Charles G. Cooper
Commissioner

TEXAS DEPARTMENT OF BANKING

2601 North Lamar Blvd., Austin, Texas 78705
512-475-1300 /877-276-5554
www.dob.texas.gov

Media Contact:
media@dob.texas.gov

INDUSTRY NOTICE 2021-07
Date: October 6, 2021

Cybersecurity Awareness Month: Focusing on the Fundamentals

October is Cybersecurity Awareness Month, an annual observation during which consumers and businesses are encouraged to take steps to protect themselves from cyberattacks.

The theme chosen by the Department of Banking for Cybersecurity Awareness Month 2021 is ***Focusing on the Fundamentals***. While many people believe most cybersecurity breaches are the act of sophisticated hackers and foreign agents, the majority of successful cyberattacks are the result of a failure to follow well-established cybersecurity practices.

The Department suggests you view this short video featuring Trey Maust, Executive Chairman of a community bank, who discusses a three-step strategy for managing cyber threats by focusing on the often-overlooked *fundamentals* of security and key cybersecurity frameworks. His strategy is applicable not only to banks, but all types of financial and nonfinancial entities.

To ensure your organization is following these best practices, the Department encourages you to take the necessary steps to collaborate with your peers, vendors, and regulators. Neither your entity nor the Department operate within a vacuum: Cybersecurity has no borders and frequently crosses infrastructures. All stakeholders must collaborate and share information.

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

State and federal regulators can provide the tools you need to build a solid cybersecurity program for your entity.

Financial institutions are encouraged to review the *Adopt a Three-Step Strategy* section below. For nonbank financial institutions and other businesses that have not done so already, the Department encourages you to begin building a cybersecurity program by referencing the Conference of State Bank Supervisors (CSBS) guide*: A Resource Guide for Executive Leadership of Cybersecurity.*

The guide addresses the challenges all entities face in an easily digestible, non-technical format to help executives develop a comprehensive, responsive cybersecurity program in line with best practices.

Each entity is different, but the advice in this resource guide can be easily customized to meet your organization's unique threats, priorities, and challenges. The information will help executive staff identify the people, processes, and technologies that, when properly leveraged, work to reduce cybersecurity risk.

Adopt a Three-Step Strategy.

1. Select specific industry recognized **cybersecurity framework(s),** for example:
    a. FFIEC Cybersecurity Assessment Tool,
    b. NIST Cybersecurity Framework, and
    c. Center for Internet Security Controls.
2. Adopt a budget for meeting your cybersecurity strategy within a reasonable timeframe.
3. Hire an audit firm to review the implementation of your framework(s) rather than simply reviewing compliance with the minimum regulatory guidelines (i.e., a mock FFIEC exam). The goal is to ensure key controls in your cybersecurity frameworks are implemented and functioning as intended.

Staying cyber-secure is not as simple as completing a single checklist. It is not a project that you do once and are finished; it is an ongoing process that must evolve with your industry and emerging threats. By following the steps above, you will be positioned for a more secure future.

Complete the Ransomware Self-Assessment Tool if You Have Not Done So.

The Department works with other state banking regulators, federal regulatory agencies, the U.S. Department of the Treasury, federal law enforcement agencies and the Bankers Electronic Crimes Task Force (BECTF), composed of community bank CEOs, to identify ways of protecting institutions from cyber-attacks.

The BECTF developed a Ransomware Self-Assessment Tool (R-SAT) community financial institutions are using to close the gaps in their security. The BECTF also developed a version of the R-SAT for nonbank businesses, which can be shared with your customers to help ensure their survival against this global threat.