California Business Law
PRACTITIONER

Volume 30 / Number 4 Fall 2015

Shifting Standards: The Changing Fiduciary Landscape for Broker-Dealers and Investment Advisers

John D. Vaughn
Peter Z. Stockburger

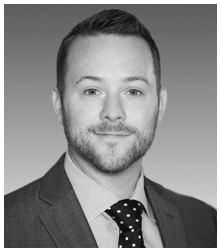
"If you would understand anything, observe its beginning and its development."
Aristotle (4th Century BCE)

Introduction

Each year, millions of Americans seek the help of financial professionals such as investment advisers and broker-dealers to help them make critical investment decisions. In turn, these financial professionals help investors understand the volatile market, navigate complicated financial products, and, ultimately, plan their future. The regulatory regime governing the provision of this advice is therefore of critical importance.

—continued on page 103

John D. Vaughn, of Perez Vaughn & Feasby Law, has a diverse national trial and arbitration practice representing clients in complex commercial litigation matters, securities fraud claims, FINRA arbitration, FINRA/SEC investigations, employment disputes, suitability claims and broker disciplinary actions, injunction cases, unfair business practices, and trade secret cases. He was formerly a litigation partner with Luce Forward Hamilton & Scripps LLP and then McKenna Long & Aldridge LLP, where he founded and chaired the firm's FINRA/SEC Dispute Resolution Practice Group. He received his J.D. degree from Santa Clara University, where he was a member of the Law Review.



Peter Z. Stockburger is a Managing Associate at Dentons, where he specializes in global labor and employment law. He is an adjunct professor at the University of San Diego School of Law, where he teaches appellate advocacy and public international law, and is currently serving as a "Virtual Fellow" with the State Department, advising on various international labor issues. He was recognized as a 2015 "Rising Star" by Southern California Super Lawyers. He received his B.A., magna cum laude, from Texas State University and his J.D., cum laude, from the University of San Diego School of Law, where he was admitted to the National Order of the Barristers.

IN THIS ISSUE

CEB® ceb.com
CONTINUING EDUCATION OF THE BAR ■ CALIFORNIA

Reprinted from the *California Business Law Practitioner* published by Continuing Education of the Bar – California.
The citation from this article is 30 CEB Cal Bus L Prac (Fall 2015).

Cyber Insurance:
An Overview of an Evolving Coverage

Russell Cohen
Alison Roffi

Russell Cohen is a litigation partner at Orrick, Herrington and Sutcliffe, LLP, San Francisco, where he focuses on cybersecurity, antitrust, and other commercial disputes, particularly in the technology sector. He is a member of Orrick's Cybersecurity & Data Privacy Group, advising clients on cybersecurity planning and response efforts, including cyber insurance. Exclusively on behalf of policyholders, he has pursued claims and litigated complex insurance disputes to recover for cyber attacks and other losses. He speaks regularly in the U.S. and Canada on cyber risk and cyber insurance and has been identified as a Benchmark Litigation "Future Star." He received his undergraduate degree from McGill University and his law degree from Osgoode Hall Law School, Toronto.

Alison Roffi is a Senior Associate at Orrick, Herrington and Sutcliffe, LLP, New York, where her practice focuses on insurance recovery disputes and commercial litigation. She is experienced in matters involving general and excess liability, first party/business interruption, and directors and officers coverage. She is on the editorial board of Orrick's insurance recovery blog, the Policyholder Insider, and writes frequently on policy issues and legal developments relevant to policyholders. She received her undergraduate degree from Skidmore College and her law degree from Boston College Law School.

INTRODUCTION

Cyber insurance has reached a tipping point. The rising costs faced by data breach victims, which can exceed $100 million for the largest breaches, have spurred an increasing number of companies across industries to turn to cyber insurance in an effort to transfer at least some of those costs to an insurer. But cyber insurance is still relatively new, at least as a mass-market insurance product, and it is evolving quickly, although not as quickly as the threat itself. The policies are complex and not standardized, and courts have yet to provide any guidance about what will be covered and what will not. This state of affairs leaves many companies that have or are considering buying cyber insurance uncertain—not only whether they will be a victim of a data breach but also whether insurance will provide them with the coverage they need if they do become a victim.

Data breaches and cyberattacks occur across all sectors. In the past year there have been highly publicized mega-breaches of technology companies, entertainment companies, retailers, financial services companies, health insurers, manufacturers, and the federal government's Office of Personnel Management. Even the most sophisticated systems are vulnerable to a data breach. And companies with any potential exposure—which includes any company that maintains employee information—are increasingly looking to cyber insurance as one way to manage the cost of a data breach.

This article provides an overview of cyber insurance. The first section (What Is Cyber Insurance?) describes the risks faced by companies and the coverage offered by cyber insurance. The second section (The Development of Cyber Insurance) describes the development of cyber insurance as a specialized coverage, the impact on cyber insurance development of breach notification laws, and the limits of coverage of existing insurance. The third section (Moving Forward) discusses the key coverage and exclusion battlegrounds in these policies, the emergence of cyber insurance litigation, and the challenges presented by the Internet of Things.

WHAT IS CYBER INSURANCE?

The Costs of a Data Breach

Data breaches impose significant costs on victim companies. These costs can include reputational costs, loss of intellectual property, and a diversion of human resources. They can also include large out-of-pocket costs paid to various third-party vendors. Trac-

ing the path of a typical data breach serves to illustrate the scope of these costs.

Many data breaches are discovered only after the fact, when signs of suspicious network activity are uncovered. In the first wave, computer forensic experts will be called in to capture images of the potentially compromised servers, conduct "root cause" investigations, and secure and restore systems. Attorneys will be retained to oversee and direct the investigation, provide legal advice regarding potential liability, and advise on compliance with laws requiring notification of regulators and affected individuals. Customer communication and retention programs will be rolled out in an effort to minimize the potential impact. Disclosure of the data breach will often prompt lawsuits—class actions or other claims by those whose data may have been accessed—as well as investigations by state attorneys general and other regulators. In addition, for organizations that accept payment cards, payment card industry (PCI) requirements impose additional forensic investigation costs, reporting requirements, and potential fines and penalties. All of these activities can take place simultaneously, across multiple domestic and international jurisdictions, requiring coordination of large forensic, legal, public relations, and other teams.

Costs are affected by the cause of the data breach. Data breaches can be caused by different factors, but malicious attacks are increasingly responsible for the greatest number of incidents and are the most expensive. In 2014, failures in business processes and information technology systems were responsible for 29 percent of data breaches. Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis (May 2015) (Ponemon Report), at 10, available at http://www-03.ibm.com/security/data-breach/. Human error, resulting from employee or contractor negligence, was responsible for 25 percent of data breaches. Ponemon Report at 10. Malicious attacks, which are typically caused by outside hackers or disgruntled insiders, were responsible for the lion's share of data breaches in 2014: 47 percent. Ponemon Report at 10.

This means that, in addition to taking steps to minimize equipment failure and human error, companies must also prepare their defenses against a motivated adversary who is using increasingly sophisticated and constantly adapting means. These malicious attacks are the most costly, with one study estimating the cost to a U.S. company of $230 per compromised record. Ponemon Report at 12. The average cost for a company that has been attacked is in the millions, with the largest, most high-profile breaches exceeding $200 million. See, *e.g.*, Target Corp., Form 8-K Current Report (Feb. 25, 2015).

Cyber Insurance Coverage

Cyber insurance obviously will not prevent a data breach. Rather, it is intended to mitigate the extraordinary costs of a data breach by transferring those costs to an insurer in exchange for payment of a more predictable premium. But cyber insurance—at least as a mass-market product—is still relatively new. Product offerings lack uniformity and contain many conditions and exclusions. There are no standard forms for cyber insurance policies, and many offer coverage on an à la carte basis, giving companies the opportunity to buy coverage for one exposure (*e.g.*, privacy notification costs) but not another (*e.g.*, network interruption coverage). Because every company in every industry may face a different exposure—with some more vulnerable to human error and others targeted more often for malicious attacks—there is no "one size fits all" approach to cyber insurance. Each company must therefore find a product that matches its unique risk profile—a risk profile that may be in flux and is difficult to quantify. The result is a complex mélange of coverages, exclusions, and conditions that must be carefully reviewed to ensure that they address the most prevalent risks in a comprehensive way.

Generally, cyber policies include coverage for costs incurred in responding to a data breach, loss resulting from claims arising from the breach, and the costs of responding to regulatory investigations and proceedings. But these policies do not cover several important exposures, such as reduction in a company's market capitalization, reputational loss, loss of economic value of intellectual property, and loss of staff time and focus. The most commonly purchased cyber coverage includes four basic coverage types: (1) remediation costs for response to the breach, (2) liability for loss or breach of data, (3) fines or penalties imposed by law or regulation, and (4) additional payment card industry (PCI) fines and penalties. Betterly, The Betterly Report: Cyber/Privacy Insurance Market Survey (2015) (Betterly Report), at 9, available at http://betterley.com/samples/cpims15_nt.pdf. Remediation costs include data breach response costs such as forensic and legal investigations, public relations, customer notification, credit monitoring, and data re-securing costs. Betterly Report, at 9. Liability coverage includes defense and judgment or settlement costs for the liability of the insured arising out of its failure to properly maintain personal or corporate data. Betterly Report, at 9. Regulatory fines and penalties coverage include costs associated with

investigating, defending, and paying or settling regulatory investigations. Betterly Report, at 9. Finally, PCI fines and penalties include forensic services investigating noncompliance with payment card industry standards. Betterly Report, at 9.

Remediation Coverage and Risk Management Services

All cyber insurance policies provide remediation or data breach coverage, which typically covers the costs of a forensic investigation, crisis management, notification, credit monitoring, and resecuring data. This coverage includes the third-party costs associated with identifying the cause of a data breach and its scope and restoring services, typically performed by a computer forensics firm; the costs of assessing legal liability and notification obligations for individuals or companies whose data may have been accessed, typically carried out by attorneys; the development of a communications plan intended to minimize adverse impacts on the company, typically managed by a public relations or crisis communications firm; and the offering of credit insurance or identity theft protection. Remediation coverage often includes sub-limits (*i.e.*, caps on total coverage) that are significantly less than the overall policy limits and other notification and vendor-approval conditions that must be carefully reviewed and scrupulously followed.

Some insurers offer policyholders a network of data breach and response specialists and may even require the use of certain vendors. Using these preferred vendors may be advantageous for organizations that do not have experience in this field or preexisting relationships with vendors—and will minimize disputes between a policyholder and insurer, particularly regarding the fees that will be reimbursed. However, such an arrangement or requirement may limit policyholders from choosing their own preferred vendor or one that offers a particular expertise. Policyholders must carefully consider the costs and benefits of these types of arrangements. Finally, insurers increasingly provide risk management services, including risk avoidance services, pre-breach planning, data breach helplines, and information portals.

Third-Party Network Security and Privacy Liability Coverage

All cyber insurance policies provide coverage for claims arising from a breach of network security or an insured's privacy violation. These claims—generally, class actions—for negligence, breach of contract, and statutory violations are brought by individuals whose personally identifiable information, or companies whose nonpublic data, may have been accessed. In addition, there is coverage for claims that third parties may have been damaged by a virus or other malware transmitted from the insured's network. Since much of an organization's data may reside and be processed outside an organization's walls, *e.g.*, by a cloud computing service provider, insureds must ensure that cyber policies cover a data breach or other event occurring wherever a company's data resides, including at their service provider. Many policies now define the insured to include the independent contractors and business associates (*i.e.*, outsourcers or vendors) who process the insured's data.

Regulatory Investigations, Fines, and Penalties

Most cyber insurance policies offer coverage for responding to and defending against regulatory investigations and proceedings, brought under privacy or other related laws or regulations, as well as for any assessed fines or penalties. These investigations can be costly, requiring extensive document and information production, can carry significant potential consequences, and can require the assistance of experienced counsel.

Other Coverage Modules

In addition to these basic coverages, cyber insurance policies typically offer, on an à la carte basis, optional coverages. For example, media liability coverage insures against claims for unauthorized use of advertising materials, copyright, trademark, trade name, trade dress, service mark, service name, libel, slander, defamation, disparagement, trade libel, and plagiarism arising from an insured's online advertising and other media activities. It does not cover patent infringement. Cyber extortion coverage provides for the payment of a ransom in response to certain threats to an insured, including threats to disclose or destroy data. Coverage can also be obtained for the costs to replace, restore, and re-collect digital assets, as well as any business interruption caused by a data breach, denial of service, or other act preventing network operations. Finally, some insurers offer cyberterrorism and cyberespionage coverage for state-sponsored or terrorist attacks.

Exclusions

Like all insurance policies, cyber policies contain numerous exclusions that can greatly limit the value of the coverage being provided. Many policies exclude dishonest, fraudulent, criminal, and malicious acts. Often these exclusions are limited to senior executives and severability is afforded. Intentional acts

are also often excluded. But many data breaches occur with the assistance of "rogue" employees, and policies often carve out these employees from the exclusion or limit the exclusion to senior executives.

Most policies exclude bodily injury, but there are occasional carve backs for claims related to mental anguish and emotional distress. See, *e.g.*, ACE Privacy Protection Privacy and Network Liability Insurance Policy ("bodily injury does not mean mental injury, mental anguish, mental tension, emotional distress, pain and suffering, or shock resulting from a [w]rongful [a]ct for which coverage is provided"), retrieved August 17, 2015 from http://www.acegroup.com/us-en/assets/ace-privacy-protection-declaration-policy-specimen.pdf. Direct property damage is also typically an exclusion, as is loss of use of property.

Contractual liability is also commonly excluded. However, liability that would have attached without a contract (*i.e.*, on account of a tort, negligence, or breach of an obligation to maintain confidentiality of personally identifiable nonpublic information or third-party corporate information) is typically carved out of the exclusion, as is a claim for violation of a privacy policy or nondisclosure agreement. See, *e.g.*, AIG CyberEdge PC insurance policy ("this exclusion shall not apply . . . with respect to a privacy event, any liability or obligation under the confidentiality or nondisclosure provisions of any agreement"), retrieved August 17, 2015 from http://www.aig.com/Chartis/internet/US/en/CyberEdge%20PC%20Policy%20Final%202014_tcm3171–595897.pdf.

Other exclusions relate to acts occurring prior to the inception of the policy. These exclusions are especially important for cyber policies because a system breach and compromise may have occurred without detection. And some policies exclude acts of war or terrorism.

A final important category of exclusions relates to failure by the insured to maintain minimum data security requirements. See discussion of *Columbia Casualty Co.,* below.

Conditions

Cyber policies contain numerous conditions for obtaining coverage. The most significant relate to prompt notice of incidents, prior approval of vendors, and choice of counsel.

THE DEVELOPMENT OF CYBER INSURANCE

A History of Cyber Insurance

Cyber insurance was first offered during the 1970s through information and communication technology liability insurance. In the 1980s and 1990s, cyber insurance became available to banks and blue-chip companies. Although more insurers began offering cyber products, few insureds made claims. The turn of the millennium marked the beginning of today's cyber insurance market. With Y2K, organizations became more aware of cyber vulnerabilities and their potential costs. At the same time, insurers began excluding cyber-related events from general liability policies.

State notification laws have been one of the key drivers of the growth of cyber insurance. Notification laws mandate communication to individuals when their personal information is accessed in a breach. Notification laws typically have provisions regarding who must comply with the law, what constitutes a breach, which parties must be notified and the requirements for notice, *i.e.*, electronic, mail, or media publication. California enacted the first mandatory breach notification law in 2003 (see CC §§1798.29, 1798.81.5–1798.84), and since then 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted their own statutory requirements.

Notification is costly. It must be given in every state in which an individual whose data has been accessed resides, and different states have different notification triggers. As a result, forensic work is required to ascertain the scope of any data access, legal counsel is required to advise on the notification requirements, and public relations or crisis communications firms are required to manage the communications. These costs have driven an increase in demand for cyber insurance.

Litigation and the Role of Non-Cyber Policies

Insurance industry resistance to providing coverage for cyber events under traditional insurance (*i.e.*, policies covering general liability, property damage, or crimes) has also accelerated cyber insurance adoption. There have been a handful of high-profile cases addressing whether a cyber incident is covered under these policies. Although courts have reached varying conclusions, insurance industry practice in resisting cyber claims under traditional policies and the devel-

opment of standard form exclusions have made pursuing cyber coverage very costly.

Commercial General Liability (CGL) insurance is an obvious candidate for covering certain costs related to a data breach. CGL policies are issued to businesses to protect them against liability from, among other things, personal and advertising injury, which includes claims relating to the publication of an individual's private information. But insurers have fought off claims for coverage of data breach class actions notwithstanding that the class actions typically include allegations that an insured negligently permitted attackers to access the confidential information of its customers.

In a recent case, *Recall Total Information Mgmt., Inc. v Federal Ins. Co.* (Conn App 2014) 83 A3d 664, 672, aff'd (Conn S Ct 2015) 115 A3d 458, the Connecticut appellate and supreme courts held that there was no coverage under the insured's CGL policy for costs incurred by the insured in connection with the loss of computer tapes containing IBM employees' personally identifiable information. The policy in that case provided coverage for "personal injury," described as "injury, other than bodily injury, property damage or advertising injury, caused by an offense of ... electronic, oral, written or other *publication* of material that ... violates a person's right to privacy." 83 A3d at 672. The courts determined that the personal injury clause presupposes publication of the information on the tapes and rejected the argument that loss of the tapes themselves equated to publication.

Whether the accessing of data by attackers amounts to a "publication" by the insured has been a recurring issue, with some cases finding no publication and other cases reaching a different result. See, *e.g., Zurich Am. Ins. Co. v Sony Corp.* (NY S Ct, Feb. 21, 2014, No. 651982/2011) 2014 NY Misc Lexis 5141) (finding no publication); *Owners Ins. Co. v European Auto Works, Inc.* (8th Cir 2012) 695 F3d 814, 820 (finding that plain meaning of "publication" is broad enough to include dissemination of fax advertisements); *Columbia Cas. Co. v HIAR Holding, L.L.C.* (Mo 2013) 411 SW3d 258, 269 (finding coverage).

Further, in May 2014, a set of new standard-form Insurance Services Office (ISO) exclusions were introduced into CGL policies. The exclusions broadened an earlier electronic data exclusion and aimed to bar all coverage for cyberattack-related liabilities. They bar coverage for damages "arising out of any access to or disclosure of any person's or organization's confidential or personal information." There are several variations of the exclusions, including one that applies to both bodily injury and property damage liability and personal and advertising injury liability; one that contains a limited exception related to bodily injury; and one that applies only to personal and advertising injury.

Similarly, attempts to recover for data breaches under property insurance policies have been challenged by insurers. Courts are inconsistent in their interpretation of coverage for cyber-related incidents under property insurance policies. Some courts have held that the term "property damage" connotes tangible property, thus damage to computer software and data are not covered. For example, in *American Online, Inc. v St. Paul Mercury Ins. Co.* (4th Cir 2003) 347 F3d 89, the Fourth Circuit defined physical property as "having physical substance apparent to the senses," and excluded software and data damage from the definition. 347 F3d at 95. Other cases, however, have reached a different result. See, *e.g.*, *NMS Servs. Inc. v The Hartford* (4th Cir 2003) 62 Fed Appx 511 (finding coverage for hacking attack); *Lambrecht & Assoc. v State Farm Lloyds* (Tex App 2003) 119 SW3d 16 (finding coverage).

MOVING FORWARD

Will Cyber Policies Provide the Promised Coverage?

The cyber insurance market is in a rapid growth phase. Unsurprisingly, the authors' experience has been that insurers are paying claims rather than contesting coverage, but there may be signs that is beginning to change.

A recent lawsuit filed in California by Columbia Casualty Company (Columbia) sought to deny coverage to its insured, Cottage Health System, based on a cyber insurance policy exclusion. *Columbia Cas. Co. v Cottage Healthcare Sys.* (CD Cal, July 17, 2015, No. 2:15-cv-03432) 2015 US Dist Lexis 93456. Cottage, which operates a network of hospitals in California, reached a $4.125 million settlement in a class-action suit arising from the disclosure of electronic medical records. The claimants alleged that Cottage or its third-party vendor, INSYNC Computer Solution, Inc., stored medical records on a system that was fully accessible from the Internet without having installed security measures to protect the patient information. Cottage was insured under Columbia's "NetProtect360" liability policy, which purported to provide coverage for data breaches. Columbia initially agreed to cover the cost of Cottage's settlement under a reservation of rights, but later sued for a declaration that the coverage was void, seeking to recoup the $4.125 million.

Specifically, Columbia claimed that Cottage triggered an exclusion barring coverage for a data breach claim arising out of any "failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application for this Insurance and all related information submitted to the Insurer in conjunction with such application whether orally or in writing." Complaint for Declaratory Judgment and Reimbursement of Defense and Settlement Costs, filed May 7, 2015 in the U.S. District Court for the Central District of California, Case No. 2:15-cv-03432-DDP-AGR (Columbia Complaint), at 6. Columbia contended that when Cottage applied for a NetProtect360 policy, it incorrectly checked the "yes" box in response to vague questions such as "[D]o you . . . contractually require . . . 3rd parties to protect this information with safeguards at least as good as your own?" (Columbia Complaint, at 8) and "Do you have a way to detect unauthorized access or attempts to access sensitive information?" (Columbia Complaint, at 9). These questions were part of a "Risk Control Self-Assessment" contained in the application. The case was dismissed on procedural grounds and it is not yet known whether any court will uphold broad exclusions for an insured's failure to maintain minimum data security requirements.

In another sign of activity in this area, in *Travelers Cas. & Surety Co. v Ignition Studio, Inc.* (ND Ill, filed Jan. 21, 2015, No. 1:15-cv-00608) (unpublished), the insurer sought to recover from a third party for amounts it paid under its cyber policy. The Travelers complaint alleged that its insured, Alpine Bank, hired Ignition Studio, Inc. to design and service the bank's website. Travelers alleged that Ignition negligently designed and maintained the website, allowing hackers to access the site through the server on which it was hosted. Alpine spent over $150,000 complying with its data breach notification obligations, for which it was reimbursed by Travelers. Travelers, as Alpine Bank's assignee and subrogee, sought to recover that amount from Ignition. In April 2015, Travelers settled with the web design company according to a stipulation filed in Illinois federal court.

It remains to be seen whether companies can expect more aggressive activity on the part of insurers to challenge coverage and press for recovery of payments made under these policies.

New and Emerging Risks

Another developing area with significant potential impact on cyber insurance relates to the so-called Internet of Things. Internet-connected devices provide a great benefit to, and have the potential to transform, our daily lives, but they also carry with them added security risks. See FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World* (Jan. 2015). One such risk is that a cyberattack involving Internet-connected devices will not just result in the unauthorized disclosure of personal or confidential information, but could also result in tangible physical harm, such as property damage or bodily injury.

The most famous example is the use of a computer virus, Stuxnet, to weaken Iran's nuclear facilities. More recent examples include attacks on a control system at a German steel mill (see http://www.wired.com/2015/01/german-steel-mill-hack-destruction/) and research targeting connected vehicles (see http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/). Unlike the financial costs of a typical data breach, these types of exposures could give rise to massive property damage and bodily injury claims.

Although coverage for liability for bodily injury or property damage is typically provided in CGL policies, cyber-related attacks may trigger coverage exclusions. And most cyber policies exclude coverage for bodily injury and property damage claims, although a few insurers offer cyber policies that cover property damage or bodily injury resulting from a cyberattack. This is a newly emerging risk that has the potential to eclipse the massive cyber losses we have seen to date.

CONCLUSION

Cyber insurance is one component in a larger risk-management program. It is evolving fast in response to an even more rapidly evolving threat landscape, and more companies across all industries are relying on it to transfer some portion of their cyber risk. But for now, these policies are nonstandard and complex and contain exclusions and conditions that must be carefully reviewed. The only thing worse for a company than becoming a victim of a data breach is paying for insurance but not getting the coverage it paid for when it needs it most.

The authors gratefully acknowledge and thank Nina Travato for her assistance in preparation of this article.