Operational Risks

by Steve Brown

Cyber crooks seem to be everywhere these days breaking into systems and stealing identities, money, health records and more. No one seems safe and it is no wonder that cybersecurity has become one of the top operational risk concerns faced by banks. Regulators say banks, their employees and their customers are all vulnerable to cyberattacks. In response, banks are looking at new security and adopting new technology and operating processes.

Some recent cyberattacks point to operational vulnerability in payment environments - particularly where fraudulent operator credentials can be created that convey the authority to create and approve account activities like fund transfers.

Worse yet, sophisticated hackers can create malware capable of disabling security systems and concealing or delaying detection of fraudulent transactions, we have even seen recently in some of the worst situations globally.

These new threats come as security teams are still dealing with a rash of cyber extortion schemes in which hackers break into and cripple systems and demand payment in virtual currency to reverse the damage.

While cybercriminals frequently enter a bank due to a human mistake of some sort (according to many insurance experts we know), sophistication is spooky so awareness and training must be at the highest level possible at banks.

One trick hackers often use involves a fraudulent email that requests expedited wire transfer to pay a phony vendor invoice. Known as business email compromise (BEC), this tactic has caused more than $2.3B in losses from Oct., 2013 to Feb., 2016, according to the FBI.

Even worse, hackers are not just attacking financial institutions and their customers, but also providers of cybersecurity products. You heard this right, hackers are compromising the very systems designed to safeguard banks and their customers.

While enforcement officials try to combat the cybercrime wave, bankers must remain vigilant to potential threats. That means adapting risk management, control systems and processes to respond to threats. This is even tougher now, due to an increasing reliance on new technology and products in the industry. This can also be further impacted by the increasing use of third-party vendors or partners that may have less familiarity with bank regulations. As such, it is critical to consider cybersecurity risks in your business strategy, risk management and strategic planning.

Ironically, one of the ways banks have tried to improve credit risk management and transparency is through the use of central counterparties or central clearinghouses (CCPs) to clear transactions. Unfortunately, these may also provide hackers with yet another huge target for mischief. After all, CCPs increase the concentration of operational and credit risk, so that one hack can harm a collection of banks.

In many ways, the technology revolution that has been a boon to banks and customers alike has also increased risk. Technology has improved business processes, efficiency, created new products and delivery methods, and helped in dealing with new regulatory requirements. In like fashion, outsourcing some activities has enabled banks to concentrate on core business lines and customers. All of these things of course have also increased operational risk from cybercriminals and some vendors can be Swiss cheese so are easy targets.

As cyberattacks make clear, sophisticated hackers are everywhere and they have a particular fondness for following the money so banks have to be very careful.

BANK NEWS

Fed

Mohamed El-Erian (from Allianz) told CNBC he sees an 80% chance the Fed will raise rates in September if the jobs report comes in strong. Another economist agreed and said if the upcoming jobs data is above 200,000 the Fed will move, but if it is 150,000 or less they will wait until December.

NIM Performance

The FDIC reported net interest margin for various asset size groups as follows: <$100mm (3.69%); $100mm to $1B (3.68%), $1B to $10B (3.60%), $10B to $250B (3.52%) and $250B or > (2.63%). The difference between the lowest and highest is 40%.

Not Using

Research by Intelligent Environments finds consumers check their bank balances on tablets only 9% of the time vs. 25% for smartphones and 53% on a personal computer.

Stronger Stocks

In good news for banks, increased discussion around the potential for Fed rate hikes soon has buoyed stock prices. The S&P Financial Sector climbed 3.6% in August vs. -.1% for the broader S&P 500. Meanwhile, financials were the best-performing sector for the first month this year.

Digital Threats

Research by Deloitte and MIT on digital disruption finds the biggest threats respondents say are facing their company due to digital trend are: a lack of resources, too much data, lack of a strategic focus (22%); lack of agility, complacency, inflexible culture (19%); product obsolescence, lower barriers to entry (17%); more intense competition, faster or new competitors (16%) and security breaches, hacking, intellectual property theft (14%).

Healthcare Costs

Research by Altarum Institute finds healthcare has now risen to 18.2% of GDP in Q2 vs. 13.3% 16Ys ago.