haynesboone
Setting precedent.

Haynes and Boone, LLP

A Desk Guide to Data Protection and Breach Response

For additional information, please contact:

RONALD W. BREAUX
Privacy and Data Breach Practice Group Leader
ron.breaux@haynesboone.com
T +1 214.651.5688

TABLE OF CONTENTS

haynesboone
Setting precedent.

A Desk Guide to Data Protection and Breach Response

Foreword

If your business is connected to the Internet, it is vulnerable to attack, either by willful perpetrators intent on exfiltrating your proprietary or sensitive data for their own personal gain, or by casual hackers or hacktivists intending to cause damage to your business. Unfortunately, companies should prepare for "when" – not "if" – they suffer a data breach. In fact, the chances are good that your business has already suffered an attack. Attacks come in a variety of forms, from viruses to spam, from Trojan Horses to network backdoors and other nefarious technology, all of which can be used to wreak havoc on your business in a variety of ways. Indeed, data breaches – and the resulting loss of critical data, business interruption, onerous disclosure requirements, regulatory scrutiny, costly third party litigation, and tremendous loss of reputation and goodwill – can threaten the very viability of your enterprise.

Haynes and Boone is pleased to present this "Desk Guide to Data Protection and Breach Response" to help you navigate the rapidly evolving cybersecurity landscape. The Desk Guide, which was prepared by the firm's interdisciplinary Privacy and Data Breach group, provides a practical approach to data security, including how to:

- identify and analyze applicable data protection and compliance issues,
- develop an enterprise data security plan,
- obtain cyber risk insurance,
- investigate and respond to a breach or cyber incident,
- address public disclosure and regulatory issues following a breach,
- refer cyber incidents to law enforcement for possible investigation and prosecution,
- anticipate and prepare for civil litigation and class actions following a data breach or cyber incident, and
- recover losses through insurance claims.

We hope this Desk Guide will be a useful reference for you as you manage your company's cyber risks and prepare for the cyber incident(s) your company will almost certainly experience. If you have any questions about the Desk Guide or about privacy, data security or data breach matters more generally, please contact any of the members of our Privacy and Data Breach group. We look forward to working with you.

Best regards,

Ronald W. Breaux
Privacy and Data Breach Practice Group Leader

The Best Defense is a Good Game Plan: A Proactive Approach to Data Protection and Compliance

Ronald W. Breaux, Emily Westridge Black, Gavin D. George, Timothy Newman

In our experience, the best defense against potential data breaches, investigations by privacy regulators, customer privacy complaints, and mishandling of sensitive data by vendors is a well-constructed and well-monitored privacy compliance and data protection plan. In this first installment of our series, we will discuss the initial steps companies should take to create an effective privacy compliance and data protection plan.

Assess Your Data Retention

Before beginning to design a data protection plan, your company should identify the types of information it collects and processes. Under current laws and regulations, the following types of commonly collected information require special handling and protection:

- Personal Information ("Personally Identifiable Information" or "PII") – State data breach laws define personal information generally to include an individual's first name or first initial and last name in combination with any one, or more, of the following identifiers: social security number; drivers' license number or state identification card number; account number, credit card number, or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. Many states add additional elements to this definition, including medical data, passport numbers, or tax identification numbers. Some states, including California, also include personal email addresses in the definition, when accompanied by a password or security question and answer.
- Cardholder Data – The Payment Card Industry Data Security Standard ("PCI DSS") defines cardholder data as: "account number, cardholder name, expiration date, and service code." The term also includes more sensitive data used for authentication of transactions (PIN, security code).
- Personal Health Information ("PHI") – Generally speaking, the federal Health Insurance Portability and Accountability Act ("HIPAA") defines protected health information to include data about health status or health care linked with certain personal identifiers. These identifiers include, among other things, name, geographic location (more specific than state-level), dates, phone/fax numbers, email addresses, and social security numbers.

Additionally, apart from information linked to an individual, companies often store business and technical information that they consider confidential or secret, and would prefer to keep from competitors and the public.

Survey the Legal Environment

Once you know how, what, when, where and why your company collects personal data, you will be able to assess the applicability of various statutes, regulations, and industry standards. Survey the surrounding privacy landscape to ensure that your company knows the applicable laws and regulations, recognizes how to achieve compliance, and understands how to implement effective precautions against data breaches. International corporations that receive data from foreign subsidiaries or affiliates must also be mindful of foreign laws that protect privacy, such as the European Union's Data Protection Directive or French Law No. 78-17 (informatique et libertés).

A survey of the privacy landscape may be simple or complex, depending on the size of your company and the type of data it handles. Smaller-sized surveys might consist of a simple collection of documents reflecting each federal and state law, each regulation, and each contractual requirement applicable to the data stored or processed by your company. Surveys performed by larger companies would include a more detailed and complex collection of documents, often managed electronically, and might include documents related to compliance with international data protection regimes, industry standards, audit protocols, and internally developed policies related to vendor contracting. Your company's survey should consider all applicable laws, regulations, and industry standards, including the following:

- Payment Card Standards – The PCI DSS outlines best practices for securing payment card data that may be contractually enforceable against companies that accept payment cards.
- Financial Data Regulations – Financial institutions are subject to a range of federal regulations, and must monitor compliance closely. The Fair Credit Reporting Act (as amended by Fair and Accurate Credit Transactions Act) applies specifically to credit reporting agencies, creditors, and insurers. The Gramm-Leach-Bliley Act contains data privacy and safeguard requirements that apply to all financial institutions.
- Health Data Regulations –The HIPAA privacy and security rules apply to health care providers, health insurers, and their vendors. The HIPAA rules (as amended by the HITECH Act) are the most comprehensive federal rules related to the protection of personal data. Some state laws also impact the management of health-related data.
- State Breach Notification Laws – Although state data breach notification laws are not identical, all of them require companies to disclose breaches of personal information to affected individuals in a timely manner. These laws will be discussed in more detail in future installments of this series.
- Marketing Regulations – Certain federal regulations apply to telephone, fax, text, and e-mail marketing to consumers. Other federal rules dictate how telecommunications companies can use personal information gathered from their customers.

- Laws Related to the Internet – The federal Children's Online Privacy Protection Act controls the collection and use of personal information from children under 13 over the Internet or via mobile apps. California's Online Privacy Protection Act requires every website and mobile app operator that gathers personal information from California consumers to conspicuously post an enforceable privacy policy.
- Public Disclosure Obligations – Guidance from the United States Securities and Exchange Commission explains that public companies should consider data security matters when preparing their financial disclosures, disclosure of risk factors, and conclusions regarding the adequacy of their disclosure controls and procedures. In the event of a breach, companies may also be required to disclose resulting material litigation. The disclosures should be reasonably detailed, but need not include information that would reveal a company's vulnerabilities or compromise its cybersecurity. Companies should proactively review their existing public disclosures in light of the SEC guidance, prior data security incidents or known risks, and the potential impact of a data security incident.
- Other Laws and Regulations – The United States Federal Trade Commission ("FTC") actively pursues companies that engage in "deceptive" or "unfair" privacy and data protection practices under Section 5 of the FTC Act. The FTC can punish violators with fines and require implementation of specific privacy programs (including lengthy monitoring and reporting periods). A number of other agencies and organizations are involved in privacy enforcement at the federal, state, and international levels.

Knowledgeable legal counsel can help companies survey the privacy landscape quickly and efficiently.

Compile Internal Compliance Information

Compile information related to your (including your contractors') compliance with each of the requirements identified in your survey. Gather and examine each internal policy, procedure, and training program related to each identified requirement with an eye to demonstrating compliance. Specifically, gather your data retention and data destruction policies, written privacy policies, data security procedures, data breach notice plans, new hire and other employee training material, computer-use agreements, and any internal auditing and monitoring processes. (We will discuss how to design effective policies in the next installment of this series.) The collection of relevant internal policies and procedures will help to avoid scrambling in response to data breach events, lawsuits, regulatory complaints, and audit requests. Regularly evaluate your organization's compliance with those policies and procedures once they are collected and regularly re-evaluate the substance of these policies and procedures in light of evolving technology, new legislation, litigation trends, and case law.

Evaluate Your Risks

There are myriad risks associated with noncompliance with privacy laws, mishandling of personal data, and data breaches. Common risks include loss of customers, loss of business, investigative costs, regulatory

actions, fines, litigation, disclosure obligations, and unfavorable publicity. An internal brainstorming session may be helpful to identify all potential risks. Each company will evaluate its risks differently. Triage each risk based on the number of relevant threats, the vulnerability of your company, and the expected loss associated with a breach. Experienced legal counsel can help your company through this process. Starting with the highest value risk, identify one or more methods for mitigating each risk. Revisit the risk assessment frequently to re-rank the risks as your company's systems for measuring and improving organizational privacy and data protection compliance improve.

Think "Privacy by Design"

Take a "privacy by design" approach to addressing privacy and data security risks. "Privacy by design" means customer privacy, legal compliance, and data protection are considered throughout the data lifecycle (collection, processing, storage, and destruction). Each high value risk identified by your company during a risk assessment represents an opportunity to design a new tool or solution to reduce that risk.

Design and Implement Your Solutions

Privacy solutions vary in complexity. The exact type and nature of the solutions will vary from company to company and depend upon the types of data collected. The most successful solutions address the privacy or data security risk without becoming overly burdensome on the resources of the company. Many solutions are mandated by statute, industry standards (such as the PCI DSS), or guidance from regulators (such as the FTC). Other potential solutions include revising internal policies, incident response plans, and vendor contracting requirements. More technically sophisticated risk mitigation tools might include software and firewalls designed to prevent and detect network intrusion. Before implementing more complex solutions, test them in a beta or pilot phase to identify shortcomings and avoid unforeseen disruptions to important business processes. Legal counsel and other outside consultants can help companies find solutions that may not have been known or considered internally.

Monitor and Evaluate Your Solutions

Once your company implements appropriate privacy solutions, measure the effectiveness of the solutions regularly. Among other things, test to ensure that employees are properly and consistently implementing the solutions.

Tailor-Made: Designing and Implementing a Bespoke Data Security Plan

Ronald W. Breaux, Emily Westridge Black, Timothy Newman

When you hear the term "bespoke," you may think suits or dresses, but you should be thinking data security plans. Savvy organizations realize that there is no "one size fits all" approach to data security. Instead, companies must develop individualized data security plans based upon the types of data they manage, the applicable laws, their perceived risk exposure and risk tolerance, and other enterprise-specific factors.

The importance of having a comprehensive data security plan in place cannot be overstated. The U.S. Securities and Exchange Commission recently announced that it will begin evaluating companies' policies designed to prevent, detect, and respond to cyber attacks in its exam process, and the U.S. Department of Health and Human Services recently fined a dermatology practice for failure to have policies in place that address the breach notification provisions of the Health Information Technology for Economic and Clinical Health ("HITECH") Act. In addition to helping companies avoid regulatory scrutiny, good data security plans help companies prevent breaches and mitigate the fallout if a breach occurs.

In this installment of our special series, *A Desk Guide to Data Protection and Breach Response*, we discuss how companies can create a tailor-made data security plan to limit their breach exposure. In your plan, you should:

- **Identify your information security team.** Your data security plan should identify the individuals in your organization who are charged with ensuring information security. Given the various business units that may be affected by a data breach, your team should include personnel from your legal, information technology, human resources, and communications/public relations departments, as applicable. It should also include at least one member of your board of directors, particularly in light of recent derivative lawsuits filed in the wake of the Target and Neiman Marcus breaches, which highlight the board's responsibility for data security and breach response.
- **Implement policies to prevent unauthorized access to your network.** A well-developed data security plan should include layers of protection (a "defense in depth" approach) to prevent unauthorized access to your data. For example, your company should have policies that require employees to use strong, complex, unique passwords that they change regularly and cannot share. You should never use generic or default passwords. Your company should also have a bring your own device ("BYOD") policy or other policies addressing whether, and under what circumstances, employees can perform work using devices that they own (including computers or smart devices). For example, you should ensure that employees' devices adequately protect confidential data by, among other things, requiring that those devices be password protected.

Additionally, you should work with your information technology department and/or information security specialists to ensure that you have appropriate technological barriers (e.g., firewalls and network segmentation) to prevent network intrusion.

- **Develop a system for tracking network access.** Effective information security requires early detection of intrusions and the ability to identify the intruders. Coordinate with information technology professionals to monitor access to sensitive information and be on the lookout for suspicious activity on your network. Among other things, ensure that your firewall logs are sufficiently verbose that you can determine when an intrusion (or any exfiltration of data) occurs.
- **Design effective employee onboarding and exit procedures.** Unfortunately, your trusted employees can become the source of a data breach when they leave your organization, especially if they leave to work for a competitor. It is not uncommon for employees to walk out the door with valuable data including customer lists, price lists, product designs, and other proprietary information. Companies may also expose themselves to liability if they do not ensure that new hires do not bring other companies' proprietary information with them to their new jobs. Your organization's onboarding and exit procedures should protect against these risks by, among other things, obtaining certifications from new employees that they are not bringing competitor information to your organization, instructing employees to report impermissible use of competitor information, and cutting off departing employees' access to information systems (including email) and company premises immediately after terminating their employment. Departing employees should be expressly asked whether they are taking any company information with them, and their answers should be documented in writing during the exit interviews. Employers should immediately demand the return of impermissibly taken information.
- **Conduct employee training.** A data security plan is only effective if your employees are aware of the plan and execute it consistently and effectively. Set expectations that your company takes data security (and unauthorized computer access) seriously. Employees should understand the importance of information security, how they can help to ensure information security, and what to do if they suspect a breach has occurred. Promote awareness and preparation through regular employee training.
- **Develop a breach response plan.** The most important part of your company's data security plan is the breach response plan, which (as the name suggests) is a detailed plan that governs how a company should respond to a suspected breach. In our experience, these plans help companies quickly and effectively initiate investigations and remediation of data breaches. Among other things, a breach response plan should identify the leaders of the response team and it should be easy to follow and scenario-based. For example, if your organization is a retailer that manages payment card data, outline the response to a breach that implicates that specific type of data. The plan should also provide for the immediate involvement of legal counsel in all aspects of the

investigation (including communications about the potential breach, remediation efforts, and disclosure and reporting) to ensure protection under the attorney-client and work product privileges.

- **Conduct regular audits.** To understand the risks your organization faces and to prepare for a data breach, you must understand your company's privacy landscape, including the types of information it collects and retains. You must also understand available risk transfer options, including cyber risk insurance. We discussed the steps to analyze the privacy landscape in our first installment, and we will discuss insurance in our next installment; but regular evaluation of these issues should be a part of your data security plan. A regular audit should also include evaluation of your information security practices and whether your company is effectively following that plan.

The parameters of your organization's data security plan will necessarily turn on the nature of your organization, the types of information it collects, and the regulatory environment in which it operates. Haynes and Boone, LLP advises clients on developing and implementing effective, bespoke data security plans.

Insurance Coverage for Cyber Attacks: What Do You Need in a Cyber Liability Policy?

Leslie Conant Thorne, Micah E. Skidmore

With more and more businesses suffering costly data breaches and cyber attacks, companies should utilize every tool they have to shift the potentially enormous expenses associated with those breaches and attacks. That's where insurance comes in. Companies can potentially shift some expenses under the traditional business policies - such as general liability, commercial property, crime/fidelity, and errors and omissions - but they are increasingly looking to specialized "cyber liability" policies for more fulsome coverage.

Cyber attacks come in myriad forms. Depending on the type of attack, trade secrets, personal customer or employee information, or even entire computer systems may be compromised. While every policy is different, cyber liability policies typically protect the insured against its own direct losses (first party coverage) as well as their liability for the losses of others (third party coverage). Depending on the policy, cyber insurance may cover:

- Forensic investigation and system restoration;
- Defense and indemnity costs associated with litigation resulting from the loss of personal information or other sensitive data;
- Defense costs and penalties associated with regulatory investigations;
- Notification costs and credit monitoring for affected customers and employees;
- Losses attributable to the theft of the policyholder-company's own data (including transfer of funds);
- Business interruption costs attributable to a cyber attack;
- Costs required to investigate threats of cyber-extortion and payments to extortionists; and
- Crisis management costs, such as the hiring of public relations firms.

It is critical to carefully review the particular provisions of each cyber liability policy with a broker and coverage counsel. Unlike many traditional policies, cyber liability policies differ significantly because they are not (yet) based on a standard form.

The first rule in choosing the right policy is to match the company's unique risks to the risks covered by the policy. Coverage needs vary significantly depending on the type of organization, the type and amount of personal information it holds, and many other factors. A credit card company, for instance, may have vastly

different needs than a hospital system or a utility company. Likewise, companies with a public profile may have a much greater need for extortion coverage or crisis management coverage than a smaller, lesser known business. Companies that fail to thoroughly understand their own needs often inadvertently purchase policies that (1) have gaps in coverage and/or (2) include unnecessary coverage.

While companies should work closely with their brokers and counsel to choose the right policy, would-be policyholders should particularly watch out for:

- **Provisions identifying who is an "insured" under the policy.** Typically, the policyholder would want to include both the organization itself and any other individuals or entities (including independent contractors or other third parties) responsible for the organization's network security.
- **Sublimits.** Some policies, despite providing significant overall coverage, cap the amount they will pay for certain categories of liability, such as notification costs.
- **Who gets to choose the lawyers, PR firms, investigators, or credit monitoring companies.** Some polices require that the policyholder use the carrier's approved vendors.
- **Late retroactive dates.** Policyholders should negotiate early retroactive dates, meaning the policy will cover breaches that occurred long before the policy was purchased, but were not discovered until after coverage took effect.
- **Exclusions for Payment Card Industry (PCI) breaches.** If your organization suffers a breach involving customers' credit card numbers, this type of exclusion could be catastrophic.
- **Provisions that exclude or limit coverage for regulatory actions.** Regulatory agencies such as the Federal Trade Commission and the HHS Office for Civil Rights are becoming increasingly aggressive in pursuing data security-related actions (see our coverage of increasing SEC scrutiny of cybersecurity disclosures and our article regarding a recent lawsuit by the California Attorney General claiming unnecessary delay in disclosing a breach). Companies that could be subject to regulatory actions should avoid policies that have these exclusions.
- **Provisions that exclude fines and penalties.** Depending on the organization's specific needs, it may need coverage for penalties assessed under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Gramm-Leach Bliley Act ("GLBA"), the Health Information Technology for Economic and Clinical Health ("HITECH") Act, and other similar state and federal laws.
- **Provisions that exclude coverage for third party vendors.** If the company uses third parties to gather, store, or process data, these exclusions could obviously present serious problems.
- **Exclusions barring coverage if the insured "should have known or anticipated" the breach.** Such provisions often lead to coverage disputes as to who should have known what and when.

- **War exclusions.** These exclusions bar coverage for losses arising from "acts of foreign enemies." Many cyber attackers are foreign nationals and some allegedly act at the behest of foreign governments.
- **Exclusions for the misappropriation of trade secrets or other intellectual property.** Some policies exclude coverage for damages stemming from a cyber-attacker's misappropriation of trade secrets. Such exclusions need to be tailored to avoid unintended consequences.
- **Exclusions for claims alleging unsolicited electronic dissemination of faxes, emails or other communications.** Such exclusions should be modified to specifically except claims based on distributed denial of service ("DDoS") attacks perpetrated using the insured's systems.
- **Insured vs. insured exclusions.** Given the potential for employee claims alleging the disclosure of personal information, exclusions barring claims brought by one insured against another can be problematic.
- **Breach of contract exclusions.** Carriers may invoke these exclusions when a customer sues based on an alleged breach of his personal information, arguing that the insured held the information under a service contract.
- **Exclusions for loss of information on unencrypted devices.** With many employees carrying sensitive information on their home computers and handheld devices, companies should consider the potential risk associated with the portable nature of certain information.

Every policyholder is unique, meaning some of these issues may not be important to a particular policyholder. But by being aware of these and similar concerns, policyholders and their brokers will be able to negotiate the policy that best meets their needs and minimize coverage disputes when claims arise.

The Clock is Ticking: Investigating and Responding to a Breach

Ronald W. Breaux, Emily Westridge Black, Timothy Newman

Once your company becomes aware of a suspected data breach, time is of the essence. Losses from the breach are likely mounting, the clock is running on your organization's legal rights and obligations, and the potential liability to claims by regulators and plaintiffs begins to expand. In this installment of our special series, A Desk Guide to Data Protection and Breach Response, we discuss strategies companies should implement once they suspect a data breach has occurred. The precise parameters of an investigation depend on a multitude of factors, but we recommend the following steps:

- **Assemble your team.** Your breach response plan should identify the best personnel to direct your organization's response. A typical response team includes members of legal, human resources, information technology, and public relations departments. Given the potentially significant ramifications of a security incident, you should also consider notifying the board of directors, as well as inclusion of a director in the response efforts.
- **Contact legal counsel immediately.** Data security attorneys are experienced in investigating cyber incidents and know how to manage sensitive relationships with third parties, including forensic investigators and law enforcement. Moreover, the information prepared during an attorney-led investigation is more likely to be protected by the attorney-client privilege or attorney work product doctrine in the event of litigation. Your breach response plan should identify a firm or attorney to call and include their emergency contact information.
- **Be cautious with terminology.** In early written communications following an incident, avoid drawing premature conclusions regarding the cause of an incident and whether information has been accessed or stolen ("exfiltrated," to data security professionals). If an investigation is ongoing, make sure that your updates and other reports reflect that reality. And avoid using the term "breach," which carries legal significance and assumes that information was exposed to unauthorized parties. Imprecise, inaccurate, or reckless communications during an investigation can hinder your organization's ability to defend against charges of liability by affected third parties or regulators.
- **Consider hiring a forensic investigator.** Legal claims and defenses and liability arising from a security incident often turn on the reliability of evidence collection and analysis. Consider retaining a reputable investigator to assist in your investigation and remediation efforts. When an entity may have suffered a breach of payment card information ("PCI"), the card brands often require the entity to retain one of their approved Payment Card Information Forensic Investigators (or "PFI") to conduct a forensic investigation, but these vendors are closely aligned with the card brands and, even in the best case scenario, have split or dual loyalties to you and the card brands. You should

seriously consider hiring your own independent forensic investigator to conduct a shadow investigation.

- **Review insurance contracts.** Some companies make the mistake of assuming that they cannot obtain coverage for breach-related liabilities unless they have cyber-insurance. However, in the absence of a cyber-specific policy, you may be covered under more general policies. Gather all of your potentially applicable policies and review their terms closely. Legal counsel can assist in identifying potential coverage and complying with applicable notice provisions. In a later installment of the Special Series, we will address obtaining coverage for a cyber incident in more depth.
- **Consider contacting law enforcement.** After the initial investigation is sufficiently complete, you should carefully consider (with assistance from experienced legal counsel) whether to contact law enforcement (if they have not already become aware of the breach). Law enforcement has access to investigative tools (for example, grand jury subpoenas and search warrants) that are not otherwise available to private sector entities, and are currently very interested in investigating cyber incidents that affect national security or have significant economic implications. However, law enforcement cannot and will not assist you in repairing damage to your computer network like independent forensic investigators can, and businesses may lose control over an investigation once law enforcement becomes involved.
- **Analyze disclosure obligations.** Release of sensitive personal information may result in notice obligations to the affected third parties, and compliance is often required within a specified (and short) period of time. Notice requirements are primarily based on a patchwork of state laws, and the residency of the affected parties determines which laws apply. If an incident potentially resulted in disclosure of personal information, as defined under the relevant state law, immediately assess your obligations and provide timely notice to appropriate recipients to avoid additional legal exposure to consumers or regulators. A recent lawsuit by the California Attorney General highlights the importance of timely disclosure. A later installment of the Special Series will address disclosure obligations in more depth.
- **Consider the prospect of litigation.** A data breach may lead to various types of litigation or regulatory actions. For example, the organization itself may choose to sue the perpetrator to recover losses, and the breach may draw attention from criminal authorities. Additionally, affected parties and regulators may sue a victim organization for failing to protect information or provide timely notice of a breach. We will discuss litigation in more detail in several future installments of the Series.
- **Manage public relations.** Companies that suffer a cyber incident often suffer reputational harm as well. Work with your public relations personnel and legal counsel to limit the harm while at the same time ensuring your organization doesn't open the door to additional legal liability. You should consider coordinating all communications with third parties through a single source to ensure that

they are authorized, accurate, consistent, and timely. A customer hotline or website can be useful in this regard.

Data breach responses necessarily vary depending on the type of organization, the type and volume of information at risk, and various other factors. We strongly recommend that you consult with legal counsel to ensure that you are taking the necessary steps to minimize your losses.

Breaking the News: Disclosing Data Breaches and Withstanding Regulatory Scrutiny

Ronald W. Breaux, Bill Morrison, Emily Westridge Black, Gavin D. George

Breached companies are often crime victims, but they are also potential targets for regulatory actions (and, as we will discuss in future installments, potential parties to a wide range of litigation). Therefore, as soon as you discover – or reasonably suspect – that your organization has suffered a breach that may have resulted in acquisition of sensitive or personal information by unauthorized parties, you should begin considering your disclosure obligations and your exposure to regulatory actions. In this installment of our special series, A Desk Guide to Data Protection and Breach Response, we discuss disclosure and enforcement actions by regulators, including state attorneys general, the U.S. Federal Trade Commission (the "FTC"), and the U.S. Department of Health and Human Services (the "HHS").

State Law Disclosures and Regulatory Actions

In the United States, disclosure of breaches of personal information (also referred to as "personally identifiable information" or "PII") is largely governed by the law of the state(s) where the affected individuals reside. Accordingly, in the event of a known or suspected breach, you should determine as quickly as possible whether PII may have been exposed and, if so, whose PII was exposed and where those individuals reside.

Currently, 46 states, the District of Columbia, and several U.S. territories have enacted laws requiring companies to notify their residents of breaches involving personal information. As we explained in our first installment, the precise definition of "personal information" varies by state, but it typically includes names combined with social security numbers, driver's license numbers, state ID card numbers, or financial information (e.g., bank account numbers or credit or debit card numbers). Some states' definitions of PII include additional information, such as medical data, tax identification numbers, or passport numbers.

Under most state laws, disclosure obligations are triggered when a company knows or reasonably believes that personal information was acquired by unauthorized third parties, and disclosures are to be made in the most expedient time possible and without unreasonable delay. However, many states provide for delayed disclosures under certain circumstances, including (1) when delay is necessary to determine the scope of the breach, (2) while the company is securing the integrity of the data system, or (3) at the request of law enforcement. Some, but not all, of the states that provide for law enforcement delay require the request to be in writing (or even require that the written request be provided to the state attorney general), so if law enforcement requests that you delay disclosure, you should examine the laws of the relevant states before complying with an oral request alone.

The timing of disclosures is critical. Disclosing companies face intense, negative scrutiny regarding perceived delays in disclosure from a variety of entities, including politicians and regulators, the media, and consumers and consumer advocacy organizations – even when the "delays" are no more than a few days. Certain state attorneys general have been active in investigating the timing of disclosures, and they have been taking action – ranging from warning letters to civil prosecution – against companies whose disclosures they deem untimely. For example, the California attorney general recently filed a case against Kaiser Foundation Health Plan, Inc. alleging that Kaiser's notification to current and former employees – who were California residents – regarding a breach of their personal information was unreasonably delayed. The attorney general alleged that Kaiser should have provided notice of the breach to affected individuals on a rolling basis as soon as it determined that each individual's information had been or was "reasonably believed to have been breached" – even before Kaiser concluded its internal investigation.

Actions by the FTC

Companies that have suffered a data breach can become the target of an enforcement action by the FTC, which is the most active federal government regulator when it comes to ensuring that businesses protect personal information. The FTC is responsible for enforcement of the Children's Online Privacy Protection Act ("COPPA"), the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act of 2003, and (along with the HHS Office for Civil Rights) the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009. And, starting in the 1990s, the FTC began bringing privacy enforcement actions to address "unfair" and "deceptive" trade practices under Section 5 of the FTC Act.

Typically, an FTC enforcement action begins with a claim against a company that it has committed an unfair or deceptive trade practice or has violated one of the statutes mentioned above. A data breach is not a prerequisite for an FTC action, but when a data breach has occurred, the FTC generally has little trouble concluding that a company has been deceptive or unfair in its data protection promises or practices.

Once a claim is initiated, the FTC will investigate the company, and may initiate an enforcement action if it believes the claim has merit. Most FTC enforcement actions are settled through consent decrees, through which subject companies agree to change their practices, but do not admit wrongdoing. The terms of consent decrees vary depending on the violation, but many recent consent decrees require companies to undergo periodic third-party audits of their privacy practices for up to twenty years. A good example of this is Twitter's consent decree to settle FTC charges related to a hack of its service in 2009. Consent decrees can also include the payment of significant monetary penalties. For example, a company agreed in 2012 to pay $22.5 million to settle claims by the FTC that it misrepresented privacy protections to consumers, even though no data breach occurred.

Occasionally, enforcement actions are not settled through a consent decree, and instead lead to a full trial before an administrative law judge. The hotel company Wyndham Worldwide and the medical facility LabMD are currently involved in separate data security suits with the FTC related to data breaches suffered by each company.

The FTC has broad discretion to label privacy practices "unfair" or "deceptive," especially if a data breach has occurred. But the FTC has not issued any regulations that would provide more detail to companies looking to avoid an FTC investigation. Counsel with an understanding of previous FTC enforcement actions is often the best source of guidance on the types of privacy practices the FTC may find objectionable. Additionally, the FTC published guidelines titled "Fair Information Practice Principles" in 2009, which highlight the FTC's privacy enforcement priorities. Those guidelines encourage companies to address five core principles of privacy and data security: (1) notice and awareness, (2) choice and consent, (3) access and participation, (4) integrity and security, and (5) enforcement and redress.

U.S. Department of Health and Human Services Enforcement

As we discussed in the first installment of this Series, personal health information is protected in the United States under the federal Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the HITECH Act. The HHS (along with the FTC) is responsible for enforcing HIPAA's Privacy and Security Rules, which apply to health care providers, health insurers, and their vendors ("Covered Entities"). When Covered Entities suffer a breach of unsecured protected health information ("PHI"), they must file a breach report with the HHS. (The size of the breach determines the timing of the report. Breaches involving more than 500 affected individuals must be disclosed within 60 days of discovery of the breach; there is more leeway on the timing of disclosure for smaller breaches.) The HHS has been active in bringing enforcement actions against companies that violate the Privacy and Security Rules. For example, it recently settled a case against Affinity Health Plan involving a breach of PHI of more than 300,000 individuals. In that case, the HHS alleged Affinity impermissibly disclosed PHI that had been stored on the hard drives of leased photocopiers by returning the copiers to the leasing agent without wiping the drives. Affinity was required to pay more than $1.2 million to settle the case.

Other Regulatory Exposure

Depending on a company's profile, it may also be exposed to enforcement actions by other regulatory bodies. For example, U.S. issuers may face scrutiny from the Securities and Exchange Commission for failure to fully or timely disclose a material data breach. Additionally, companies that do business internationally may own or control databases in the United States that contain personal data belonging to foreign citizens, potentially subjecting U.S. companies to foreign privacy laws and enforcement action by foreign regulators.

Pursuing Justice: How to Refer a Cyber Incident to Law Enforcement

David Siegal, Jason S. Juceam

When a company falls victim to a damaging cyber attack or suffers a theft of sensitive data or intellectual property, the incident very well may fall within the ambit of one or more criminal statutes designed to deter and punish perpetrators with the prospect of jail time, financial penalties and restitution. Under appropriate circumstances, the company should give serious consideration to making a referral to law enforcement as part of its response strategy. In this installment of our special series, *A Desk Guide to Data Protection and Breach Response*, we highlight three relevant federal criminal laws, and outline some practical considerations for making such a referral.

Computer Fraud and Abuse Act

Under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, any person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" is guilty of a federal crime.[1] This statute has wide-ranging application, because courts have interpreted the words "protected computer" to cover any computer that is connected to the Internet. An outsider who bypasses firewall protections and hacks into a company to steal valuable data or destroy or disrupt a company's service is subject to the criminal penalties of CFAA which, in the case of a felony violation, can include up to five years imprisonment (or ten years for repeat offenders) in addition to a fine of up to $250,000 or two times the loss to the victim, a mandatory order of restitution and forfeiture. Conduct rises to a felony if it is committed for commercial advantage or private financial gain, or if the value of the information obtained exceeds $5,000.

A key issue in any CFAA case will be whether the alleged conduct constitutes access "without authorization" or access that "exceeds authorization." As we discussed in prior alerts, the federal circuits are split on whether the statute applies to situations where the perpetrator's initial "access" to data was permitted (such as by an authorized employee with password permissions), but who then used the data for an impermissible purpose – i.e., in a disloyal manner or in violation of the employee's contractual or fiduciary duties.[2]

Notably, although initially adopted as a criminal statute, CFAA was subsequently amended to incorporate a civil private right of action. A company may bring suit under CFAA for damage or loss stemming from violations of the Act if the harm exceeds $5,000.

The Economic Espionage Act

The Economic Espionage Act ("EEA"), 18 U.S.C. § 1832, makes it a federal crime to steal trade secrets for the benefit of a corporation or an individual. Defendants violate the EEA if, with the intent to convert to their own use, and with the intent of, or knowing that their conduct will injure the owner of the trade secret, they

either (i) steal a trade secret, (ii) without authorization communicate a trade secret to a third party, (iii) receive or purchase a trade secret with knowledge that the trade secret has been stolen, or appropriated without authorization, (iv) attempt to commit any of (i) through (iii), or (v) conspire with one or more persons to commit any of (i) through (iii).

Under the EEA, individuals are subject to up to 10 years imprisonment in addition to fines, restitution and forfeiture, and corporations are subject to fines of up to $5 million.

The EEA adopts an expansive definition of what qualifies as a trade secret. All forms of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, regardless of how they are stored, can be considered trade secrets under the statute.[3] In order for such property to fall within the statute, the owner must have taken measures to protect it from being disclosed, and it must possess independent economic value.

When determining whether to prosecute under the EEA, the government will consider the protective measures a company adopted to preserve the secrecy of the information, and the extent to which keeping the information exclusively in the possession of the company (and out of the public domain) would preserve its actual or potential economic value. Protective measures such as use of confidentiality agreements with employees and non-disclosure agreements with outside entities, implementation of electronic firewalls, requiring of password-only access, and designating documents "confidential" can all be considered sufficient to warrant trade secret protection under the EEA.[4]

Importantly, it is not enough to prove that the defendant took some valuable data or idea to use for their own benefit. The EEA further requires the government to prove that a defendant intended by his conduct to injure the trade secret's holder, and this is often the issue upon which the viability of such a charge turns. The statute seeks to prevent employees (and their future employers) from taking advantage of confidential information gained and taken from one employer and transferred elsewhere, to the detriment of its original owner.

The National Stolen Property Act

The National Stolen Property Act ("NSPA"), 18 U.S.C. § 2314, makes it a criminal offense for a person to "transport[ ], transmit[ ], or transfer[ ] in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud."[5] Federal courts interpret the words "goods, wares, or merchandise" to require proof that the property in question came in some tangible form. As a result, a primary inquiry in NSPA cases involving electronic data theft is whether the stolen property can be considered "tangible" in some respect.

Courts have held that the theft of purely intangible property embodied in a purely intangible format – such as the unauthorized uploading of proprietary trade data onto a third-party server – does not violate the NSPA. Accordingly, indictments lacking an allegation that the stolen property was taken in some physical

form will be dismissed.[6] By contrast, individuals charged with stealing electronic data through a physical manifestation – such as by printing computer code onto sheets of paper, or saving data to a CD-Rom or thumb drive which is then carried out of the building – are subject to criminal liability under the NSPA.[7]

An NSPA conviction carries with it the prospect of up to 10 years imprisonment, fines, restitution and forfeiture.

Practical Considerations

A successful referral of a data security intrusion to law enforcement carries the prospect of obtaining a swift resolution and potential court-ordered and government-enforced restitution, as well as potential favorable collateral effects on any related civil litigation. However, when contemplating the prospect of making a criminal referral, a company must consider a host of complex and sensitive issues including, among other things, whether the conduct rises to a level warranting criminal punishment; whether a referral might unduly delay or hinder pursuit of civil remedies; how (if at all) the lack of control over the pace and scope of a government investigation would impact the company's own internal investigation efforts; and whether the company will be waiving privilege over investigative findings for purposes of future litigation if it turns information over to law enforcement.

Knowledge of the criminal standards in advance, however, can help a company improve the likelihood of a successful referral should it ultimately decide to employ such a strategy in the wake of an attack. Implementing effective access restrictions over sensitive or valuable electronic data on a need-to-know-only basis can be important to establishing a CFAA violation in an employee data breach scenario. Similarly, taking various measures to protect trade secret information, such as the use of confidentiality and non-disclosure agreements, the appropriate labeling of sensitive materials with the words "confidential" or "secret," and the regular enforcement of employment rules respecting proprietary information, can help the government establish the elements of an EEA infraction. Instituting such safeguards demonstrates not only the secret nature of the information in question, but can also help prove its value.

For purposes of satisfying jurisdictional or sentencing thresholds relating to the amount of loss incurred, expenses relating to remediating the damage caused by a cyber attack are counted, so companies should take care to keep records of those expenses as they work through their recovery.

Finally, nothing helps speed the process of making a successful criminal referral as much as strong, irrefutable proof of the electronic theft or intrusion conduct. In cyber attack situations, the best proof will often be found in technological computer evidence stored in a company's servers – logs of activity such as log-in times, transaction trails and keystroke recordings – information typically mined and analyzed by computer forensics teams. This evidence, if not immediately preserved in the wake of the discovery of a cyber incident, is susceptible to loss through normal system operations. Thus, companies should take care to know and understand how their systems work, and when responding to an attack, take immediate steps to prevent loss of data, including metadata and other system information not typically accessed by the business in the normal course.

_____

1 18 U.S.C. § 1030(a)(2)(C).

2 Compare United States v. Jones, 597 F.3d 263, 271-73 (5th Cir. 2010) (broad view) with United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (restrictive view); see also JBCHoldings v. Pakter, 931 F. Supp. 2d 514 (S.D.N.Y 2013) (collecting cases and describing Circuit split).

3 18 U.S.C. § 1839.

4 See United States v. Shiah, 2008 U.S. Dist. LEXIS 11973, at *60-62 (C.D. Cal. Feb. 19, 2008).

5 18 U.S.C. § 2314.

6 See, e.g., United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012); United States v. Zhang, 2014 WL 199855 (E.D. Pa. Jan. 17, 2014).

7 See, e.g., United States v. Agrawal, 726 F.3d 235, 247 (2d. Cir. 2013).

The Firestorm: Civil Litigation and Class Actions Following a Cyber Incident

Ronald W. Breaux, Thad Behrens, Daniel H. Gold, Emily Westridge Black, Pierre Grosdidier, Ph.D.

As soon as your company has tangible evidence of a data breach, you must start thinking about what a lawsuit would entail, especially in light of the complexity of electronic evidence. In this installment of our special series, *A Desk Guide to Data Protection and Breach Response*, we discuss the firestorm of litigation that can arise following a breach and provide practical guidance for preparing for the worst.

In general, your company should anticipate two types of lawsuits following a breach or cyber incident. First, you might want, or might have no choice but, to sue the perpetrator. This situation typically arises when a rogue or disgruntled employee leaves with confidential information, deletes information on company computers, or - worse - plants a time bomb that will do damage long after the employee is gone. But offensive litigation may also arise in the context of an outside hacker if the company has enough evidence to identify the perpetrator. In all of these cases, your company would be the plaintiff and could decide whether or not to sue.

Second, companies that are victims of data breaches can be - and often are - sued by third parties. This situation most commonly arises when a hacker seizes consumer private information held by the company, and the suit typically takes the form of a class action against the company. In this fact pattern, the company is the defendant and has no option but to defend itself. Planning for this litigation early is critical.

Offensive Litigation

Before filing a lawsuit based on a cyber incident, it is important to think through your litigation objectives. An offensive lawsuit might seem like the right thing to do, but further publicizing the data breach could rattle your clients' confidence in your company. Consider also the difficulty of presenting abstract computer forensic evidence to a jury and the difficulty of recovering any judgment you might obtain. In addition, always consider whether the facts of the case merit referral to law enforcement for possible criminal investigation, which might put the bad actor out of business at no cost, and perhaps with less publicity, to your company than offensive litigation.

The next step, if you decide to sue, is to identify your causes of action. Victims of data breaches almost always pursue common law causes of action, such as breach of fiduciary duty, trade secret theft, and trespass to chattel. If the defendant is a former employee, causes of action may lie in the terms of employment. Consider also whether claims exist under the Stored Communications Act (18 U.S.C. § 2701 et seq., the "SCA") or the Computer Fraud and Abuse Act (18 U.S.C. § 1030, the "CFAA"). Both of these federal statutes create private rights of action for criminal conduct. The CFAA, for example, criminalizes unauthorized access (or exceeding authorized access) to computers involved in interstate commerce, which today effectively means any computer connected to the Internet.

There is a split among the federal circuit courts regarding key issues related to both the SCA and the CFAA so it is important to first analyze how federal courts in your circuit have construed these statutes. Consider also whether to sue under your state's computer trespass law. These laws often prohibit conduct more broadly than either the SCA or the CFAA.

Defensive Litigation

The more likely result following a data breach is that the breached company will be sued by those allegedly impacted by the breach. Following a breach involving payment card data, for example, consumers whose data was stolen may sue your company under negligence theories or state consumer protection laws. These claims are typically filed as class actions but (could also be filed on an individual basis). To date, these actions have been largely unsuccessful because consumers typically are not responsible for fraudulent charges on their accounts, and breached companies typically offer credit monitoring or other fraud resolution services to affected consumers. Thus, courts have routinely held - with some exceptions, primarily in the context of statutory damages claims - that consumers impacted by a payment card breach have not suffered any damages and have no standing to sue the breached company.

In putative class actions where plaintiffs survive a motion to dismiss, they face the additional hurdle of class certification. Issues of standing and damages suffered in a breach will likely be individualized, making it difficult to argue that common questions "predominate" over individual questions - a mandatory showing under Federal Rule of Civil Procedure 23(b)(3), the provision upon which most classes seeking monetary relief rely. There may also be individual issues regarding liability (such as issues of reliance or consent) or ascertainability problems with the proposed class definition.

In the wake of the Target breach, it is clear that defensive litigation following a data breach may not be limited to consumer lawsuits. For instance, banks that issued payment cards impacted by the breach have sued Target directly to recover their costs of replacing stolen payment cards and reimbursing consumers for fraudulent charges on their accounts. It is too early to know whether these claims will be successful, but the Fifth Circuit recently allowed negligence claims brought by issuing banks to proceed against a payment card processor that suffered a breach allegedly due to its lax security. Target's directors and officers have been sued derivatively as well. Target investors have brought claims for breach of fiduciary duty, gross mismanagement, waste of corporate assets, and abuse of control.

Practical Guidance

In case of a breach or cyber incident, think data preservation immediately. Electronic data preservation is essential to reconstruct what happened in a breach, foreclose any accusation of spoliation, potentially assist law enforcement in identifying the perpetrators, and provide the grounds to prosecute or defend future litigation. Skilled counsel, typically with the assistance of forensic experts, can help you decide what to preserve and how to preserve it.

What to Know When Pursuing Coverage For A Cyber/Privacy Breach

Micah E. Skidmore, Leslie Conant Thorne

During an investor conference call on Wednesday, February 26, Target CFO John Mulligan reported that the highest profile data breach of 2013 cost the retailer $61 million in out-of-pocket expenses during the fourth quarter, of which $44 million was covered by insurance.[1] While Target has not disclosed additional detail regarding the costs insured under any network/privacy policy, this much is clear - Target was successful in pursuing coverage for a significant portion of its existing breach-related losses. Just as placing cyber coverage involves a series of important considerations, pursuing coverage for a cyber breach also requires understanding of the various rights and duties owed by and to insureds under their policies. In this final installment of our series, *A Desk Guide to Data Protection and Breach Response*, we outline four key considerations that every company should be aware of in pursuing coverage for claims and losses arising out of a cyber/privacy breach.

Notice to the Insurer

In the event of a cyber-attack, and particularly one involving the disclosure of "personal information," notice to regulators, law enforcement and affected individuals may be mandated by statute. For companies responding to a network/privacy breach, compliance with contractual notice obligations - including those in applicable insurance policies - is also mandatory. Each network security or privacy liability policy contains a section describing the insured's duties in the event of a claim or loss. Because network and privacy liability policies contain attributes of both first-party and third-party insurance, the insured's duty to give notice may depend on the type of exposure at issue.

With respect to liability, or third-party coverage, inevitably, the insured must give written notice to the insurer "as soon as practicable" after a defined individual or set of individuals becomes aware of a claim or suit. In any event, notice under "claims made" policies must be given during the policy period or an extended reporting period (usually 30-90 days after policy expiration), if applicable. So long as the notice is given within the applicable policy/reporting period, the insurer may have to show prejudice to deny coverage on the basis of notice that is otherwise not given "as soon as practicable."

Most policies will also allow the insured to give notice of a potential claim or circumstances likely to give rise to a claim, with the understanding that a future claim will be deemed to have occurred at the time the original notice was given, even if the potential claim is made after the expiration of the noticed "claims made" policy. Because future policies may not insure claims about which the insured was or should have been aware at the time the future policy is placed, companies should also carefully determine whether circumstances exist that are likely to give rise to a claim and report appropriately before existing coverage and notification periods expire. This decision should be made in consultation with counsel to the extent that notification of a potential claim could have implications for the insured's liability in a future claim.

Depending on how broadly the term "claim" is defined in a given policy, policyholders must be careful to provide notice of "claims" that may not intuitively merit reporting to the insurer, including regulatory actions and any demand for monetary or other relief. Policyholders should also consider which individuals' knowledge will trigger reporting obligations under an applicable network security or privacy liability policy and plan accordingly to ensure that information flows appropriately from those with critical knowledge to those with responsibility for giving notice to the insurer.

With respect to first-party coverage, a policyholder's notice obligations may be triggered by one or more individuals' awareness (or reasonable belief) that an event, injury or wrongful act, as opposed to a claim or suit, has occurred. Notice requirements for first-party coverage may also include the obligation to alert law enforcement and to document the insured's loss in a "sworn proof of loss." As with third-party coverage, policyholders seeking coverage for first party exposure should know which persons' awareness and which events require notice to the insurer.

Timely compliance with a network and privacy liability policy's notice provisions is important and should be part of the company's breach response plan. If a company is reliant on third-party contractors to facilitate network security, policyholders should demand or otherwise ensure that appropriate notice is given under policies that cover the company as an additional insured or may provide a source of redress for damages sustained in a cyber-attack.

Selection of Counsel & Forensic Investigators

When a data breach occurs, the benefits afforded under a network security or privacy liability policy may include the retention of legal counsel as well as forensic investigators to identify and respond to the cause of first-party and third-party loss. In connection with these benefits, disputes may arise regarding the choice of the counsel or consultant to be retained. With respect to counsel, in most cases, the insurer assumes no duty to defend under a network and privacy liability policy. The insured typically retains the right to select counsel. Although, textually, the insurer may also retain the right to consent to defense costs incurred by the insured. In other cases, depending on the policy terms, the insurer may in fact have a "duty to defend," and a concomitant right to select counsel, or have designated pre-approved panel counsel from among whom the insured is contractually required to choose for its defense.

After receiving notice from an insured of a third-party claim, the insurer generally has three options: (1) accept coverage without qualification; (2) deny coverage outright; or (3) issue a reservation of rights identifying potential issues that may affect coverage for indemnity while agreeing to pay for the insured's defense. Many jurisdictions have long recognized that when an insurer has asserted coverage defenses that overlap with the facts that are to be adjudicated in an underlying claim or suit, defense counsel selected by the insurer has a conflict of interest that justifies the insured in retaining independent counsel to be paid for by the insurer. If and when disputes arise regarding the right to select counsel, policyholders should review the insurer's "reservation of rights" carefully to determine whether a disqualifying conflict of interest exists, entitling the insured to select the lawyer of its choosing to defend the claim or suit.

With respect to experts and consultants, policyholders may be obligated by contract to undergo a forensic investigation upon discovery of a data breach. Particularly, if the breach involves unauthorized access to payment card information, the major payment card brands may contractually require an investigation by a forensic investigator pre-approved by PCI Security Council, which consists of representatives from the card brands. The insured may elect to perform its own investigation, and may seek coverage for the cost of that investigation from a network security or privacy liability carrier. The insurer responding to notice of a breach under a cyber/network security or privacy policy may insist upon the retention of a select group of forensic consultants with whom the insurer has negotiated reduced rates. If there are unresolved coverage issues, the policyholder should again consider whether a disqualifying conflict exists that would enable the insured to select its own independent consultant to be paid for by the insurer. Alternatively, if the insurer does not identify any coverage issues before pursuing an investigation using its own "panel" consultant, the question becomes whether the insurer waived coverage defenses if the results of the investigation would otherwise prejudice the insured.

Protecting Privileged Communications

Communications made in responding to a network or privacy breach are important. Characterizations, whether well-founded or speculative, of events and circumstances relating to the breach, including whether personal information has been compromised, when the breach occurred, and when it was discovered, may have significant implications for the policyholder's liability to third parties and its insurance coverage. Ideally, the insured's data breach plan will include some procedure to control the flow of external communications regarding the breach. When appropriate, counsel should be engaged early to ensure that specific communications, including those made in anticipation of litigation or otherwise entitled to privilege, are controlled.

As a general proposition, materials prepared and communications made in anticipation of litigation, including communications with an "insurer," may be protected from disclosure as "work product." In some jurisdictions, communications between an insured and its liability insurer regarding a matter of common interest between them are deemed privileged. In other jurisdictions, this "common interest privilege" does not extend to communications with an insurer that is not a party in pending litigation. Moreover, given the dual nature of network security and privacy liability policies in insuring both third-party and first-party claims, some communications between the insured and its cyber insurer may not qualify as being made in anticipation of litigation. Policyholders and their counsel should be aware that communications with a network and privacy insurer may not be protected from disclosure to third-party claimants or regulators and should act accordingly (particularly when unresolved coverage issues remain between the insurer and its insured).

Do Not Overlook Traditional Insurance Coverage

Even for those policyholders benefitting from a dedicated network or privacy liability policy, pursuit of coverage for a data breach should include consideration of the recovery potentially available under more

traditional policies, including general/E&O/D&O liability insurance, commercial property insurance, and crime/fidelity insurance.

Commercial general liability ("CGL") insurance typically contains two principal coverage parts, A & B. Coverage A insures sums that the insureds become legally obligated to pay as damages because of "bodily injury" or "property damage" caused by an "occurrence" during the policy period. Coverage B typically insures sums that the insureds become legally obligated to pay as damages because of "personal and advertising injury" caused by various enumerated "offenses" committed during the policy period, including false arrest or imprisonment, malicious prosecution, wrongful eviction, slander, libel, business disparagement, publication that violates a person's right of privacy, use of another's advertising idea in an advertisement, or infringing on another's copyright, trade dress or slogan.

In some circumstances, "property damage" may arise out of a cyber breach. Moreover, Part B's specific coverage for "[o]ral or written publication, in any manner, of material that violates a person's right of privacy" may apply to a data breach that results in the "publication" or disclosure of customers', employees', or other parties' private, personally identifiable information.

Commercial property insurance generally provides coverage for all risks of direct physical loss or damage to real and personal property, subject to exclusions. The loss of use of computer hardware and even data caused by a cyber-attack may qualify as direct physical loss, and the resulting damage, including business interruption, may be covered by a traditional commercial property policy, subject to the particular terms and exclusions that may be found in any given policy form. Likewise, the loss of an insured's product, the theft of trade secrets or other personal property in a cyber attack may also result in physical loss or damage triggering coverage under a commercial property policy. Physical damage to property, such as the damage reported to a water pump from a cyber penetration at an Illinois utility in 2011,[2] would also fit within the coverage traditionally afforded by a commercial property policy.

While crime and fidelity insurance usually excludes coverage for the loss of intellectual property and there may not be coverage for the theft of personal information or other intangible data from a cyber-attack, policyholders faced with a data breach should not overlook the potential for recovery under such policies. Even some quasi third-party liabilities directly resulting from the theft of customer information may be insured under a crime policy under recent authority.

_____

1 Dhanya Skariachan & Jim Finkle, Target shares recover after reassurance of data breach impact, Reuters.com (Feb. 26, 2014), available at http://www.reuters.com/article/2014/02/26/us-target-results-idUSBREA1P0WC20140226.

2 See, e.g., Ellen Nakashima, Foreign Hackers Targeted U.S. Water Plant In Apparent Malicious Cyber Attack, Expert Says, THE WASHINGTON POST (Nov. 18, 2011) (describing damage done to a water pump at an Illinois water utility through controls exerted from an ip address in Russia), available

athttp://www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html.

The Haynes and Boone Team

Thad Behrens
Partner
thad.behrens@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5668
F +1 214.200.0886

Ronald W. Breaux
Partner
ron.breaux@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5688
F +1 214.200.0376

Randall E. Colson
Partner
randy.colson@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5665
F +1 214.200.0405

Daniel H. Gold
Partner
daniel.gold@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5154
F +1 214.200.0526

Bill Morrison
Partner
bill.morrison@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5018
F +1 214.200.0604

David Siegal
Partner
david.siegal@haynesboone.com

New York
30 Rockefeller Plaza
26th Floor
New York, New York 10112

T +1 212.659.4995
F +1 212.884.8230

Micah E. Skidmore
Partner
micah.skidmore@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5654
F +1 214.200.0659

Leslie Conant Thorne
Partner
leslie.thorne@haynesboone.com

Austin
600 Congress Avenue
Suite 1300
Austin, Texas 78701

T +1 512.867.8445
F +1 512.867.8615

John Podvin
Counsel
john.podvin@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5059
F +1 214.651.5490

Kenya S. Woodruff
Counsel
kenya.woodruff@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5446
F +1 214.200.0945

Emily Westridge Black
Associate
emily.westridgeblack@haynesboone.com

Austin
600 Congress Avenue
Suite 1300
Austin, Texas 78701

T +1 512.867.8422
F +1 512.867.8605

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

Gavin D. George
Associate
gavin.george@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5148
F +1 214.200.0453

Pierre Grosdidier, Ph.D.
Associate
pierre.grosdidier@haynesboone.com

Houston
1221 McKinney Street
Suite 2100
Houston, Texas 77010

T +1 713.547.2272
F +1 713.236.5664

Samuel S. Jo
Associate
sam.jo@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5397
F +1 214.200.0618

Jennifer S. Kreick
Associate
jennifer.kreick@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5492
F +1 214.200.0381

Timothy Newman
Associate
timothy.newman@haynesboone.com

Dallas
2323 Victory Avenue
Suite 700
Dallas, Texas 75219

T +1 214.651.5029
F +1 214.200.0611

William O'Neill
Associate
william.oneill@haynesboone.com

Orange County
18100 Von Karman Avenue
Suite 750
Irvine, California 92612

T +1 949.202.3054
F +1 949.202.3154