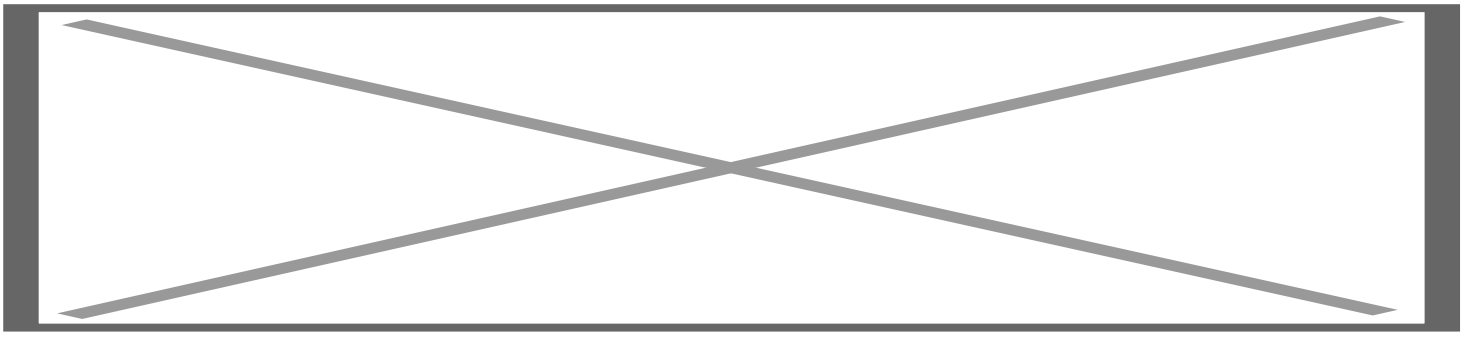
State Regulators Issue Ransomware Mitigation Tool

PRESS RELEASES

State Regulators Issue Ransomware Mitigation Tool

October 13, 2020
|
Download PDF
Share:



Washington, D.C. – State financial regulators, joined by the Bankers Electronic Crimes Task Force and the U.S. Secret Service, today issued a self-assessment tool to banks they supervise in an effort to help mitigate ransomware attacks.

“Ransomware is a major threat to the financial services industry,” said Texas Banking Commissioner Charles G. Cooper, who leads the Bankers’ Electronic Crimes Task Force on this effort. The taskforce, composed of U.S. community financial institution CEOs, law enforcement, state bank regulators and other industry stakeholders, addresses the security needs of community financial institutions.

“State regulators are offering this tool because the rapid advancements in ransomware and potentially devastating consequences require financial institutions to be vigilant. There is no single measure to prevent ransomware attacks. It requires strong adherence to fundamental cybersecurity controls,” Commissioner Cooper said.

Incidents of ransomware across industries have been on the rise and appear to be spreading. One global cyber insurer reported 775 ransomware incidents for its U.S. customers in 2019, representing a 131% increase from the year prior. Eleven percent of those customers were financial institutions.

“This is another example where close cooperation and developing robust partnerships is critical to accomplishing our shared goal of protecting the nation’s financial infrastructure,” said William Smarr, Special Agent in Charge of the U.S. Secret Service Dallas Field Office. “Working with the CSBS, the Secret Service recognizes the value of our trusted partners and the acumen they provide to combat cyber enabled fraud. Together, we are committed to keeping the Homeland safe from cyber threats.”

Using the ransomware tool, a bank can assess its efforts to control and mitigate risks associated with the threat of ransomware and identify gaps that require increased security.

“This newly developed and comprehensive tool gives our bank’s executive managers and board of directors an overview of our preparedness towards identifying, protecting, detecting, responding and recovering from a ransomware attack,” said Trey Maust, executive chairman of Lewis & Clark bank in Oregon City, Ore., and a Bankers’ Electronic Crimes Task Force member.

Media Contact: Susanna Barnett, 202-407-7156, sbarnett@csbs.org

The Conference of State Bank Supervisors (CSBS) is the national organization of bank regulators from all 50 states, American Samoa, District of Columbia, Guam, Puerto Rico and U.S. Virgin Islands. State regulators supervise 79% of all U.S. banks and are the primary supervisor of non-depository financial services. CSBS, on behalf of state regulators, also operates the Nationwide Multistate Licensing System to license and register non-depository financial service providers in the mortgage, money services businesses, consumer finance and debt industries.

Related Topics
Cybersecurity

Related Posts