AN ALERT FROM THE BDO FINANCIAL INSTITUTIONS & SPECIALTY FINANCE PRACTICE

BDO KNOWS:

FINANCIAL INSTITUTIONS & SPECIALTY FINANCE

BANGLADESH CENTRAL BANK MALWARE ATTACK HIGHLIGHTS INDUSTRY INADEQUACIES IN CYBERSECURITY

The February 2016 cyber attack on the Bangladesh Central Bank resulted in the loss of more than $100 million from its account at the Federal Reserve Bank of New York. The hackers, posing as Bangladesh Central Bank officials, stole the bank's credentials and sent dozens of secure messages to the New York Fed, authorizing the transfer of funds from the country's Fed account to private bank accounts in the Philippines and Sri Lanka. The Bangladesh Central Bank governor ultimately resigned, and bank officials have launched a potential lawsuit against the New York Fed.

The $100 million theft is one of the largest cyber banking heists in history — but it won't be the last. As increasingly sophisticated cyber attacks against financial institutions become more frequent, banks need to heighten their defenses to protect their businesses and their customers.

SUMMARY

Regulators have increased their examination of financial institutions' cybersecurity measures and protocols in recent years. Since June 2013, the Federal Financial Institutions Examination Council (FFIEC) has focused on cybersecurity as a top priority, developing resources and guidance for financial institutions to increase awareness of, assess and mitigate cyber risks. In July 2015, the FFIEC launched a cybersecurity assessment tool designed to help financial institutions measure their cybersecurity preparedness over time. Later in the year, the FFIEC issued guidance alerting its members to the increasing frequency and severity of extortion-based cyber attacks, implying regulatory examinations and enforcement to follow.

In November 2015, an interagency working group comprised of the Financial Services Information Sharing and Analysis Center (FS-ISAC), the National Institute of Standards and Technology (NIST), the Department of Homeland Security, the National Security Agency, and the Securities Industry and Financial Markets Association released additional guidance on the threat from destructive malware, not unlike the malicious code that enabled cybercriminals to hack into the Bangladesh Central Bank's system. Destructive malware is defined as "a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs or otherwise compromise the confidentiality, integrity or availability of the victim's data, applications or operating systems." FS-ISAC

Read more ▶

HOW DO I GET MORE INFORMATION?

For more information about how financial institutions can safeguard their organizations against cyber attacks, please contact:

SHAHRYAR SHAGHAGHI
BDO Consulting Technology Advisory Services National Practice Leader and Head of International BDO Cybersecurity
sshaghaghi@bdo.com

JIM CARTER
Leader of BDO's Financial Institutions & Specialty Finance Practice
jcarter@bdo.com

strongly recommends implementing the NIST Cybersecurity Framework, based upon the following five-part risk management framework:

- **Identify:** Pinpoint critical data, backup processes and systems in the organization necessary for critical business functions, along with where they come from, where they are located and how they are used.
- **Protect:** Implement a variety of controls to protect corporate data and personally identifiable information as well as critical infrastructure across all levels of the organization, including high-risk vulnerabilities arising from third-party relationships.
- **Detect:** Cement in place mechanisms that swiftly detect malware when it enters a system, and that are able to assess its full potential impact — and whether it is destructive in nature.
- **Respond:** Train management on how to adequately protect information systems and confidential data while ensuring business continuity if subject to a cyber attack. Should unauthorized access occur, a financial institution's computer systems could fail, potentially compromising confidential information.
- **Recover:** Adjust cyber incident response processes and procedures to prepare for a destructive malware incident that has the potential for catastrophic business impact. In light of the attack on the Bangladesh Central Bank, financial institutions need to update mitigation and contingency strategies and align all parts of their organization—from the management level and communications teams to customer-service departments, business partners and third-party providers.

BDO INSIGHTS

BDO assists financial institutions in conducting ongoing security risk assessments and testing controls in line with the FFIEC's guidelines, in addition to implementing and updating cybersecurity risk management programs, strategy and governance. Financial institutions are well-advised to seek assistance from consultants and technology specialists experienced in developing risk management frameworks and strategies that meet regulatory standards and are customized to individual needs.

Despite ample warning from the FFIEC and other industry regulators, as well as the daily news' constant reminders of the prevalence of data breaches, financial institutions haven't fully embraced the cyber tools available to them. According to a recent FIS survey, only 62 percent of bank executives said their organization is using the FFIEC's cybersecurity assessment tool. Just 39 percent said their organization validates the results.

The Bangladesh Central Bank incident demonstrates just how costly it can be to not continually assess vulnerabilities and put a comprehensive security framework in place. The FFIEC's recommendations, made in the context of the NIST Cybersecurity Framework, provide a good starting point. The guidelines are intended to ensure that financial institutions take proactive—and recurring—steps to address their cyber risks. However, any cybersecurity framework needs to be tailored to reflect the organization's unique cyber risks and potential impact to customers and other company stakeholders.