Digital Cash = More Cyber Criminals

by Steve Brown

About 25% of Americans say they now conduct most of their transactions in cash vs. 36% who said so 5Ys ago, according to Gallup research. Interestingly, while 10% say they make all of their purchases with cash (vs. 19% 5Ys ago), about 41% say they make some of their purchases with cash (vs. 33% 5Ys ago). People are adjusting their cash usage it would seem as demographics take hold and people shift toward electronic payment methods over time.

For some crooks, all of this electronic money movement is a dream, and community banks like other banks are still juicy targets. Banks not only provide entry to financial accounts and sensitive information, but also can present an easier route to access the wider financial system.

By manipulating the interconnectedness of the financial industry, organized cyber-crime rings and individual hackers are increasingly using vulnerabilities and weaknesses among community banks as a stepping stone to gain entry into payment networks, financial exchanges and much larger financial institutions, according to industry experts. While community bank IT personnel are no less talented than their larger counterparts and industry service providers, they often lack the budget and the resources to execute cybersecurity initiatives, conduct thorough and on-going staff training and vet downstream vendors as much as bigger banks can.

Executives and board members at community banks are vulnerable, so care must be taken. Crooks are targeting community banks and seeking access points that can include such areas as inconsistent encouragement for regular password updating, intermittent security training and perhaps not staying on top of the broadened scope of cyber crooks.

Cyber criminals have discovered how much community banks lean on third party-providers. Such things as core banking, payment processing, software, retail delivery development, and online or physical security are all on the list. Here again, experts say that cyber-crooks often poke and prod at these connections seeking soft spots that they can misuse for their own purposes.

While JP Morgan has made public its $500mm cybersecurity expenditures, this is clearly not an option for community banks that may be of total asset size of that amount. The president of at least one $350mm community bank said that his institution spends $20k a month on information security. That is not too bad, considering that the bank only rakes in about $2mm a year in overall profits, according to published reports. However, not all community banks can devote ever higher levels of spending commitment to cybersecurity.

While cybersecurity needs to be a focus in your budget allocations each year, there are other things to consider as well. Experts recommend that for community banks the best recourse is to engage in frequent staff training. Then, be sure to share either informally or under the auspices of industry groups, any information about common and current threats.

Also, remember to be extremely vigilant in vetting and reviewing your most mission-critical third-party vendors. These are the ones with the greatest or deepest access to the most sensitive data on

your systems. As such, extra care should be taken.

In this undertaking, banks can develop cross-functional teams to leverage expertise from your own internal financial, legal and IT departments. Then bring in lines of business to help them in reviewing the "riskiest" relationships to determine your best course of action.

BANK NEWS

Better Situation

Fed research finds 70% of American households say they are living comfortably or doing okay vs. 62% in 2013. Also of note, 82% of adults with a bachelor's degree or more in education said they fit these categories.

Adding Risk

Code42 research finds 75% of CEOs and 52% of business decision makers say they use applications and programs that are not approved by their IT department.

BSA Costs

A KBW survey of compliance professionals finds about 50% of compliance employees at banks focus on BSA/AML vs. about 17% who focus on Dodd Frank.

CMO Reporting

A Korn Ferry survey of Chief Marketing Officers finds 90% are part of the executive team and 85% report to the CEO or President.

Loan Shift

Research finds loans issued <$1mm in size have tumbled from providing financing to about 17% of business investment in 2010 to 13% as of 2017.

Biz Conditions

A Deloitte survey of CFOs at major companies finds 66% of those in the Americas rate current business conditions as good (a 4Y high), while 62% expect even better conditions in 2018.

AML Systems

Research by Dow Jones and SWIFT of risk executives worldwide on AML finds 65% say their organizations have systems in place to check their own payments for transparency and data quality.

Better Decisions

A Segmint survey of bank customers finds 80% expect their bank to provide them with information to help them make better financial decisions. Despite this, only 28% said they felt their bank did so.

Mobile Banking

A JD Power banking study finds the percentage of customers using mobile banking now by cohort is: millennials (49%), Gen X (31%) and baby boomers (16%).