Focus | LAW

Data breach Security: A new world of litigation

• A knowledgeable data breach attorney can assure that the threat of litigation is managed correctly.

The phrase "data breach" conjures up an image of Tom Cruise dangling horizontally from two cables in a room full of lasers as he attempts to steal secret files from a government database. However, in the real world data breaches are much less glamorous. They occur whenever a company's information pertaining to its customers is compromised. That information includes social security numbers, credit and debit card numbers, checking account numbers, and information about the customer's identity.

How the company loses those documents varies from simple accidents — such as leaving customer information in public spaces — to malicious activity wherein disgruntled employees and hackers deliberately leak private information. A breach can be devastating to a company and can result in negative publicity, legal fees, fines, and costs associated with identifying and fixing the breach. Expert guidance regarding state and federal laws regulating data breaches can be invaluable in saving a company's time, money and reputation.

Data breaches are not just a problem faced by Fortune 500 companies. In fact, most data breaches require very little sophistication and very little effort. According to a report published by Verizon, 78 percent of data breaches required very low computer sophistication. The report broke down four different groups of people that participate in data breaches: activists, criminals and corporate spies; however, the fourth and fastest growing group is a company's own employees.

The report analyzed which employees were likely to contribute to an internal data breach and found that customer service employees have a high chance of leaking customer information because of dissatisfaction in the work place. In addition to disgruntled employees, a company's administrators have a high likelihood of leaking information due to accidentally leaving information in public or by failing to properly secure the information. Surprisingly, the Verizon report found that small and mid-size companies like "mom and pop" stores and retailers are the most susceptible to a breach.

In Utah, a data breach occurs if a company loses an electronic document containing a person's name and any of the following: a social security number, debit or credit card number, checking or savings account number or a driver license number. Utah's law requires the company to notify each person affected by the breach. If the company fails to comply with the law, the attorney general can issue a $2,500 fine for each person affected.

The maximum fine for a data breach affecting more than one person is $100,000. This law is troublesome because compliance requires the company to notify each individual affected by the breach. Those people will likely disclose the breach to others, which has a high potential to harm the company's public image. Another risk of compliance with the law is that notifying the individuals affected by the breach increases the chance that the affected people will pursue costly litigation, which will likely cost more than the fines issued by the attorney general.


Tsutomu Johnson


Adam M. Pace


Robert Denny

A knowledgeable attorney can assist with three primary concerns when it comes to protecting a company from a data breach: how to prevent a data breach; how to manage a crisis if a data breach occurs; and how to prepare for litigation if a data breach does occur.

A company can prevent a data breach by working closely with attorneys and network system specialists who can review the entry and exit points for data pertaining to their customers, and create policies that strictly manage access to information. The company should also implement procedures to encrypt data and allow the company to monitor whether that data is being accessed without authority. While there are many companies that provide network systems testing, very few provide actual legal analysis to prepare customers for the legal ramifications of a data breach. Therefore, it is important to identify counsel who can provide expert legal advice about the various state and federal laws affecting a company after a data breach.

When a data breach occurs, it is essential to involve knowledgeable attorneys early on so that they can organize efforts to identify what data has been lost, what cus-

see DATA BREACH pg. F10

Focus | Law

STOP, LOOK

from p. F1

ball arbitration" provision. In "baseball arbitration," each party puts on its evidence and then gives the arbitrator a number. The arbitrator is required to choose one number or the other.

Again, your legal counsel can best advise you on the advantages and disadvantages to your business of an arbitration provision. Getting that advice before you sign the contract makes a lot more sense than getting it after you have received an arbitration demand in the mail.

Another provision that must be scrutinized during negotiations is any indemnification provision. Many contracts contain these provisions, and they are often overlooked as a "standard" provision having little impact. That is a trap for the unwary, and can prove fatal to a business. I have seen companies struggle mightily when on the wrong end of one of these provisions.

An "indemnity" is a contractual promise by which one party agrees to save another party from the legal consequences of certain conduct. If your business promises to "defend" the other company and "hold it harmless" (which is what the indemnification provision usually looks like in a contract), watch out. You have just issued an insurance policy.

If a claim is made on that insurance policy, you could be paying lawyers to defend that company from a broad array of claims, even if the lawsuits are frivolous. And if that company loses, you may have to pay the judgment on its behalf.

My best advice on indemnification provisions is always to get one from the other side and never give one. Sometimes that works. More often, however, parties insist on indemnification provisions applying to both sides. It is critical for your business to stop and look at the proposed transaction very carefully before agreeing to indemnify.

By way of example, if you are buying potentially dangerous products from a company that is new to you, it would be critical to get indemnification "insurance" from the seller. If you are the seller, you likely do not want any indemnification provision in the agreement.

Just as with arbitration provisions, indemnification provisions can be improved (from your company's standpoint) if the other side insists on having one. Issues such as choice of law may be tremendously important. For instance, if you are providing the indemnity, you likely would prefer to have New York law apply than California law. In New York, indemnification provisions are generally construed far more narrowly than in California.

Under Utah Law the duty to defend and the duty to indemnify are construed broadly (similar to California's approach). However, most states, including Utah, have what are known as "Anti-Indemnity" statutes which restrict parties under certain circumstances from agreeing to indemnify another party for that party's own negligence. Typically, these statutes are limited to the construction industry, but each state's laws in this area are different. Once again, this underscores the importance of carefully choosing what law applies to your contract and understanding how that state's law applies in the context of each provision of the contract, such as indemnification.

If you are the party providing indemnification, there also are specific ways you can control your exposure, such as a cap on the total amount to be paid under the indemnity, or even deductibles that must be paid before the indemnity obligation kick in.

If you are the party receiving indemnification, you should ensure that the contractual language covers claims for breach of contract as well as negligence. Further, it is critical that you make clear that the indemnification provision includes the duty to defend. In some states, such as New York, such "duty to defend" language must specify that all reasonable attorneys fees and costs will be paid as they come due by the indemnifying party.

Again, the best practice with respect to indemnification provisions is to seek the advice of counsel before agreeing to one.

Entering into a contract is a bit like trying to cross a busy street: Stop before you sign, look carefully at each part of the agreement and make sure you understand your obligations, and seek and listen to the advice of your lawyer. A slight delay to take these key steps is much better than being hit by the litigation bus.

Jonathan O. Hafen is a shareholder with the law firm of Parr Brown Gee & Loveless. He can be reached at jhafen@parbrown.com or 801.257.7915.

DATA BREACH

from p. F3

tomers have been affected, and whether the lost data triggers the notification requirements under Utah and federal law. Not every loss of documentation constitutes a data breach under the law. The ultimate goal is to minimize the notifications that the company has to make publicly in order to decrease potential lawsuits against the company, protect the company's image, and avoid unnecessary public fear. Employing a qualified team of attorneys to manage a data breach crisis can help the company identify whether a data breach even exists and put their best foot forward when it comes to responding to an actual breach.

Finally, as data breaches become more and more prevalent, the threat of a lawsuit from multiple plaintiffs in class-action lawsuit increases. A knowledgeable data breach attorney can make sure that the threat of litigation is managed correctly, that data has been properly identified, and that the company has properly complied with the law. Moreover, because data breaches potentially affect thousands of documents and customers, it is important to have attorneys who can, from the outset, identify weaknesses and strengths in a data breach case and properly situate the case should it go to trial.

For questions or comments, please contact Tsutomu Johnson, Data Security Practice Group Leader with Snow, Christensen & Martineau. He can be reached at tj@scmlaw.com or (801) 322-9112.

TITLE VII

from pg. F4

would have made it easier for employees to bring Title VII claims. The Supreme Court, however, rejected this approach and chose to define a "supervisor" as one who has the power to hire, fire, demote, promote, transfer or discipline the victim. This ruling limits the number of "supervisors" whose actions might subject an employer to Title VII claims.

The *Vance* and *Nasser* decisions continued a business-friendly trend that was evidenced earlier in the term by the court's decision in *Comcast Corp. v. Behrend*. *Comcast* was not an employment law case, but it dealt with issues of class action certification that routinely arise in employee wage and hour cases. The Supreme Court's holding in *Comcast* makes it more difficult to certify a class and will therefore be a new favorite of employers attempting to defeat class certification in wage and hour cases.

Employer-friendly kick, this is not necessarily the trend in other courts across the country. A recent decision from a federal district court judge in Manhattan should cause employers to examine their unpaid internship programs. The New York court ruled that Fox Searchlight had violated wage laws by failing to pay its interns on the movie "Black Swan" minimum wage and overtime. This decision has opened the floodgates for the filing of similar suits, including actions against PBS host Charlie Rose, Saturday Night Live/NBC Universal, Warner Music Group, Conde Nast, Hearst, and Gawker. Could a similar lawsuit be coming your way? Although the initial focus has been on glamour industries such as film, publishing, and media, other employers would be wise to take a close look at their unpaid internship programs and determine whether the savings really justify the risk.

Finally, with an increasing number of enforcement actions being brought by the Department of Labor and EEOC, employers also need to continue to be vigilant with regard to basic employment law compliance issues including the proper use and classification of independent contractors, determination of exempt status, time and record keeping, tip pooling and proper payment of tipped employees, and maintenance of a discrimination free workplace. Despite some favorable rulings from the Supreme Court, it is still wise for employers to proactively examine their employment practices to prevent, identify and correct potential problems early on, rather than having to rely on this favorable precedent after a claim has been filed.

Joan M. Andrews is an attorney at Fabian, Attorneys at Law. She is chair of the firm's Labor and Employment Group. She can be reached at jandrews@fabianlaw.com

SOCIAL MEDIA

from p. F2

ing comments that "disparage or criticize" the organization, or that discuss wages or other terms and conditions of employment. If in doubt about what activities are protected by the NLRA, consult with an attorney knowledgeable about the NLRA.

Second, be specific about the conduct that is prohibited and give examples that illustrate that the prohibited conduct does not include protected activities. For example, rather than stating generally that employees may not post "confidential" information, state that employees may not post trade secrets, such as confidential information about manufacturing processes, proprietary formulas or technology or products in development; and may not post internal reports or internal, confidential business-related communications. Similarly, rather than stating that employees may not post messages that damage any person or organization's reputation, state that employees may not post statements they know to be false or that reasonably could be viewed as obscene, threatening or contributing to a hostile work environment on the basis of race, sex, religion, disability, age or other legally protected status.

Third, distinguish work from personal time. Employees are entitled to more freedom when on their personal time and using their personal computers than they are when on company time using company computers and systems.

Fourth, include limiting language in the policy to make clear that the policy will not be construed or applied to interfere improperly with rights under the LMRA. As noted above, however, do not stop with just a general statement, but specifically list the rights that are protected such that a reasonable employee would not believe that such rights are prohibited by the policy.

Finally, as always, have your social media policy reviewed by legal counsel for potential noncompliance with the NLRA. Your social media policy should reduce the risk of problems, not increase them. Keep in mind, however, that NLRB rulings are not necessarily the final word on how broadly employers may regulate social media activity of employees, as courts have yet to weigh in.

Mark A. Wagner is a shareholder at Van Cott, Bagley, Corwall & McCarthy, P.C., a member of Van Cott's Litigation Section and Chair of Van Cott's Employment and Employee Benefits Practice Group.