Mobile Banking App is HERE!

UNION BANK

February 2022

Insider Threats are a Quiet Risk in your System

Member FDIC

EQUAL HOUSING LENDER

The Ripple Effects that Extend Outward from a Breach

According to the Verizon 2020 Data Breach report, insiders account for 22% of all security incidents. In addition, the costs of insider breaches – caused either by human error or bad actors are rising, with Ponemon finding a 47% increase in cost over the past two years. As an organization, it makes sense to trust internal users and their access, but recent hacks are showing that internal users are a threat to systems too.

What is an insider threat?

An Insider Threat is the threat of sensitive, critical assets getting compromised, stolen, or mismanaged by internal users. It can be caused by insiders with malicious intent or can be caused by accident. From termination gap threats — where an internal user is terminated and still has time to use their access for harm — to basic human error, to even account abuse or access creep, the threat comes in many forms and any one of them could lead to a costly, devastating breach.

The Consequences Of Insider Threats

No matter the root cause, the result is the same: reputation damage, fines, compliance issues, and of course the ripple effects that extend outward from a breach.

The biggest risk is, of course, the exposure of sensitive information. It could be an employee maliciously stealing valuable assets for another party, or an employee who has too much privileged access and falls for a phishing scam, or even simple human error that accidentally exposes assets. No matter the root cause, the result is the same: reputation damage, fines, compliance issues, and of course the ripple effects that extend outward from a breach.

For example, in 2020, a terminated employee of a medical device packaging company decided to act maliciously. They gave themselves administration privileges and deleted over 100,000 records, causing massive delays in medical device delivery (during the height of the pandemic).

How To Mitigate These Threats

While any access carries with it an inherent threat, there's a few ways to make sure insiders aren't the cause of your organization's next data breach.

Continued on Page 2

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

Best practices include:

- **Zero Trust Network Access.** ZTNA specifically limits which sensitive systems a user can access and is implemented with various security controls, such as multi-factor authentication, least privileged access, access and employment verification and attestation, credential vaulting and detailed auditing. It removes all trust from every user, therefore removing the threat of an internal attack.

- **User Access Reviews.** A user access review is a periodic inventory of access rights to certain networks and systems, and the users who have access permissions into those networks and systems. Reviewing internal access is the simplest way to make sure that no user 1. Has access they shouldn't and 2. Isn't accessing assets they don't need to be accessing. It can catch a potential breach before it even occurs.

- **Access Control.** The goal of access control is to create friction between a user and their access and stop any unauthorized access that could lead to a security or privacy breach. Whether it's through time-based access schedule, manual access approvals, or access notifications, access control can stop a user from accessing an asset they shouldn't, therefore mitigating the insider threat.

These 3 trends will be competitive dealbreakers in 2022

If the first year of COVID-19 felt like a fast and turbulent roller-coaster ride for community banks, the second had many in the industry perplexed and wondering if the wild ride was finally over and if it's OK to settle down and get back to normal.

But as we found out in 2021, that old normal — going back to doing business the way we did before the pandemic — is never coming back.
A steady stream of new variants — from delta, lambda and epsilon to the fast-spreading omicron — have made a mockery of many return-to-office plans. But they've only accelerated change that was already on its way: customers' increasing need for access to fast and convenient banking service from any touchpoint.

With almost two years of the 'new normal' now behind us, what does the future of community banks look like? What are the key challenges and trends that the banking community will face in the coming year as they strive to compete and earn the loyalty of customers?

Three trends that grew steadily over the past two years have shown for good reason that they're not going anywhere. Here's why they'll be ever-critical in 2022, and how community banks can implement them to position themselves for success in the coming year:

1. Digital and mobile banking will be expected to cover an even larger majority of transactions in 2022
Completing many if not most transactions and requests digitally — that's become a competitive prerequisite for community banks in 2021. The line between what customers expect from their bank and what they receive from digital experience trailblazers like Amazon and Apple has rapidly vanished since the pandemic.

With today's digital-first consumers more comfortable than ever buying banking products from emerging neobanks and fintech services, traditional financial institutions face unprecedented competition to earn new customers and grow lifetime value.

Digital laggards, even at the community level, can't afford to delay investing in capabilities that are not in step with both market evolution and customer expectations. That means banking processes that can be handled digitally absolutely must be available to customers and easy to use.

Community banks must eliminate legacy processes that rely on customers searching for and fetching PDF documents from their email inbox, or printing those crowded documents and scanning or faxing them back. That kickstarts high-effort customer journeys that generate paperwork and admin overhead for banking employees, delaying and frustrating everyone involved.

2. It's time to call time on overdraft fees
For decades, overdraft and NSF fees on checking accounts and lines of credit have been an infuriating and costly inconvenience for customers. But over the past couple of years, the profits banks have gained by collecting overdraft fees are becoming a dealbreaker for customers and a reputational nightmare, attracting the ire and scrutiny of the U.S. Senate.

Between national, community and neobanks, it's never been easier for customers to virtually walk their business elsewhere. For community banks, supporting their customers by doing away with overdraft fees will be key as they compete for their loyalty against larger and digital-first counterparts.

3. Branches will continue to close — but also adapt to be where their customers are
In the face of a new and rapidly spreading variant, many community banks will need to close more branch locations to fight the spread and protect the health and safety of their staff. But community banks can apply lessons from the past two years to adapt both their digital and physical presence.

By bringing in an innovative partner, community banks can get the most out of their existing systems and operations. A proven technology partner can analyze a community bank's current processes and how digitizing them can eliminate barriers, make data agile and accessible in a remote and hybrid environment, and cut away operational costs and overhead.

Adapting your physical footprint can prove to be a major competitive differentiator for community banks, enabling them to be where their customers are and build meaningful and profitable long-term relationships.

Source: Isa Jones, January 14, 2022, BankInfoSecurity.com
Zvoki Ben Ishay, CEO Lightico, January 20, 2022, Bankbeat.biz

One Simple Step to Securing Your Accounts

Overview

Does it seem like cyber criminals have a magic wand for getting into your email or bank accounts and there's nothing you can do to stop them? Wouldn't it be great if there was one single step you could take that would help protect your from cyber criminals and let you securely make the most of technology? While no sole step will stop all cyber criminals, one of the most important steps you can take is to enable something called two-factor authentication (sometimes called 2FA, two-step verification, or multi-factor authentication) on your most important accounts.

The problem with passwords

When it comes to protecting your accounts, you are most likely already using some type of password. There are several ways to authenticate yourself into an account: something you have, something you know, something you are, somewhere you are. When you employ more than one method of authentication, you are adding an additional layer of protection from cyber criminals – even if they crack one method, they'd still need to bypass the additional factor(s) to access your account. Passwords prove who you are based on something you know. The danger with passwords is that they are a single point of failure. If a cybercriminal can guess or compromise your password, they can gain access to your most important accounts. In addition, cyber criminals are developing faster and better techniques at guessing, compromising, or bypassing passwords. Fortunately, you can fight back with two-factor authentication.

Two-factor authentication

Adding two-factor authentication is a far more secure solution than relying on just passwords alone. It works by requiring not one but two different methods to authenticate yourself. This way if your password is compromised, your account is still protected. One example is your ATM card; when you withdraw money from an ATM machine, you are actually using a form of two-factor authentication. To access your money, you'll need two things: your ATM card (something you have) and your PIN number (something you know). If you lose your ATM card, anyone who finds your card cannot withdraw your money as they do not know your PIN. The same is true if they only have your PIN and not the card. An attacker must have both to compromise your ATM account. The concept is similar for two-factor authentication; you have two layers of security.

Using Two-factor authentication online

Two-factor authentication is something you set up individually for each of your accounts. It is actually quite simple: you usually need to do nothing more than syncing your mobile phone with your account. That way when you need to log into your account, not only do you log in with your account username and password, but you also use a unique one-time code you get from your phone. The idea is the combination of both your password and unique code are required to log in. Usually, this unique code will be sent via a text message to your mobile device or email. Your phone may also have a mobile app (such as Google or Microsoft Authenticator app) that will generate the unique code for you. When possible, mobile apps are considered the most secure option for obtaining your unique code.

What makes this so simple is that you usually only have to do this once from whatever computer or device you are using to log in. Once the website or your account recognizes your device, moving forward you often only need your password to login. Any time you try (or someone else tries) to log in with your account but from a different computer or device, they will have to use two-factor authentication again. This means if a cybercriminal gains your password, they still can't access your account as they can't access the unique code.

Remember, two-factor authentication is usually not enabled by default, so you'll have to enable it yourself for each of your most important accounts, such as banking, investments, retirement, or personal email. While this may seem like more work at first, once it's set up it's very easy to use.

Source: Lysandra Capella, September 1, 2021 SANS OUCH! Newsletter