Analyzing Online Banking & Cyber Risk

by Steve Brown

A Bloomberg analysis of company earnings calls and other corporate events for the most recent quarter shows the top 3 things executives are most worried about based on analyzing the transcripts. It finds the term Amazon was mentioned the most by far. Over the past 90 days in the analysis, Amazon was mentioned almost 400% more often (635x) than President Trump in second position (at 162x) and wages in the third position (at 111x).

No matter how often you mention things at your bank, as an industry, bankers talk a lot about cybersecurity risks. That is because it is scary and a security breach can be very costly too.

For instance, a recent Kaspersky Lab report on the financial sector puts a figure to this issue. It finds a cybersecurity incident involving a bank's online banking services costs the bank $1.75mm on average. That's 2X the price of recovering from a malware incident, which costs as much as $825k on average.

According to Kaspersky, 61% of cybersecurity incidents affecting online banking pile on extra costs for the targeted institution. These extra expenses include data loss, reputational loss and confidential data leakage, among other things.

Certainly, the dollars involved in cleaning up cybersecurity attacks aren't trivial, which underscores the importance of banks implementing appropriate measures to ward off potential trouble.

Distributed denial-of-service (DDoS) attacks are becoming more prevalent, powerful and costly for banks. Earlier this year, for instance, Lloyds Banking Group came under a DDoS attack that hampered access to its online banking services for about two days, according to published reports. Banks in South Korea have also recently been threatened with DDoS unless they pay several hundred thousand dollars in bitcoin.

These attacks are typically designed to immobilize banking websites. The report shows that when organizations are attacked by DDoS, customer-facing resources suffer more in banking than in any other sector. A notable 49% of banks that have suffered a DDoS attack have had their public website impacted vs. 41% of non-financial institutions. What's more, 48% of banks have had their online banking services affected when targeted by DDoS.

Despite the high occurrence rate, the report also shows that banks aren't placing as much emphasis on warding off threats from DDoS as they are for, say, malware and targeted attacks. This is true, even though DDoS is more costly to recover from compared with a malware attack. The report found that a single DDoS incident can cost a financial institution $1.17mm.

To be sure, there is no magic bullet to ward off cyberattacks of any sort, but that doesn't mean banks shouldn't take proactive steps. There are several best practices to follow.

For instance, it's important to locate servers in different data centers and ensure those centers are on different networks.

What's more, certain types of attacks have been around for a long time, so continually update patches and hardware.

Another good idea is to scale up your network bandwidth and identify outsourcing partners who specialize in responding to attacks to have extra support.

No bank wants a problem when it comes to cybersecurity because the stakes are simply too high. The benefit of better securing your systems, remaining diligent and continually educating and adapting your teams and company far exceeds the price you'll pay should a breach occur.

Now may be the time to shore up your system against any such attacks before they happen. At least then you can start to mention it in your earnings calls.

BANK NEWS

Elder Fraud

CNBC reports retiree financial fraud has mushroomed to an estimated $36.5B per year. The most cases by type of fraud are: third party abuse or exploitation (27%), account distributions (26%), family member, trustee or power of attorney taking advantage (23%), diminished capacity (12%) and combined diminished capacity and third party abuse (12%).

Blockchain and Cryptocurrencies

Bloomberg reports Barclays, CIBC, Credit Suisse, HSBC, MUFG and State Street have recently joined UBS, BNY Mellon, Deutsche Bank, Santander, NEX and a blockchain startup in a project designed to assist global banks with a multitude of transactions using a customized blockchain. If this is successful, it may help set the stage for central banks to possibly use blockchain technology to issue cryptocurrencies.

Telecommuting

Around the world about 20% of workers do some or all of their work at home. By comparison, about 60% of US companies offer remote working arrangements today.

Real Estate Sentiment

NREI's retail real estate survey shows that key stakeholders in the retail market - including operators and investors - have the gloomiest view of the market over the past 2Ys. Approximately 37% of respondents believe it is a good time to sell.

Mall Stress

CBRE research finds department stores in the US occupy about 50% of the gross leasable area of shopping malls, while apparel and accessory retailers occupy about 29% more. CBRE indicates both of these sectors are heavily under attack from online players, so mall owners will need to bring in tenants in growing sectors and redevelop spaces to attract them.

ROA Improvement

FDIC data finds that from Q2 2016 to Q2 2017 the average ROA for financial institutions with assets <$1B climbed from 0.99% to 1.02%.

CHICAGO ROAD TOUR REGISTRATION STILL OPEN!

Join your peers and industry experts in Chicago for the Executive Management Road Tour, September 25-26. Register today!

Copyright 2018 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.