Bloomberg BNA

Corporate Law & Accountability Report™

DATA SECURITY

Data Security Plans: Why Financial Institutions Must Continuously Assess and Update Their Data Security Plans

BY ROBERT J. HANNA AND PAUL L. JANOWICZ

A few years ago, news of a data security breach was an eyebrow-raising anomaly. Not anymore. Recent breaches suffered by Target, J.P. Morgan, Sony and countless others have resulted in the wide-spread realization that digital attacks are now a common threat faced by individuals, corporations, government agencies and financial institutions alike. As a result, 84 percent of financial institutions surveyed by the Depository Trust & Clearing Corporation ''identified cyber-risk as one of their top five concerns—an increase of 25 points since the last survey was conducted *in March 2014*.''[1] This year brings a greater expectation of compliance—and compliance that doesn't stop at the CIO's doorstep. Everyone in the organization must get involved. Simply put, entities that house or store sensitive personal information must be adequately prepared to defend against all forms of data security threats.

Beginning Work

Financial institutions have taken important steps to implement appropriate data security measures, but work still needs to be done. The New York State Department of Financial Services' May 2014 *Report on Cyber Security in the Banking Sector* reveals that many financial institutions have successfully implemented some form of a data security program. According to the report, nearly 90 percent of large institutions and 80 percent of medium institutions[2] have a documented information security strategy in place.[3] Less than half of the institutions surveyed, however, claimed that their information security program adequately addresses new and emerging risks.[4] Worse, less than 15 percent of financial institutions conduct tests to identify vulnerabilities a hacker could exploit more than once per year.[5] Finally, many institutions fail to conduct ''compliance audits of third parties that handle personal data of customers.''[6]

If the 154 financial institutions surveyed are in any way reflective of national trends, it is fair to note that while financial institutions have made progress in the realm of data security, there is still work to be done. The implementation of a data security plan is the vital first step for any data security defense system. Most financial institutions already have that. Financial institu-

[1] *DTCC Risk Survey Reveals That Threat of Cyber Attack Ranks as the Principal Concern of Global Financial Institutions*, DTTC (Oct. 23, 2014), *available at* http://www.dtcc.com/news/2014/october/23/cyber-risk.aspx (emphasis added).

Robert J. Hanna (robert.hanna@tuckerellis.com) is a partner and head of the Data Privacy & Security Practice Group at Tucker Ellis LLP, a law firm headquartered in Cleveland, Ohio. Paul L. Janowicz (paul.janowicz@tuckerellis.com) is an associate with the firm.

[2] The report classifies institutions as follows: ''small'' (less than $1 billion in assets); ''medium'' (more than $1 billion in assets but less than $10 billion); and ''large'' (more than $10 billion in assets). N.Y. STATE DEPT. OF FIN. SERVS., REPORT ON CYBER SECURITY IN THE BANKING SECTOR 2 (2014).

[3] *Id.*

[4] *Id.*, at 10.

[5] *Id.*, at 3.

[6] *Id.*, at 5.

 ISSN 2330-6300

tions, however, cannot allow themselves to be lulled into thinking that the mere creation of a data security program today will satisfy their legal and ethical obligations. It won't. Instead, only a vigilant, ever-evolving approach toward the protection of information is appropriate.

Ongoing Evaluations Required

The law requires ongoing evaluations and modifications to data security programs. The Gramm-Leach-Blilely Act and the Federal Trade Commission's accompanying Safeguards Rule[7] dictate data security requirements for financial institutions[8]. The primary goal of the Safeguards Rule is praiseworthy: it requires financial institutions to have reasonable ''measures in place to keep customer information secure.''[9] When it comes to specifics, however, the Safeguards Rule is, perhaps by design, vague. That is, it fails to specifically define what constitutes a ''reasonable'' data security plan. Instead, it simply demands institutions implement plans that fit their circumstances.[10]

Despite the lack of specifics contained in the Safeguards Rule, at least one thing is clear: simply having a data security plan in place is insufficient. The Safeguards Rule places an increased scrutiny on policies, procedures and compliance after a plan is in place.

[7] 16 C.F.R. § 314 (2015).

[8] Under the Safeguards Rule, the term ''financial institution'' has the same meaning as in FTC Privacy Rule, 16 C.F.R. § 313.3 (2015). That is ''[f]inancial institution means any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution that is significantly engaged in financial activities is a financial institution.'' FTC Privacy Rule, 16 C.F.R. § 313.3(k)(1).

[9] *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FTC, *available at* http://www.ftc.gov/tips-advice/business-center/financial-institutions-customer-information-complying-safeguards-rule (last visited June 17, 2015).

[10] *Id.*

Avoid Stagnation

A stagnant data security program will have severe practical consequences. Even if limited reviews and evaluations of a data security plan could satisfy the requirements of the Safeguards Rule, a stagnant data security program is unreasonable in light of the evolving threats to financial institutions. Such threats to financial institutions are not only increasing in sophistication, but also in number. The time, money and human resources it may take to continuously guard against such threats is well worth the investment—especially when an institution's reputation is involved. According to research performed by Kaspersky Lab and B2B International, ''82 percent of businesses would consider leaving a financial institution that suffered a data breach and [] 74 percent of companies choose a financial organization according to their security reputation.''[11]

Conclusion

As data security threats continue to evolve and grow in number, financial institutions must respond in kind. The creation and implementation of a data security plan is the essential first step. But it's not enough. Unless the provisions of the plan are consistently evaluated, tested and updated, the plan will quickly prove obsolete—an unacceptable result regardless of how you measure it. As a result, financial institutions should:

1. conduct an assessment of their data security plan at least twice per year;
2. stay apprised of all new or emerging data security threats and respond accordingly;
3. assess third-party vendors' data security measures at least annually; and
4. provide all employees with data security training at least annually.

[11] Nathan Eddy, *Financial Institutions Under Constant Threat from Cyber Criminal*, EWEEK (Sept. 9, 2014), *available at* http://www.eweek.com/small-business/financial-institutions-under-constant-threat-from-cyber-criminals.html.

   ISSN 2330-6300