Principles for Data Sharing

The Facebook/Cambridge Analytica scandal has turned the spotlight on data privacy and protection. While third-party financial apps often help consumers make more informed financial decisions, they also expose consumers to personal data risks. With the growing use of these apps giving fintech providers access to consumer banking data, SIFMA (Securities Industry and Financial Markets Association) has released a set of industry-wide principles for protecting, sharing and aggregating customer financial information.

SIFMA's Data Aggregation Principles provide guidance for financial firms when working with data aggregators to protect consumer data and ensure third parties adhere to stringent data and security standards. The principles cover data access, security and responsibility, transparency and permission, and scope of access and use.

SIFMA encourages financial firms and aggregators to move toward more secure technologies for gathering customer data, such as the use of application programming interfaces (API) to share data between the bank and data aggregator via a portal, without the need for consumers to share logins with financial apps. Get the details at: https://www.sifma.org/resources/general/data-aggregation-principles/.

Get Ready for GDPR

Europe's landmark data privacy regulation, the General Data Protection Regulation (GDPR), goes into effect May 25, 2018. The GDPR demands that all businesses, including banks, take steps to protect personal data, and gives data owners new rights around the access to and portability of their data. Companies located in, or doing business in, the EU will no longer be able to collect and use personal data without the individual's consent, that includes U.S.-headquartered banks and fintech companies with global operations. In preparation for GDPR, start with a privacy risk impact assessment. For regional and community banks, an analysis of your customer base and any exposure to European data is needed. Ensure everyone in your institution who handles personal data is aware of the new requirements and their obligations to adhere to the GDPR requirements. Compliance with the GDPR should involve people, policy and processes. The cost of ***not*** complying with GDPR risk could result in a loss of up to 4 percent revenue. So be ready!

Focus on Threat Assessments

by Mary Gates, CFSSP, CHPA-III, VP of Security, GMR

Banks and other financial institutions are faced with the critical challenge of ensuring the protection of their people, assets and information. Threat Assessments should be a core component of any corporate security risk analysis program. Threat Assessments, however, should not be confused with a Security Review or a Security Audit. A Security Review or Security Audit assess how effectively your bank's security policies and procedures are being implemented, uncovers where security gaps exist and helps identify issues driving non-compliance with the security program. The Threat Assessment will identify your most critical resources and the weaknesses that can be exploited along with the likelihood of occurrence.

Mitigate Risk through a Comprehensive Evaluation of Threats and Vulnerabilities

From insider threats to external forces, it is important for security professionals to remain vigilant in their understanding of the risks, threats and vulnerabilities in and to their organizations. A threat assessment methodology should include:

- Analyzing the operating environment, inclusive of the surrounding area;
- Reviewing the property and its current areas of exposure, including security incidents, to identify potential vulnerabilities;
- Interviewing employees and other key personnel;
- Providing a gap analysis to identify areas where your security program does not address vulnerabilities or meet industry best practices; and,
- Recommending and guiding executive leadership in implementing security measures to mitigate any identified areas of vulnerability to reduce your risk.

What are the Differences between Threats, Risks and Vulnerabilities?

Threat, risk and vulnerability are not interchangeable; rather, they are the essential ingredients of an accurate risk analysis. In their simplicity,

Threats:
- Need to be identified
- Generally, cannot be controlled

Risks:
- Can be mitigated
- Can be managed to lower vulnerability or impact on the business

Vulnerabilities:
- Can be treated
- Weaknesses should be identified
- Proactive measures should be implemented to correct identified vulnerabilities

In closing, the Threat Assessment is not a one-time review. The world continues to evolve as does your organization. Risk analysis is complex and the threats are always there. Security measures, processes or procedures put in place three years ago may not address the threats or risks your organization faces today. Understanding the magnitude of the consequence associated with those threats and risks, their likelihood to occur and the possible effects on your bank are the primary components to managing security risk at your bank.

Mary joined GMR in March 2018 following a corporate security management career with a leading global financial institution. Her experience includes investigations, regional and national project management, serving as a multi- state physical security manager; managing internal risk and control programs, consulting on policies, procedures and standards, and serving as the security officer program compliance manager.

Managing Third-Party Risk

Faced with increased regulatory scrutiny, financial institutions must effectively manage risks regardless of whether the institution performs an activity internally or through a third party. Therefore, an institution's risk management program must include fintech partners and other outsourced providers. In November 2017, a consortium of several major financial servics companies, including JP Morgan Chase, Bank of America, Wells Fargo and American Express, founded TruSight to standardize the way financial institutions manage third-party relationships and risk, and ensure that third-party suppliers and partners are adequately prepared to manage and mitigate risk. TruSight screens vendors to ensure their practices and processes are compliant, and stores that information on a secured, shared platform that can be accessed by financial institutions before engaging vendors.