Costly and Damaging Cyberattacks: Who Will Pay, and for What?

by Samantha D. Wolff

As our economy is progressively driven by and dependent upon technology, so too have our networks increasingly become targets for attack. A number of high-profile cyberattacks drew worldwide attention in 2014 and 2015, including the attacks on Target[1], Anthem[2], Home Depot[3], Sony[4], and Ashley Madison [5]. But those are just some of the attacks that were well-publicized; a 2015 Accenture survey found that "[n]early two-thirds of companies face 'significant' cyberattacks on a daily or weekly basis."[6] Tech Insider reported that more than $1 billion was stolen and 300 million records were leaked in 2015.[7] Industry insiders predict the severity and frequency of these attacks to increase, including in the areas of cyber-warfare and espionage.[8] Cybercriminals are becoming even more skilled so that they may undertake long-term data theft on a victim's computer while remaining undetected.[9] As the incidences and severity of cyberattacks grow, law enforcement, corporations, and individuals alike must confront the new realities and concerns posed by this emerging threat, including who must pay for it.

The Government's Response to Cyberattacks

Federal and state governments seem to have established a carrot and stick approach to dealing with cybersecurity threats. Last year, President Obama announced that the government must partner with private corporations and public organizations to share information and oppose cyber breaches. To that end, in February 2015, President Obama signed Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," which recognizes that private companies, nonprofits, and government agencies alike "must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible" so as to best address cyber threats.[10] Executive Order 13691 encourages the formation of Information Sharing and Analysis Organizations (ISAOs) "to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis."[11] Through Executive Order 13691, the Department of Homeland Security is directed to develop more efficient means to grant clearances to private sector individuals who are members of an ISAO and to collaborate with ISAOs to share cybersecurity information.

California has also undertaken efforts to safeguard personal data through legislation and enforcement actions aimed at companies and agencies that fail to protect consumers' private information. In 2004, the California Legislature enacted Civil Code section 1798.81.5 with the stated goal of ensuring the protection of California residents' personal information by encouraging businesses to provide "reasonable security" for that information.[12] Civil Code section 1798.81.5 mandates that businesses that retain customer data "shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[13] In the event of a data breach, a business or agency must notify consumers "in the most expedient time possible and without unreasonable delay."[14] California Civil Code section 1798.82 prescribes the form and content of the notification, including, among other items, the exact title of the notification and subheadings, contact information of the reporting business, the toll-free number of major credit reporting agencies, and an offer to provide identity theft prevention and mitigation services.[15] The failure to timely notify consumers of a data breach may subject a corporation to civil penalties in the amount of $2,500 for *each* violation in addition to monetary damages and injunctive relief.[16]

In an effort to ensure enforcement of these and other privacy laws, California Attorney General Kamala Harris announced the creation of the Privacy Enforcement and Protection Unit ("Privacy Unit") within the Department of Justice in July 2012.[17] The Privacy Unit holds corporations responsible for data beaches through the enforcement of California's Unfair Competition Law, which acts as the predicate for an unlawful data breach violation.[18] For instance, the State initiated an enforcement action against Kaiser Foundation Health Plan, Inc. in 2014 after Kaiser delayed notification to its employees that an unencrypted USB drive was discovered at a Santa Cruz thrift shop containing more than 20,000 employee records.[19] Kaiser ultimately paid $150,000 in penalties and attorneys' fees, among other terms, to settle the matter.[20] The State also filed an enforcement action against Citibank, N.A. in 2013 following a data breach of its website which affected more than 80,000 California account holders.[21] The case resolved after Citibank agreed to pay $420,000 in penalties and attorneys' fees to California and $55,000 to the Connecticut Attorney General.[22]

The costs and penalties associated with these and other government enforcement matters pale in comparison to the putative class actions and shareholder derivative suits brought by those whose personal data was breached. By way of example, following the massive data breach that affected approximately 56 million Home Depot customers, a shareholder derivative action was filed in September 2015 naming twelve of Home Depot's directors and officers individually, and Home Depot, Inc. as a nominal defendant.[23] The complaint alleges that Home Depot failed to employ reasonable security measures to protect its customers' private information and that the individual defendants "were complacent, leaving in place glaring vulnerabilities that not only allowed hackers to enter the system undetected but permitted them to continue siphoning customer cardholder and personal data for almost five months without detection."[24] The complaint alleges causes of action for breach of fiduciary duty and waste of corporate assets.[25] At least forty-four other lawsuits were filed by victims of this same cyberattack. As of October 2015, the breach had already cost Home Depot $232 million and it is believed that the attack could end up costing into the billions.[26] This naturally begs the question, who pays for this?

What Does the Future Hold in Terms of Insurance Coverage for Cyberattacks?

Unlucky insureds who were among the first to suffer large, public cyberattacks initially attempted to obtain coverage for the resulting losses under Coverage B (for personal and advertising liability injury) of standard commercial general liability policies with mixed results. In one notable case, Zurich American Insurance sought a determination that no coverage was available to Sony Corporation under Sony's CGL policy. Zurich successfully argued that the policy did not protect against Sony's estimated $2 billion loss, which

was caused by third-party acts.[27] The parties settled while the court's decision was up on appeal. Conversely, the Central District of California upheld coverage under a CGL policy for a hospital data breach of 20,000 patient records.[28]

Given the uncertainty stemming from these (and many other) inconsistent holdings, increasingly savvy corporations are obtaining cyber insurance policies, which are essentially a grab-bag of coverages for data breaches. However, these nascent policies are not always adequate to cover the damage resulting from a breach. In the case of Home Depot, its cyber insurance policy covered only $100 million of the breach, just a small fraction of its estimated damages.[29] Large retailers find it challenging to purchase adequate insurance coverage in excess of $125 million.[30] As retailers face mounting expenses resulting from a data breach, including costs to repair and upgrade systems, credit-monitoring services, and litigation costs, sufficient coverage is hard to come by given the potential for vast exposure.

Even when companies obtain adequate cyber insurance, coverage issues may arise where they fail to properly implement risk-control procedures. In the case of a December 2013 breach of Cottage Health System, which resulted in the dissemination of more than 32,000 patients' protected health information and a subsequent $4.13 million class action settlement, Columbia Casualty Company sought recovery of the settlement and attorneys' fees after it determined that Cottage Health did not implement the risk controls that it had identified in its application.[31] The matter was dismissed in July 2015 following the parties' agreement to pursue alternative dispute resolution.

With the increasing severity and frequency of damaging cyberattacks on the horizon, the insurance industry will have to find a way to offer adequate coverage to policy holders seeking to avert the costs associated with such attacks. At the same time, policy holders must not ignore the risks of cyber-attack, through their own systems or those of their third-party vendors, and must actively implement risk-control procedures to safeguard against such attacks.

[1] In January 2014, hackers stole the personal data (names, addresses, phone numbers, and credit card information) from approximately 40 million shoppers. Sharone Tobias, *2014: The Year in Cyberattacks*, Newsweek, Dec. 31, 2014, http://www.newsweek.com/2014-year-cyber-attacks-295876. The hackers raised an estimated $53.7 million by selling some of that credit card information on the black market. *Id.*

[2] In February 2015, 80 million records of those using health plans like Amerigroup, Anthem Blue Cross, and Blue Shield were hacked by still-unknown cybercriminals. *See* Paul Szoldra, *The 9 Worst Cyber Attacks of 2015*, Tech Insider, Dec. 29, 2015, http://www.techinsider.io/cyberattacks-2015-12.

[3] Home Depot's systems were hacked in April 2014, exposing the financial information of 56 million customers. *See Mary Lou Bennek v. F. Duane Ackerman, et al.*, United States District Court for the Northern District of Georgia, Case No. 1:15-cv-2999, filed Sept. 2, 2015.

[4] In November 2014, the personal data of 47,000 employees and actors was hacked after an attack on Sony Pictures Entertainment, in addition to film budgets, contracts, salary lists, and embarrassing personal emails of corporate executives. Ben Fritz and Danny Yadron, *Sony Hack Exposed Personal Data of Hollywood Stars*, The Wall Street Journal, Dec. 5, 2014, http://www.wsj.com/articles/sony-pictures-hack-reveals-more-data-than-previously-believed-1417734425; *see also* Michael Cieply and Brooks Barnes, *Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm*, The New York Times, Dec. 30, 2014, http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html?_r=0.

[5] In July 2015, a hacking group called Impact Team stole user's data from adultery website Ashley Madison in an attempt to blackmail the site's parent company. When parent company Avid Life Media refused to take down the Ashley Madison website, Ashley Madison's 37 million users' personal data (including emails and addresses) was made public.

[6] Katy Barnato, *Most firms face 'significant' daily or weekly cyberattacks: Report*, CNBC, July 29, 2015, http://www.cnbc.com/2015/07/29/most-firms-face-significant-daily-or-weekly-cyberattacks-accenture.html.

[7] Paul Szoldra, *The 9 Worst Cyber Attacks of 2015*, Tech Insider, Dec. 29, 2015, http://www.techinsider.io/cyberattacks-2015-12.

[8] Rob Lever, *Cyberattacks Are Just Going To Get Worse From Here*, Business Insider, Dec. 9, 2014, http://www.businessinsider.com/afp-cyberattacks-to-worsen-in-2015-mcafee-researchers-2014-12.

[9] *Id.*

[10] Exec. Order No. 13691, 80 F.R. 9349 (Feb. 13, 2015).

[11] *Id.*

[12] Cal. Civ. Code § 1798.81.5(a).

[13] Cal. Civ. Code § 1798.81.5(c).

[14] Cal. Civ. Code § 1798.82(a).

[15] Cal. Civ. Code § 1789.82(d).

[16] Cal. Bus. & Prof. Code § 17206.

[17] Press Release, State of California Department of Justice, Office of the Attorney General, Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit (July 19, 2012), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection.

[18] Cal. Bus. & Prof. Code § 17200.

[19] *See The People of the State of California v. Kaiser Foundation Health Plan, Inc.*, Superior Court for the State of California, County of Alameda, Case No. RG14711370, filed Jan. 24, 2014.

[20] State of California Department of Justice, Office of the Attorney General, Privacy Enforcement Actions, https://oag.ca.gov/privacy/privacy-enforcement-actions.

[21] *See The People of the State of California v. Citibank, N.A.*, Superior Court for the State of California, County of Alameda, Case No. RG13693591, filed Aug. 29, 2013.

[22] State of California Department of Justice, Office of the Attorney General, Privacy Enforcement Actions, https://oag.ca.gov/privacy/privacy-enforcement-actions.

[23] *See Mary Lou Bennek v. F. Duane Ackerman, et al.*, United States District Court for the Northern District of Georgia, Case No. 1:15-cv-2999, filed Sept. 2, 2015.

[24] *Id.*, Verified Shareholder Derivative Complaint, ECF No. 5 at ¶¶ 4-5.

[25] *Id.* at pp. 36-37.

[26] *See* Julie Creswell, *As Online Data Theft Escalates, Banks Look to Retailers to Bear the Losses*, The New York Times, Sept. 28, 2015, http://www.nytimes.com/2015/09/29/business/as-online-data-theft-escalates-banks-look-to-retailers-to-bear-the-losses.html?_r=0.

[27] *Zurich American Ins. v. Sony Corp. of America* (N.Y. Sup. Ct. Feb. 21, 2014).

[28] *Hartford Casualty Ins. v. Corcino & Assoc.*, No. 13-3728 GAF (C.D. Cal. Oct. 7, 2013).

[29] *Id.*

[30] *Id.*

[31] Erin McCann, *Health system's data breach insurance claims get challenged*, June 1, 2015, Healthcare IT News, http://m.healthcareitnews.com/news/health-systems-data-breach-insurance-claims-get-challenged.

For more information, please contact:

Samantha D. Wolff, Partner
415-995-5020
swolff@hansonbridgett.com