New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 251—NO. 26
MONDAY, SEPTEMBER 21, 2015

Expert Analysis

Big Enough For Your **Breaches**?

Be diligent with cyber risk management and insurance issues as data security perils shift.

BIGSTOCK

BY JOSHUA GOLD

Data security breaches are now legion. Cyber attacks often prove to be multifaceted, resulting in fraudulent transactions, class action litigation,[1] identity theft, liability for regulatory actions, and a slew of other disruptions and damages to business operations. It has become clear that hackers can easily cause liability and losses to even the most well-prepared businesses.

To date, the risk management emphasis has largely been dedicated to addressing potential third-party liability threats. Many companies have focused their efforts on buying cyber insurance to protect against a future privacy rights class action litigation, regulatory investigation, or responsibility for credit card assessments and fines. Similarly, those companies that actually have had to call upon their insurance after data theft have largely sought coverage for charges imposed by others for the theft of data belonging to others. Coverage has been sought for defense of suits alleging theft of medical information and fraudulent card charges, as well as for attorney fees incurred for responding to regulatory lawsuits or inquiries.[2]

JOSHUA GOLD *(jgold@andersonkill.com) is a shareholder of Anderson Kill, a national law firm headquartered in New York, and chairs the firm's cyber insurance recovery group.*

What Are Hackers Now After?

What are cyber thieves after these days? In a word, "You." In isolation, this may seem like an obvious proposition. But the conventional wisdom for the last several years has been that the targets of most serious computer hacks were those possessing sensitive *third-party* information (usually that of their customers, students or patients). Thus, a prime target of computer hacking was often (and continues to be) retailers, financial institutions, hospitals, universities, and medical services companies. Financial account numbers and personal health information were thought to be the crown jewels in the world of data theft.

Lately, however, several high profile attacks appear to suggest a distinctive interest by cyber criminals in the hacked institutions' *own* data. Recent targets of this focus include Ashley Madison, Sony Pictures, and the so-called "Internet of Things."

One way to look at the *Ashley Madison hack* is that it stole third-party information, i.e., member data. The hackers dumped a huge cache of compressed data on the so-called "dark web" of account information for nearly 33 million users. But the hackers reportedly also stole data belonging solely to Ashley Madison. If you take the hackers at their word, they are not doing this to sell credit card numbers to criminal gangs overseas. Instead, their stated goal is to have Ashley Madison shutter its business. The stated rationale: morality.

The attack on Ashley Madison's computer systems is an attack on the core of the company's business model: secrecy. Reportedly, the hackers also obtained internal business information including details concerning server architecture. Apparently, the damage from the hack has been great enough to scuttle a planned IPO.

The *Sony Pictures hack* was another significant cyber breach in which it appears that the hackers' primary focus was to harm Sony Pictures' business rather than grab third-party data to sell to financial criminals for a profit. The hackers stole internal communications between senior company executives as well as proprietary information, and threatened widespread imminent violence at cinemas. The breach ultimately caused Sony Pictures to scrap plans for the distribution of one of its films just before its commercial release.[3] The hackers' stated justification: nationalism, morality, and politics.

Hacks against the Internet of Things[4] constitute yet another example of this shift in focus. While third-party information may be stolen in association with such an attack, a hack upon a device, vehicle or system controlling critical infrastructure will often aim primarily to cause direct injury to or chaos for a hacked party. The implications are harrowing.

As a recent New York Times Op-Ed observed: "Recently, two security researchers, sitting on a couch and armed only with laptops, remotely took over a Chrysler Jeep Cherokee speeding along the highway, shutting down its engine as an 18-wheeler truck rushed toward it. They did this all while a Wired reporter was driving the car."[5]

In Europe some years ago, police suspected a 14-year-old of using an electronic remote device to cause a tram to derail, resulting in numerous injuries.[6] In California, computer hackers admitted to accessing a municipality's traffic network in order to congest traffic as part of a labor dispute. Obviously, such a feat imperils safety, given the effect on emergency vehicles, among other things.[7] Speculation abounds over whether hackers can wrest control of an airliner's turbo fans or infiltrate power plants. Hackers are actually being employed by device and vehicle manufacturers to help insulate and secure computer systems from remote unauthorized access.

Risk Management

From a risk management perspective, these hacks are a reminder that hackers may target an institution with no profit motive in sight. Instead, their attack may be designed to damage your business if not shut you down altogether. If this trend continues, your company may have "first-party" exposures that equal or exceed any liability you may face in the throes of a cyber breach. If your network is damaged, if your website is taken down, if the patronage of your services/merchandise

is tainted by threats of violence, then business income losses can reach catastrophic levels.

New, Specialized Cyber Products

Insurance coverage is available for losses of business income when computer systems are attacked, hacked or damaged. This may be in the form of business interruption insurance coverage, "reputation damage" insurance coverage, network extortion insurance coverage, or some other formulation. Such policies may promise to pay the policyholder for its own losses of business income due to a covered cyber-related event.

There are insurance coverage options specifically dedicated to instances where a hacking incident leads to loss of business income, extra expense, or some other form of loss to the business.[8] For example, one form of cyber insurance promises to pay for "Income Loss and Interruption Expenses … incurred by the Insured during the Period of Restoration as a direct result of the suspension or deterioration of its business caused by the total or partial interruption, degradation in service or failure of the Insured's Network … ."[9] But policyholders will still need to be very careful about how they construct their insurance programs.

For example, if hackers attack an airliner, there can be horrific injuries to passengers, those on the ground, and emergency personnel. In addition, there can be property damage claims and loss of business income. Thus, a catastrophic event like this will lead to liability claims for injuries and property damage, and first-party losses for property and lost income (at a minimum). But many cyber policies will have exclusions for bodily injury or death claims. Meanwhile, some insurance companies are imposing cyber-related exclusions (there are multiple versions of these exclusions varying in scope) into the liability and umbrella insurance policies they sell that protect against liability for bodily injury and property damage. We have even seen cyber related exclusions in some marine cargo policies.

If hacks against the Internet of Things are going to lead to losses, injuries and damage from hijacked elevators, cars and power grids, then the challenge is to apply a big picture approach to insurance coverage. This in turn requires that policyholders work with insurance brokers who are capable of identifying cyber-related insurance gaps and filling them where possible.

Even where there are no gaps in insurance coverage, remember that insurance policy sub-limits often can come into play to limit coverage. Many cyber forms have not only a "module" approach to the various insuring grants they offer for cyber claims, but also sub-limits applicable to certain aspects of insurance coverage within those particular modules. A large "blanket limit" of insurance is a lot less valuable when the majority of important coverages are subject to an absurdly low sub-limit. Again, be very careful here and work with a seasoned broker who can benchmark certain levels of insurance coverage that are right for a policyholder your size and appropriate to your industry.

Cyber Insurance Fine Print

Just because you purchase insurance with the word "Cyber" in the title, does not mean your cyber insurance company intends to pay. A pair of recent insurance coverage lawsuits involving "Cyber" policies make this painfully clear. In *Travelers Property Cas. Co. of America v. Federal Recovery Services*, a May 11, 2015 decision from a federal trial court in Utah denied the policyholder coverage for a customer suit over the handling and return of customer data. While this may be a somewhat odd case, it is a reminder that you have to look beyond the titles of insurance policies.

In another recent case, *Columbia Casualty v. Cottage Health System* (C.C.D. 2015), the insurance company filed a lawsuit in California federal court against its policyholder, Cottage Health System. The policyholder had suffered a breach of patient data and was sued over it. The underlying suit ended with a settlement that the insurance company then argued was not covered due to the policyholder's alleged lax computer security. The insurance company argued that the alleged lax security violated the insurance policy conditions.

The California trial court recently dismissed the insurance company's action for failing to engage in alternative dispute resolution before proceeding to litigation against its policyholder. However, because the dismissal of the insurance company's complaint was made without prejudice, it is possible that this dispute will make its way back to the federal trial court for ultimate rulings on the merits. The issue of coverage conditioned on the robustness of computer security measures employed by the policyholder will be one with major implications for those purchasing cyber insurance.

Damage Systems and Hacking

Even where dedicated cyber insurance is purchased, policyholders should still consider insurance coverage under other business insurance policies that they regularly purchase in the event of a cyber claim.[10] While more and more cyber exclusions are being imposed on other types of insurance policies to encourage the purchase of stand-alone cyber insurance, coverage often still exists under non-cyber policies. For example, in one lawsuit, *NMS Services v. The Hartford*, 62 Fed. Appx. 511, 514 (4th Cir. 2003), the U.S. Court of Appeals for the Fourth Circuit held that the deliberate destruction of computer files and databases by a former employee was covered damage to the policyholder's computer systems.[11]

In *American Guarantee & Liability Insurance v. Ingram Micro*, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. April 18, 2000), a policyholder's computer system went down after a power outage. The federal trial court held that the insurance policy covered the loss, including loss of business income, because the loss of use of programming instructions and custom configurations left the system inoperable and was a covered event under the policyholder's property insurance. See also *Southeast Mental Health Center v. Pacific Ins. Co.*, 439 F. Supp. 2d 831, 837 (W.D. Tenn. 2006) (holding that the corruption of the pharmacy computer was a covered loss of property and the policyholder was owed business income coverage); *Lambrecht & Assoc. v. State Farm Lloyds*, 119 S.W.3d 16 (Ct. App. Tex. 2003) (holding coverage for costs of restoration of data resulting from computer virus).

In *Retail Ventures v. National Union Fire Insurance Co. of Pittsburgh*, 691 F.3d 821 (6th Cir. 2012),[12] the U.S. Court of Appeals for the Sixth Circuit affirmed the federal trial court rulings and found insurance coverage for all losses suffered by a retailer as the result of a computer hack. The losses recovered under the subject crime insurance policy included amounts for stolen credit card account information, checking account data, computer forensic investigation costs, legal fees, call center expenses, P.R. expenses, FTC compliance costs, among other categories of loss.

Conclusion

It is increasingly clear that liability for the theft of third-party data is not the only cyber peril to be concerned about. The risk of hackers targeting a company's core assets to inflict harm or damage to its ability to operate is very real. With the Internet of Things gaining greater traction, this risk profile will only increase. Policyholders are wise to conduct an insurance and risk management check-up that extends beyond safeguarding employee health data and customer account data. There are options in the insurance marketplace to help protect against these broader operational and reputational risks. The insurance products, however, sometimes leave something to be desired. Having a good broker or insurance consultant by your side can help greatly.

1. Kevin LaCroix, "O.K., This Is a Big Deal: 7th Cir. Reinstates Neiman Marcus Consumer Data Breach Class Action," The D&O Diary, July 22, 2015.

2. See, e.g., Jeff Sistrunk, "11th Circ. Partially Revives HIPAA Data Theft Coverage Suit," Law360, Aug. 17, 2015; *Retail Ventures v. National Union Fire Insurance Co. of Pittsburgh*, 691 F.3d 821 (6th Cir. 2012) (in which author Joshua Gold was coverage counsel for the plaintiffs).

3. The U.S. OPM breach also can be fairly viewed as one directed at the "institution." While the OPM cyber breach did concentrate on stolen information concerning millions of federal employees, most agree that the aim was an attack on the U.S. government through espionage and knowledge of state secrets. Not only was personal employee information stolen, but so too were the actual background investigation reports compiled by the government.

4. The Internet of Things refers to the network of objects or machinery via a wired or wireless connection.

5. Zeynep Tufekci, "Why 'Smart' Objects May Be a Dumb Idea," N.Y. Times, Op. Ed., Aug. 10, 2015.

6. "Could hackers take down a city?" Hamilton Spectator, Aug. 18, 2015.

7. The California hack on the traffic system is also a reminder that the threat can come from those working for you or from subcontractors you or your vendors hire.

8. Some cyber events do not involve hackers but may be the result of system error, human error, or natural causes such as severe weather. Many cyber policies extend insurance coverage to losses and claims caused by circumstances other than just hackers or viruses.

9. Paragon Cyber and Privacy Insurance specimen policy form, dated April 2013.

10. See, e.g., Jeff Sistrunk, "11th Circ. Partially Revives HIPAA Data Theft Coverage Suit," Law360, Aug. 17, 2015.

11. If you do find yourself making a cyber claim with your insurance company, be careful to preserve information including any computer system components and forensic reports. Whether it is financial information used to support a business income loss, or damaged computer parts, err on the side of preserving evidence. In *Southeast Mental Health Ctr. v. Pac. Ins.*, 439 F. Supp. 2d 831, 840, (W.D. Tenn. 2006), the defendant insurance company accused the policyholder of spoliating a damaged computer drive and sought to bar the introduction of any evidence related thereto. The court rejected the insurance company's position, finding that the policyholder kept the damaged drive for a year after promptly inspecting it and noting that the defendant never requested that the drive be made available for examination.

12. Author Joshua Gold was coverage counsel for the plaintiffs in this insurance litigation against National Union.