Long Island BusinessNEWS
OCTOBER 13-19, 2017 | VOL. 64 | NO. 41 | $2.00 | LIBN.COM

COMMENTARY

The C-Suite must become involved in cybersecurity

By RICHARD M. FRANKEL and NICOLE DELLA RAGIONE

The Equifax breach reported on Sept. 7 has rocked consumers and businesses across the nation and created media frenzy, all with good reason. Equifax, one of the three major credit bureaus, announced it had suffered a data breach from mid-May through July, 2017 that exposed personally identifiable information (PII) for 143 million United States consumers.

Social Security numbers, driver's license numbers, birth dates, addresses, and credit card information were all revealed. While this may have been the largest breach to date for PII, Equifax is not alone in suffering from similar attacks. Companies in all industries and of all sizes are at risk, and a data breach is not a question of if for a company, but when.

In the wake of this breach, it has become evident that not only must a company do more to protect its data from unauthorized persons; the C-Suite must become more aware and involved in cybersecurity decisions. Cybersecurity requires attention to not only technical safeguards at a company, but also administrative and physical safeguards. Due to the multitude of decisions that must be made in a coordinated manner, the C-Suite is best suited to address the multidimensional problems that arise out of cybersecurity. Furthermore, if a company has a lax cybersecurity program, it could mean thousands to millions of dollars spent if a data breach does in fact occur, and unquantifiable reputational damage. Proactive cybersecurity steps can help to mitigate the risks of a cybersecurity breach, and provide possible defenses to any suit that may arise following such incident.

Additionally, appropriate cybersecurity measures within a company can prevent embarrassment and possible legal action against an executive. In the aftermath of the data breach at Equifax, three executives sold a large portion of their stock holdings after the company learned about the hack, but before the hack became public knowledge. While the executives claimed to not have knowledge of the breach at the time the stock was sold, such actions leave many questions unanswered and has led to federal and state investigations being opened. Further consequences came upon the C-Suite when on Sept. 26 the chief executive officer of Equifax, Richard Smith, stepped down from his position—ending his 12-year leadership of the credit reporting bureau.

As shown by the Equifax breach, it is best practice for the C-Suite to be actively involved in cybersecurity decision making. However, while this framework is currently only a best practice for most industries, it is slowly becoming the law. The New York Department of Financial Services ("NYDFS") regulation now requires a member of the C-Suite to certify to the NYDFS Superintendent compliance with the NYDFS cybersecurity regulation. This certification requires the C-Suite to be aware of the NYDFS compliance program at that company and be able to certify that it is in fact compliant with the regulation. While this regulation is currently only enforceable against the financial services industry in New York, it is likely that more regulations will follow this model

Already the governor of New York has proposed legislation that would apply this regulation the credit reporting bureaus. As more industries suffer public data breaches, strict regulations will follow, especially on C-Suite executives.

As such, the C-Suite should be proactive in taking responsibility for the cybersecurity health of their company. Not only can harm come to the company, but the executives can face liability for lack of due care in the governance of the company. As such, the creation of a robust cybersecurity program, periodic risk assessments, quarterly meetings, up to date security measures and adequate remediation of any ongoing issues can protect a company, and its executives, from the potential impact of a public data breach. Equifax taught and continues to teach a lesson to all executives: you are swimming in shark-infested waters at your own risk if you are not a part of cybersecurity decisions.

Frankel is Of Counsel at Ruskin Moscou Faltischek P.C. and co-chair of the firm's Cybersecurity and Data Privacy practice group. His e-mail is rfrankel@rmfpc.com.

Della Ragione is an associate at Ruskin Moscou Faltischek P.C. and a member of its Cybersecurity and Data Privacy practice group. Her e-mail is ndellaragione@rmfpc.com.