Internal Security Threat

by Steve Brown

You probably saw the story about how researchers at UCSD analyzed the molecules left behind on a cell phone and found out some interesting things about the user. In it, the researchers were able to determine things such as whether the owner was male or female, drinks coffee, eats spicy food, wears high end cosmetics or sunscreen, and is being treated for depression. Some hailed this as a way to help solve crimes where fingerprints are not available, leverage when doing environmental exposure studies, or perhaps even help with patient compliance. Speaking of compliance, today we focus on employee compliance of a slightly different nature in banking.

Banks diligently protect against outside risks that could threaten business and cause havoc. But, it is also important to keep an eye on security risks coming from the inside as well.

We say this because breaches occur all the time it seems and insiders are often involved. Consider research by Kroll that found 81% of cases at companies where fraud had occurred had at least 1 insider involved. Meanwhile, an updated study by Verizon found 77% of internal breaches were deemed to be from employees vs. 11% from external actors. Finally, research by Carnegie Mellon around insider fraud in the financial services sector found that cases, where the role of insiders who committed a fraud was known, were about evenly split between managers or supervisors (51%) and those who did not hold supervisory positions (49%).

Clearly fraud remains an issue and insiders are a key area of concern for banks. After all, the threat from an insider doesn't have to be a malicious one. There are plenty of good-hearted employees that can fumble your security goals. Most employees know not to open e-mail attachments from people they don't know, and to avoid suspicious links in e-mails, websites, and online advertisements. However, as hackers get smarter, not all employees may know what to do or what to look for. Ongoing education programs are critical to protect the bank.

Another area bank security teams can focus on is data protection. Here, research by Ponemon finds 62% of employees say they have access to much more data than they need to in order to do their job. Further, less than 30% of companies say they have a searchable record of what insiders do with data.

It is critical to limit employee access to company information and supply on an as-needed basis. One way to do this is through a data audit to determine what sort of data you have, where it resides, how it is protected and who can access it. Then you can determine whether you have enough controls.

Finally, consider research by SailPoint that finds 27% of US employees are willing to sell their passwords to someone else and about 44% of those would do so for less than $1,000. Even worse, about 65% said they used a single password among all of their work applications and 33% actively share credentials with other employees. These are huge holes that can open your bank up to insider and cyber risks, so take steps now to close them.

Many community banks we know do a great job in protecting their data and customers, but more can always be done. After all, the bad actors are constantly probing and testing things, as they modify their attacks in order to penetrate banks. The key is to verify that you have layered security throughout the bank and that you constantly test to identify potential areas of weakness. That will allow your bank to tighten things up over time. In the meantime, maybe swabbing phones will become the new thing, as bankers seek to better understand even more about the comings & goings of employees using biometric-related methods.

BANK NEWS

M&A Activity

1) Southern Bank ($1.5B, MO) will acquire Capaha Bank, SB ($194mm, IL) for about $23.4mm in cash and stock and assume $3.8mm in debt for total consideration of about 1.40x adjusted capital. 2) MVB Bank ($1.5B, WV) will invest an undisclosed sum in bill pay startup BillGO, and its president and CEO will join the board.

Competition

Amazon has announced a new Visa card (in collaboration with JPMorgan) for its Prime members. The card offers 5% back on all Amazon purchases; 2% back at restaurants, drugstores and gas stations; and 1% back on all other purchases. There is no cap on rewards earned, no expiration of rewards, no foreign transaction fees for cross-border travel and shopping, no annual fee for fraud liability, travel and purchase protection benefits and 24/7 concierge service through Visa Signature.

Spooky Survey

A survey by Accenture finds 31% of people would consider switching their accounts to Google, Amazon or Facebook if those companies offered banking services (29% would switch for insurance).

USA Credit

Rating agency Fitch said President-elect Trump's plans to cut taxes could lead to a downgrade on our AAA credit rating over the medium term. Fitch indicated the US already has the highest level of government debt of any AAA country.

Marketplace Funding

Despite recent struggles in the marketplace lending sector, UK peer to peer business lending platform Funding Circle has raised $100mm.

Credit Cards

TransUnion projects the average credit card balance per consumer will reach $5,509 by the end of 2017 vs. 5,437 as of the end of this year.

Inadvertent Actors

IBM defines an inadvertent actor as "any attack or suspicious activity sourcing from an IP address inside a customer network that is allegedly being executed without the knowledge of the user."