WHEN A CLIENT SUFFERS A CYBER-ATTACH

BY GREGG A. RAPOPORT AND DAVID LAM, CISSP, CPP

A BUSINESS LAWYER MAY NEVER RECEIVE a late-night jailhouse call from a client trying to make bail, but should not be too surprised to get a frantic call from one whose computer network has been hacked. Corporate clients these days need and expect their counsel to be somewhat conversant in information security matters. In a recent survey, more than 500 IT professionals who had dealt with corporate data breaches ranked hiring legal counsel as among the top three steps to reduce the negative consequences of a data breach incident.[1]

A data breach, or cyber-attack, can expose a company to a loss of proprietary data, expensive forensic and remediation costs, privacy lawsuits, regulatory enforcement actions and immeasurable competitive and reputational losses. Successful intrusions make the news almost daily, with victims running the gamut from global banks and businesses to local retailers, public agencies, healthcare providers and educational institutions.[2] Valuable and confidential network information is vulnerable regardless of the client's IT budget and adherence to best practices in information security.

As with any criminal enterprise, the means employed by hackers is limited only by their ingenuity; attacks have involved insider theft and sabotage, spear phishing,[3] spoofing, social engineering scams, advanced persistent threat malware, bot-nets, and denial of service (DDoS) attacks.

Companies unwittingly heighten their vulnerability in the name of productivity and efficiency by integrating cloud-based services and embracing the use of consumer-friendly smartphones and ever-evolving tablet devices which rely on those services and/or provide access to corporate networks.[4] In 2011, the risk of outsourcing the custody of sensitive customer data was exposed by incidents involving "secure" cloud vendors Epsilon[5] and Dropbox.[6]

Media coverage of cyber-attacks has given businesses a better understanding of the risks, but small and mid-size clients may be less aware that if they are attacked, they could be legally mandated to take swift action to notify affected customers as well as certain public agencies. Data breach notification legislation has become a central component of the government's policy to protect consumers from the perils of fraud and identity theft.[7]

Well before cyber-crime became commonplace, in 2002, California enacted the nation's first data breach notification statute for all businesses, Civil Code §1798.82.[8] This law provides that anyone conducting business in California and owning, licensing or maintaining computerized data containing personal information must disclose any security breach to any California resident "whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person."

The disclosure notice—which is non-waivable[9]—must be given "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement" or "any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." (Cal. Civ. Code §1798.82(a)-(c).) If a notice is sent to more than 500 California residents, it also must be sent to the state's Attorney General. (Cal. Civ. Code §1798.82(f).) If a business fails to comply with the notification statute,[10] it may be liable for civil damages. (Cal. Civ. Code §1798.84.) Several key aspects of the law remain vague and untested, despite its having been amended twice and central to many privacy lawsuits since its enactment.

Breach notification obligations do not stop there. For a client conducting business beyond California's borders, a data breach could trigger distinct and often more onerous notification requirements imposed by up to 48 other U.S. jurisdictions.[10] In coming months, Congress could simplify matters by passing a long-anticipated preemptive federal breach notification law, and its requirements are likely to be stricter than those of the California statute. If the client does business abroad, international privacy laws may also apply.[12] On top of these requirements, in 2011 the SEC advised publicly-traded companies that, "as with other operational and financial risks," companies must report any material risks to the security of their data, including past cyber-attacks, "if these issues are among the most significant factors that make an investment in the company speculative or risky."[13]

The emergence of breach notification rules has proven to be problematic because when they have been followed, businesses have suffered expensive and embarrassing fallout even when the risks of consumer fraud or identity theft were insubstantial. For example, in 2011, Sony's PlayStation Network suffered an attack at the hand of the "Anonymous" underground hacker group, which illegally infiltrated Sony Online Entertainment's servers and acquired names, email addresses, and in some cases encrypted debit or credit card numbers, on approximately 77 million users of the Playstation Network. Upon discovering a possible data breach, Sony shut down the network for several weeks, publicly disclosed the incident within a week of the discovery, and offered customers identity theft protection.[14]

Soon after, Sony was named in 58 putative class actions filed in the United States and Canada on behalf of users of

PlayStation and other Sony online services.[15] None of the plaintiff classes alleged it had suffered identity theft as a result of the Sony incident;[16] instead, damages were sought by putative classes merely for the "risk of fraud and identity theft," and similar inchoate harms.[17]

Other recent cyber-attack incidents have involved similar consequences flowing from breach notification, i.e., class action filings predicated on "fear of identity theft" allegations.[18] California courts in particular have seen a growing trend of these cases. For example, in late 2011, Sutter Health and Sutter Medical Foundation in Northern California announced on their website that a desktop computer containing patient information had been stolen.[19] Within a month, at least 13 putative class actions were filed.[20] As one class representative alleged, she "and the Class she seeks to represent now face years of constant surveillance of their financial and medical records, monitoring [etc] ...."[21]

California businesses should take heed of recent federal data breach cases that have fed into and accelerated this trend. In contrast to earlier cases in which consumer class actions were dismissed for failure to plead compensable injury from the data breach,[22] both the Ninth Circuit[23] (applying Washington law) and the First Circuit[24] (applying Maine law), have held that such actions do not require the pleading of actual damages.[25] Further, the Ninth Circuit in a California case[26] has held that a consumer whose records have been stolen in a data breach incident has Article III standing due to being "at greater risk of identity theft," although the court did not resolve the question under California law of "whether time and money spent on credit monitoring as the result of the theft of personal information are damages sufficient to support a negligence claim."

Before a client actually faces a cyber-attack incident, the attorney may want to call attention to this emerging pattern of class action filings made on the heels of breach notifications. At minimum, this should spark a discussion about how the client is using technology and employee training to manage its risk of a data breach.

Clients should also be made aware that there now are dozens of insurance companies offering some form of cyber-coverage, thereby enabling them potentially to transfer some of their uncovered financial risk.[27] The client should involve the attorney in a careful review of its existing coverage and possible endorsements or stand-alone policies recommended by a knowledgeable broker.

Counsel may also wish to recommend a review of the client's contracts with cloud providers and other vendors who may be handling or storing protected customer information. Such a review will enable the client to assess how those vendor relationships may create added exposure, whether the vendors are themselves adequately secured and appropriately insured, and whether the client is covered as an additional insured.

Beyond focusing the client on the cyber-risk equation, an attorney who has previously handled data breach incidents may offer to refer the client to a back office suite of pre-vetted independent IT and information security professionals. These vendors are invaluable in helping to harden the client's defenses, to respond immediately to an attack, and to provide critical forensic support, preferably under an umbrella of attorney client and/or work product privilege where possible.[28]

If a data breach does occur, the informed attorney is well-positioned to work with the client as a trusted advisor, together with its information security professionals and forensic consultants, in order to assess exposure, critically evaluate breach notification requirements, direct required notifications, advocate against fines and penalties, and pursue potential insurance recovery.

Both the client and the lawyer will sleep better knowing that they are prepared to deal with the legal ramifications of potential cyber-attacks.

Gregg A. Rapoport *practices privacy litigation as part of a business and insurance litigation practice in Pasadena and may be reached at gar@garlaw.us and (626) 585-0155.*

David Lam, CISSP, CPP *is an IT and information security professional and author, and works as a CIO/CISO in Los Angeles. He is vice president of the Los Angeles chapter of the Information Systems Security Association. He may be reached at dlam@wisela.org and (310) 889-2342.*

---

[1] "Aftermath of a Data Breach Study," Ponemon Institute and Experian Data Breach Solution, Jan. 2012. http://ex.pn/w11rS3. The other steps were to assess harm to victims and employ forensic experts. .

[2] E.g., http://www.datalossdb.org.

[3] A glossary of information security terms may be found here: http://bit.ly/yM4FpF.

[4] Between October 2009 and November 2011, 39% of all Protected Health Information [PHI] breaches "occurred on a laptop or other portable media...." Breach Report 2011 - Protected Health Information. http://bit.ly/zYvLXI.

[5] Prepared Statement of Jeanette Fitzgerald, General Counsel, Epsilon Data Management, LLC, 6/2/11. http://bit.ly/zyKvdf.

[6] The Dropbox Blog. http://blog.dropbox.com/?p=821.

[7] White House Fact Sheet: Cybersecurity Legislative Proposal. http://1.usa.gov/wNepQw.

[8] A separate data breach notification law applies to California state agencies. Cal. Civ. Code §1798.29.

[9] Cal. Civ. Code §1798.84(a).

[10] Healthcare entities covered by federal breach notification laws are deemed to comply with California's notification law if in they comply with 42 USC §17932. Cal. Civ. Code §1798.82(e).

[11] At present, 46 states plus the District of Columbia, Puerto Rico and the Virgin Islands, have breach notification laws. http://bit.ly/zwv6ww.

[12] For a discussion of pending changes to privacy laws in the European Union, see http://bit.ly/wJcUmy.

[13] SEC Div. of Corp. Finance, CF Disclosure Guidance: Topic No. 2, 10/13/11. http://1.usa.gov/yG-dw1G. The disclosure of such risks need not be so detailed as to "itself compromise a registrant's cybersecurity."

[14] In June 2011, Playstation Network's President, Tim Schaaff, appeared before a Congressional panel focusing on cyber crime and data security, and was called to task for waiting seven days to notify the public. http://bit.ly/x5yoC2.

[15] The class actions are described in a declaratory relief complaint brought against Sony by one of its insurance carriers. http://zra.com/attachments/article/73/zurich.pdf.

[16] See http://www.jpml.uscourts.gov/ (MDL 2258).

[17] See Complaints filed in MDL 2258, *supra.*

[18] E.g., *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) (payroll processing firm's data breach triggered putative class action, although no tangible harm was alleged and it was "not known whether the hacker read, copied, or understood the data."); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. (Wash.) 2010) (after Starbucks notified 97,000 employees whose records had been on a stolen laptop, two putative class actions were brought, although no tangible harm was alleged).

[19] http://www.sutterhealth.org/noticeforpatients/.

[20] Reply in Support of Petition For Coordination of Actions, filed 11/23/11 in *Pardieck v. Sutter, etc.*, Sacramento County Superior Court, Case No. 34-2011-00114396.

[21] Complaint filed on 11/29/11 in *Atkins v. Sutter, etc.*, San Francisco Superior Court Case No. CGC-11-516204.

[22] E.g., *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629 (2007); *Hendricks v. DSW Shoe Warehouse, Inc.*, 444 F.Supp.2d 775 (2006).

[23] *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. (Wash.) 2010).

[24] *Anderson v. Hannaford*, 659 F.3d 151 (1st Cir. 2011).

[25] But see *Paul v. Providence Health System-Oregon*, --- P.3d ----, 2012 WL 604183 (Or.,2012) (upholding dismissal of negligence and unfair trade practices class action claims stemming from theft of patient data, where plaintiffs "alleged no actual identity theft or financial harm, other than credit monitoring and similar mitigation costs."); *Katz v. Pershing, LLC*, --- F.3d ----, 2012 WL 612793 C.A.1 (Mass.),2012 (distinguishing *Hannaford* where hackers had in fact "acted on the ill-gotten information.")..

[26] *Ruiz v. Gap, Inc.*, 2010 WL 2170993 (9th Cir. 2010); *Claridge v. RockYou, Inc.,* 785 F. Supp. 2d 855, 861 (N.D. Cal. 2011).

[27] For a discussion of this subject, see "The Coverage Question" http://bit.ly/yReaRV. .

[28] A good place to start is with the Los Angeles chapter of the Information Systems Security Association (ISSA, www.issala.org), which offers numerous resources and educational seminars.