MENTORING & EDUCATING STAFF ON CYBER ATTACKS

by Steve Brown

As we wind down the work year, we share an interesting poll from MTV. It found 75% of Generation Y workers (those in their 20's and early 30's) want to work for themselves one day; 89% want to be constantly learning on the job and 85% think their familiarity with technology makes them a faster worker. In addition, 92% feel their company is lucky to have them as an employee and 80% want regular feedback and recognition (50% want feedback at least once a week). It takes work to mentor employees of all ages, but it is incumbent upon management teams to try and do so to make the bank a better organization and support employee growth. Maybe this year it is time for each executive to make it a resolution to spend time mentoring key staff in 2013. Learning is a continuous process, so helping the members of your team master new skills is wholly good for the bank. Bank executives have also learned a valuable lesson recently. That is, cyber criminal activity has increased so awareness and action must follow. Regulators recently provided guidance in this area and reiterated expectations that banks should have risk management programs in place to identify and deal with new and evolving online threats. Updated authentication, layered security and other controls were all identified as critical processes of a sound risk management program. This is all the result of recent and ongoing distributed denial of service (DDoS) attacks on banks. The goal of the criminals is to deny internet service to customers of the bank (and gain public attention) or distract bank personnel (to gain unauthorized access to systems and commit fraud through wires or ACH). Such attacks can block customers from reporting suspected fraud on their accounts and alert communications between the bank and the customer. Training for technology and other staff, conducting deeper due diligence of technology service providers and raising awareness throughout the bank, are all important elements of risk management programs in this area. For technology and security teams specifically, regulators expect information of any attacks (or as a source of pre-preparation efforts) to flow through organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) or the United States Computer Readiness Team (US-CERT). Banks that are attacked should also inform regulators and law enforcement agencies and voluntarily file a Suspicious Activity Report (SAR) if critical bank information is affected. As for customers, regulators want banks to provide timely and accurate communication. This effort needs to include information about any internet site problems, resulting risks to customers, precautions they could take and alternate channels customers can use to conduct banking activities. It is clear from the recent cyber attacks on some of our largest banks that the bad guys out there intend to do harm to the banks and your customers. It is only a matter of time until they begin to try this on community banks, so being prepared is critically important. As identified by regulators with this guidance, it is time cyber risks are incorporated into risk management programs. That will allow your team to identify risk mitigation techniques, create a plan for response, have policies and procedures and test, train and educate customers and staff. As you mentor your employees and educate everyone on the team this coming year, be sure to include the subject of increased cyber criminal activity into the mix to help protect the bank and your customers.

WEAK HOLIDAY SALE

Consumers parted with fewer dollars this holiday shopping season, rising only 0.7% the past 3 mos. through 12/24, according to research firm, the Purchase. Fiscal cliff uncertainty and after effects of Hurricane Sandy were the primary drivers of the weakness.

BANK NEWS

Economic Growth

Bloomberg reports the average U.S. Gross Domestic Product (GDP) economic growth rate for the U.S. has been 3.2% since 1947. The most recent reading was 2.7% for 3Q.

Getting Better

Right now there are about 1.8mm homes for sale on the market vs. about half the level of the peak hit in 2007.

Housing Sector

TransUnion projects the single family residential mortgage delinquency rate for borrowers 60 days+ past due will be 5.32% this year and 5.06% by the end of 2013. In more normal times, that rate is about 1.5% to 2.5%.

Household Leverage

A report from the Fed finds household debt declined at a 2% annual rate in 3Q, following a 2Q increase of 1.2%. Total household debt now sits at $12.9T, down about 13% from the start of the recession in 2008.

Business Jobs

The WSJ reports businesses currently employ about 3.3mm fewer workers than before the financial crisis.

GSE Borrowing

FNMA and FHLMC have borrowed $187.5B from the Treasury since being placed into conservatorship in 2008.

Less SFR

A study by the American Action Forum finds the impact of Dodd Frank and Basel III could result in 20% less single family residential mortgages in 2013.

PE/BankM&A

SNL Financial reports that since the beginning of 2008 there have been 187 private equity transactions involving banks and more than $31B has been invested.