August 21, 2015

CLIENT ALERT:
Sex, Money and Cybersecurity - Reminders for Public Companies

Recent events have highlighted the importance of comprehensive cyber-security programs for publicly-traded companies. Although the circumstances differ, in each case the impact of employee behavior with electronic communications - and the need to shape, inform, and monitor that behavior - is clear. Further, both cases provide reminders of the particular risks public companies face with respect to their cybersecurity and the particular responsibilities of such companies.

SEC TAKES ACTION AGAINST HACKERS USING CORPORATE INFORMATION FOR ILLEGAL TRADING

Two actions by the Securities and Exchange Commission have targeted hackers' use of inside information to generate illegal trading profits. On August 11, 2015, the SEC announced fraud charges filed in connection with a scheme involving hackers gaining access to newswire services and using nonpublic information about corporate earnings announcements to generate more than $100 million of illegal profits. In June, the SEC requested information from eight listed companies about data breaches experienced by those companies to determine whether corporate e-mails were accessed for "outsider trading" (trading on company inside information by individuals masquerading as insiders, but who are actually "outsiders" to the company in question). In both cases, the hackers targeted employees with fake credentials and login pages - in the case of the listed company breaches, hackers were able to obtain user names and passwords from attorneys and executives of the companies in question and could insert themselves into confidential e-mail threads to receive information continuously.

ASHLEY MADISON HACK IMPLICATES COMPANY RESOURCES

The recent release of millions of records from the Ashley Madison website has placed the site's users - and their e-mail addresses - in the spotlight. While the slogan of the online dating website Ashley Madison is "Life is short. Have an affair®.", the consequences of the release of approximately 36 million e-mail addresses will likely stretch out for a long time. Beyond the personal embarrassment of the individual users lies the potential "corporate embarrassment" for those companies whose e-mail domains are associated with those users. News outlets are already highlighting the public domains identified - .gov, .mil -

and private domains are equally accessible. Combined with the anticipated flood of divorce filings, companies can likely expect to be inundated with subpoenas for e-mails sent from company accounts that may implicate a cheating spouse.

CYBERSECURITY RESPONSIBILITIES REVISITED

Companies' responsibilities for disclosure of cybersecurity risks may be clarified as the SEC proceeds with its investigations. Since 2011, companies have been required to publicly disclose "the risk of cyber incidents if [such] issues are among the most significant factors that make an investment in the company speculative or risky"[1], along with any costs or consequences of cybersecurity risks or incidents that "represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the [company's] results of operations, liquidity, or financial condition"[2]. Although the specific disclosure of such risks has been inconsistent, these recent examples of cybersecurity weaknesses directly impacting the market may provide the SEC with sufficient incentive to provide specific requirements - or at least cause those SEC personnel reviewing public filings to question a company's silence on the issue.

RECOMMENDED STEPS FOR COMPANIES

While no company is completely safe from a breach, many types of breaches can be prevented - for those that can't, the damage can be mitigated - with the appropriate cybersecurity framework in place. Most public companies already have some type of program, but the following steps represent some useful maintenance for existing programs (and essential elements to incorporate in not-yet-established programs):

- **Board of Directors:** The Board should be regularly made aware of the types of cybersecurity issues facing the company, and such issues should be a regular point of discussion. The recent dismissal of a shareholder derivative suit brought against the directors of a hotel demonstrates particular steps that can be taken to limit the liability of the board for such issues. While the suit alleged the Board caused harm to the company in failing to prevent breaches of personal information of hotel customers, it was dismissed due to various indications of the board's awareness of cybersecurity issues, including regular discussion of such issues at fourteen meetings before the shareholder demand letter was received (including discussions during the audit committee) and presentations from the general counsel at quarterly board meetings.

---

[1] Division of Corporate Finance, Securities and Exchange Commission, *CF Disclosure Guidance: Topic No. 2 - Cybersecurity*" (October 13, 2011) (the "Cybersecurity Guidance"), referencing Item 503(c) of Regulation S-K and Form 20-F, Item 3.D.

[2] Cybersecurity Guidance.

- **Human Resources/Training Department:** To the extent that the company has a specific policy regarding internet and/or electronic mail usage, employees should be trained on that policy - in particular restrictions on personal usage - before being granted any access to either. In addition, as hacking techniques continue to become more and more sophisticated, employees should be regularly trained on these new techniques and how to spot (and avoid) them. More often than not, breaches don't occur because of the lack of a policy - they occur because of the actions of a specific employee.

- **General Counsel:** In addition to the involvement with the Board described above, general counsel should ensure the insertion and discussion of cybersecurity issues at key meetings and decision points within the company - not only during discussions of public filings, but in new product development, company expansion, and at the origination or modification of key vendor relationships. General counsel should similarly be integrated into any breach identification and notification process - not only to ensure appropriate confidentiality (and terminology - "It's not a breach until the GC says it is!"), but also to appropriately direct any resulting notification requirements, either to customers or other parties such as a state's Attorney General[3].

Tom C. Vincent, II
(918) 595-4857
tvincent@gablelaw.com

1100 ONEOK Plaza
100 West Fifth Street
Tulsa, Ok 74103-4217

www.gablelaw.com

Tom C. Vincent II is an attorney with the law firm of GableGotwals and a former bank compliance officer. His practice areas include banking and financial services compliance and data security.

[3] Breaches of individual information are currently governed by various state statutes - coverage is determined by the state of residence of the individual whose information is breached, not the state of domicile of the company subject to the breach - and more and more states are explicitly requiring notification of their Attorneys General in the event of certain data breaches.