ALERT

pillsbury

Cyberattacks Are the New Norm

How to respond and get insurance recovery for government investigations.

By Joseph D. Jean, Carolina A. Fornos, Brian E. Finch

TAKEAWAYS

- Companies that suffer cyberattacks can expect not sympathy but scrutiny from legal authorities.
- D&O insurance can cover not only litigation but also investigation costs.
- Strategic negotiation of D&O and E&O policy language can mitigate risk that may arise.

09.21.17

The script is well-worn by now: a major corporation suffers an embarrassing data breach that has led to the loss of tens of millions of customer records. Compounding the embarrassment is the quick reaction by state attorneys general launching investigations and lawsuits against the corporation and executives. Will your insurance carrier help cover the costs associated with defending against the AGs' claims?

Background: State AGs Are Aggressively Using Their Authority under Data Privacy and Unfair/Deceptive Advertising Laws to Pursue Claims Following Cyberattacks

The last ten years have seen an explosive growth in the number of data privacy protection laws enacted and updated across the country. Nearly every state now has a law requiring companies of all shapes and sizes to disclose when "personally identifiable information" (or PII, a term whose meaning varies from state, but typically involves some combination of a person's name and a unique identifier like a social security number, credit card or other payment account number, or driver's license number) has either been accessed without authorization or stolen.

Under those laws, companies will have a set amount of time to notify affected individuals as well as provide them some form of recourse, typically through free access to credit monitoring services. Additionally, the data privacy protection laws also usually give attorneys general the authority to pursue litigation against the companies whose databases were stolen. Such actions initially were only

taken following the most egregious data breaches (extremely large size or the security failure appeared to have been the result of gross negligence on the part of the company.) Now, however, attorneys general are increasingly filing such lawsuits simply upon receipt of news that a data breach has occurred. Most troublesome for some companies is that they might be sued before they even know how the breach occurred or who conducted it.

Such investigations tend to be expensive, protracted, and disruptive to the company's efforts to conduct day-to-day business. Executives and officers often find themselves being deposed by multiple attorneys general offices as well as civil plaintiffs while simultaneously being excoriated in the press for their alleged malfeasance or perceived lack of interest in protecting the data of their customers. Even though a determination as to whose actions were ultimately responsible the cyberattack may be months or even years away—and may require the resources of federal law enforcement and national security agencies to make a definitive conclusion—the costs of internal investigations, settlement negotiations or even lawsuits can seriously impair the day-to-day operations of a company.

Strategies for Managing and Responding to Civil Investigative Demands and Subpoenas

In the event of a cyberattack, a company can anticipate Civil Investigative Demands (CIDs) or subpoenas will be issued. How the company responds will be critical. The company should review the subpoena, Civil Investigative Demand or other investigative demand carefully to ensure that it understands the scope of information requested, terms used, and time frame affected. It is highly advisable that counsel experienced in handling government investigations be consulted. Counsel can begin the conversation with the issuing government official to respond properly to the information being requested by the Government. Counsel can help to evaluate whether the scope of the request may be narrowed to (i) effectively target the relevant information sought by the Government, and (ii) efficiently respond to the Government's requests and minimize the disruption that collecting such information entails. Counsel can also advise on the potential for working with the government to identify the culprit of the cyberattack. These initial discussions will greatly impact the government's perception of the situation and how it treats the company throughout the investigation. Moreover, it is highly likely that the company will want to conduct an internal investigation to address potential risks and liabilities that may flow from the Government request.

Insurance Coverage for Data Breach/Cybersecurity Investigations

Targets of cyber-related attacks can expect to incur significant expenses if they are forced to respond to government investigations into a data breach. The categories of costs faced by the subject of such an investigation (apart from the costs associated with the breach itself and the resultant lawsuits) could include:

- Outside counsel fees for the review of a subpoena, CID or other information request, and for the review and production of documents;
- The cost of any internal investigation commissioned by the company;

- Outside counsel fees for ongoing interaction with the AG or other enforcement officials; and
- Settlements or judgments associated with the investigation or resulting lawsuits.

In addition, publicized government scrutiny of a data breach could inspire civil actions such as shareholder derivative suits and securities class actions and lawsuits by individuals whose PII was stolen.

Fortunately, companies should be able to call upon their directors and officers (D&O) and possibly other liability insurers to help defray these costs. D&O policies, for example, 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. 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. Third-party vendors may also owe indemnification to companies who have been the victim of a data breach and, in some cases, may also have named such companies as additional insureds on certain liability policies. Be sure to investigate all potential sources of recovery.

Getting Coverage for Subpoena Response Costs under a D&O Policy

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.

The typical D&O policy contains a definition of "claim" similar to the following:

(1) a written demand for monetary or nonmonetary relief;

(2) a civil, criminal, administrative, regulatory or arbitration proceeding for monetary or nonmonetary relief which is commenced by:

(i) service of a complaint or similar pleading;

(ii) return of an indictment, information, or similar document (in the case of a criminal proceeding); or

(iii) receipt or filing of a notice of charges

A number of courts have held that a subpoena constitutes a "demand for nonmonetary relief."

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 NYAG'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 in other jurisdictions have also found D&O coverage for subpoena response costs: *Protection Strategies v. Starr Indem. and Liab. Co.* (E.D. Va.) (applying Virginia law and finding defense coverage for NASA subpoena and search and seizure warrant); *Minuteman International Inc. v. Great American Ins. Co.* (N.D. Ill.) (applying Illinois law and finding coverage for compliance with SEC subpoena); *Polychron v. Crum & Forster Ins. Cos.* (8th Cir.) (applying Arkansas law and finding coverage for grand jury subpoena served on a bank).

Courts have also found coverage under errors and omissions (E&O) policies for subpoenas and CIDs. 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.

Coverage for Other Investigation-Related Costs

In addition to responding to a subpoena, companies facing an AG 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 NYAG'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 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

Companies should keep the following points in mind in order to maximize coverage for government investigations:

- Be proactive. Even before a subpoena or "target letter" lands on the GC's desk, work with your broker to negotiate a relatively broad definition of "claim" in your D&O and E&O policies. 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. A government investigation may begin with a formal subpoena, or even informally at an earlier point in time. It is essential that you understand when, under your 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 policies, the law and their risks before they are subject to an investigation.

Our Cyber, White Collar and Insurance Recovery and Advisory attorneys routinely evaluate 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 enable us to assist our clients to proactively improve our clients' position and minimize their risk.

ALERT

pillsbury

Do Recent Events Make You "Wanna Cry"?

Massive ransomware attacks are just another reason to have robust cyber insurance in place.

By James P. Bobotek, Peri N. Mahaley

TAKEAWAYS

- Inclusion of cyberextortion coverage as part of cyber insurance program is gaining acceptance as a best practice in today's commercial risk management world.
- Review/confirm your cyber-privacy insurance now.

05.19.17

On May 12, a massive ransomware cyber-attack infected over 100,000 computers in more than 150 countries. This malware, a Trojan virus known as "WannaCry," "WanaCryptor," or "Wcry," encrypts files, and then threatens to destroy them, unless the victim pays a ransom. As of May 14, WannaCry had victimized at least 200,000 users in more than 100,000 organizations, including the UK's National Health Service, global shipper FedEx, Chinese universities, Russia's Interior Ministry, Telefonica, Gas Natural and Iberdrola, and Renault. The attack, which continues to spread, reinforces the need to procure cyber insurance, and to ensure that coverage extends to exposures resulting from ransomware attacks.

What is WannaCry?

WannaCry takes advantage of a vulnerability in older versions of Windows, including Windows 7 and Windows XP. In March, after the NSA discovered the "EternalBlue" exploit that would later be used by WannaCry, Microsoft issued a security update that prevents WannaCry and other malware from affecting computers and networks using Windows 7. However, many Microsoft users did not upload the patch. Further aiding the hackers is the fact that, while Microsoft no longer supports Windows XP, many still use it. Or, as is common in some Asian countries, users are running pirated versions of Windows and are afraid to run updates and risk discovery. As a result, computers without security patches for the various Windows versions in use are common in some areas, and easy prey for WannaCry.

Those in control of WannaCry seek ransom payments in the form of Bitcoin. The initial ransom demand starts at $300, with a threatened increase to $600 if not paid within 3 days. The hackers claim that, absent payment within 7 days, the encrypted files will be deleted and all data not backed up elsewhere will be forever lost.

WannaCry is indiscriminate in its end product. It is unfocused on a distinct target or trade. Even worse, it is designed to spread throughout systems that have not taken appropriate defensive measures. Remarkably, it can spread through networks without users taking any action.

What Is Ransomware?

Ransomware is a form of malicious software that penetrates computer systems or networks and uses tools like encryption to deny access or hold data hostage until the target pays a ransom, frequently in Bitcoin. A ransomware attack is typically delivered via an e-mail attachment which could be an executable file, an archive or an image. Once the attachment is opened, the malware is released into the user's system. It can be in the form of encryption (individual PCs or a server), lock screen, or mobile device (typically affecting Androids).

The infection is not immediately apparent to the user. The malware operates silently in the background until the encryption mechanism is deployed. Then, a dialogue box appears that tells the user the data has been locked and demands a ransom to unlock it again. By then it is too late to save the data through security measures.

Ransomware attacks are on the rise—there are now more than 50 families of this malware in circulation—and it is quickly evolving. With each new variant comes better encryption and new features. This is not something to ignore. One of the reasons why it is so difficult to find a single solution is because encryption in itself is not malicious. In fact, many benign programs use it.

Do Not Despair—There Is an Insurance Product that Covers Many Ransomware Damages.

The necessity of cyber insurance in some form or another cannot be questioned today. Reliance on cyber insurance in some form or another has become a necessity. Most cyber insurance policies offer various grants of coverage on an à la carte basis. One of these grants is commonly referred to as "cyberextortion" or "ransomware" coverage. Typically, this coverage will pay for: (i) the money necessary to meet the ransom demand; (ii) the costs of a consultant or expert to negotiate with the extortionist; and (iii) the costs of an expert to stop the intrusion and block future extortion attempts. Another commonly available coverage, typically referred to as "business interruption" or "time element" coverage, may cover lost business income arising from an attack.

What Should You Do if You Are the Victim of a Ransomware Attack?

- **Notify your insurers immediately.** Some cyber insurance policies provide coverage only for costs incurred after the insured notifies the insurance company. Some policies also require that the policyholder inform the applicable law enforcement agency and obtain the insurer's consent before

making any ransom payment. Therefore, despite the urge to move swiftly in response to this crisis, we recommend policyholders understand and comply with the notice provisions of their policies in order to preserve their right to insurance coverage.

- **Consider whether you will pay the demanded ransom.** Paying the ransom is tempting, but there is no guarantee that paying will actually lead to your files being decrypted. In addition, you are supporting the criminal's business model and thus are partly responsible for more and more people getting infected with ransomware.

- **Document your losses.** Properly documenting your losses is crucial. Establish separate accounts to track losses, including any extra expenses, professional fees, mitigation costs, and other expenses associated with the attack. Keep a log of all actions taken. Save all receipts and other records of additional expenses.

- **Engage** It is usually prudent to engage professional claim consultants, such as forensic accountants, particularly where there is business interruption loss. Additional experts may be needed to model the unique financial aspects of your business. Their professional fees and other mitigation expenses are frequently covered under cyber/privacy policies, subject to sub-limits, and usually subject to carrier pre-approval. It is also a good idea to retain an experienced insurance coverage lawyer, not just when you need an advocate, but to help you protect the privileged nature of your communications and to avoid many of the traps for the unwary when presenting your insurance claim. Counsel may work in the background, without revealing their involvement to carriers. Carriers usually do the same thing. Cooperate with the insurance company adjuster, but don't forget they work for your insurer, not for you. If you need an advocate, hire your own.

What Can You Do to Prevent a Ransomware Attack?

- **Confirm that all of your computers and networks are current with security updates.** Windows users should confirm they have the latest Windows security updates installed, and should only use fully-supported software. Failure to do so could impact coverage under many policies.

- **Implement application "whitelisting."** Only allow systems to execute programs known and permitted by your security policy.

- **Secure backup.** Make certain that you have secure data backup to media not connected or mapped to a live network.

- **Implement incident response plans.** Address distributed ransomware attacks and perform "tabletop" exercises tailored to ransomware scenarios.

Don't Let It End in Tears.

Aside from enterprise risk management endeavors such as vigilance, secure data backup to media not connected or mapped to a live network, disabling macros, and diligent installation of software updates and patches, inclusion of cyberextortion coverage as part of your cyber insurance program is not only recommended, but is gaining acceptance as a best practice in today's commercial risk management world. Not having it in today's world will surely make you WannaCry.

pillsbury