Is Cybersecurity Part of Your Risk Management Plan?

April 27, 2017 / in TLI 417 / by Marc Riccio

In working with financial institutions across the country on their operational risk management programs one area that regulators and auditors have recently had a keen focus on is Cybersecurity. More and more states and regulators are going to enact similar rules to the one listed below by the New York Department of Financial Services.

"The New York Department of Financial Services yesterday issued final regulations that will require its state-chartered banks and affiliates to establish and maintain a cybersecurity program as part of an ongoing effort to protect consumers and the state's financial system from cybercrime. The rules take effect March 1, and with limited exceptions, banks will have 180 days to comply."

"The regulations — the first of this kind to be issued by a state regulator — require banks and other financial services providers to maintain a cybersecurity program based on the institution's level of risk; maintain written cybersecurity policies and procedures; designate a chief information security officer; and maintain an audit trail for cybersecurity events. The rules also impose additional requirements related to annual certification, risk assessments, reporting, recordkeeping, and periodic reviews of access privileges, among other things."

"The final rules were revised from an earlier NYDFS proposal, which received significant pushback from bankers and other industry stakeholders, including ABA. While the final rules take a risk-based approach, ABA remains concerned that they will add significant regulatory burden to banks of all sizes, and that the short compliance window does not give banks enough time to put the necessary systems and processes in place. In addition, the rules could come in conflict with existing federal regulations, and may not provide enough flexibility to address the constantly evolving nature of cyber threats, the association noted." This article appeared in the ABA Daily Newsbytes.

This is another reminder of the importance of have a comprehensive operational risk management program in place before the auditors come knocking.

Specialized Data System's RemoteComply is an all-in-one web based suite containing solutions for business continuity planning, vendor management, incident response, and alert notification. The suite creates one centralized area to easily update and maintain all operational risk management criteria to satisfy the regulators and effectively prepare IT and compliance personnel for an inevitable disruption.

As a leading software provider in the financial industry for over 25 years, Specialized Data Systems is known for developing quality solutions to better the industry. They have developed RemoteComply with the intentions of creating a system that will centralize all risk management in one log-in to easily maintain and present to regulators. The suite will drastically improve the process of operational risk management by saving countless man-hours, ensuring compliance, and alleviating the frustrations typically associated with operational risk management.

About the Author: Marc Riccio

Marc Riccio, President of Specialized Data Systems, Inc., has over thirty years of experience providing software solutions to the financial industry. Marc is known for his forward thinking and vision of introducing new and innovative technologies including "rules-based" Loan Origination software, COLD/Document Image Systems, Internet Security Services on Demand, Cloud Computing and now Operational Risk Management software. Prior to founding Specialized Data Systems in 1989, Marc worked for several technology companies as a Systems Analyst, Account Manager and Sales Manager. Among his significant previous positions, Marc served as Senior Marketing Representative for FiServ-Connecticut and worked in the Retail Banking and Systems group for Bank of America.