When Attorneys General Attack

Cybersecurity Investigations and Related Insurance Coverage Issues

By Joseph D. Jean, Brian E. Finch, Carolina A. Fornos, Sheila M. Harvey and Benjamin D. Tievsky

Are criminal cyberattacks increasing in sophistication and frequency? Yes.

Is every company, in every industry, that collects or stores sensitive customer, employee, or business data vulnerable to cyberattacks? Yes.

Has there been an increase in cyberattacks that interrupt a company's ability to conduct business? Yes.

Can a victim of a cyberattack, or even a potential victim, also become the target of a government investigation and face fines and other penalties? Yes.

Can these investigations extend to whether a company's cybersecurity programs are "reasonable," even with respect to software or products they sell? Yes.

Is there insurance coverage? Maybe.

Introduction

Government agencies, including law enforcement officials, have made their intentions loud and clear: they will undertake proactive and reactive measures against private businesses to "ensure" better cybersecurity. This holds true even in cases where the company is the *victim* of a cyberattack. It sometimes seems that, as far as government officials are concerned, if a company suffers a cyberattack or is vulnerable to one it is because the company, not the criminal, has done something wrong.

While companies in all industries may be subject to such investigations, government officials are increasingly targeting publicly traded companies that are subject to certain cyber disclosure requirements. Other targets include companies whose operations are potentially vulnerable to a cyberattack, whose resulting disruption could pose personal and property risks to the public or sow financial chaos in the economy. Examples of potential targets include brokerage firms that store customers' personal financial

information and health care providers and employers that store massive amounts of private medical and other data. Critical infrastructure owners and operators are also thought to be vulnerable to the type of attack that brought down Ukraine's power grid earlier this year, also putting them in the crosshairs of regulators.[1] As cyber-crime becomes even more sophisticated and prevalent, investigation and enforcement priorities will only broaden.

This Client Alert discusses some of the types of investigations undertaken by government and industry regulators, what you can do to manage and minimize exposure to such investigations, and related insurance coverage issues.

State AG and Federal Investigations

Given the variety of consumer protection, financial fraud, privacy, and other concerns that are implicated by cyber-crime, it is not surprising that state attorneys general, federal prosecutors and a wide array of other agencies and regulators investigate cybersecurity-related issues as preventative (but also seemingly punitive) measures.

State attorneys general and federal prosecutors have demonstrated an interest in aggressively investigating network security issues. For example, in 2014, California's Attorney General launched an investigation focused on whether Kaiser Foundation Health Plan took too long to notify thousands of current and former employees that their personal information had been compromised in a data breach.[2] The findings of California's AG led it to bring suit against Kaiser.

Similarly, Connecticut's Attorney General sought information pertaining to hackers' breach of point-of-sale keypad card terminals at Barnes & Noble stores. The Connecticut AG requested detailed information on how the breach occurred, what steps the company took to protect affected customers, and whether and how the company had implemented enhanced security procedures on a going-forward basis.[3]

Attorneys general may coordinate with various others regulators that conduct their own investigations, including the U.S. Securities and Exchange Commission (SEC), the U.S. Commodity Futures Trading Commission (CFTC), the Federal Trade Commission (FTC) and the Financial Industry Regulatory Authority (FINRA). The SEC, CFTC, and FINRA (the latter of which is not a government agency, but an industry membership-run regulator) have indicated that they are focused on protecting investors' personal information, monitoring the public disclosure of cyber-risk, and preventing the theft of non-public information that can be used for illegal market manipulation and insider trading. The FTC has indicated that it views the protection of private consumer financial and personal data as part of its mission to stop unfair, deceptive, and fraudulent trade practices. These regulators have investigated, and on occasion brought suit against, corporate victims of cyber-crime.

Investigations such as those described above are expected to become all the more common as cyber-risk continues to increase, which is also an inevitable consequence of the "internet of things" (*i.e.*, the interconnectivity of "smart" household and other devices).

[1] David E. Sanger, Utilities Cautioned About Potential for a Cyberattack after Ukraine's, N.Y. TIMES, Feb. 29, 2016, http://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html.

[2] http://www.law360.com/articles/505160/calif-ag-sues-kaiser-over-slow-data-breach-response

[3] http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=512804

Strategies for Minimizing Exposure in Cybersecurity Investigations

Cyber-risk cannot be eliminated, but it can be mitigated by taking certain measures. The following steps may help keep regulators at bay in the wake of a cyberattack, or at least minimize exposure in an investigation:

- In-house counsel and C-suite executives should carefully understand and be involved in their company's cybersecurity policies and procedures. They should have an understanding of the types of information that could be vulnerable to theft by cyber-criminals as well how their operations could be disrupted by cyberattacks;

- In-house counsel and C-suite executives should be aware of the types of "personal" data being collected, accessed, or transmitted, and where and how it is stored. They should also know what protections are in place to protect that data when it is "in motion" or "at rest." Questions about the necessity of such data collection and the adequacy of encryption should not be left to IT personnel, but should be thoroughly vetted at all levels. Stay up to date on the latest vulnerability patches and encryption enhancements;

- Board members of public companies should stay abreast of the cybersecurity policies and procedures the company has implemented. The board should also create a formal structure to ensure regular oversight of general cybersecurity procedures within the company;

- Have an incident response plan involving IT, information security, and other key employees. What would the company actually do if a cyber-incident occurs, and who would it notify and when? Rehearse mock scenarios, and make decisions in advance about how and when law enforcement will be contacted. On that note, it may be helpful to build a relationship with the local FBI cybersecurity field officer before an attack actually happens, and to keep in mind that local law enforcement may not have the capability to investigate data breaches which are often international in scope and/or originate overseas;

- Have a cybersecurity firm lined up to hit the ground running with a forensic investigation the moment a cyber-event is discovered. Similarly, research competent data breach counsel;

- Know what your regulatory reporting requirements are: to which agencies must a data breach be reported, and when?;

- Keep abreast of trends and threats in the cyber world. The FBI and industry groups such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) provide up-to-date information about known cyber-threats; and

- Train *all* employees about best security practices, such as ways to avoid inadvertently downloading malware.

AGs and regulators may weigh the above measures in deciding whether to launch an investigation or bring an enforcement action.

Insurance Coverage for Cybersecurity Investigations

Companies responding to cybersecurity investigations can expect to incur significant costs, including:

- Outside counsel fees for the review of a subpoena or other information request, and for the review and production of documents;

- The cost of any internal investigation commissioned by the company, and the cost of engaging a cybersecurity firm;
- Outside counsel fees for ongoing interaction with enforcement officials;
- Crisis management costs, such as public relations firm fees; and
- Fines associated with the investigation, or settlements or judgments in resulting lawsuits.

In addition, publicized government scrutiny of a company's data security practices could inspire class action privacy lawsuits by customers and former or current employees.

Fortunately, companies victimized by cyber-crime should be able to call upon their cyber, directors and officers (D&O), and possibly other liability insurers to help defray these costs. Depending upon the wording of each particular policy, investigation-related expenses may be covered. Potential sources of recovery should not be overlooked simply because an insurer or broker asserts that the "conventional wisdom" is that a certain policy is not "meant" to cover subpoenas or other investigation response costs.

Coverage under Cyber Policies

Perhaps the most obvious sources of coverage are specialized liability policies covering cyber-events, *i.e.*, "cyber" policies. Cyber policies often include modules providing coverage for government and regulatory investigations arising out of a cyberattack, as well as "crisis management" costs. The coverage may include defense costs and regulatory fines.

Policyholders should scrutinize their cyber policies to make sure they understand any prerequisites to obtaining such coverage. For example, a policy may provide coverage only if the company was in compliance with certain industry data security standards at the time of the attack, and the company may be required to prove as much to the insurer. The company may likewise be required to engage certain forensic investigators to analyze the security breach, subject to the insurer's approval.

When deciding whether to purchase cyber insurance, companies should consider consulting competent insurance counsel to review proposed policy language and explain the scope of the coverage and exclusions. Certainly, in the event a cyberattack, coverage counsel should be involved as early as possible.

Coverage for Investigations under D&O and E&O Policies

D&O policies cover "claims" arising from alleged "wrongful acts" of certain officers, directors, and employees of the company, as well as, in some cases, those of the company itself. As discussed in our previous alert in the "When Attorneys General Attack" series, D&O coverage is often available for subpoena response costs and may be available for other investigation-related costs as well.

The subpoena—a written order commanding the production of documents and/or witness testimony—is a widely used tool in government investigations, and is often the first step in a larger investigation. As a threshold matter, insurers often dispute that a subpoena is a "claim" within the meaning of that term in D&O policies. There is an emerging consensus in various jurisdictions that insurers are wrong on this issue.

An important recent New York case is *Syracuse University v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa*., in which the New York Supreme Court, affirmed by the Appellate Division, held that under the policy's definition of "claim," the plain meaning of the term "nonmonetary relief" encompassed subpoenas issued by

the U.S. Attorney's Office and a county district attorney's office in connection with their investigations into sexual abuse. The court relied heavily on *MBIA Inc. v. Federal Ins. Co*., in which the U.S. Court of Appeals for the Second Circuit found coverage for subpoena response costs, stating: "We reject the insurers' crabbed view of a subpoena as a 'mere discovery device' that is not even 'similar' to an investigative order. New York case law makes it crystalline that a subpoena is the primary investigative implement in the [attorney general's] toolshed." The *Syracuse University* court also noted that, pursuant to both New York and federal law, failure to comply with a subpoena is a punishable offense.

Courts have also found coverage under errors and omissions (E&O) policies for subpoenas and Civil Investigative Demands (CID). For example, *Ace American Insurance Co. v. Ascend One Corp*. involved a policyholder that was subject to an administrative subpoena issued by the Maryland Attorney General's office and a CID issued by the Texas Attorney General's office. The E&O policy at issue defined "claim" to include "[a] civil, administrative or regulatory investigation . . . commenced by the filing of a notice of charges, investigative order or similar document." Applying Maryland law, the U.S. District Court for the District of Maryland held that the subpoena and CID were part of an investigation into potential consumer protection law violations, and were therefore an "investigation" under the policy.

In addition to responding to a subpoena, a company facing a cybersecurity investigation may engage in many other costly tasks. For example, in some cases, a subpoena may be preceded by a less formal information request from the authorities, and decisions will have to be made (often with the advice of outside counsel) as to whether and how to respond to such requests. In the *MBIA* case mentioned above, the Second Circuit found coverage for costs incurred by the insured in voluntarily complying with the SEC's and New York Attorney General's informal, oral document requests. The Second Circuit held that this activity was covered because it was intended to head off formal subpoenas and additional public relations damage.

A company under investigation may also engage a public relations firm, security service, and other vendors to help manage the fallout from publicized government or regulatory scrutiny. While these "indirect" response costs are arguably investigation defense costs, there is scant case law on whether they are covered. But a policy with "crisis response" coverage might provide some relief. Coverage might also be available for resulting shareholder lawsuits, because such lawsuits commonly fit into the definitions of "claim" in D&O and E&O policies.

Practical Tips for Policyholders

The following should be kept in mind in order to maximize coverage for government and regulatory investigations:

- Be proactive. In the first instance, work with your broker to negotiate relatively broad cyber and D&O coverage. Some newer policy language can provide coverage for certain "pre-claim' inquiries from government agencies and specifically for subpoenas, which would also include attorneys' fees and costs associated with interviews or meetings with enforcement authorities. Policy exclusions must also be scrutinized. Consult competent coverage counsel to review proposed policy language.

- Understand and comply with notice obligations. It is essential that you understand when, under your cyber, D&O, and E&O policies, notice of claim, or notice of circumstances giving rise to a claim, must be given. On a similar note, it is important to understand your obligation to provide information to and cooperate with your insurer in defending an investigation. Best practice is to involve coverage counsel early—the advice will be protected by the attorney-client privilege, whereas conversations with a broker may not be.

When faced with a government investigation, policyholders should carefully examine all potentially available sources of coverage. The law is different in many states and some courts have not addressed the issue. Policyholders should be careful to understand their policy, the law, and their risks before they are subject to an investigation.

Our Cyber, White Collar and Insurance Recovery and Advisory attorneys routinely evaluate cyber-related issues, CIDs and subpoenas and help clients not only to develop strategies to respond, but to maximize the potential that our clients' insurance companies pay for that response. In most cases, we are able to review and evaluate specific situations for relatively low cost or fixed fee arrangements, which enables us to assist our clients to proactively improve our clients' position and minimize their risk.

If you have any questions about the content of this alert please contact the Pillsbury attorney with whom you regularly work, or the attorneys below.

Joseph D. Jean (bio)
New York
+1.212.858.1038
joseph.jean@pillsburylaw.com

Brian E. Finch (bio)
Washington, DC
+1.202.663.8062
brian.finch@pillsburylaw.com

Carolina A. Fornos (bio)
New York
+1.212.858.1558
carolina.fornos@pillsburylaw.com

Sheila M. Harvey (bio)
Washington, DC
+1.202.663.8224
sheila.harvey@pillsburylaw.com

Benjamin D. Tievsky (bio)
New York
+1.212.858.1015
benjamin.tievsky@pillsburylaw.com

Mark R. Hellerer (bio)
New York
+1.212.858.1787
mark.hellerer@pillsburylaw.com

Maria T. Galeno (bio)
New York
+1.212.858.1833
maria.galeno@pillsburylaw.com

William M. Sullivan, Jr. (bio)
Washington, DC
+1.202.663.8027
wsullivan@pillsburylaw.com

Pillsbury Winthrop Shaw Pittman LLP is a leading international law firm with 18 offices around the world and a particular focus on the energy & natural resources, financial services, real estate & construction, and technology sectors. Recognized by *Financial Times* as one of the most innovative law firms, Pillsbury and its lawyers are highly regarded for their forward-thinking approach, their enthusiasm for collaborating across disciplines and their unsurpassed commercial awareness.

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.
© 2016 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.