Avoiding Getting Zapped By Tougher Cyber Rules

by Steve Brown

The Army reports it has technology that can shoot things out of the air as small as individual mosquitoes. This laser technology could be used to zap enemy drones and a host of other things. While interesting for sure, we wondered what would happen if the technology were hacked. After all, cyber breaches continue to hit all industries, which is why banking regulators are raising the bar for ours.

In October, federal regulators proposed strict new cybersecurity standards for big banks that have assets $50B+. The proposed standards for this group come on the heels of a separate proposal by the NY Department of Financial Services that would affect all NY state-regulated banks - regardless of their size.

Both efforts come amid an increasing number of cyberattacks against banks across the globe, some with significant monetary consequences. Earlier this year for instance, hackers stole around $80mm from Bangladesh's largest bank. In April, thieves then hacked the Qatar National Bank, and in June banks in South Korea and Indonesia were hit with a large-scale DDoS attack.

The federal standard for large US banks focuses on 5 main areas: cyber risk governance; cyber risk management; internal dependency management; external dependency management; and incident response, cyber resilience and situational awareness. Federal regulators are also calling for more cybersecurity oversight from boards and senior management by holding them accountable for implementing cyber risk management frameworks. Regulators are also considering requiring directors to have "adequate expertise" in cybersecurity.

Generally speaking, most community banks won't be governed by the federal proposals, but as with most things there could be a trickle-down effect to avoid getting zapped. As it now stands, community banks would only be subject to the standards if they are part of a larger banking organization that meets the asset threshold. The standards will be finalized after a comment period ending Jan.17.

Meanwhile, the NY proposals would require regulated financial institutions to establish a cybersecurity program; adopt a written cybersecurity policy; and designate a Chief Information Security Officer responsible for implementing, overseeing and enforcing its new program and policy.

Banks, insurers and other financial institutions would also have to adopt policies and procedures designed to ensure the security of information systems and nonpublic information accessible to, or held by, third-parties. There are also a variety of other requirements to protect the confidentiality, integrity and availability of information systems.

Certainly, many community banks fall outside the jurisdiction of both these proposals, so all is not lost. However, cybersecurity is an ongoing concern to all, so banks need to be paying attention to these changes too.

At minimum, banks should consider the final rules as good practices to live by. Certainly, most large banks have an IT budget that dwarfs that of community banks, so not all the proposed standards will be practical to implement. Nonetheless, community banks aren't immune to cyberattack so there's a real benefit to being proactive vs reactive.

Even if regulators aren't explicitly requiring this for all banks, community banks could benefit from enhancing security around the cyber world.

BANK NEWS

Stable Outlook

Moody's indicates it has retained a stable outlook on the US banking system for 2017. Moody's pointed to positive signs such as strong liquidity, good consumer credit, strong capital and an improving economic picture and indicated those balanced out negative concerns over commercial credit and ongoing profitability pressure.

Fintech Risk

Fed Governor Brainerd in a recent speech said that as a general rule, introducing new products or services typically involves heightened risks as banks enter into areas where they may not have experience or that are not consistent with business strategy and risk tolerance. She indicated banks must manage outsourced relationships consistent with supervisory expectations, consider their business model and risk management infrastructure, and ensure new products and services have strong fallback plans to limit risks around those that may not survive. In short, banks bear the responsibility to provide innovative financial services safely to customers.

Efficiency

FDIC research finds the efficiency ratio as of Q3 for various asset sized institutions is as follows: <$1B (71%), $1B to $10B (62%), $10B to $250B (55%), $250B+ (58%).

US M&A

Dealogic research finds more than 8,000 M&A combinations have been announced in the US this year worth about $1.55T.

Mega Data

Community bankers will be interested in McKinsey's research that finds the volume of data is doubling every 3Ys.

Dividend Payouts

Fed research finds the average dividends to net income for banks in the 12th Fed District was 15% as of Q3. This compares to the same level as of Q3 2015, a low of 4% as of 2010 and a high of 25% as of 2007.

Mobile Usage

A survey of millennials worldwide by Gemalto finds the following usage of mobile banking services: paying bills (40%); do not use (17%); view balances or statements (9%); apply for credit or loan (4%); domestic transfers (26%); international transfers (2%); and other (2%).