True Crime And Cyber Security

by Steve Brown

The news is filled with stories about hapless crooks whose carelessness helps bring about their capture. There was a FL man who fled from a car crash but left his wallet at the scene. There is also a PA man who used his own credit card to jimmy open a garage door, then left it behind when the homeowner suddenly appeared. Finally, consider the three would-be thieves in MN who mistakenly pocket-dialed 911 while attempting a heist.

These examples aside, criminals are often very crafty. This means that banks have to be very shrewd to protect themselves from attack. It's true in a physical sense but especially in the virtual world where cybercrime is a growing problem.

Banks should expect to see more attention being placed on cybersecurity in the months ahead as the problem grows and as regulators place ever more emphasis on the enterprise risk it creates for banks. Banks need to find actionable ways to prevent cyber breaches before they happen and respond quickly when this cannot be avoided.

The statistics are sobering. In 2014, there were 7,945 new technology security vulnerabilities identified. That is 22 new vulnerabilities a day or nearly 1 per hour according to a recent white paper from NopSec. Meanwhile, 78% of all compromised records were the result of hacking in 2014, according to the same study. While these figures are not specific to the banking industry, they drive home the message of just what's at stake for banks in the war against cybercrime.

A good way to begin is to start thinking like a hacker. Before a bank can devise solutions, an understanding of how criminals are likely to take aim is necessary. This means, for instance, identifying possible exploits and paying special attention to back door entry points. It also means setting priorities. A system may be considered vulnerable but then ignored if there's no business-sensitive data. Remediation may not be at the top of the list for that particular system, but if it offers an entry into other systems, the danger can be significant.

When it comes to thinking like a hacker, we also suggest enlisting the help of experts. Think of it as another form of business insurance, because hackers typically are opportunity seekers and are likely to move on if a system is difficult to crack.

Banks should pay special attention to the vulnerabilities of third-party vendors, as this has become an area of regulatory focus. The New York State Department of Financial Services recently released a report that found that nearly 33% of banks polled do not require their third-party vendors to notify them in the event of an information security breach or other cyber security breach. Further, less than 50% of the banks surveyed conduct an on-site assessment of their third-party vendors and 20% do not require vendors to disclose their minimum information security requirements. Moreover, only 33% of banks require information security requirements to be extended to subcontractors of third-party vendors. Since banks are only as strong as their weakest link, if it's third-party relationships, then this is an area demanding more attention.

Statistics also show that it takes a hacker around a week to exploit security vulnerabilities. Banks that don't take this seriously risk getting caught in a web of their own undoing. No bank wants to make the list of bumbling criminals like the ones above, so take steps to be sure your bank is prepared.

Economy & Rates

Yesterday

Treasury yields rose 4bps as a stronger-than-expected core consumer prices revived talks of inflation reaching the Fed's 2% target.

Today

Yields are down 1bp ahead of a full schedule of releases, including Case-Shiller and Durable Goods.

Rates As Of: 05/26/2015 11:02AM (PDT)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.01	0.00	0.00

6M	0.07	0.00	0.00
1Y	0.21	0.00	0.00
2Y	0.61	0.00	0.00
5Y	1.53	0.00	0.00
10Y	2.14	0.00	0.00
30Y	2.89	0.00	0.00

FF Market	**FF Target**	**Fed Disc**
0.00	0.25	0.00

Prime	**Unemployment**	**Oil**
3.25	0.00	$0

More Market Rates

Bank News

M&A Activity

1) Bank of Communications ($1.1T, China) will acquire 80% of Banco BBM ($1.1B, Brazil) for $173mm. China is Brazil's largest trading partner.

Yellen Speaks

The 2 goals of monetary policy of the Fed are -maximum employment and price stability (managing inflation/deflation). A few notable comments from a speech by Fed Chair Yellen include: "the unemployment rate has come down steadily"; "the labor market is approaching its full strength", however "in my judgment we are not there yet"; "inflation remains below the Fed's stated objective"; the FOMC believes "inflation will move up" as "the economy strengthens further and as other temporary factors weighing on inflation recede"; expect GDP of around 2.50% and the unemployment rate to move down near 5.0% by year-end so "I think it will be appropriate at some point this year to take the initial step to raise the federal funds rate target and begin the process of normalizing monetary policy". At this point market investors are taking this to mean the first rate hike will be at either the Sep or Dec meetings, but we will continue to monitor and report back.

Branch Activity

1) Nicolet National Bank ($1.2B, WI) will sell 2 WI branches to Unity Bank ($95mm, WI) for an undisclosed sum. Unity gets about $38mm in deposits and $13mm in loans.

Board Oversight

A Deloitte survey of global risk managers finds: 85% say their board of directors spends more time on oversight of risk than 2Ys ago.

Multifamily Risk

CoStar Group reports 82% of the 370,000 multifamily rental units completed over the past 2Ys (ended 2014) were in the "luxury" category (rents in the top 20% of the market) and have been as high as 95% in some markets. Bankers should take note and be cognizant of the building risk in the higher end of the market.