21CFS
INNOVATIVE BANKING

Free Resources Your Bank Can Use to Evaluate your Security & Elevate Awareness

October is officially designated National Cyber Security Awareness Month. As executives of Financial Institutions, we have a higher standard to meet in terms of our responsibilities to protect the sensitive data and transaction capabilities on our corporate networks. This month should be used as a reminder to proactively examine, test, adjust, and implement a comprehensive plan to secure and protect our valuable digital data.

21 CFS has provided strategic steps to help you in your executive oversight role to ensure that you are both in compliance with any relevant regulations and that you are maintaining an active knowledge on the state of security in your systems. Your active participation, along with the management team in charge of your IT infrastructure, will help to lay a solid foundation from which to build a safe and secure infrastructure.

STEP 1: REVIEW AND EDUCATE YOURSELF ON RELEVANT REGULATIONS AFFECTING YOUR ORGANIZATION

This base level knowledge is essential in understanding the intent and purpose for the regulations and to equip you to protect your business properly. For each major regulatory, included are links to the actual regulatory guideline document, followed by a link to a more easily distilled executive summary resource.

a. SarbanesOxley Act (SOX) regulates the secure storage and management of internal financial records.

Sarbanes Oxley Act

Sarbanes Oxley Key Provisions

b. GrahamLeach-Bliley Act (GLBA) establishes guidelines for the collection, safekeeping and use of private customer financial information.

Understanding Graham Leach Bliley

Graham-Leach-Bliley Act Compliance Cheat Sheet

c. Payment Card Industry Data Security Standard (PCI DSS) regulates the storage, processing, and transmission of cardholder data

Requirements and Security Assessment Procedures

Understanding the Payment Card Industry Data Security Standard

STEP 2: ASSESS COMPLIANCE

Assess compliance via direct communication with responsible Security team within your organization and verifying that you have in place a robust structure of internal and external auditing.

STEP 3: UPDATE CORPORATE POLICIES

Ensure that all corporate polices are updated appropriately to reflect procedures and documentation that will meet or exceed all regulatory items listed above.

STEP 4: PLAN FOR THE FUTURE

Participate in planning for the future. Work actively with your IT Security personnel to ensure that system security is a required element in all development and system infrastructure projects.

National Cybersecurity Awareness Month occurs every October as a national campaign designed to increase the public's awareness of cybersecurity and cyber crime issues. By taking these steps you can ensure that IT Security will remain in alignment with executive directives and stay within the scope of all regulatory guidelines.

If you have questions, or need additional guidance and a sounding board to ensure you're bank is secure from cyber threats, contact the 21 CFS team today.