# Davis Brown Employment and Labor Law Blog

## Hacked and Left Holding the Bag – Cyber Liability Issues – May 27, 2016

Jo Ellen Whitney

If you read any newspaper, trade publication or twitter feed, you know that ongoing concerns regarding cyber security continue to grow. We have seen an article in the *New York Times* discussing hacking of major law firms with the belief that some stolen information could facilitate insider trading and another about the termination of an employee of Iowa City Clinics for violating a popular athlete's girlfriend's medical privacy. Data breaches can take many forms and planning for these items involves coordination with your IT department and others to create security protocols, ongoing audits, management of portable devices and employee training. However, what happens when something goes wrong? It is the inevitable truism of all employment law, something will always go wrong.

Early damages in a data security breach case can be extremely difficult to assess as circumstances tend to change rapidly and may depend upon the type of data breached as well as how the breach occurred and how that data might be used. Many industries turn to their existing insurance policies to help mitigate the cost of any data breach issue. However, insurance isn't necessarily a panacea that will resolve all of the problems as multiple cases across the country have shown. If you exclusively manage HR and you don't work with the IT department or compliance, you may be wondering, "Why do I care about the insurance coverage? That's not my area." However, personnel data has proven to be both a popular and very lucrative target for cyber thieves as it is a pirate's treasure trove of saleable information. You manage Social Security numbers, insurance numbers, and all of the information necessary for ongoing identity theft, whether for the creation of fake passports or filing false tax returns. Additionally, personnel processes tend to be very porous with a lot of information coming both in and out of the system at any given point in time making a hack easier to pull off.

Many companies have assumed that they could rely on their existing commercial or other insurance policies to cover the damages that may occur as a result of any data breach. However, as Recall Total Information Management, Inc. v. Federal Insurance Co., 317 Cp, 46; 115A.3d 458 (Conn. May 2015) shows, the exclusions will get you every time. In this case, there was a question as to whether a commercial general liability policy would be


sufficient to cover a fairly significant data breach where stuff - "fell off a truck." Of great concern in this case were the "mitigating" expenses that were incurred, in an attempt to minimize illegal use of the data. Every company that has a data breach is going to attempt to get ahead of the breach. That may include new security, data analysis, audits of systems, notice to the individuals whose information has been compromised and potentially paying for ongoing credit monitoring for those individuals. These issues do not even begin to address the potential cost of mitigating damages for large companies when it is proprietary data such as trade secrets that has been taken. In Recall Total, the Court looked at the issue of the costs of these mitigating measures before any actual damages had occurred to the person referred to in the data. However, when looking for coverage under the commercial liability policy, the Court made a determination that the loss of the data was not the same thing as information being actually used by someone else, and mitigating measures were not covered under the policy. This was true even though the insurance policies in Recall Total did not have a specific exclusion for privacy liability issues that may be found in other companies' insurance policies. In this particular instance, the company at issue had spent more than 6 million dollars in mitigating expenses not related to damage caused by the actual misuse of the information.

Cottage Health System might be the case where you learn by example. In this matter, there was a significant data breach of personally identifiable health information for patients in the Cottage Health System entity. After a settlement was reached regarding these matters, Cottage Health Systems looked to its insurer, Columbia Casualty and its cyber liability policy to provide coverage. However, Columbia Casualty asserted that coverage was not appropriate in this instance because Cottage Health had not taken reasonable security precautions. It had answered the security questionnaire at the time it was seeking insurance coverage in an "aspirational" rather than factually based manner. This included a contention that Cottage Health Systems failed to meet minimum required practices for privacy and security as based upon law and its prior statements. In essence, the company seeking the insurance coverage said it had various security practices in place and the insurance company alleged those weren't really there. It can't insure something that didn't actually exist, calling into place the "you are a big liar" exclusion from coverage.

Another case involving Travelers Property Casualty Company of America and Federal Recovery Services, Inc. looks to the intentional acts of the insured. Travelers Property Casualty Company of America v. Federal Recovery Services, Inc., 103 F. Supp 3d 1297; 2015 WL 2201797 (D. Utah May 11, 2015). In this particular instance, the question became whether or not the insured, Recovery Acceptance, Inc., had engaged in an intentional bad act which resulted in the alleged cyber damages. Global Fitness had a contract with Federal Recovery Services, Inc. to manage credit card and bank account information as well as monthly membership payments. When asked to return all the member data due to a company sale, Federal Recovery refused unless the client paid significant additional sums. This led to a claim of intentional bad acts. It was the contention of Travelers Insurance Company

that intentional bad acts were excluded from its cyber liability policy. This was upheld in the United States District Court for the District of Utah. Case No. 2:2014-CV-00170 (January 27, 2016)

## As an employer there are several things you can do to help limit your risks in these situations:

- **Read The Fine Print**-we are all tempted to skip the fine print. Whether it relates to the exclusion clause or any kind of coverage, insurance policies can be dense and usually don't have the same fun factor as your average summer beach read. However, for budget and crisis planning, it is critical to know what the policy will and will not cover. As noted in the Recall Total Information case, many costs may accrue in the preliminary mitigation stage which might not be covered and other coverage limitations can also apply.
- **How Do Your Policies Work Together-**HR groups are not generally going to rely on a commercial or general liability insurance coverage but will rely on employment practices liability (EPL). Once you have your reading glasses on, you want to look to the issues of how any cyber liability policy and the EPL policy fit together and whether the exclusions carry over or contradict each other. For example, what happens if wages are affected by the data breach; such as an interruption in automatic deposit or if other payroll issues occur? Typically, in many instances EPL policies would exclude damages for unpaid wages or wage hour issues. This may also be true in a cyber liability policy if it works in conjunction with EPL even though the reason was not an intentional failure to pay wages but a data security breach. Make sure you have specific language or riders to cover areas of concern.
- **Don't Make Promises You Can't Keep**-Cottage Health Systems apparently made promises it couldn't keep, including basic security measures and management processes for access and other items relating to its data security. Don't tell the insurance company that you have a 30 day policy for firewall patches, secondary audit capability or that you use two methods of authentication if you don't really do those things. If you have to lie on your insurance questionnaire, it's probably time to rethink your actual practices.
- **Do The Basics**-regardless of whether or not you look to a cyber liability insurance company or choose to wait until the products become more standardized, or never even obtain insurance, do the basics. Do the things that you need to do to at least be able to track and maintain basic security measures. This includes everything from performing regular security and privacy audits, training staff and employees, maintaining physical security and given the large number of data breaches that relate to portable data, inventorying and installing security measures on all portable data devices.