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 2020-15
Date: December 16, 2020

Self-Assessment Tool for Mitigating the Risks of Ransomware for Nonbank Financial Service Businesses

Money Services Businesses

Ransomware has become the top cybersecurity threat to businesses and cybercriminals are utilizing the pandemic to take advantage of weaknesses in operations and controls. To assist your business in mitigating this risk, we are providing you a Ransomware Self-Assessment Tool (R-SAT).

The R-SAT is a brief questionnaire that walks you through key measures to protect your business and can assist management and your Board (as applicable) in evaluating preparedness.

A similar R-SAT was released to the banking industry and was developed by a national task force of community bankers, state bank regulators, and the U.S. Secret Service. This nonbank financial institution version includes several embedded banking resources which are applicable and helpful for all industries. An overview of ransomware preparedness released with the banking industry version of the R-SAT provides an important overview of the threat and important mitigation strategies.

This self-assessment tool will assist you in evaluating your current security operations and identifying areas to upgrade. History indicates that the attackers take advantage of weaknesses in systems. Because of the extreme impact a ransomware incident can have and the rapid expansion of its use by criminals, this version of the R-SAT is being distributed via multiple channels, including various state regulators. Therefore, you may receive multiple notifications regarding this matter. We encourage you to promptly begin assessing your preparedness with this tool.

If you have any questions regarding the R-SAT, please contact Phillip Hinkle, Director of IT Security Examinations, or Senior IT Security Examiner Linda Pearson via email.