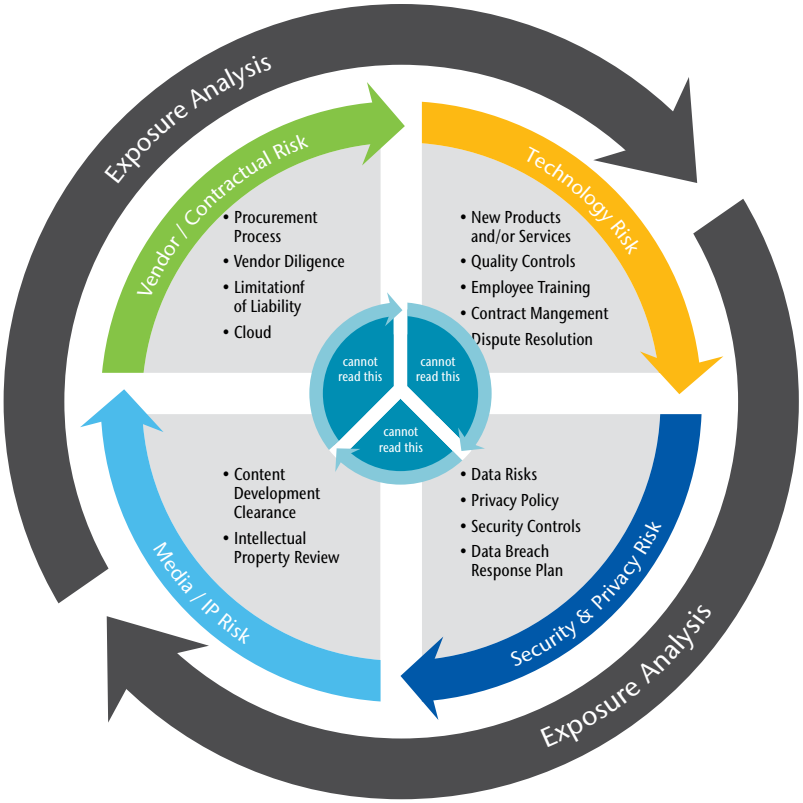
26 http://one.aon.com/shifting-landscape-cybercrime

The Role of Corporate Counsel

Lawyers advising corporate clients on sophisticated data security matters understand that breaches do occur and the stakes can be high. While proactive measures to mitigate risk can be costly and time-consuming, they are far less demanding than the consequences of a serious breach, which can require dealing with a seemingly endless list of critics, including the client's General Counsel, the Board of Directors, the SEC, the FTC, prosecutors, politicians, customers, patients, students, aggrieved employees, shareholders, plaintiffs' class-action lawyers, the media, and the public. Moreover, having a robust, well-documented program to monitor security matters may provide favorable evidence of the company's efforts, thus reducing liability should an incident occur. A network security and privacy risk mitigation program should start with the following:[26]

- Identify, classify and quantify the use of information assets & electronic methodologies, including reliance on third party outsourced service providers
- Implement risk management best practices, such as IT security, corporate policies & procedures and contractual allocation of liability
- Train and monitor employees, subcontractors, parties and others regarding such best practices
- Model the range of potential frequency and severity of losses from network security and privacy incidents for your unique industry and entity specific circumstances
- Determine the entity's risk appetite to retain, mitigate and transfer network security and privacy exposures compared to the entity's overall enterprise risk management
- Analyze existing insurance policies for possible partial network security and privacy exposures coverage
- Consider customized network security and privacy insurance to stabilize the entity's financial statements and mitigate the risk of breach of fiduciary of management and the board of directors

Network Security and Privacy Liability Discovery Process



27 Cybersecurity: The Corporate Counsel's Agenda: http://www.hoganlovells.com/custom/eDocs/Cybersecurity%20Advisory_Pearson_11152012.pdf

Lawyers can play a proactive role in assisting their clients with risk mitigation and risk transfer. Capable legal advice can not only prevent or limit information security breaches, but risk management advice can mitigate the most adverse consequences of such breaches. In this regard, lawyers may wish to consider the following tips when advising their clients. [27]

Comprehensive Cybersecurity Program

In light of the increased significance of cybersecurity matters, it is essential that corporations develop a comprehensive program. A team consisting of IT, legal, risk management, CIO, security, human resources, product development, sales, marketing and other pertinent personnel should be involved in developing and executing the program. Corporate counsel should advise clients on the source and scope of their data security and privacy obligations. Different industries in different jurisdictions may have widely varying obligations, and the first step is to determine the client's compliance responsibilities under applicable laws and regulations.

An effective cybersecurity program will not be static, but rather will be subjected to regular reevaluation and improvement. Changes in the company's business may require modifications to the program. Virtually every corporate transaction should be evaluated for potential cybersecurity implications. For example, should an acquisition occur, the cybersecurity situation of the acquired entity should be made a priority in the due diligence process, and necessary improvements may be required to bring the acquired company in line with the security standards of the acquiring company.

Once a program is developed, it is essential that it be well-documented, so that it can be used as evidence of good faith should a breach occur.

Thorough Review of IT Use Policies

Advise clients to audit and regularly review their reliance on different forms of technology (i.e. pcs, smartphones, iPads, USBs) and ensure that various uses of such technology (i.e. work, social media, personal use) are appropriately regulated in company IT and/or Social Media policies and guidelines. In particular, the increased use of mobile devices carries security risks for corporate networks. Data breaches caused by smartphones are becoming more common than lost or stolen laptops.[28] Lawyers should advise their clients to expand existing corporate Data Security and Privacy Use policies to address these new exposures.

Third Party Exposures

Businesses may take great care in protecting their own electronic systems, but utterly fail to take into account the vulnerabilities in the systems of the various third parties with whom they share confidential information. Vendors, suppliers, consultants, IT providers, and a range of other third parties have occasion to access various types of confidential corporate information. A number of steps can mitigate the exposure in these situations.

Vendor/Supplier Management[29]

Once a client's third party providers have been identified, counsel should guide the client's IT Security Risk Management Department in taking steps to protect against unauthorized access, use and disclosure of confidential information by these third parties. A risk assessment should be conducted for each third party provider and, depending on the type of data being shared, additional steps should be considered to prevent security breaches: The more sensitive the information being shared, the more thorough the steps to be taken.

Initially, counsel should advise their clients to undertake an evaluation of the vendor's privacy and security infrastructure. A team of IT, risk management, and legal professionals should consider the third party provider's policies, practices, security procedures, and oversight. For example, lawyers can assist their clients in obtaining detailed information from vendors, such as 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. Lawyers can recommend that multiple client departments should coordinate to 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 encryption is possible, whether customers must be notified that their information will be stored in a cloud, whether the cloud provider has its own adequate insurance coverage (possibly requesting that your client be named as an "Additional Insured"), and whether some information is simply too sensitive to turn over to a third party.

28 http://www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011. http://ag.ca.gov/cms_attachments/press/pdfs/n2630_updated_mobile_apps_info.pdf. http://www.itu.int/ITU-D/ict/facts/2001/material/ICTFactsFigures2011.pdf

29 Contracting in a World of Data Breaches and Insecurity: Managing Third-Party Vendor Engagements: http://lexisnexis.com/in-house-advisory/fullArticle.aspx?Bid=62741

30 Corporate Board Member and FTI Consulting, 2012 Law and the Boardroom Study: Legal Risks on the Radar, 13 Aug. 2012. http://www,fticonsulting.com/global2/critical-thinking/reports/legal-risks-on-the-radar.aspx (reporting that "for the first time, data security was earmarked by the largest percentage of responding directors (48%) and

Third party providers that are found to have lax security procedures should be replaced or given a relatively short period of time to bring their practices within acceptable standards. Counsel should ensure that clients recognize the enhanced risk of continuing to share information with third parties who are not committed to the same level of security as the client organization.

Contractual Considerations, Including Allocation of Liability

Corporate counsel should assist clients with mitigating cyber exposures by developing consistent contractual language to be used in vendor agreements. Third parties should, at a minimum, be expected to accept inclusion of language in which they warrant that they are in compliance with applicable laws relating to information privacy and security. Clients should also expect that third party providers will commit contractually to follow the client organization's privacy policies. Depending upon the type of information to be shared, contracts may also include specific provisions outlining the vendor's security procedures which require the vendor to conduct regular risk assessments and report to the client. In some situations, it may be useful to specify that the client has the right to engage an outside firm to audit the service provider's security infrastructure. In all cases, contracts should contain a clear requirement that any security breach be reported to the client immediately upon discovery.

Many third party contracts contain indemnification provisions which commit the third party providers to indemnify the client should a security breach occur due to the vendor's negligence or intentional act. Where possible, such indemnification should be sought, and should be as broad as possible, including all direct and indirect costs associated with a breach. Clients should inquire about, and perhaps insist upon, third party providers maintaining adequate levels of cyber insurance to cover the cost of potential breaches. Where such coverage is required, clients may wish to require that the client be named as an "Additional Insured" on such policies. It may also be advisable to specify that disputes be resolved through arbitration rather than litigation in the courts, given the sensitivity of some of the information involved.

Vendor/Supplier Audits

Corporate counsel may discover that corporate clients may be unaware of which vendors and suppliers have access to their confidential data, such as personally-identifiable information on customers and employees, or proprietary information about the company's products. The first step in implementing a system to manage this exposure is to first identify the various suppliers and vendors and to determine precisely which type of information each third party entity is being sent (or otherwise accessing). A robust audit is essential. These audits should examine not only the outsourced IT service providers, such as data processors, but also any other type of third party organization or individual who might have access to corporate data. The audits should be conducted regularly and systematically so that both existing and all new third party providers are tracked and monitored. For each provider identified, careful consideration should be given to whether the level of access is appropriate and necessary in light of the service being provided or whether more limited disclosure may be warranted to avoid exposing data unnecessarily.

Client Education on Legal Exposures

Corporate counsel has an important role in educating clients about the evolving legal exposures for both companies and individuals in the area of cybersecurity. Fortunately, corporate leaders now recognize data protection as a top concern.[30]

Coordinated Approach in Law Enforcement or National Security Matters

Corporations may be asked to share information with law enforcement or national security agencies. It is essential that the appropriate corporate personnel be assigned to oversee these interactions so that the company's legal obligations are satisfied without unnecessarily risking disclosure of confidential company data. Legal oversight is essential, as these issues often require an extremely sophisticated and difficult balancing of competing legal obligations. There is also an argument that, in the event of a security or privacy incident, legal counsel, rather than the risk manager or insurance broker, should engage forensics, investigative and other third party experts to enable attorney-client privilege protection.

Data Breach Management Policy

Counsel should consider the benefits of implementing a Data Breach Management Policy to address and outline internal corporate prevention, detection and incident response processes in response to a security breach. It could help in defending an allegation that the company failed to take reasonable care in handling a data security breach.

general counsel (55%) as an issue of concern").

31 Tips For Maximizing the Value of Insurance Assets: http://www.metrocorpcounsel.com/pdf/2013/June/09.pdf

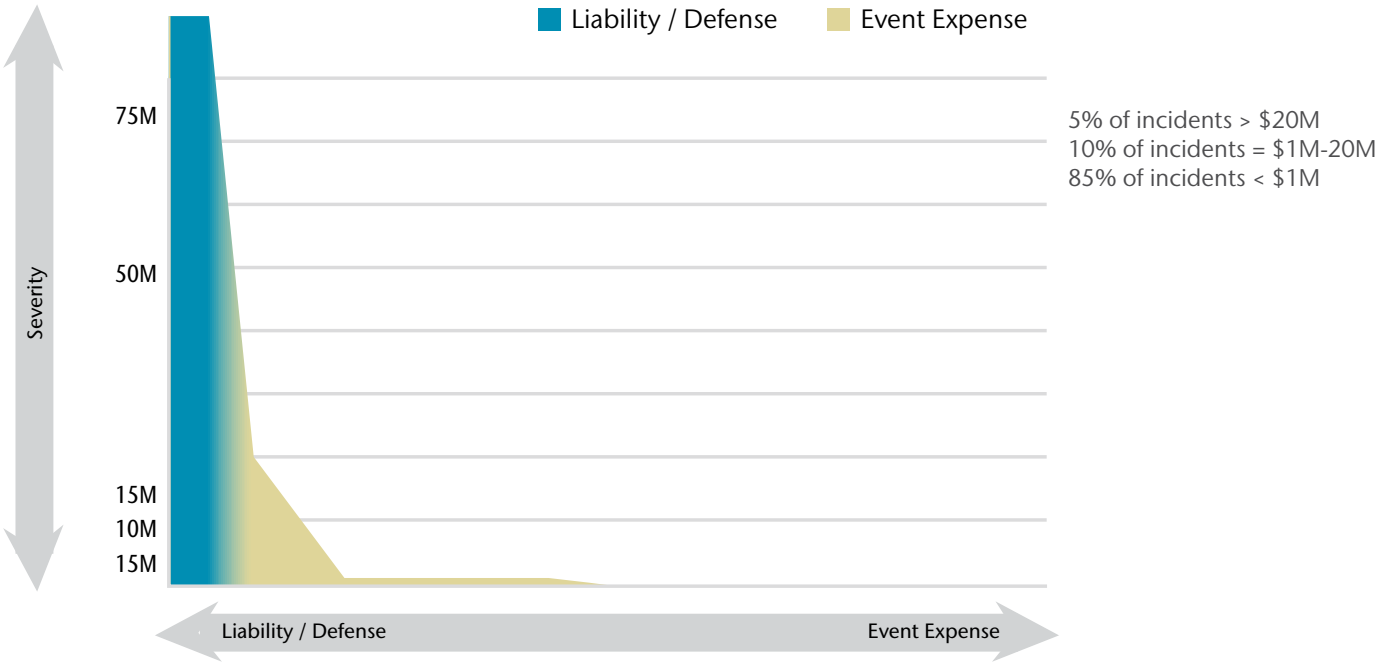
32 Zurich Am. Ins. Co. et al. v. Sony Corporation of America, et al., Case No. 65198, filed 20 July 2011 (N.Y. Sup. Ct.), https://iapps.courts.state.ny.us/fbem/DocumentDisplaySe

The first step in creating such a policy is defining a "breach." Everyone understands that when criminals hack into a company's network that a security breach has occurred. However, a security breach occurs virtually every time an employee loses a cell phone or has a laptop stolen. A useful policy must define what a breach is, and set forth a process designed to respond effectively to each specific incident based on the specific circumstances of the breach and the precise nature of the information compromised. Different measures are required depending on the sensitivity of the information involved. Failure to respond promptly, effectively, and in compliance with applicable laws can expose a business to material liability. Furthermore, insurance underwriters assume that nearly every entity will suffer some type of security or privacy incident at one time or another and reducing the impact of a breach is essential. Therefore, insurance underwriters focus almost as much on the robust data breach incident response policy as all of the prevention measures.

Network Security and Privacy Insurance

Work with your client's insurance broker to analyze property and general liability insurance policies and determine any potential gaps in existing coverage. Your client should consider specific network security and privacy insurance to fill any obvious gaps.[31]

Cyber Maximum Probable Loss Curve



Source:

rvlet?documentId=tirVQewp3WujFno1EgNuTA==&system=prod (Zurich sought declaratory judgment that it has no duty to defend or indemnify Sony against class actions relating to hacking of 100 million PlayStation customers under the primary commercial general liability and excess liability policies because, Zurich asserts, the customers'

Transferring Risk Through Cyber Risk Insurance

Insurance specifically designed to cover the unique exposures of data privacy and security can act as a backstop to protect a business from the financial statement harm resulting from a breach. While there is an argument that some cyber risks could be covered under traditional insurance policies, such as Property (e.g. business interruption from a computer hack) or Commercial General Liability (e.g. third party data privacy breach litigation), it is wise to consider specialized cyber risk insurance coverage in order to comprehensively cover network security risks.

Traditional policies were developed years ago and typically do not contemplate exposures such as those discussed in this paper. While some categories of losses might be covered under standard policies, many gaps usually exist. In the US, insurers are filing declaratory judgment actions against their insureds to deny coverage for cyber exposures under Property, General Liability, Professional Liability and Crime policies.[32] Some courts are finding that these traditional policies, such as property policies, do not cover the types of intangible harm that results from data breaches.[33] Coverage may also be denied if intentional acts are excluded from coverage.[34]

Insurers are also denying coverage under professional liability/ Errors & Omissions[35] and Directors & Officers' policies, with mixed outcomes in the courts.[36] With these other types of non-cyber specific insurance policies, the outcome of a coverage dispute is far from certain, and will turn on the precise policy language, the specific circumstances of the claim, the identity of the victim, the nature of the harm caused, and the court's willingness to find coverage where policy language appears to preclude it. For example, in Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797 (8th Cir. 2010), the Court of Appeals for the Eighth Circuit concluded that coverage existed despite the insurer's fairly persuasive claims to the contrary. Eyeblaster, the insured, an online marketing company, was sued for allegedly causing the plaintiff's computer to malfunction due to spyware attached to Eyeblaster's online advertising. Eyeblaster submitted a claim to its insurer, but the claim was denied. The insurer asserted that since the policy covered only "tangible property," and excluded losses resulting from "software, data or other information that is in electronic form," it was not covered. The insurer also denied coverage under the Errors & Omissions policy on the grounds that the plaintiff had failed to allege a wrongful act by the insured, since the policy defined a wrongful act as an error, unintentional omission, or negligent act in connection with a product failure. The court disagreed, finding that coverage existed under both policies. The General Liability policy was held to cover damage for the loss of the plaintiff's computer, which was tangible property. The E&O policy provided coverage because "error," defined as including "intentional, non-negligent acts but to exclude intentional wrongful conduct," would include actions such as the insured's causing of software to be installed on the plaintiff's computer. Though intentional, Eyeblaster had disclosed to the insurer that its core business was online advertising, so its actions in causing software to be installed on the plaintiff's computer was not an intentional wrongful act because it was in the ordinary course of its business. In a case decided May 23, 2013, The Illinois Supreme Court held that

claims are not covered by the "bodily injury," "property damage," or "personal and advertising injury" provisions in the policies); Arch Ins. Co. v. Michaels Stores, Inc., Case No. 1:12-CV-00786, filed 23 Feb. 2012 (N.D. Ill.) (Arch sought declaratory judgment that the general liability policy it sold to Michaels Stores does not require coverage for customer data stolen by tampering with PIN pad terminals. Arch cites the electronic data and breach of contract exclusions , and also claims that the customers' suits do not claim property damage, bodily injury, or advertising injury, as the policy requires; the case appears to be near settlement on undisclosed terms); Retail Ventures Inc./ DSW Inc. v. Nat. Union Fire Ins. Co. of Pittsburgh, PA, 691 F.3d 821 (6th Cir. 2012) (Insurer sought to avoid coverage under crime policy for losses caused by hacker who stole credit card data, but the Sixth Circuit disagreed, holding that third-party losses were covered despite requirement that loss be "resulting directly from" theft, and that exclusion for loss of "confidential information of any kind" would not preclude coverage for theft of credit card information because to allow that result would vitiate the coverage the policy intended).

33 Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., No. X07CV095031734, 2012 Conn. Super. LEXIS 227, filed 17 Jan. 2012 (Conn. Super. Ct.) (The insured, a third party provider of distribution services for IBM, lost data tapes containing personal data on 500,000 IBM employees, and sought coverage under its general liability and umbrella policies; the Court denied coverage because IBM sought damages for the lost electronic data, not the tapes themselves, and the policy defined covered property as only tangible property). See also Union Pump Co. v. Centrifugal Tech., Inc., Case No. 05-0287, 2009 LEXIS 86352 (W.D. La, 18 Sept. 2009) (CGL policy which covered only "tangible property" held not to cover electronic data including design drawings and models).

34 Union Pump Co. v. Centrifugal Tech., Inc., Case No. 05-0287, 2009 LEXIS 86352 (W.D. La, 18 Sept. 2009) (CGL policy held not to cover claims that insured had used and destroyed plaintiff's data due to intentional act exclusion).

35 State National Insurance claims no responsibility to pay for Global Payments' breach costs: http://www.databreaches.net/?p=27378

36 Compare United Westlabs, Inc. v. Greenwich Ins. Co., Case No. 09C-12-048 MMJ, 2001 De. Super. LEXIS 261 (Del. Super., June 13, 2011), aff'd, Case No. 337, 2011, 2012 Del. LEXIS 130 (Feb. 28, 2012) (policy intended to cover cyber and technology held not to cover lawsuit initiated prior to policy period involving continuous series of related acts) and Tagged, Inc. v. Scottsdale Ins. Co., Case No. JFM-11-127, 2011 U.S.Dist. LEXIS 75262 (S.D.N.Y., May 27, 2011) (dismissing declaratory judgment action and finding no coverage based on professional services exclusion in the D&O Coverage Section of policy issued by Scottsdale to Tagged, a social networking site targeted to teenage users, because the site falsely advertised that it had features in place to remove sexually explicit and predatory content and conduct from its website) with St. Paul Fire and Marine Ins. Co. v. Compaq Computer Corp., 539 F3d 809 (8th Cir. 2008) (technology E&O policy covered "error," which as defined included insured's alleged unintentional selling of defective computers). Another case involving an E&O policy remains pending. See Vonage Holdings Corp. v. Hartford Fire Ins. Co., Civ. No. 11-6187 (U.S. Dist. Ct. N.J. 2012) (Vonage suffered loss over $1M due to server hacking but insurer denied coverage because losses were not tangible property; case remains pending).

37 Standard Mutual Insurance Company v. Lay, 2013 IL 114617 (Ill 2013).

38 See also Owners Ins. Co., v. European Auto Works, Inc., 2012 WL 4052406 (8th Cir. Sept. 17, 2012) http://caselaw.findlaw.com/us-8th-circuit/1612035.html (Eighth Circuit required insurer to cover insured's $2 million settlement in a junk fax class action); and Landmark Amer. Ins. Co., v. Gulf Coast Analytical Labs, 2012 U.S. LEXIS 45184

claims based on alleged violations of the Telephone Consumer Protection Act are covered under a traditional general liability policy.[37]

Similarly, in Retail Ventures[38], the Sixth Circuit found third-party coverage under a first party commercial crime policy despite language stating that only direct losses would be covered. However, clients should not take comfort from the Sixth and Eighth Circuits decisions in Eyeblaster and Retail Ventures, because both cases are far from clear and are limited to the unique facts involved in the claims at issue. In light of the high stakes involved, a cyber policy which clearly covers first and third party, non-tangible losses is the prudent choice.

The onus is upon the company to seek coverage for potential risks to its electronic data. While the world's data is expected to grow 50-fold in the next decade and information assets are now considered to account for a majority of the value of Fortune 1000 entities, non-life insurance premiums are estimated to be $667 billion,[39] while total cyberinsurance premiums are estimated at $1.3 billion[40]—a small fraction of the total non-life insurance market. As mentioned above, the prudent board will consider directing its management to:

1 Qualify and quantify its cyberexposures, including the potential effect upon the balance sheet.[41] Management must "buy-in" and support the Network Security and Privacy team in order to ensure its success.

2 Mitigate cyberexposures, including due diligence and contractual allocation.[42] Note that insurance underwriters will rely on third party security assessments when conducting due diligence to quote a premium and coverage for cyber insurance.[43] Updates to written policies and procedures with ongoing training assists in creating a culture of best practices.

3 Conduct actuarial modelling to determine whether to assume and/or transfer such risks

"Cyber" exposures have the potential to affect the entire spectrum of risks—from physical property that is vulnerable to attacks from "Stuxnet" like computer viruses, to products that contain chips with embedded software, to degradation or complete failure of critical infrastructure stakeholders.[44] As a result, cyber events have the ability to impact numerous lines of insurance coverage.[45] Consider some of the issues related to insurance coverage afforded under traditional policies of insurance and under cyber polices for a cyber event. Insurers are stakeholders because their coverage obligations may be triggered under various policies of insurance after an accident, disaster, cyber event or the cataclysmic meltdown of national critical infrastructures. Insurers can help manage cyber risks and offer insurance coverage for losses and claims arising from cyber events. However, not all risks or claims are covered and some insurers are limiting or excluding coverage afforded under traditional policies, and even some cyber policies may have narrow tailored coverages. Thus, all insurance policies and coverages should be thoroughly reviewed and the provisions and conditions for coverage should be understood by all parties to the insurance contract.

The majority of developments to date on the cyber risk transfer front relate to privacy or data breach risk, and specifically, breaches of Personally Identifiable Information ("PII"). Many breached entities and other responsible parties have been aided tremendously by their insurance policies.[46] Privacy, however, is only a fraction of the entire cyber spectrum, and companies that

(Louisiana) (Court denied summary judgment for insurer where a different company's data had been corrupted).

39 Industry communication group, The Insurance Information Institute Inc.

40 Betterley Risk Consultants Inc.

41 "We ignore the risks that are hardest to measure, even when they pose the greatest threats to our well-being." Nate Silver, The Signal And The Noise: Why so many Predictions Fail – But Some Don't.

42 A Checklist for Corporate Directors and the C-Suite: Data Privacy and Security Oversight: http://www.networkedlawyers.com/a-checklist-for-corporate-directors-and-the-c-suite-data-privacy-and-security-oversight/

43 ISO 27001 is the Litmus test for information security: http://blogs.computerworld.com/saas/21379/iso-27001-%E2%80%93-litmus-test-information-security

44 The Department of Commerce has described cybersecurity insurance as a potentially "effective, market-driven way of increasing cybersecurity" because it may help reduce the number of successful cyber attacks by promoting widespread adoption of preventative measures; encouraging the implementation of best practices by basing premiums on an insured's level of self-protection; and limiting the level of losses that companies face following a cyber attack. http://www.dhs.gov/publication/cybersecurity-insurance

45 The Securities and Exchange Commission requires public companies to report to its shareholders any "material losses" from cyber attacks, plus any information, "a reasonable investor would consider important to an investment decision." SEC guidance promulgated October 13, 2011 (not mandatory) suggests that such disclosure include the impact of cyber insurance coverage.

46 2012 Cyber Liability & Data Breach Insurance Claims: A Study of Actual Payouts for Covered Data Breaches: http://netdiligence.com/files/CyberClaimsStudy-2012sh.pdf

47 Betterley Report; Cyber Privacy Insurance Market Survey June 2013, http://betterley.com/samples/cpims12_nt.pdf

48 http://www3.ambest.com/bestweek/bestweekreports.asp?rt=ir

49 U.S. Department of Homeland Security National Protection and Programs Directorate Cybersecurity Insurance Workshop: Defining Challenges to Today's Cybersecurity

are not consumer facing or do not participate in the PII chain are struggling with the insurability of their cyber risk. Consider also that while annual cyber premiums may exceed $1B on an annual basis[47], annual commercial property and general liability premiums are in excess of $151 billion[48]. Defined cyber premiums account for a mere 1/151th of P & C risk transfer and 1/667th of non-life premiums in an economy where more businesses put a higher value on intangible assets than on traditional assets like plant, property, equipment and inventory.

The insurance industry has been slow to embrace this evolving reality to provide true end-to-end solutions that provide confidence to policyholders that the majority of cyber risk is covered. The insurance industry can serve as a catalyst and facilitator to significantly improve cyber security solutions.[49]

Cyber Exposure Spectrum

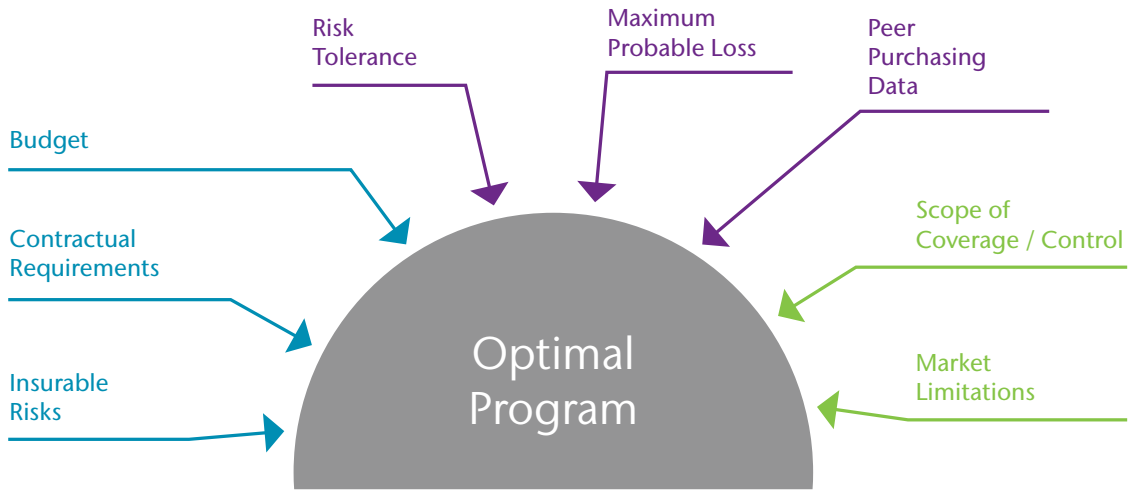
1 **First Party Financial Loss**—The party that experienced the cyber event suffers financial losses or costs associated with the event. The most commonly cited examples include costs associated with data breach response, lost income attributable to network/IT interruption, as well as future lost income and reputational harm. Note that you want your first party business interuption trigger to kick-in upon partial degradation and not simply total outage.

2 **Third Party Financial Loss**—A party other than that which experienced the cyber event suffers financial losses or costs associated with the event. This could be a customer, business partner, or unrelated third party. Examples of losses in this category include the business interruption losses of users of cloud services should such services suffer outages, or recall costs of clients of electronic component manufacturers should such components malfunction due to the failure of embedded code and not any tangible damage.

3 **First Party Bodily Injury or Property Damage**—The party that experienced the cyber event suffers bodily injury or property damage.

4 **Third Party Bodily Injury or Property Damage**—A party other than that which experienced the cyber event suffers bodily injury or property damage.

Optimal Cyber Program



Source:

http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf

50 Cyber Risk Insurance – Navigating the Application Process: http://www.sah.com/NewsAndEvents/View/1AFCBA99-5056-9125-63918F3AD79A2940/

51 Top Tem Tips For Buying Cyber Insurance: http://www.acc.com/legalresources/publications/topten/tttfcbcsic.cfm; http://www.pillsburylaw.com/publications/10-tips-for-buying-cyber-insurance

Cyber Risk Transfer World as We Know It

1 **Privacy Breach Coverage—**Policies cover privacy breach notification and crisis management, regulatory defense and civil penalties, and liability resulting from a breach. Limits up to $300 million+ are available.

   a. Premiums are fact specific depending upon deductible/self-insured retention, losses, revenue, scope of business and risk mitigation employed

      i. Small and Middle Market Companies = $5K-$10K/million of limits

      ii. Large Companies = $10K-$50K/million of limits

   b. Deductibles/Self-Insured Retentions

      i. SMB = $5K-$100K

      ii. Large Companies = $250K-$10 MM+

   c. Limits

      i. SMB = $25K-$5MM

      ii. Large Companies = $1 MM-$100 MM+

   d. Application Process becoming streamlined whereby multiple carriers will quote pricing, terms and conditions based on one common application.[50] However, it is well advised to jointly develop with each unique client a comprehensive list of specific priority coverage grants and dictate such requests to the insurance carriers in the form of a submission priority coverage matrix.

   e. Policy wording is paramount to successful coverage.[51]

2 **Ancillary Financial Loss Products—**Most available policies include first party network business interruption—to cover loss of revenue during network interruption; information asset—to cover restoration costs or loss of value associated with electronic data; cyber extortion—to pay an extortion threat if doing so successfully wards off a cyber event; and Contingent Business Interruption—to cover loss of revenue during the downtime of a critical outsourced IT provider (i.e. cloud services, etc).

3 **Future Loss of Revenue Products—**Currently developing coverage with limits around $100M when the event ends and the firm returns to normal operations, but the negative reputational effect from the cyber event produces customer churn and a diminished ability to increase sales.

4 Property, Comprehensive General Liability ("CGL"), Crime/Bond, Director's & Officers, Professional Liability and Kidnap & Ransom, insurers should also be notified in the event of a cyber incident. Review the "Notice" section of each potentially applicable insurance policy to ensure compliance with the timing, form and content of proper notice. Failure to properly notify pursuant to the terms of each policy could result in insurance carriers attempting to deny an otherwise covered claim.

Beyond these four areas of risk transfer, coverage is either unavailable entirely, uncertain[52], or unavailable in a quantity that matches the magnitude of the risk. The most concerning area is likely coverage for cyber resultant bodily injury and property damage risks given exclusions found in policies designed to cover those risks—which are intended to exclude claims related to the loss or destruction of electronic data. However, the manner in which such exclusions are construed presents the possibility that they could be used to deny coverage for a loss that originated from a cyber attack or virus. Consider the following exclusion, which is typically inserted in both property and general liability insurance policies:

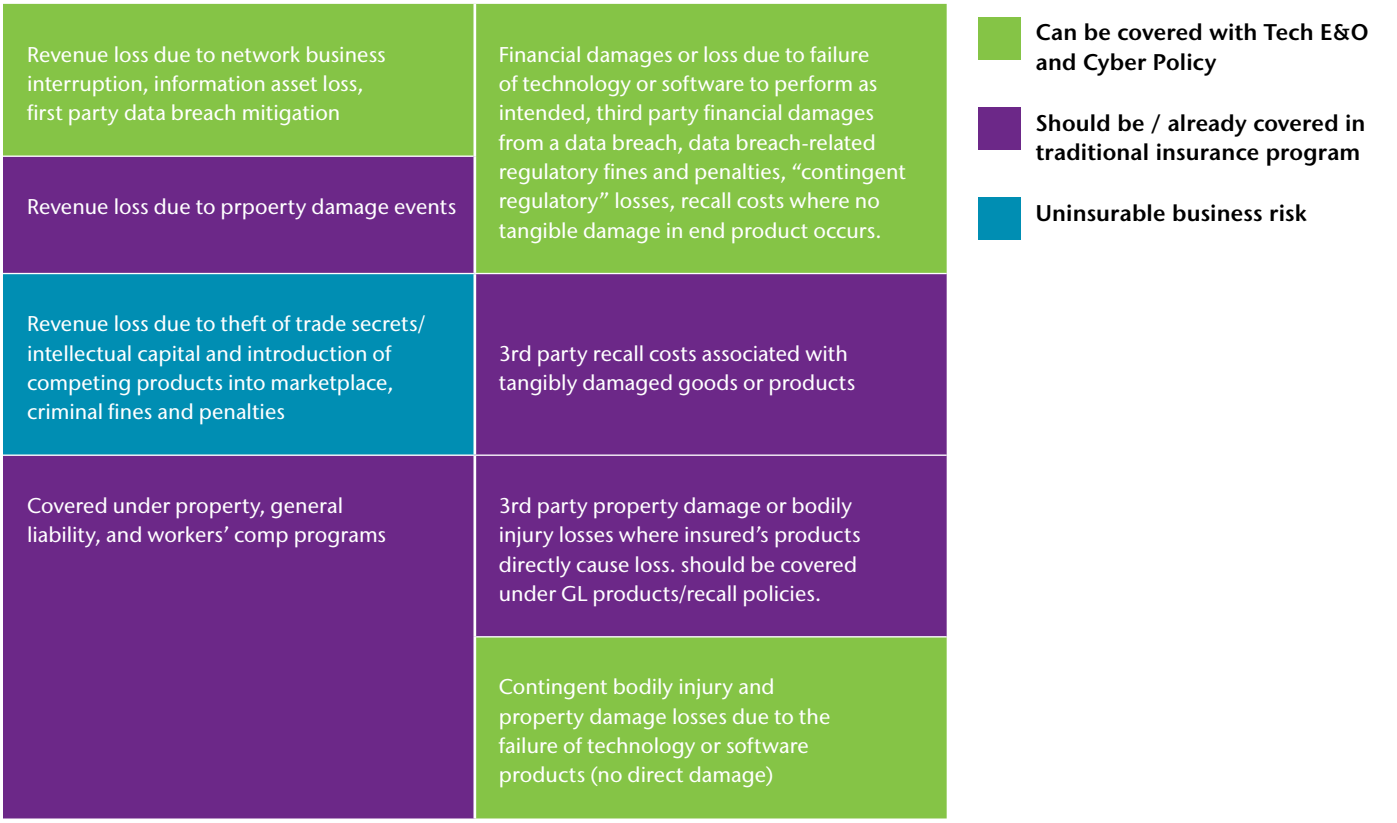
Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

Based on the defined cyber policies that are available and uncertainty surrounding traditional coverage, the representation of cyber insurability as it currently exists is as follows:

52 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 a battle 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. 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 considered weak protection for covering security breaches. A copy of the Complaint for Declaratory Judgment can be found online at https://iapps.courts.state.ny.us/fbem/DocumentDisplayServlet?documentId=tirVQewp3WujFno1EgNuTA==&system=prod.

53 Similar declaratory judgment general liability insurance 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). See Arch Ins. Co. v. Michaels Stores, Inc., No. 12-0786 (N.D. Ill., Feb. 3, 2012); 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?12945444616052-L_1_0-1. In its case against Michaels Stores,

Cyber Insurability as it Currently Exists



Source:

This has resulted in vastly disparate cyber insurance purchasing trends. Consumer facing industries have led the charge (mainly specific to "privacy" coverage), and various estimates put adoption rates between 20%-60% for certain segments—financial, healthcare, retail, and hospitality. Beyond those industries, uptake is more limited. Business-to-business firms (predominantly technology centric[53]) that participate in the PII chain can blend cyber coverage into a commercial errors and omissions policy to contemplate a large percentage of the risks, but such firms continue to struggle to identify their exposures and the related insurability. For firms that do not fit this classification, buying drops off precipitously—and while knowing that their cyber exposures are significant, companies in industries such as manufacturing, industrial, and critical infrastructure are struggling with the available products as well as the debatable nature of their existing coverage.

Another significant problem is limits sufficiency, which is not high enough to provide catastrophic coverage levels required by large firms involved in critical infrastructure.

While underwriting for privacy and related financial loss products is good (and usually under one roof), know-how and consistency for more traditional products drops off significantly. This dynamic is further exacerbated by the silo approach at many insurers whereby the "cyber" underwriters don't interact

54 Arch Insurance 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.

with their counterparts in other divisions. This ultimately results in everything ranging from flat out cyber exclusions to shaky coverage extensions and attempted clarifications to responses from traditional underwriters that "you need a cyber policy for that"—when the fundamental nature of the risk should fall within the boundaries of traditional property and general liability policies (i.e. the yellow areas of the risk quadrant above).

The Future of Cyber Insurance

$1 billion (or more) of "Cyber Complete" coverage is being developed, which would span the entire spectrum of exposure as identified above, except for areas that are difficult to insure (or entirely uninsurable) such as criminal fines/penalties and the theft of trade secrets and intellectual capital. Coverage would be structured as catastrophic protection with substantial retentions (equivalent or greater to those taken on property programs), but firms would maintain the ability to infill such retentions with smaller policies for privacy breach mitigation, defense costs and any other areas where stand-alone policies can be structured.

Given the size of the program we anticipate that a syndicated structure (in the large property model) could work best, with each insurer or re-insurer sharing proportionally in loss from the ground up. As for the rest of the dynamics required in order to create this structure:

1 **Underwriting Approach and Expertise—**We envision an approach similar to what various top insurers deploy in the property world—engineers that evaluate/assist clients with risk and that just happen to offer insurance. In this case the approach would involve top IT professionals with expertise tied to the various domains of the underwriting framework as further described below. We believe that this is critically important in order for the participating insurance carriers to gain confidence that risks are being evenly and expertly evaluated, and that the baseline evolves in accordance with the constantly changing nature of the cyber world.

2 **Underwriting and Policy Compliance Framework—**The underwriting and policy compliance framework needs to be Enterprise-Wide and inclusive of both physical and IT security. This will allow for a far better and more comprehensive analysis; rather than focusing on granular elements such as firewalls and anti-virus software, the approach needs to evaluate critical domains such as Enterprise Assets, Cyber Governance, External Threats, Internal Threats, Regulatory Compliance, and Event Preparedness. The framework needs to constantly evolve based on the changing threat climate; this will not be a standard that is instantly outdated and one that gives firms the ability to achieve minimum compliance and "check the box." Additionally and as further described below, the framework will form the basis for dynamic interaction between insurers and policyholders.

3 **Link to Reputational Risk—**It is important that the framework needs to tie to, and therefore evaluate the reputational profile of the Insured. Our research shows that firms with outstanding reputational rankings that suffer significant cyber events will recover far more quickly and effectively than firms that rank poorly.

4 **Information Sharing and Dynamic Interaction—**We believe that the insurance industry sits on a treasure trove of information that, if used appropriately with the right precautions, could be utilized for the benefit of all parties involved. Numerous insurers underwrite the cyber risk of firms across all industries and see claim activity in close to real time and have more insight into the macro cyber climate than most security providers who generally focus on narrow verticals. This data should be used to evolve the framework and by establishing certain compliance thresholds, policyholders would be incented to continually improve their security posture in order to maintain coverage. Prior to the 2013 Executive Order on improving critical infrastructure[54], there was no industry-wide information sharing mechanism and most insurers do not interact with their insureds until subsequent policy renewals.[55]

55 In Hartford's declaratory judgment actions against Crate & Barrel and The Childrens Place stores, the insurer claims that it has no duty to defend the stores against Song-Beverly claims ("Pineda-type" lawsuits) 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 centre, etc.) costs related to the breach.

56 The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, provides limitations on liability and damages for claims against sellers of anti-terrorism technologies arising out of the use of anti-terrorism technologies, contingent on having liability insurance.

57 http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

58 The federal government can increase the supply of cyber-insurance by providing reinsurance to cyber-insurance companies for a limited time. This would increase the adoption of cyber-insurance by reducing prices, with price reduction caused both by decreased supply cost and increased competition in the cyber-insurance market. Precedent for this action may be found in the Terrorism Risk Insurance Act of 2002, which for a limited period provides compensation for insurers who suffer sufficiently

Given the exposures and constantly evolving risks associated with cyber events that could cripple companies, industries and critical infrastructures, prudent insureds should review their insurance program with their insurance producer and seek out professionals who understand the cyber insurance market before those catastrophic cyber events take place. Relying on traditional insurance to protect against cyber events is wishful thinking. Due diligence and due consideration should be undertaken so that all companies can understand the insurance coverage they have and just as importantly, understand what cyber insurance coverage they deliberately decided not to purchase for their cyber liability risk management program. Additionally, the financial strength of the insurers should be considered because in the event that multiple critical infrastructures are taken down, an insurer may be have to pay too many or a number of large claims that may impact its surplus and impede its ability to pay all claims. A competent insurance producer can help companies understand the options and alternatives for cyber insurance thereby giving the insured the proper information to make an educated decision as to what type and how much insurance will be in place for the next big cyber catastrophe.

large losses resulting from designated acts of terrorism, subject to recoupment through risk-spreading premiums on other insurance products.

Contact Information

Kevin P. Kalinich, J.D.
Global Practice Leader – Cyber Insurance
Aon plc
kevin.kalinich@aon.com

#13342 – 10/2013

Risk. Reinsurance. Human Resources.

Empower Results®