Former Employees - Potential Risk

by Steve Brown

We found out recently about a scam involving certain food delivery companies and restaurants. It seems some food delivery companies said they offered food from restaurant X, but when ordered online an entirely different restaurant Z was actually cooking the food for the delivery firm. Obviously this situation means you need to be careful about what you order, from whom you order it and also who delivers it, to be sure you are indeed getting what you want.

There are lots of risky things in life to be sure and one that bankers don't always think about relates to previous employees. Depending on the position and how long the person has been there, this can lead to unintended consequences.

For instance, forgetting to block outgoing workers' computer system access can lead to problems, as can using the same password combinations internally too many times in a row. After all, these folks know your bank inside and out, so if they are seeking to cause issues they have a good way in perhaps.

For example, in April an engineering company co-owner admitted that he'd spent 2Ys accessing his former employer's servers after he left the company. He had started a competing firm and the information he got by using his old login let him download digitally rendered engineering schematics and more than 100 documents containing project proposals and budgetary documents. He also gained access to emails containing information about his prior firm's marketing plans, project proposals, company fee structures and the rotating account credentials for the company's internal document-sharing system, the Justice Department says.

Planning ahead and educating your customers to such risks can help avoid similar messes. Maintain a list of employees and the access and devices they have. Then, when someone changes jobs within the organization, review and adjust that person's access. When someone leaves, ensure that system access ends when the job does. Be sure to retrieve or remotely wipe any remote or mobile devices as well. Finally, reset all devices for those who are changing roles within the bank and suggest the same for your customers.

As an added precaution, be sure to keep your eyes open for shared, loaned, or sold access credentials. Even innocent sharing can cause problems. Edward Snowden, for example, got access to information he later leaked because someone with more official access typed that code into his computer. By creating a baseline of how normal behavior looks, you can get a sense of when someone is using your system inappropriately.

Regular password changes, as well as encouraging employees to use long, complicated passwords that aren't easily remembered can also help block credential reuse. For accounts containing sensitive information, be sure to use two-factor authentication solutions to make it even more difficult.

Your master list should include information about the physical access your employees have, too. Retrieve keys to your office or company cars for example. For extra safety, rekey your door locks and change your alarm system's PIN code when a worker leaves. Make sure that person's fingerprint or badge code no longer unlocks your office door. Finally, inform the staff at your reception desk when someone leaves the company that they shouldn't be allowed back in without an escort.

This may all sound a bit alarming, but intellectual property theft is rampant and people do bad things to try and get ahead so you have to be extra careful. While most departing employees mean you no harm, some do and willingly will take steps to hurt your company so be prepared.

BANK NEWS

M&A Activity

1) Atlantic Bay Mortgage Group (VA) will acquire Virginia Community Bank ($238mm, VA) for an undisclosed sum in stock (100%). 2) First Financial Bank ($8.5B, OH) will acquire MainSource Bank ($4.0B, IN) for about $1.0B in stock (100%) or about 2.72x tangible book. 3) Valley National Bank ($23.2B, NJ) will acquire USAmeriBank ($4.4B, FL) for about $816mm in stock (100%) or about 2.38x tangible book.

CFPB Arbitration

The House voted to overturn the CFPB's arbitration rule under the Congressional Review Act that gives Congress the ability to reject new federal regulations within 60 legislative days of publication in the Federal Register. The Senate has introduced a similar measure.

SEC Crackdown

The SEC said rules meant for stock sales also apply to companies that raise money using sales of digital coins and they are subject to federal oversight. Startups have taken this route recently, with more than 70 companies so far this year raising about $1B. The SEC ruled that these coins are the functional equivalent to shares of stock as they offer investors the potential for a return on their investment.

Affluent Opportunit

A JD Power banking study finds: 64% of millennial customers with incomes above $80,000 currently have mobile payment services linked to their accounts.

Credit Search

A TD Bank survey of small businesses with <$1mm in annual revenue finds 11% say they don't know how to seek credit when they are ready to do so.

SAVE $100 ON CHICAGO ROAD TOUR REGISTRATION THROUGH 7/31!

Need to know more on CECL? Or cybersecurity? Join us for our Executive Management Road Tour in Chicago from September 25-26. Register by July 31st & save $100!