SECTION REVIEW
MASSACHUSETTS BAR ASSOCIATION

Business Law

Expanding enforcement: The developing field of cybersecurity

BY LAWRENCE G. CETRULO, ELIZABETH S. DILLON AND BRIAN D. FISHMAN

It goes without saying that we live in a digital age, and that the analog is gone and buried. Digital information propels the modern economy on the so-called "cyber wave." Merriam-Webster defines "cyber" as "relating to or involving computers or computer networks." As reliance on digital information grows, the risk that digital information will be compromised also increases. Digital information may be compromised through a "cyber incident" or a "cyber breach." The term "cyber incident" refers to unauthorized access to cyber data or private servers. A hacker who changes the homepage of a company's website has caused a cyber incident. The term "cyber breach" refers to the unauthorized acquisition or use of data. A hacker who steals Social Security numbers or credit card information from a company's private server has committed a cyber breach.

In an effort to combat cyber breaches, Massachusetts and the federal government have increased enforcement of their cybersecurity laws. Many corporations have responded to increasing cyber threats by bolstering cybersecurity measures. Corporations failing to adequately protect against cyber incidents face potential litigation by consumers whose personal data is breached, as well as penalty actions by Massachusetts and federal agencies. Accordingly, attorneys advising corporate clients must be aware of cybersecurity best practices, as well as increased governmental cybersecurity enforcement efforts.

Cyber incidents on the rise and corporations are bearing the cost.

Cyber incidents are increasing throughout the country. According to PricewaterhouseCoopers, 79 percent of American corporations detected a cybersecurity incident in the past 12 months, up from 44 percent in 2014.

In Massachusetts, the number of cyber breaches has increased (1,999 in 2016, compared to 1,835 in 2015), as has the number of Massachusetts residents affected by those breaches. According to the Massachusetts Office of Consumer Affairs and Business Regulation, cyber incidents compromised the personal information of 700,918 Massachusetts residents in 2008. In 2015, cyber incidents compromised over one million Massachusetts residents' personal information.

Cyber attacks are a growing menace to corporate America. There are more of them, and they are becoming more costly to corporations victimized by them. The British insurer, Lloyd's, estimates that cyber attacks cost businesses over $400 billion globally each year, and Forbes Magazine estimates that the cost of cybercrime in the United States will reach $2 trillion by 2019. Whether these costs are largely borne by corporations that maintain personal information of employees and consumers, or are passed along to consumers, the impact on the global economy is potentially catastrophic.

Breaches come in a variety of sizes. Breaches may be large, like the January 2016 breach of healthcare company Centene Corporation, in which the personal information of 950,000 Centene members was compromised. Smaller, but nonetheless costly breaches also plague corporations. Of the 135 breaches reported to the Massachusetts Office of Consumer Affairs and Business Regulation during the month of January 2017, 95 breaches affected five or fewer Massachusetts residents. Larger breaches, unsurprisingly, cost corporations more than smaller breaches. According to the independent research organization Ponemon Institute, data breaches of fewer than 10,000 records cost corporations on average $4.9 million in 2016, whereas breaches of greater than 50,000 records cost corporations an average of $13.1 million during the same time period. According to the Ponemon Institute, the average organizational cost to a business after a data breach was $7.01 million in 2016, whereas in 2015, the average organizational cost was $6.53 million. The average costs associated with each stolen record increased from $217 to $221 over the same period.

Corporations are increasing efforts to protect consumer information.

In response to the increased threat and cost of cyber attacks, many corporations have increased their focus on cybersecurity. According to the Ponemon Institute, corporations nationwide have increased their investment in "forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors" to bolster cybersecurity. According to the Wharton School, 80 percent of corporate boards of directors discuss cybersecurity at most meetings, and according to the website CFO.com, "[a]lmost three quarters (74 percent) of 160 public-company directors said their boards are now involved with cybersecurity than they were last year …, and 80 percent have expanded their cybersecurity budget, by an average of 22 percent."

Corporations not adequately addressing cyber threats face increased penalties as the federal government increases enforcement of cybersecurity laws.

Massachusetts and the federal government have also increased their focus on cybersecurity. Federally, no single agency is tasked with cybersecurity enforcement. Rather, many federal governmental agencies regulate cybersecurity.

The Securities and Exchange Commission (SEC) identifies cybersecurity as one of the greatest risks to investors. Accordingly, in 2017, the SEC announced an increased focus by its Office of Compliance Inspections and Examinations on cybersecurity compliance. In June 2016, the SEC announced that Morgan Stanley Smith Barney LLC agreed to pay a $1 million penalty to settle charges related to its failure to protect consumer information and failure to adopt written policies and procedures reasonably designed to protect customer data, as required by 17 C.F.R. 248.30.

Similarly, the Federal Trade Commission (FTC) has increased its focus on cybersecurity enforcement. Following the now-infamous breach of AshleyMadison.com (resulting in the 2015 theft of 36 million registered Ashley Madison users' personal information), Ashley Madison entered into a settlement with the FTC in which it agreed to pay $1.6 million, and to implement more robust data security practices to protect user information from hackers. The Ashley Madison case is one of the largest the FTC has investigated, although the FTC has investigated smaller matters as well. Since 2001, the FTC has charged 60 corporations for failing to reasonably protect consumers' personal information. Acting FTC Chairman Maureen Ohlhausen has stated that the FTC has also increased its efforts to educate the public about closed cases and about the FTC's data security expectations for corporations.

The Federal Communications Commission (FCC) has also made cybersecurity a priority. In the FCC's Jan. 18, 2017, White Paper on Cybersecurity Risk Reduction, former FCC Public Safety and Homeland Security Bureau Chief David G. Simpson stated that the FCC's cybersecurity oversight and enforcement efforts are "important component[s] of the [government's] larger effort to protect critical communications infrastructure and the American public from malicious cyber actors." Simpson further stated that the FCC is "actively working with [internet service providers] to address and minimize network vulnerabilities," and is currently developing "voluntary industry-wide best practices that promote cyber security on specific areas that fall within the FCC's purview."

In addition to the above-described enforcement efforts, it is likely that Congress will enact new cybersecurity laws in response to increased cyber threats. Indeed, new bills relating to cybersecurity have been proposed, including the Active Cyber Defense Certainty Act (ACDCA). The ACDCA's proponent, Rep. Tom Graves of Georgia, has stated that the Act "is about empowering individuals to defend themselves online, just as they have the legal authority to do during a physical assault." If enacted, the ACDCA would amend the Computer Fraud and Abuse Act (18 U.S.C. § 1030) (CFAA) to permit so-called "hacking back" when an individual is the victim of a cyber attack. Specifically, the ACDCA would permit victims to: (1) identify the perpetrators of an attack by accessing an intruder's network; (2) disrupt ongoing attacks; and/or (3) report attacks to law enforcement. Currently, hacking back is illegal. The Department of Justice views hacking back as a violation of the illegal access without authorization provisions of the Computer Fraud and Abuse Act, as well as a threat to innocent parties, and a potential source of interference with ongoing governmental investigations.

Massachusetts will likely increase enforcement of its comprehensive cybersecurity laws.

Similarly, Massachusetts will likely increase enforcement of its already rather comprehensive cybersecurity laws and regulations. These include M.G.L. c. 93H (the Data Privacy Act), which obligates companies (and individuals) possessing Massachusetts residents' personal information to notify the Massachusetts Attorney General and the Office of Consumer Affairs of any breach, and 201 C.M.R. 17.03, which obligates companies (and individuals) possessing such information to maintain certain safeguards, including a written information security program.

Massachusetts Governor Charlie Baker and Massachusetts Attorney General Maura Healey have consistently indicated that cybersecurity is a priority for the commonwealth, and are expected to increase efforts to ensure the privacy of information as cyber threats continue to grow.

Healey has stated that because "most any crime today involves some digital element," cybersecurity is, "from [her] perspective as attorney general … an issue that [she] actually lay[s] awake ➤ 27

SECTION REVIEW
MASSACHUSETTS BAR ASSOCIATION

Business Law

Recent Massachusetts decision addresses shareholder remedies

BY DAVID A. PARKE

On March 6, 2017, the Massachusetts Supreme Judicial Court issued a decision that illustrates the limited remedies available to shareholders challenging the merger of a Massachusetts corporation. In *Local No. 129 Benefit Fund v. Joseph M. Tucci et al.,* 476 Mass. 553 (Mass. 2017), shareholders of a publicly traded Massachusetts corporation claimed that the directors breached their fiduciary duties by failure to take actions to maximize the value of the corporation's stock and by agreeing to unreasonable deal protection provisions that discouraged the possibility of better bids.

This action began as a direct suit against the corporation's board of directors. The SJC held that the shareholders' claim should have been pursued as a derivative claim on behalf of the corporation, and not as a direct claim, against the directors. The court based its decision largely on the language of M.G.L. c. 156D, Section 8.30(a). Section 8.30(a) which says that a director must discharge the director's duties "(1) in good faith; (2) with the care that a person in a like position would reasonably believe appropriate under similar circumstances; and (3) in a manner the director reasonably believes to be in the best interests of the corporation." The court indicated that because these clauses are conjunctive and conclude by requiring that the director's actions must be in a manner reasonably believed to be in the best interests of the corporation, the directors' duties run to the corporation, and not the shareholders.

The court also indicated that a statement in a 2007 SJC decision (*Chokel v. Genzyme Corp.*), that directors owe a fiduciary duty to shareholders, was too broad. The court acknowledged that there are certain circumstances, not present in this case, where a director may have a direct duty to a shareholder. One involves close corporations, where Massachusetts common law recognizes that directors' duties of loyalty run to shareholders. Another situation involves where a controlling shareholder/director causes a self-interested transaction to the detriment of minority shareholders.

The result was that the SJC approved dismissal of the plaintiffs' complaint, because the challenge to the directors' actions was not brought as a derivative action on behalf of the corporation. While the corporation may arguably have suffered damage if the directors' actions exposed the corporation to unreasonably restrictive agreements, the loss from an unreasonably low merger price more directly harms the shareholders. Under the court's decision, a shareholders' lost value may not be directly recoverable in many situations.

This outcome contrasts with how a similar loss to shareholders of a Delaware corporation would be treated under Delaware law. In *Tooley et al. v. Donaldson, Lufkin & Jenrette, Inc. et al.*, 845 A.2d 1023 (Del. 2004), the Delaware Supreme Court addressed a claim of loss by shareholders resulting from the directors' action to delay a merger of the corporation. The Delaware court had to determine if the shareholders' claim could only be made derivatively on behalf of the corporation, or could be made directly against the directors. The Delaware court held that the analysis must be based on the nature of the wrong and whether the relief should go to the shareholders or to the corporation. In the Delaware case, because there was no claim of injury to the corporation, the court found no basis to require shareholders to assert a derivative, rather than a direct, claim against the directors.

It is interesting also to note that the Massachusetts Business Corporation Act differs from the Model Business Corporation Act with respect to some provisions relating to directors' duties. The Model Act has language that indicates that directors have duties to both the corporation and its shareholders in sections dealing with standards of liability for directors and with the corporation's right to have exculpatory provisions in its charter that limit the liability of directors. Such language in the Model Act, referring specifically to directors' liability to shareholders, is missing from the Massachusetts Business Corporation Act. In addition, Section 8.30(a) of the Massachusetts Business Corporation Act has the unusual language, carried over from Chapter 156B, the older Massachusetts Business Corporation Law, which says that in determining what is in the corporation's best interest, the directors may consider constituencies and factors other than the shareholders.

It thus appears that some non-standard language in the Massachusetts Business Corporation Act led the court to limit the recourse of shareholders where, in other states, the shareholders would likely have direct claims arising from merger transactions. ■

David A. Parke is a partner with Bulkley, Richardson and Gelinas, LLP, of Springfield, and Chair of the MBA Business Law Section Council. He is the co-author of *The Massachusetts Corporation: Legal Aspects of Organization and Operation*, published by BNA; the author of *Forming a Business Corporation Under Chapter 156D*, published by MCLE; and a contributor to other publications and CLE programs regarding business entities.

CYBERSECURITY
Continued from page 26

thinking about." In 2016, Healey hosted a data privacy forum in conjunction with the Massachusetts Institute of Technology and Harvard University, "in support of her office's continued efforts to protect the privacy and security of consumers' data." Among these "continued efforts" are the attorney general's enforcement of the Data Privacy Act against Massachusetts and foreign corporations. Less than two years after the Data Privacy Act was enacted in 2010, the Massachusetts Attorney General's Office charged Belmont Savings Bank for failing to comply with its cybersecurity program, and for keeping personal information on an unencrypted backup tape, which it subsequently misplaced. Belmont Savings Bank ultimately settled with the Attorney General's Office for $7,500, and promised to encrypt all personal information, store backup data tapes containing personal information securely, and train employees to properly secure personal information. The attorney general's investigations have also lead to a $15,000 settlement with Maloney Properties, Inc. in 2012; a $150,000 settlement with the Women & Infants Hospital of Rhode Island in 2014; and a $1 million multi-state settlement with Adobe Systems, Inc. in 2016, among others.

Baker has also demonstrated his interest in cybersecurity. During the governor's December 2016 Economic Development Mission to Israel, leaders from the public agency Massachusetts Technology Collaborative entered into a memorandum of understanding with Israeli venture CyberSpark. This memorandum of understanding focused on key areas of cybersecurity collaboration between the Massachusetts agency and the Israeli venture, including "practical training for students in the cybersecurity fields," "applied research projects focusing on healthcare technology-related cybersecurity issues," and "roundtables to discuss emerging trends in technology, policy, and regulation."

As cyber threats continue to become more numerous, more complicated, and more costly, it is likely the commonwealth will increase enforcement, in order to combat increasing cybersecurity risks.

Conclusion

Although cyber threats are increasing in frequency, corporations can take measures to reduce their risk of cyber breaches, and to reduce their liability if breaches occur.

First, corporations should adopt appropriate cybersecurity measures. Companies may reduce cyber risk by installing and regularly updating anti-virus software, blocking suspicious emails and websites, requiring employees to regularly change passwords, encrypting emails sent externally, and providing access to confidential data on a need-to-know basis. Corporations should document cybersecurity policies in a written information security plan, train employees on cybersecurity, and perform periodic audits to ensure compliance with cybersecurity protocols.

Second, corporations should develop a written cyber incident response plan to provide employees with a step-by-step procedure to follow in the event of a cyber incident. Corporations should also test the plan to further prepare employees to respond to a cyber incident if and when it occurs.

Third, corporations should develop relationships with the Federal Bureau of Investigation (FBI), the Department of Homeland Security, and/or local law enforcement agencies. During Boston College's March 8, 2017, Conference on Cybersecurity, then-FBI Director James Comey encouraged corporations to develop such relationships. Comey stated that where such relationships are developed, law enforcement is better prepared respond to breaches. Comey cited the relationship that Sony Pictures developed with the FBI, and stated that this relationship permitted the FBI to quickly respond when the group "Guardians of Peace" breached Sony in 2014.

Fourth, corporations should hire attorneys with experience in the field of cybersecurity to advise on changing cybersecurity laws and regulations, as well as cyber best practices. Attorneys familiar in cybersecurity law can also advise corporate clients on legal obligations to disclose breaches that compromise confidential employee or customer information.

Corporations face an increased risk of cybersecurity breaches, and an increased risk of liability due to efforts to enforce cybersecurity laws by Massachusetts and the federal government. By working directly with counsel experienced in cybersecurity, corporations can reduce the risk of being breached in the first place, and may be able to limit liability if breaches do occur. ■

Lawrence G. Cetrulo is a 1971 graduate of Harvard College, with a master's degree in education from the Harvard Graduate School of Education in 1972, and is a 1975 graduate of the Northeastern University School of Law. Cetrulo has been a national leader in the defense and trial of toxic tort litigation for over 39 years and is the founding and managing partner of Cetrulo LLP with offices in Boston, on the refurbished Boston Seaport, Providence, New Haven and New York City.

Elizabeth S. Dillon is an associate attorney at Cetrulo LLP. Her practice focuses on employment advice and counseling, as well as employment, business, real estate, and probate litigation. Dillon serves on the board of directors for the MBA's Young Lawyers Division, and is a member of the MBA's Labor and Employment Section.

Brian D. Fishman is an associate attorney at Cetrulo LLP, where he is a member of the firm's toxic tort litigation group. Fishman's practice also focuses on insurance defense, real estate, employment and environmental law. He is a member of the Massachusetts Bar Association.