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

INDUSTRY NOTICE 2013-3
Date: November 1, 2012

Executive Officer Oversight of Cyber-crime Risks

To Chief Executive Officers of All State-Chartered Banks

Introduction

The Federal Bureau of Investigation (FBI), Financial Services-Information Sharing and Analysis Center (FS-ISAC), and the Internet Crime Complaint Center (IC3) recently released a **Fraud Alert** that cyber thieves have been targeting bank employees to gain their log-in credentials, enabling the thieves to handle all aspects of originating a wire transfer through the bank's wire transfer service, including the approval process. Equally troubling, cyber thieves are targeting smaller to medium sized financial institutions.

Often, cyber thefts are not reported to the public and losses from corporate account takeover (CATO) thefts are more commonly being settled out of court. If your bank has not experienced a theft, it can be easy to get a false impression that these thefts are not a risk to your bank or that they are no longer occurring. Cyber-crimes are continuing to occur and they represent a risk to all banks. One bank this year has experienced more losses through one cyber-crime than in the loan portfolio. Unlike the loan portfolio, there was no loss reserve to buffer the impact to earnings and capital.

Action is needed by the banking industry before thieves expand this particular threat. Cyber-crime is rapidly becoming a significant risk in the banking industry. As such, complying with information security regulations and standards, and following a check list of security measures is no longer sufficient. Information security must be an actively managed risk, just as in other areas of the financial institution. It requires a corporate culture of security.

Executive Officer Oversight of Cyber-crime Risk Reduction

With the release earlier this year of Supervisory Memorandum 1029 and the *Best Practices for Reducing the Risk of Corporate Account Takeovers* developed by the Texas Bankers Electronic Crimes Task Force, all Texas state-chartered banks have begun developing risk mitigation plans for CATO. However, we have recently observed a troubling pattern. Over the past few months, three large cyber thefts have occurred from smaller community banks. One theft was approximately a quarter million dollars, another $1.7 million, and the third $6 million. In all three incidents, multiple employees at each bank had been trained on CATO risks, but these employees failed to follow procedures or observe very obvious indications that a wire was fraudulent. These incidents indicate that employees did not understand the importance of information security. And, following written procedures isn’t always enough since cyber thieves shift techniques frequently. Employees must take ownership of their role in reducing / preventing electronic thefts.

Some banks have developed very good cultures of security where all employees take ownership of being vigilant against fraud while also providing helpful services to customers. Other banks, especially those that have not experienced a large theft, may need to work on further developing or expanding that culture, encouraging employees to take ownership, and having a process to maintain a culture of security. Achieving these things requires a retraining of thought processes so all employees keep in the forefront of their daily activity the knowledge that large thefts are just key strokes away. A culture of security can be difficult to develop when cyber-thefts are not regularly occurring at a bank; however it must be done, as the impact of these thefts can be devastating. Implementing the risk management approach of Protect, Detect, and Respond, as addressed in Supervisory Memorandum 1029, is one way to start creating a strong culture of information security in the bank.

A CEOs daily / weekly management thought process must now include more than the traditional risk areas that have dominated a bank manager’s attention (lending, deposit operation, investments, etc.) Before cyber-crime incidents increased, most fraud risks had been manageably small. Cyber-crime has changed that. Potentially devastating cyber-crime losses should be part of the budgeting and capital planning process, as well as insurance planning. Creating a culture of security is a top-down process. I encourage you to discuss this with your Board and senior management team. Consider appointing an individual to lead a program of developing or expanding a culture of information security that encourages employees to take ownership and includes steps to maintain the culture. In the coming weeks I will be asking our examination staff to discuss with you and your Board the steps that your institution is taking to create a culture of security. There are challenging times ahead, but with proper planning the challenges can be overcome.

For further information about this Industry Notice contact the **Chief IT Security Examiner** or by **email**.