CLIENT ALERT

Recent Data Breaches Highlight Need for Comprehensive Cybersecurity Practices

December 7, 2018

AUTHORS

Daniel K. Alvarez | Elizabeth J. Bower | Elizabeth P. Gray | Jill Guidera Brown

On November 30th, 2018, Marriott International notified its customers that it had experienced a breach of its Starwood guest reservation database that potentially exposed the personal information of up to 500 million customers. Breaches present problems for the individuals whose data have been compromised, but can also affect indirect victims. As targets of what is sometimes called "CFO Fraud," companies can themselves be victimized when their employees' data, compromised in the original breach, is used in "spear-phishing" campaigns targeting company leaders — usually in the form of very convincing emails asking for wire transfers or other forms of payment. The FBI estimates that between October 2013 and May 2018, businesses around the world lost more than $12 billion through this kind of email scam.

This alert identifies steps companies can take to protect themselves.

The Problem and How Companies Can Protect Themselves

In the aftermath of data breaches, hackers often gather information about businesses and their employees, such as names, work emails, personal details, signatures, and even writing styles, and use it to craft convincing "spear-phishing" emails designed to lure employees to transfer funds or provide unauthorized persons with account information or other sensitive data. For example, on the heels of the Marriott data breach, reports have highlighted a group of cybercriminals called London Blue that has launched extensive and coordinated attacks designed to trick thousands of businesses into transferring company funds to fraudulent accounts. While there does not appear to be a direct connection to the Marriott breach specifically, these criminal efforts have worked because they typically leverage information that has been

compromised in another breach to craft emails that appear to be from a Chief Financial Officer or other official source, but actually originate from a forged email address.

This serves as a reminder of the importance of thoughtful internal practices designed to protect the data under a company's control against unauthorized access, use, manipulation, or theft. Safeguarding customer and personal data is critical for every business, not only because breaches can lead to costly fines, expensive technical fixes, and reputational damage, but because information exposed in breaches can fuel even more sophisticated social engineering attacks. In a recent Report of Investigation ("Report") citing business e-mail compromises, the U.S. Securities and Exchange Commission reiterated the need for public companies to calibrate their internal accounting control systems to the current cybersecurity risk environments.[1] The Report emphasized the importance of public companies' reviewing and adjusting their policies and procedures to consider cyber threats in order to comply with the requirements of Section 13(b)(2)(B) of the Securities Exchange Act of 1934. The Report followed the Commission Statement and Guidance on Public Company Cybersecurity Disclosures released earlier this year that advises public companies that "[c]ybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws."[2]

There are a number of low-cost, high-yield steps companies can take today to fortify against cyber attacks,[3] such as:

- **Employee Training:** Facilitate regular employee training designed to empower employees to detect, report, and avoid phishing email scams.
- **Manage Exposed Data:** Provide employees with resources to check whether they were impacted by a breach, and where appropriate, to place fraud alerts or credit freezes.
- **Password Management:** Implement a dynamic password policy that requires employees to strengthen and regularly change online log-in credentials.

---

1 *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Control Requirements*, Securities Exchange Act of 1934 Release No. 84429 (October 16, 2018). The Report was based on the SEC Enforcement Division's investigations of nine public companies that fell victim to cyber fraud and lost millions of dollars in the process.

2 *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* at 2, Release No. 33-10459; 34-82746) (February 21, 2018).

3 The Federal Trade Commission has outlined a number of helpful steps that individuals can take to protect themselves in the event that their data has been compromised. FED. TRADE COMM'N, *The Marriott Breach* (Dec. 4, 2018), https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach?utm_source=govdelivery. While encouraging employees to consider these steps can be an important part of creating a culture of good cyber hygiene in an organization, they are by no means sufficient to ensure that the organization itself is protected from hackers who want to use fraudulently obtained data to commit further cyber crimes.

- **Multi-Factor Authentication:** Even if credential data — usernames and passwords — are exposed, multi-factor authentication can provide an additional layer of protection against unauthorized access.

- **Update Systems:** Ensure that all company operating systems are up-to-date and software has all appropriate security patches.

In the long term, companies should develop a comprehensive written information security program that is designed to protect the security, integrity, and confidentiality of its data. The security program should include physical, organizational and technical measures, and be tailored to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the personal and business information it maintains. Companies should regularly audit these controls to identify any vulnerabilities, and take action to remediate any security issues raised in its review.

How Willkie Can Help

The Willkie Farr & Gallagher Cybersecurity & Privacy Practice Group can help your company develop a comprehensive information security program to ensure that your company has sufficient mechanisms in place to protect against potential breaches, and where necessary, formulate a response in the critical hours following a breach.

(1) **Information Management Policies and Procedures**. We can help your company develop policies and procedures that are tailored to the company and its customers' needs, compliant with applicable data protection regulations (including international laws), and consistent with industry standards and best practices. These efforts regularly include developing, or reviewing and updating existing, information security policies and procedures, document retention and destruction policies, incident response plans, or other resources to help your company implement and maintain strong information security controls.

(2) **Tabletop Exercises**. We can work with your company to develop a targeted tabletop exercise that will help your IT, legal, HR, and executive teams prepare for, respond to, and mitigate potential risk in a simulated cybersecurity event. Tabletop exercises present a unique opportunity to test the company's information security and incident response plans, discover unknown vulnerabilities, and ensure that teams across the company understand their role in mitigating risk in the high-pressure environment following a cybersecurity event.

(3) **Incident Response**. Even companies with strong information security controls can fall victim to data breaches. Should your company experience an actual or suspected information security incident, our team can quickly develop and implement an incident response plan to help you identify what happened, who was affected, and what you need to do. Cybersecurity incidents can trigger a maze of regulatory, legal, and contractual obligations. We can help you navigate those obligations, and tailor a response that rebuilds trust with your clients, customers, partners and regulators.

If you have any questions regarding this client alert, please contact the following attorneys or the attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Elizabeth J. Bower
202 303 1252
ebower@willkie.com

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Jill Guidera Brown
202 303 1217
jgbrown@willkie.com