A Not So Comical Menace

by Steve Brown

Dennis Mitchell, aka Dennis the Menace, has been entertaining comic strip fans with his various antics for more than 60Ys. The blond-haired, freckle-faced boy with a sizeable cowlick has a knack for finding trouble, especially when it comes to annoying his cantankerous neighbor Mr. Wilson. Dennis the Menace, whose immense popularity spawned a live-action TV show and two movies over the years, has mellowed somewhat from his initial portrayal as an aggressive trouble-maker. He's still a mischievous 5-year-old, but contrary to what his nickname suggests, he does not intend to cause real harm.

In banking, however, there is nothing comical about the kinds of menace former employees can intentionally or unintentionally inflict on your bank. Accordingly, it's particularly important for community banks to implement strict policies to protect sensitive data when people leave. Even in cases when a separation is amicable, banks must take necessary precautions so that data doesn't inadvertently leave the organization.

To see how big an issue this really is, we discuss Intermedia's 2014 SMB Rogue Access Study that explores the security threat companies face when workers leave. While the findings of this particular study are not specific to banks, they should nonetheless resonate with everyone in our industry.

The study found 89% of those surveyed walked away with their passwords, retaining access to such key systems as Salesforce (with customer lists), PayPal (to do ACH), email (to monitor company comings and goings) and other sensitive corporate apps after they were no longer working at the company. If that's not eye-opening enough, here are some more troubling statistics: 45% retained access to confidential or highly confidential data, 49% logged into ex-employer accounts after leaving the company and 68% admitted to storing work files in personal cloud storage services.

Soon after Intermedia's report came out, the FBI issued a warning that insider threat poses significant risks to business networks and proprietary information. Stolen trade secrets, lost data, regulatory compliance failures, data breaches and deliberate sabotage are a few examples of the malfeasance that companies are battling. Further, the FBI said a review of its recent cyber investigations revealed victim businesses incur significant costs ranging from $5K to $3mm due to cyber incidents involving disgruntled or former employees.

To prevent potential problems, banks must implement rigorous data access guidelines to guard against data leakage. It is important to regularly review employee access points and to terminate any accounts that aren't needed for workers to perform their daily tasks. Banks also need to be vigilant about revoking access to systems once someone is no longer employed. The same also goes for contractors, who may come and go even more often than full-time staffers. Finally, always make sure that outside companies you work with know when employees or contractors leave so they too can terminate access.

In addition to these steps, the FBI also recommends that companies change administrative passwords to servers and networks when IT personnel leave. They also warn banks to avoid using shared

usernames and passwords for remote desktop protocols and to avoid using the same login and password for multiple platforms, servers or networks.

As an industry, banks have increasingly sought to raise our defenses against unknown hackers, but we've got more work to do when it comes to safeguarding ourselves from the people we know. Erecting proper fences will help protect our backyards from intentional or unintentional menaces against those who may wreak havoc with our data.

BANK NEWS

M&A

Alerus Financial ($1.5B, ND) will acquire Interactive Retirement Systems (MN) for an undisclosed sum. The move boosts retirement plan assets under administration to over $17B with 278k participants and expands the company's push into the recordkeeping, consulting and administration business for retirement plans.

Bank Size

SNL Financial crunched the data and found the top 4 largest US banks and thrifts by total assets in order as of Q3 were JPMorgan ($2.5T), Bank of America ($2.1T), Citigroup ($1.9T) and Wells Fargo ($1.6T). This group adds up to a whopping $8.2T. Also of interest but well behind this pack of behemoths, the rest of the top 10 list are: US Bank ($391B), Bank of New York Mellon ($386B), PNC Financial ($334B), Capital One ($300B), HSBC North America ($280B) and State Street ($275B). This group adds up to about $2.0T. Finally, banks ranked 11 to 20 add up to $1.6T and include: TD, BB&T, SunTrust, American Express, Ally, Charles Schwab, M&T, Fifth Third, Citizens Financial and USAA.

FDIC Budget

The FDIC approved a $2.3B budget for 2015 (down 3.0%) with total staffing of 6,875 (which represents a 4.5% reduction vs. 2014).

Mortgage Fraud

LexisNexis released its annual mortgage fraud report for 2014, finding the worst states for reported mortgage fraud during 2013 in order were FL, NV, NJ, AZ, IL, NY, UT, GA, MD and CA. Meanwhile, the worst MSAs nationwide were Miami-Fort Lauderdale-Pompano Beach, FL; Chicago-Joliet-Naperville, IL-IN-WI; and New York-Northern New Jersey-Long Island, NY-NJ-PA.

Easier Lending

The OCC released its annual report on the banking industry and said US banks have been gradually easing their loan underwriting standards, similar to what took place before the economic crisis occurred.