Thursday, June 4, 2015

Executives must get down and dirty with cybersecurity

Hsiao C. (Mark) Mao *is a partner in the San Francisco office of Kaufman Dolowich & Voluck. He is co-chair of the firm's Technology Practices Group, and is an IAPP certified information privacy professional in the United States (CIPP/US). You can reach him at mmao@kdvlaw.com.*

Jonathan Yee *is an attorney in the Los Angeles office of Kaufman Dolowich & Voluck where he is a member of the Professional Liability, Financial Services and Cyber Liability practice groups. You can reach him at jyee@kdvlaw.com.*

Corporate executives often delegate cybersecurity matters to lower management. In the age of high-profile breaches, however, this is risky. There is increasing scrutiny of all involved in the collection, handling, processing, safeguarding, use and destruction of personally identifiable information (PII). Until there is greater clarity in the law, executives may benefit from participating directly in the selection of the technological, physical and administrative safeguards of their organizations.

The Federal Trade Commission demonstrated that it is not afraid to take executives to the mat in *FTC v. Kristy Ross*, 897 F.Supp.2d 369 (D. Md. 2012). There, the FTC alleged the executive, Ross, and her company tricked consumers by claiming that a scan of their computers had revealed viruses, spyware, system privacy issues and pornography - prompting consumers to purchase security software. After advertising networks began to receive complaints, the defendants allegedly continued to advertise using sham names.

The court found Ross liable as a "control person." It found dispositive that Ross was a purported marketing expert, was involved in key partnership decisions, and helped to create and disseminate deceptive advertisements. The 4th U.S. Circuit Court of Appeals later affirmed the $163 million judgment against Ross.

Ross is not a data breach case, but the potential cybersecurity applications were apparent. Indeed, in September 2014, a senior FTC attorney suggested that Ross should apply in data privacy cases.

Other federal agencies have joined the FTC, too. Last year, the Federal Communications Commission fined telecom companies YourTel America and Terracom $10 million for failing to store PII without firewalls, encryption or password protection. And in April, AT&T settled with the FCC for $25 million over the leak of customer proprietary network information relating to 280,000 subscribers.

These actions are notable given the FCC traditionally has left such matters to the

FTC. Executive management of companies holding FCC licenses would do well to remember the case against Telseven LLC, where the FCC disregarded corporate formalities and held the principals of Telseven individually liable. Notably, the FCC applied a legal standard for piercing the corporate veil that was lower than those taken by civil courts. The FCC merely assessed whether: (1) there is commonality of management and control, and (2) piercing the corporate veil was "necessary" to preserve the integrity and purpose of the Communications Act. *In re Telseven*, FCC Action No. 12-62 (June 12, 2012).

Even more feared than the FTC and FCC is perhaps the Securities and Exchange Commission. Although the SEC has issued guidance on cybersecurity, it has provided little guidance on whether there is a private right of action against directors and officers for cybersecurity violations based on security laws more traditionally associated with securities class actions.

Then in *Palkon ex rel. Wyndham Worldwide Corp. v. Holmes*, 14-01234 (D. N.J. Oct. 20, 2014), plaintiff-shareholder Dennis Palkon brought a derivative action against the hotel company after the FTC brought action against Wyndham for data breaches and alleged failure to implement sufficient data-security mechanisms. Palkon alleged that defendants "failed to timely disclose the data breaches after they occurred."

Although the defendants' motion to dismiss was ultimately granted, the court nonetheless assessed the reasonableness of the defendants' investigation into the data breach. The court was persuaded by the board's time and interest taken in discussing the data breaches, and implementing certain recommendations made by the retained technology firms.

Authorities will continue to scrutinize safeguards undertaken by directors and officers, a point underscored by SEC Commissioner Luis Aguilar in a speech last year. Aguilar stated, "ensuring the adequacy of a company's cybersecurity measures needs to be a part of a board of director's risk oversight responsibilities." "Boards that choose to ignore or minimize the importance of a cybersecurity oversight responsibility do so at their own peril," he said.

There are several other reasons directors and officers should document their cybersecurity efforts immediately. First, since the alleged North Korean attack on Sony Pictures, much talk on Capitol Hill has focused on passing more comprehensive cybersecurity legislation. The tides seem to indicate that something comprehensive will pass soon.

Second, *Palkon* has not discouraged the plaintiffs' bar. In response to a 2013 data breach, shareholders of Target Corporation have filed two derivative lawsuits against directors and officers, alleging they failed to "implement any internal controls at Target designed to detect and prevent such a data breach." It is not unreasonable to expect the plaintiffs' bar to be encouraged by the *Palkon* court's assessment of what the executives actually did as a sign that courts may be willing to impose executive liability with the "right facts."

Third, initially it appeared that cybersecurity class actions would be defeated by the U.S. Supreme Court's decision in Clapper v. Amnesty International USA (2013), requiring a showing of damages in-fact to confer Article III standing. The majority of subsequent cases followed the Supreme Court and required a showing that damages are "certainly impending to constitute injuries in fact," as opposed to merely speculative. Few plaintiffs have passed this test.

However, some courts - including ones in the 9th Circuit - have taken efforts to avoid applying the Clapper standard. See *In re Target Corp. Customer Data Security Breach Litig.*, MDL No. 14-2522 (D. Minn. Dec. 18, 2014) (finding that Target had set "a too-high standard for Plaintiffs to meet at the motion-to-dismiss stage."); *In re Adobe Systems Inc. Privacy Litig.*, 13-05226 (N.D. Cal. Sept. 4, 2014) (finding an "immediate and very real" risk of harm); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, MDL No. 11MD2258 AJB (MDD) (S.D. Cal. Jan. 21, 2014) (finding a "credible threat of impending harm"). Such decisions are a minority, but their existence does not bode well for deterring future class actions.

Finally, venture capital firms have also begun stressing the importance of proper cybersecurity safeguards in companies in which they invest. One only needs to review

Fitbit's recent filings for its initial public offering to find disclosures regarding how it handles PII. Such disclosures evidence an increasing fear of running afoul of securities fraud laws.

Simply put, executives may be well-served by increasing their participation in the data security decisions of their organizations. An unprecedented decision in the courts, or sweeping federal legislation, may ultimately "open the floodgates" for privacy-based lawsuits against corporate executives, and early action and best practices could be the deciding factor in potential lawsuits.

Hsiao C. (Mark) Mao *is a partner in the San Francisco office of Kaufman Dolowich & Voluck. He is co-chair of the firm's Technology Practices Group, and is an IAPP certified information privacy professional in the United States (CIPP/US). You can reach him at mmao@kdvlaw.com.*

Jonathan Yee *is an attorney in the Los Angeles office of Kaufman Dolowich & Voluck where he is a member of the Professional Liability, Financial Services and Cyber Liability practice groups. You can reach him at jyee@kdvlaw.com.*