Protecting Your Bank & Customers From Risk

by Steve Brown

Good numbers are in vogue. According to the FBI, violent crimes declined nationwide in 2014 by 0.2%. Of course 0.2% doesn't sound that great, but it reflects the downward trend seen since the 1980s. Murders, robbery, burglary and theft have been going down. New York University reports violent crime has declined 51% since 1991 and property crime has dropped by 43% during the same period.

It is good to see violent crimes are declining, but unfortunately for banks, the same cannot be said for cybercrimes. Things are so bad that in 2014 the US Director of National Intelligence ranked cybercrime as the top national security threat, higher than terrorism, espionage and weapons of mass destruction.

One area bankers continue to focus on is protecting against phishing. That makes sense when you consider the most recent Verizon data breach report finds a full 23% of recipients will opening phishing messages and 11% will click on attachments. For every 10 emails sent, criminals have a greater than 90% chance that at least one person will take the bait. Even scarier perhaps, testing finds close to 50% of users open emails and click on phishing links within the first hour. This is all critical for banks to know and understand, because prior Verizon reports have pointed out that phishing is associated with over 95% of incidents attributed to state-sponsored actors.

Another thing to point out from the Verizon survey is data on the frequency of data disclosures by incident patterns and victim industry. For the financial services industry, it found data breaches would most frequently surface from crimeware (36%), Web app attacks (31%), payment card skimmers (14%), insider misuse (11%) and miscellaneous errors (7%).

This brings us to our discussion around the ubiquitous personal identification number (PIN). More specifically, we look at the brutally slow nationwide rollout of EMV microchip enabled cards and the risks that remain even when fully deployed. The good news according to a recent bulletin from the FBI is that EMV transactions at chip-enabled point of sale terminals at merchants do provide more security of personal data than magnetic strip transactions. The bad news is that EMV chips do not stop lost and stolen cards from being used in stores, or for online or telephone purchases when the chip is not physically provided to the merchant (this is known as a card-not-present transaction). Also, data on the magnetic strip of an EMV card can still be stolen if the merchant has not upgraded to an EMV terminal and it becomes infected with data-capturing malware.

When it comes to your customers, the FBI suggests telling them to closely safeguard the security of their EMV cards and PINs. Customers should be careful from the point the new card arrives in the mail, should review bank statements for irregularities and should promptly report lost or stolen credit cards. Further, the FBI suggests consumers should attempt to shield the keypad from bystanders when entering a PIN because such numbers are solid gold to criminals who use stolen ones to commit ATM and cash back crimes.

Bankers continue to fight cybercrime everywhere criminals attempt to gain access, so we hope this information has assisted in those efforts in some small way. In the meantime, remain vigilant and continue to warn your customers to stay up to speed with the latest security as you explore upgrades of your own.

BANK NEWS

M&A Activity

Five Star Bank ($3.3B, NY) will acquire investment advisory firm Courier capital for $11.3mm to $14.0mm in cash and stock. Courier has more than $1.2B in assets under management.

Branch Risk

CNBC reports Bain research finds customers are 33% more likely to enjoy a mobile transaction than visiting a branch; those who use branches are 300% more likely to switch banks than those who are infrequent visitors; those who use apps frequently are 40% less likely to switch banks; and a branch visit is 230% more likely to end up with an annoyed customer than using an app.

More Flexibility

A Consumer Reports survey finds about 90% do some banking online and 10% have reportedly switched to virtual banks.

Industry Warning

The ex-CEO of British bank Barclays warns technological advances could lead to a 50% reduction in the number of branches and people employed in the financial services industry over the next 10Ys.

Mobility

The Wall Street Journal cites Juniper Research as projecting 1B people will access their bank accounts through smartphones and other mobile devices by the end of this year and 2B by the end of 2016.

Wearable Banking

Juniper Research projects smartwatches will be used to access banking apps 10mm times in 2017, rising to 100mm in the next 5Ys.

Branch Changes

Codigo reports 51% of banks and credit unions say they are remodeling at least one banking center/branch through 2016 vs. 26% who said so in 2014. The top reasons cited were to improve the branch experience (64%); improve profitability (14%) and to update the appearance (5%).

Cyber Worry

A survey by Travelers finds American consumers say their biggest cyber concern is that their bank account gets hacked (62%); followed by malware infections of computers and phones (60%); online identity theft (59%); offline ID theft (59%); retailer hacks exposing their personal information (58%); and breaches of their medical records (43%).

Odd Behavior

A survey by HR consulting firm Mercer finds that despite the fact that about 48% of people said they are happy with their current job and their company, 37% said they are considering leaving. About 42% said they were concerned or very concerned with losing their job, which could be a large contributor.

Copyright 2021 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.