October is National Cybersecurity Awareness Month

Focusing on the Fundamentals

Too often financial institutions are using only portions of different cybersecurity frameworks (standards) but fail to focus on key elements that prevent hacking.

This year we are promoting the theme of ***Focusing on the Fundamentals***. Watch the short video of a community bank CEO discussing a three-step strategy for managing cyber threats by focusing on the often overlooked ***fundamentals*** of cybersecurity controls and frameworks. His strategy is applicable to not just banks, but all types of financial and non-financial institutions.

CAT stands for Cybersecurity Assessment Tool
NIST stands for National Institute of Standards and Technology

Cybersecurity Awareness Month is an annual reminder that encourages both businesses and consumers to take steps to strengthen cybersecurity. This is an opportunity for you to re-evaluate your strategy and also encourage your customers (both consumers and businesses) to become more cyber-aware.

While many believe that most cybersecurity breaches are the act of sophisticated hackers and foreign agents, most successful cyberattacks are because of a failure to follow well-established cybersecurity practices.

To ensure your entity is following these best practices, we encourage you to collaborate with your peers, vendors, and regulators. Your entity is not an island. Cybersecurity has no borders and crosses infrastructures. We must collaborate and share information.

October is National Cybersecurity Awareness Month

Focusing on the Fundamentals

How can you protect your entity from a cyber-attack?

State and federal regulators as well as a taskforce of CEOs provide you with the tools you need to secure your IT infrastructure and data. Below is the Three-Step Strategy discussed in the video.

Adopt a Three-Step Strategy

1. Select an industry recognized **cybersecurity framework(s),** for example:

   a. FFIEC Cybersecurity Assessment Tool,

   b. NIST Cybersecurity Framework, and

   c. Center for Internet Security Controls.

2. Establish a **budget** for meeting your cybersecurity strategy within a reasonable time.

3. Hire an audit firm to review the implementation of your framework(s) rather than to review compliance with the minimum regulatory guidelines (a mock FFIEC exam). The goal is to ensure **key controls** in your cybersecurity frameworks have been implemented and are functioning as intended.

Complete the Ransomware Self-Assessment Tool

The Massachusetts Division of Banks works with other state banking regulators, federal regulatory agencies, the U.S. Treasury Department, Federal Law Enforcement agencies and a *Bankers Electronic Crimes Task Force* (BECTF) of community bank CEOs that identified ways to protect institutions from cyber-attacks. The BECTF developed a Ransomware Self-Assessment Tool (RSAT) for banks that community financial institutions are using to close the gaps in their security. The BECTF also developed a version of the RSAT for businesses, which is perfect for you to share with your business customers to help ensure their survival against this global threat.

Building a Cybersecurity Program from Scratch

For smaller or non-bank financial institutions that haven't done so already, begin building a cybersecurity program by referencing the **Center for Internet Security Controls** as well as the CSBS Resource Guide for Executive Leadership of Cybersecurity. These resources address challenges faced by all entities. They are easily digestible, non-technical, and will help executives develop a comprehensive, responsive cybersecurity program in line with best practices.