In-House Counsel's Role in Corporate Data Security

Not that long ago, quarantine orders by various state and local governments might well have been terminal, rather than "merely" crippling, for numerous industries. Part of the reason for this is that companies were increasingly able to offer their employees the opportunity to work from home, rather than shutting down completely—and at least some companies are not planning on returning to the office at all.[1] While the jury is still out on whether remote work will become the norm, one thing is clear: increased reliance on telework means increased vulnerability to cyberthreats. As these threats have increased over the last year—and legal liabilities for cyber-attacks have correspondingly increased as well—in-house counsels should be prepared to add "cybersecurity expert" to their portfolio of responsibilities.

The Pandemic and the Cyber-Pandemic

By far the most widely reported cybersecurity incident that occurred during the pandemic is the widespread Russian hack of SolarWinds, which "affected upward of 250 federal agencies and businesses, that Russia aimed . . . [at the] United States government and many large American corporations."[2] However, politically motivated hacking is far from the norm and increased use of remote computing and cloud technologies has resulted in a "cyber-pandemic": a dramatic increase in cyberattacks that targets businesses for financial gain.[3] One cybersecurity expert explained:

> Employees are no longer sitting behind corporate networks, nor are they utilizing the best security practices while working from home. A company's data, privacy, and security are only as good as its employees' ability to utilize appropriate cyber hygiene, lock down their device security, and employ business security policies, software, and practices. Put all these factors together, and it's not hard to see how the stage is set for a possible cyber pandemic.[4]

Thus, it has been reported that during the COVID-19 shutdowns (1) there has been a two hundred and thirty-eight percent increase in cyberattacks on banks and financial institutions;[5] phishing attempts have increased by six hundred percent; most distressingly, since the start of the pandemic, a cyberattack has occurred, on average, once every thirty-nine seconds.[6]

Legal Risks from Data Breaches

A comprehensive analysis of the legal risks of cyberattacks is made somewhat more complicated by the fact that the United States does not have a single set of cybersecurity regulations in the way that the Eurozone has adopted the GDPR—a single, comprehensive set of data protection rules that are universally applicable throughout much of the Eurozone.[7] Instead, information in the United States is protected *transactionally*; that is, privacy and data security laws govern *in specific contexts*.[8]

For example, HIPAA and HITECH provide protections for "personal health information;"[9] Gramm Leach Bliley protects consumer information held by financial institutions; and the Fair Credit Reporting Act contains provisions to protect credit data.[10] As a further complication, states may well pass their own set of additional data security laws; Michigan, for example, recently enacted the Data Security Act, which requires additional cybersecurity measures on those licensed by the Michigan Department of Insurance and Financial Services.[11] Thus, it is imperative that counsel be familiar with the specific data security and privacy regulations governing its business.

Nevertheless, *direct* liability for data breaches is rare. First, many of the data security laws do not create a direct cause of action. HIPPA, for example, does not.[12] Moreover, even where a private cause of action exists, data-security litigation has proven difficult for plaintiffs. While not addressing a data breach specifically, *Spokeo Inc. v. Robins*, explains why. In that case, Thomas Robins sued Spokeo (an online "People search engine" that "allows users to search for information about other individuals by name, e-mail address, or phone number"[13]) for allegedly posting incorrect information about Robins, in violation of the Fair Credit Reporting Act (FCRA)[14] and sought statutory damages in a putative class action. The Supreme Court held that without showing the incorrect posting *actually* caused harm to Robins, he lacked Article III standing to sue.[15] In other words, Robins *might* be subjected to the risk of harm by the posting of incorrect information, but *without more*, he had not suffered an actual redressable harm.

In a cyberbreach context, this ruling has significantly curtailed plaintiffs' ability to sue for data breaches. In *Bassett v. ABM Parking Services Inc.*, for example, the 9th Circuit, relying heavily on *Spokeo,* held that even a clear violation of the FCRA and the Fair and Accurate Credit Transactions Act (FACTA)[16] requires an actual harm to be actionable. In that case, Basset used his credit card at an ABM garage, and the business returned to him a receipt that failed to redact his credit card number. The appellate court held, dismissively, that "[w]e need not answer whether a tree falling the forest makes a sound when no one is there to hear it. But when this receipt fell into Bassett's hands in a parking garage and no identity thief was there to snatch it, it did not make an injury."[17] Thus, without an allegation that "his receipt was lost or stolen, that he was the victim of identity theft, or even that another person apart from his lawyers viewed the receipt" neither Bassett nor his class could sue for statutory damages. Since it is very difficult to establish that an act of identity theft is related

to any particular data breach, without a change to the law, this sort of direct data breach liability will be rare.

Data breach liability might be rare, but it does happen. In one recent Pennsylvania Supreme Court case, the court held that an employer has a "legal obligation to exercise reasonable care to safeguards its employees' sensitive personal information stored by the employer on an internet-accessible computer system."[18] In that case, the employer was alleged to have "fail[ed] to adopt, implement, and maintain adequate security measures … and [among other things] 'establish adequate firewalls to handle a server intrusion contingency.'"[19] Consequently, a result of a hack of the employer's databases, "Employees 'incurred damages relating to fraudulently filed tax returns' and are 'at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse.'"[20] The case was remanded back to the trial court.

Moreover, even those regulations that lack a private right of action can be administratively enforced. Examples of such actions are common. The Department of Health and Human Services can levy fines for HIPAA violations that, in the most egregious cases, can exceed $1,754,698 per violation.[21] In 2019, the Federal Trade Commission settled a case against Facebook for "unfair and deceptive business practices" related to the Cambridge Analytica data breach.[22] The FTC is also in the final stages of approving a settlement with Equifax over the 2017 data breach; a settlement which includes a payment by Equifax of $380,500,000, among other payments, costs, and actions required by the settlement. Finally, while not technically a legal risk, companies that fail to protect their customers' data may well see their customers take their business elsewhere.

(Cyber) Protecting Your Data

Given the risks of direct, indirect, reputational, and administrative liability, it is imperative that in house counsel review the corporate data protection protocols. In this regard, HIPAA's security rule is instructive for every industry—and not just for health care companies obligated to follow it.

HIPAA's security rule provides a flexible approach, which permits covered entities to use "any security measures that allow the covered entity … to reasonably and appropriately implement the standards … and specifications as specified [under the rule]."[23] Thus, the rule creates a flexible approach to data security, which may be tailored to each individual entity. The rule requires that covered entities set up safeguards along five different parameters: administrative safeguards; physical safeguards; technical safeguards; organizational safeguards; and policies, procedures and documentation.[24]

Administrative safeguards might entail hiring a vendor to perform a cyberrisk analysis, or a long-term risk management program to reduce IT system risks and vulnerabilities.[25] Physical safeguards are the actual, real world (opposed to online or electronic) barriers put in place to protect data; these might include locked server rooms and other physical measures intended to keep physical access to servers or other data storage to a minimum.[26] Technical safeguards include firewalls, anti-malware scanning, and other electronic mechanisms designed to keep data secure.[27] Organization safeguards address the entities' relationships with its vendors and may require best practices such as indemnification for outside data breaches, warranties that vendors will use industry standard encryption protocols, and other contractual measures.[28] Policies, procedures, and documentation mean having a written data breach plan, data backup plans, and other set procedures for staff to follow in the event of a cyberattack.[29]

Addressing each of these different types of safeguards can be important for creating a robust data protection regime; doing so is likely to require the combined effort of management, along with both legal and IT departments. On the other hand, there are also simple, commonsense best practices that can be immediately implemented that may make data more secure, including:

- Install remote-wipe programs on laptop and phones that have access to sensitive data;
- Create a culture of password discipline, including regularly changing passwords, requiring strong passwords (passwords which include alphanumeric digits and special characters), and two-factor authentication.
- Ensure that your workforce is properly trained to identify phishing attempts and spam/malware attacks.

Conclusion

Cyberthreats are legal threats and are here to stay for the foreseeable future. Now, more than ever, a vigilant and strategic approach to cybersecurity must be enacted by in-house counsel as a proactive priority. Adopting a data protection policy and articulating the risk of cyberthreats across the organization will provide a platform of security. And while the threat of a cyberbreach may never go extinct, with intelligence-led measures, you may achieve herd-immunity.

NOTES

1. Get A Comfortable Chair: Permanent Work From Home Is Coming (npr.org) https://www.forbes.com/sites/forbestechcouncil/2020/08/18/cyber-pandemic-survival-guide-three-things-for-future-consideration/?sh=54e127382442.

2. David E. Sanger, Nicole Perlroth, and Julian E. Barnes, *Scope of Russian Hacking Far Exceeds Initial Fears* New York Times, A-1, Jan 3, 2021.

3. 2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic (govtech.com) https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the cofid-19-crisis-brought-a-cyber-pandemic.html.

4. Cyber Pandemic Survival Guide: Three Things for Future Consideration (forbes.com) https://www.forbes.com/sites/forbestechcouncil/2020/08/18/cyber-pandemic-survival-guide-three-things-for-future-consideration/?sh=1a787e6b2442.

5. The 2020 Cybersecurity Stats You Need to Know—Fintech News https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/.

6. *Id.*

7. The General Data Protection Regulation ("GDPR") is an international regulation on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It applies to the 27 Member States in the European Union: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Ireland, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Spain, Slovakia, Slovenia, and Sweden. The GDPR also applies to several non-EU members by international agreement: the United Kingdom, Norway, Iceland, and Liechtenstein.

8. It may well be argued the American approach to data security has created a hodgepodge of conflicting security standards. Data Protection Law: An Overview (fas.org) https://fas.org/sgp/crs/misc/R45631.pdf. ("Despite the rise in interest in data protection, the legislative paradigms governing cybersecurity and data privacy are complex and technical, and lack uniformity at the federal level."). On the other hand, it may be argued that the GDPR approach creates a simplistic "one-size-fits-all" that leaves open system-wide vulnerabilities. *See, e.g.* A One Size Fits All Approach Doesn't Work for Europe and Eurasia | Morrison & Foerster (mofo.com) https://www.mofo.com/resources/insights/210112-one-size-fits-all.html. Regardless, the American approach is the system in which we find ourselves, and, absent legislation and/or regulation at the federal level, this will be the approach for the foreseeable future.

9. *Data Protection Law: An Overview,* Congressional Research Service (CRS), March 25, 2019, https://crsreports.congress.gov/product/pdf/R/R45631.

10. Id.

11. MCL 500.557 *et seq*.

12. *Thomas v University of Tennessee Health Sci Ctr at Memphis*, No 17-5708 at *2 (6th Cir Dec 6, 2017) (finding that the district court did not err in dismissing claims under HIPAA where no private right of action existed, citing, *Bradley v Pfizer, Inc*, 440 F App'x 805, 809 (11th Cir 2011); *Carpenter v Phillips*, 419 F App'x 658, 659 (7th Cir 2011); *Dodd v Jones*, 623 F3d 563, 569 (8th Cir 2010); *Wilkerson v. Shinseki*, 606 F3d 1256, 1267 n4 (10th Cir 2010); *Miller v Nichols*, 586 F3d 53, 59-60 (1st Cir 2009); *Webb v Smart Document Sols, LLC*, 499 F3d 1078, 1081 (9th Cir 2007); *Acara v Banks*, 470 F3d 569, 571 (5th Cir 2006)).

13. *Spokeo, Inc v Robins,* ___ US ___, 136 S Ct 1540 (2016), *as revised* (May 24, 2016).

14. 15 USC 1681 *et seq*.

15. *Spokeo, Inc*, 136 S Ct at 1549. ("Robins could not. . . allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement.") Justice Scalia, however, did caution that "This does not mean, however, that the *risk* of real harm cannot satisfy the requirement of concreteness." *Id.* (emphasis added).

16. The FCA and FACTA require that "no person that accepts credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration date upon any receipt provided to the card holder at the point of sale or transaction" 15 USC 681c(g) and that "any person who willfully fails to comply with [this requirement] with respect to any consumer is liable to that consumer for statutory damages between $100 and $1000 per violations or actual damages suffered by the consumer."

17. *Bassett v. ABM Parking Servs, Inc*, 883 F3d 776, 783 (9th Cir 2018).

18. *Dittman v UPMC*, 196 A3d 1036 (PA 2018).

19. *Id.*

20. *Id.*

21. *What Are The Penalties for HIPAA Violations?,* HIPAA Journal, Jan 15, 2021, https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/.

22. *United States v Facebook, Inc,* No 19-cv-02184-TJK (DDC July 25, 2019).

23. 42 CFR 164.306(b)(1).

24. *See generally* 42 CFR 164 et seq.

25. 42 CFR 164.308.

26. *Id.*

27. 42 CFR 164.310.

28. 42 CFR 164.312.

29. 42 CFR 164.314.

J

Jordan B. Segal is the General Counsel for 814 CRE LLC, a real estate developer headquartered in Troy, Michigan, and is a Co-Chair of the Business Law Section's In-House Counsel Committee.