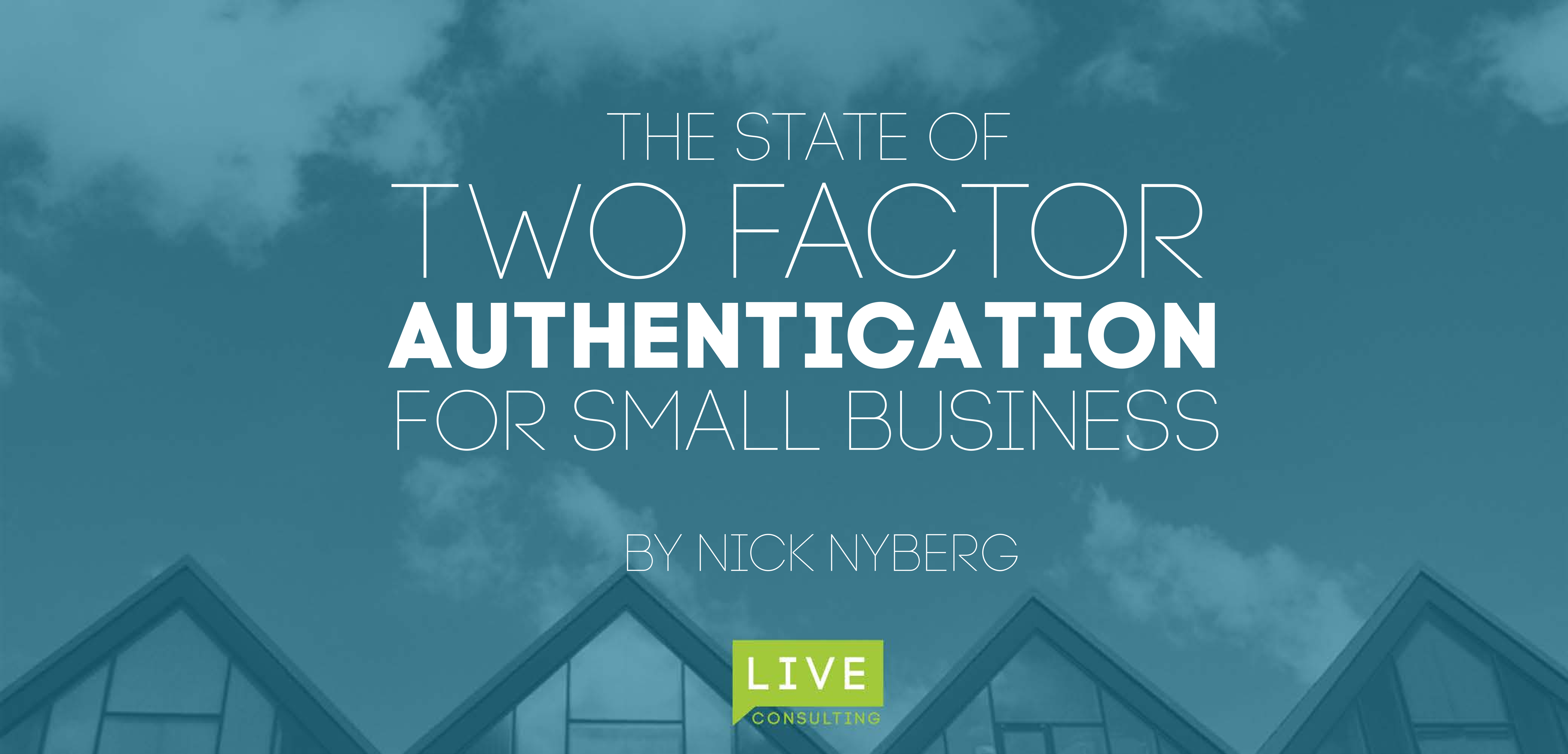


THE STATE OF TWO FACTOR **AUTHENTICATION** FOR SMALL BUSINESS

BY NICK NYBERG

LIVE
CONSULTING

TABLE OF CONTENTS

LIVE
CONSULTING

INTRO

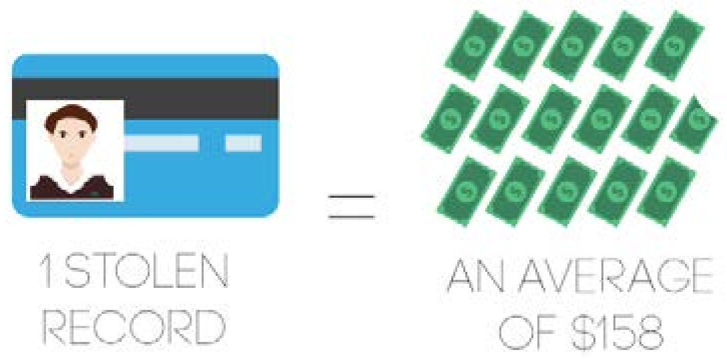
The threat to both enterprise and small business data has never been greater. The expanding use of cloud-based systems, a larger number of remote employees, and an increasing amount of consumer devices that are used to access work applications all increase the opportunities for malicious and criminal attacks, system glitches, and human error.

Every mistake in IT security creates a risk element that nefarious agents can use, and these gaps are being exploited at an ever-increasing rate according to the latest studies.

The average cost of each lost or stolen record that contains sensitive or confidential information costs a business $158, according to IBM's 2016 Cost of Data Breach Study . Overall, the average breach will cost even a small or mid-sized business about $4 million, which is nearly a 30% increase from 2013.
Most breaches are caused specifically and intentionally by individuals or organizations looking to do financial harm to a company, whether that's taking down a service, reducing consumer trust, stealing company secrets, or stealing records in order to use them to defraud customers.

Each client lost due to a breach only compounds the overall monetary loss that a company will experience.
Organizations just like yours are realizing that it is taking longer to detect and resolve data breaches and that costs rise dramatically for every day before a breach is not caught. The methods that we use to look for and stop breaches are also becoming more expensive because the cloud systems we employ are increasing in complexity.

To address these concerns, many businesses are starting to look to new security protocols such as two-factor authentication, or 2FA. Two-factor authentication provides an additional layer of security to any login or access point by requiring an additional piece of information beyond the username and password.



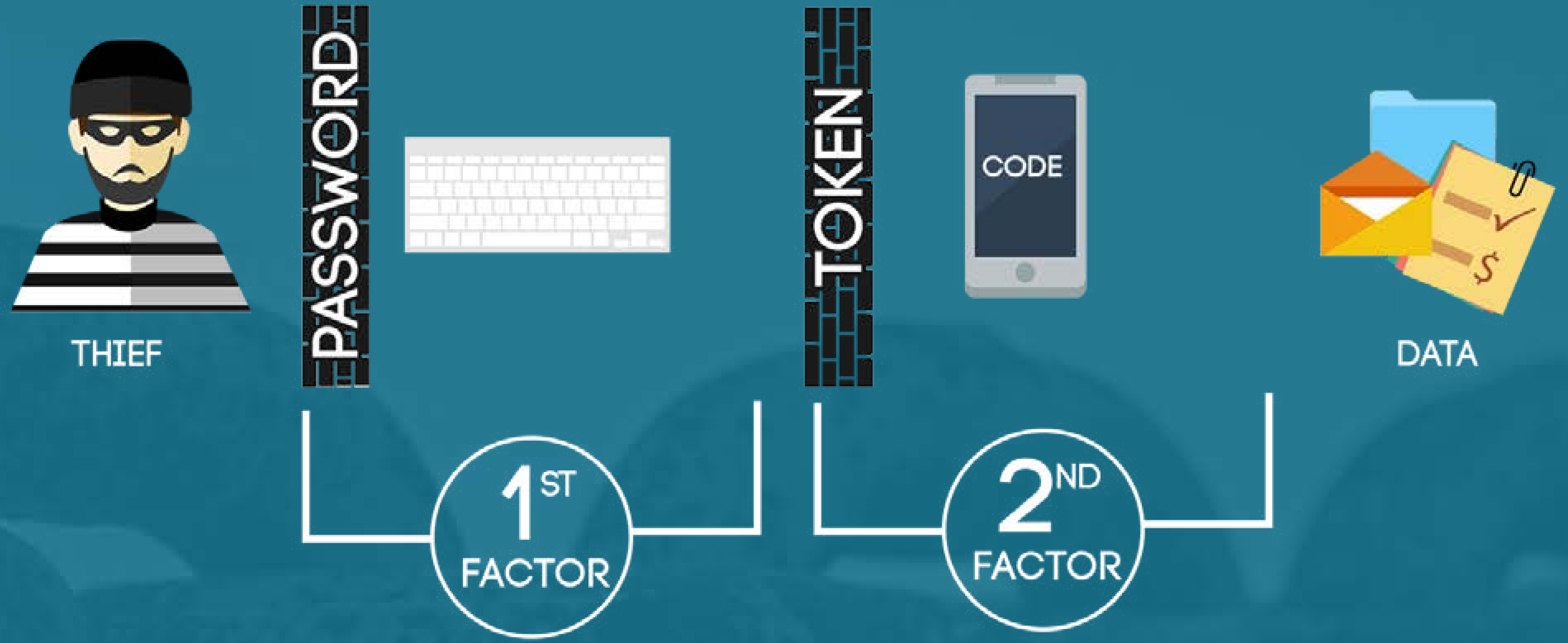
COSTING THE AVERAGE SMALL BUSINESS

$4,000,000

These secondary factors can include a device someone has in their possession/ information that is sent directly to a device only they have access to, the information they know inherently, or information about who they are, such as biometrics.

Security firms are presenting 2FA as one of the top ways to protect a network against remote attacks and exploitation because many of these authentication tokens have a physical aspect that limits access. It gives basic protection against brute force attacks and other simple hacking techniques, but has not necessarily proven itself against more complex infiltration attempts.
This report aims to provide you with a comprehensive look at 2FA, its standard deployments, benefits and weaknesses in its protections, adoption likelihood, and likely future developments.

WHAT IS TWO FACTOR AUTHENTICATION?

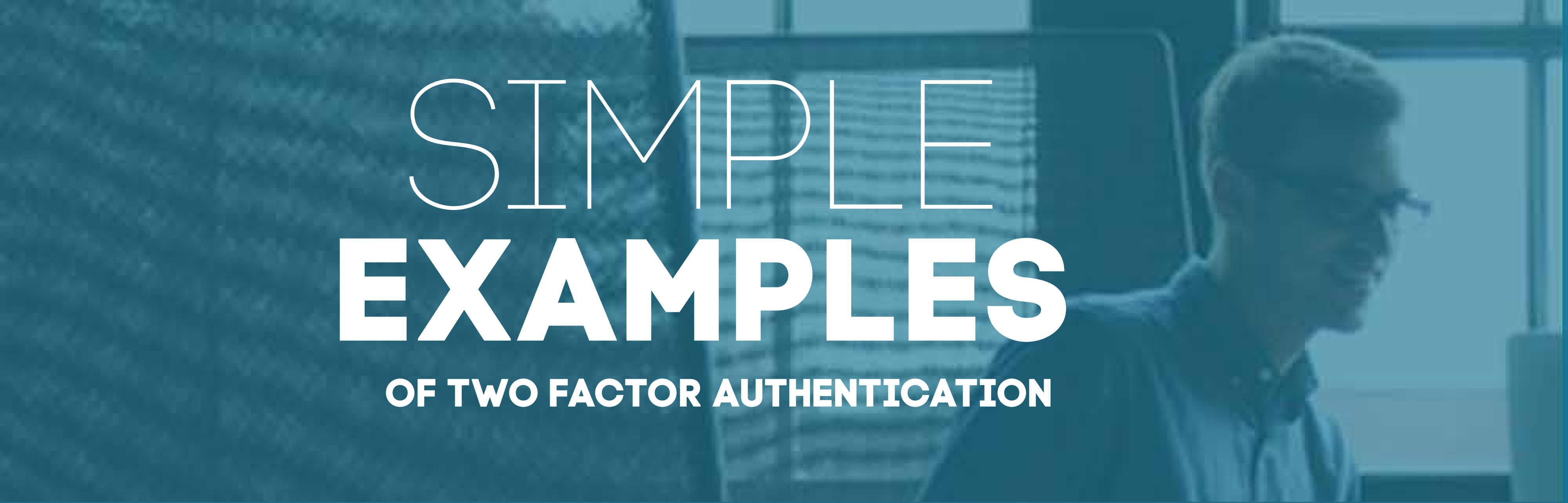


Two-factor authentication, often listed as 2FA or TFA, is a security practice that uses two different pieces of information to verify the identity of a user. Typically, at least one of the two components is something that should be inseparable from the user, such as information or an assigned device like a keycard, or a mobile phone.

The premise of 2FA is that it will be extremely unlikely that someone trying to assume the identity or credentials of another person will be able to secure both components. The system hopes to keep the unauthorized user – let's call them an infiltrator for clarity – at bay because it will lockout access when either of the components is incorrect or not present.

Adopting 2FA has allowed service providers to take proactive steps to reducing identity theft, limit the success of phishing attempts, and increase the likelihood of stopping brute force intrusions into their systems.

The movies like to show us that 2FA pairs voice recognition with fingerprint or retinal scans, but the mode of thought and the application of 2FA is much older.



SIMPLE EXAMPLES

OF TWO FACTOR AUTHENTICATION

One of the earliest cases of machine-based two-factor authentication we came across comes from London in 1967. The British bank Barclays installed the very first ATM which paired a punch card with a PIN (personal identification number) to allow people to access their accounts.

While the ATM today you use has a couple of significant differences – the first didn't have a usage fee but it did use checks that had the radioactive isotope carbon 14 – much of the underlying process is the same. These two factors combined internal knowledge (PIN) with a token (the punch card).

As the digital age has progressed, companies are turning to the smartphone to be the receptacle for the token. You've probably seen this with your email account. Enabling 2FA in Gmail , for example, means that you'll have to sign in to the account with your username and password, then receive a code on your phone via text, phone call, or its mobile app.

Facebook also has a 2FA option that sends a code to your mobile device. Both it and Gmail will request a verification code each time you log into a computer the service does not recognize or if you select an option for the service to not "remember" that device.

THE MANY DIFFERENT WAYS TO COUNT TWO

Companies are currently using a wide range of 2FA methods. There has been a recent push toward using a mobile device to help 2FA because of the prevalence of consumer device and ease of proximity. They also meet a desired principal: the out-of-bond authentication. This is when your primary password and the second factor use two different delivery mechanisms.

Consider inputting a password on your PC and then needing a smartphone to receive a text message for a code. Someone trying to break into the account would need access to both the PC and the smartphone, which negates some risk, especially if the intrusion is from a remote attacker.

KNOWLEDGE

This secondary factor focuses on something that's also in the brain of the user. Beyond a password, this is often seen as answers to questions like "What street did you grow up on?"

The latest iterations of these concerns have moved away from common questions that are easy to look up to complex or even unique questions, custom to each user. Some in the financial sector, especially banks and loan programs, have asked users to select a photo during sign-up and then use selecting the photo during log-in as a simple 2FA option.

This option is easy to implement and can be rolled-out to all of your users or employees quickly. Another nice element is that they can be quickly changed in the event of a breach that exposes a database.

A downside on all knowledge-based units is that they can be retrieved easily through social engineering. Both the customer and the service can be targets of social engineering, making these keys very risky when you consider that those two avenues represent about 55% of all data breaches .

BIOMETRICS

Biometrics are a common 2FA method that uses something usually inherent to the individual user. These can include fingerprint scans, retinal scans, voice recognition, cardiac rhythm scans, and even the recognition of ambient background noise. Because of the uniqueness of each individual, these are some of the more secure 2FA when they're done properly.

British banks have started to use fingerprint readers as part of their customer logins, and such scans can also be used to unlock smartphones on almost all platforms. MasterCard is also working on a platform that will replace passwords on smartphones with selfies.

While security seems strong, there are a couple concerns that may slow a larger rollout. The first problem is that equipment isn't always able to properly scan a person to provide the right match.

As equipment ages, scanners and sensors become imperfect. In this case, that can mean either locking out a customer or allowing someone who has a similar face or fingerprint to the user to inappropriately access the account. Think of a time where you've been at an ATM and needed to swipe your card multiple times. Time can wear down the system's scanner. Now imagine applying that to your face, and trying to get recognition to work when you have a new haircut or have tried out a makeup technique like contouring, which aims to make the face look thinner. Devices like ATMs that are out in the open are also often exposed to a significant amount of dust and dirt, which could interfere with a proper scan.

UNCONNECTED HARDWARE TOKENS

There are many new hardware tokens that generate codes you input after a password in order to access a system. When these devices are not plugged into your computer or other equipment, they're considered unconnected or disconnected tokens. Typically, these will be a self-contained unit that displays your auto-generated authentication data.

The good news about these types of tokens is that intrusion can be difficult. The downside to these tokens is that they can be lost or stolen easily. They're also often kept near the main access device – such as being kept on a keychain that's connected to a laptop bag or being located in one of the bag's pockets. Theft makes up about 17% of all data breach beginnings and lost or improperly disposed of devices account for another 6%, creating a notable risk, according to a report from BakerHostetler .

Also, tokens can be expensive to replace and IT tickets can take longer or be more complex when the user needs access before they can receive a replacement token.

CONNECTED HARDWARE TOKENS

Like the unconnected tokens, these are pieces of hardware that you need to complete 2FA. The main difference is that this token needs to be connected to a computer and automatically transmits data to serve as the second factor.

Among the most common is a USB stick though other options include card readers and wireless tags. RFID readers are a growing segment of authentication when a single workstation has multiple users. The station can have an RFID reader installed and then users are verified when their RFID tag is presented along with a password. RFID tags can be very small and need no power source, so they can be inserted into employee equipment from hard hats and vests to ID cards.

Connected tokens have much the same dangers as unconnected hardware, with theft and loss being a significant source of risk and cost but also being more difficult because of the required connection. One new danger is that the units are sometimes hackable – such as cracking a USB and retrieving the data inside or using an advanced RFID reader to see what information is returned – which can increase the risk of specific theft or corporate espionage.

SMS CODES

Services that are tied to a cell phone or smartphone can text a passcode out using SMS protocols. This is common for banks, email accounts, and other consumer-facing controls. Whenever the 2FA service wants to verify a connection or request, it simply sends out a new SMS passcode and often the code is timed so it must be inputted within a few minutes.

Again, a lost or stolen device is the chief concern. The device's security is the main concern and main breach point. If a smartphone uses a fingerprint lock, then it is unlikely an infiltrator will be able to bypass that security and access the device.

If your company turns to SMS codes but allows a user to reset their password via email without any identification questions, then you may be at risk. The infiltrator can simply request credentials be reset and send to email – which is likely on the phone without further protection – then reset and use these plus the subsequent SMS code to access your service.

PUSH NOTIFICATIONS

Push notifications are essentially an SMS passcode in app form. Apps will send the notification specifically to the smartphone and if the phone is unlocked the device will display the code. It has much the same risk as SMS.

However, push notifications may be more secure because an app install is needed and notifications are hidden within an app, allowing more access or even a separate 2FA to be in place. The chief note is that the user will need to ensure that their notification settings do not display the notification content – and the app developer would need to do the same.

There's a risk that users may turn on notification display settings to give the notification in full because it would make their access much easier.

PHONE CALLS / CALL BACKS

Though not used too often, another system can be to physically call the user on a specific phone to ensure verification. This 2FA method has two distinct options:

1. The person receiving the call is told a code they need to input in order to gain access to a system.

2. The call recipient must provide a password or code to the caller in order for access to be granted.

Phone calls may be less secure than SMS or push notifications simply because most smartphones do not require the user to unlock the phone before accepting a call. That means physical access to the device – and not necessarily access to its data – is all that's required. That's a major risk of allowing the callback to reach smartphones if you're using option one.

In some instances, calls can be more secure if they are directed to a phone number that's tied to a specific location. If you implement this in the office, then you can have the call go to a specific desk or extension, meaning the user must be physically present in most cases.

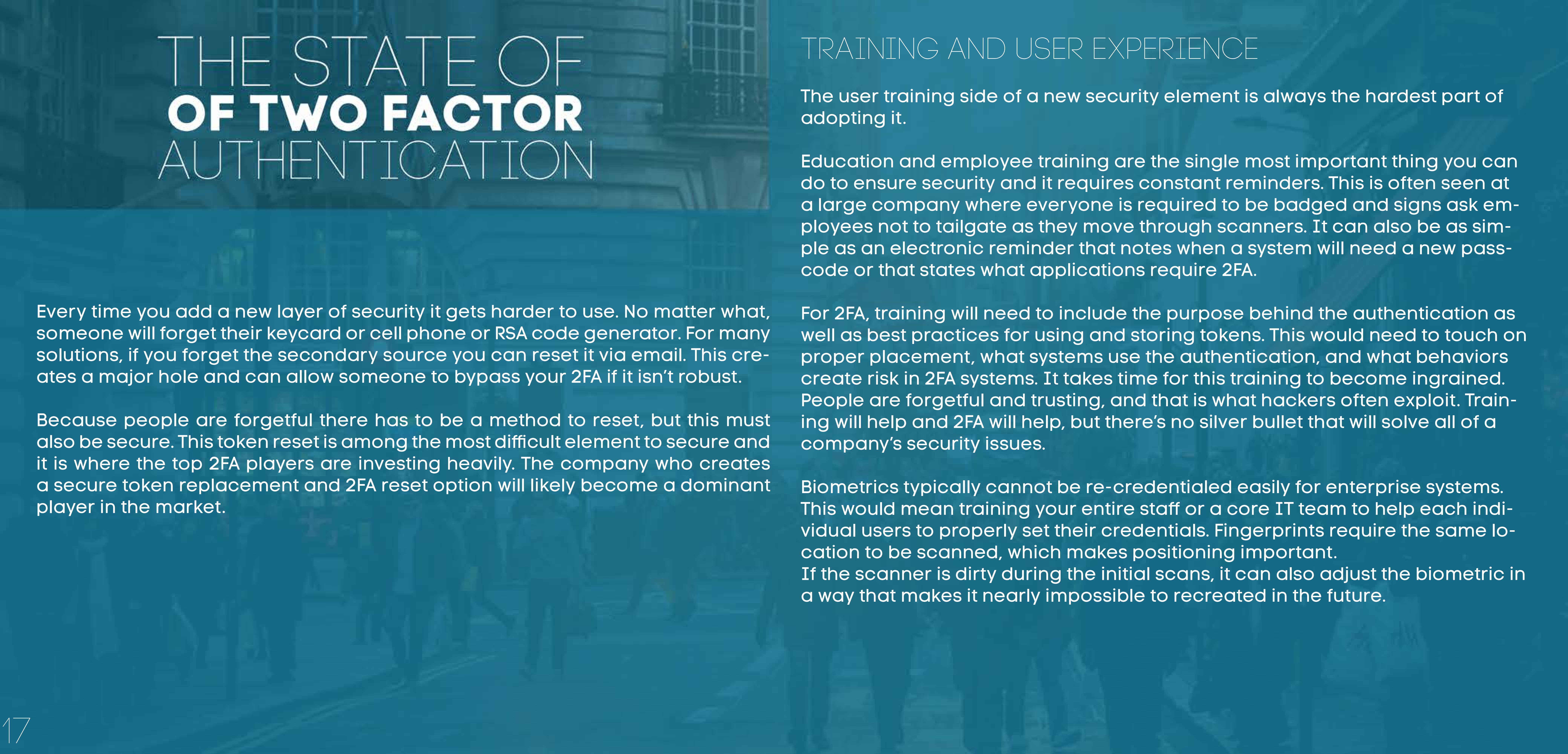
In virtually every scenario, the second option above is more secure. This 2FA relies on "knowledge" section listed above but merely specifies an unusual method of providing the knowledge token.

WEARABLES AND TOKENS

Wearable devices are the latest IoT craze and many companies are implementing them for uses related to health insurance and employee tracking via GPS. Smart watches and other personal devices are also being more accepted in the workplace because they can sync with a phone to support phone calls, SMS messaging, app notifications and more.

At this point, it is unclear how vulnerable these options are and that may not make them a proper method for many. While they do make receipt of a token easier in many scenarios, their display settings may cause some secure methods to be less secure simply because unlocking a device might not be required to see the 2FA token.

However, their current reliance on connection to a smartphone – meaning both access and needing to be in a close physical proximity – may mean that the risk won't be significant expect under very direct, threatening circumstances like internal corporate espionage.



THE STATE OF OF TWO FACTOR AUTHENTICATION

Every time you add a new layer of security it gets harder to use. No matter what, someone will forget their keycard or cell phone or RSA code generator. For many solutions, if you forget the secondary source you can reset it via email. This creates a major hole and can allow someone to bypass your 2FA if it isn't robust.

Because people are forgetful there has to be a method to reset, but this must also be secure. This token reset is among the most difficult element to secure and it is where the top 2FA players are investing heavily. The company who creates a secure token replacement and 2FA reset option will likely become a dominant player in the market.

TRAINING AND USER EXPERIENCE

The user training side of a new security element is always the hardest part of adopting it.

Education and employee training are the single most important thing you can do to ensure security and it requires constant reminders. This is often seen at a large company where everyone is required to be badged and signs ask employees not to tailgate as they move through scanners. It can also be as simple as an electronic reminder that notes when a system will need a new passcode or that states what applications require 2FA.

For 2FA, training will need to include the purpose behind the authentication as well as best practices for using and storing tokens. This would need to touch on proper placement, what systems use the authentication, and what behaviors create risk in 2FA systems. It takes time for this training to become ingrained. People are forgetful and trusting, and that is what hackers often exploit. Training will help and 2FA will help, but there's no silver bullet that will solve all of a company's security issues.

Biometrics typically cannot be re-credentialed easily for enterprise systems. This would mean training your entire staff or a core IT team to help each individual users to properly set their credentials. Fingerprints require the same location to be scanned, which makes positioning important.
If the scanner is dirty during the initial scans, it can also adjust the biometric in a way that makes it nearly impossible to recreated in the future.

COST AND 5 THINGS YOU CAN DO RIGHT AWAY

There's no clear 2FA winner, and most of the most popular solutions are designed for Fortune 500s. That means pricing hasn't come down yet, and it is unclear how soon overall pricing will decline. That puts many small businesses in a tough position.

Do you choose the expensive but full-featured system or a feature-limited platform that tends to have vulnerabilities – such as easy bypassing of the second factor? And, does your small business control everything you use or do you need to rely on other services that supply 2FA?

Those can be difficult questions, especially when you're trying to balance growth with security. Here are a few of our chief thoughts on how small businesses can make the most out of 2FA:

1. Stick with smartphones or tablets first because your staff or users are less likely to lose these. Also, according to 2FA brand Duo, the cost of tokens can approach more than $100 per user. Damage, malfunctions, loss, and theft mean absorbing that cost again in the near-term, while Duo also notes that the average lifespan for a token is three years.

2. Start off with an app. They can be safer than SMS because you have more control over who can log in, when 2FA tokens or notifications are sent, and you control the app's code so you have a chance to make changes based on usage or industry best practices.

3. Keep it simple at first, protecting your most vital systems. This gives you a chance to adjust to the increased time and money demands that crop up based on trouble tickets related to unauthorized access, lost tokens, and broken access points.

4. Turn to secondary systems that already offer 2FA. The good news is that there are utilities, payment options, email, communications, hosting, and much more. Here's our favorite site to check your options or see if the platform you want to use offers 2FA: https://twofactorauth.org/

5. Look to developers and vendors as soon as you can. Duo is a great place for small businesses to start, but your budget forecast should look for vendor support in the near term. No off-the-shelf solution is perfect for every situation or product, so you'll want a tailored option when it's affordable.

These suggestions will require you to have a BYOD plan in place or for you to supply devices to your employees initially. This is a smart path for most small businesses and it has a few major benefits that we'll get into in a following section looking at the evolution of "BYOT."

DOES 2FA **PROTECT YOU FROM** HACKERS?

Imagine the joy you feel when you come home and the smell of your favorite meal is wafting through the air. Like cartoons of old, we seem to float on air as we approach the dinner table, salivating like a hungry wolf.

That's the experience a hacker has when they realize a targeted system is only protected by a single password. It's a tantalizing treat that is quickly devoured, giving them access to your most important systems and data.
Two-factor authentication is also a bit like those old cartoons, except in the moment right before our wolfish hacker snatches a pie off of a windowsill, the 2FA rolling pin flashes to quickly bat them away. Try as they might, there's almost no getting past it.

Now, that's not to say that 2FA is bulletproof. There are ways for hackers to get around the security, often with social engineering tactics that help them retrieve a token or passcode from an unsuspecting – or poorly trained – customer service rep.

But in most cases, the hackers will need access to the physical token or will have to ferret out where cookies or tokens are placed on a device by the authentication mechanism. This can occur via phishing attacks, malware, or account recovery services.

2FA is becoming more secure as attempted breaches become more commonplace. The industry is learning how hackers are attempting to infiltrate the network and can begin to address those security gaps.
The most significant threat-point today is still the end-user because training and proper use remain a challenge.

BYOD AND MOBILE

TWO FACTOR AUTHENTICATION

For most 2FA experiences in our daily lives, the mobile device is the repository for the secondary token. It supports app notification and push messages, SMS messaging, email, phone calls, and much more. For customer-facing activities, it's an easy method to adding 2FA and making it that much harder for any illicit access to take place.

Internal systems, however, look at the personal smartphone with greater skepticism. The Bring-Your-Own-Device push varies in success by industry. For 2FA, we've seen minimal interest in BYOD on its own because of the cost it takes to lock down devices and platforms.

However, we think that it's just a matter of time before BYOD platforms enable more 2FA protocols. Unfortunately, it will likely take a major BYOD breach to force small and mid-sized businesses to adopt 2FA as a need to fix known security problems.

As business grow, they tend to start looking at BYOD as a more cost-effective solution to ensuring employees have proper cloud access. So, the industry will need to start focusing on the smartphone as the 2FA element of choice.
Adoption of BYOD does have a benefit: people tend to notice sooner when they've lost their phone or had it stolen. Most mobile platforms also have options for remote locking or even wiping of a phone when it's stolen, making the user able to render it inert sooner.

The future of mobile 2FA will include these systems as a method of learning how to block a user even on the network before they've been authenticated or as they start the authentication process. Not only does that protect your system against unauthorized access but it can notify the user immediately when any authorization attempt is made – giving the user the ability to flag an inappropriate login attempt and adding another layer of security.

TWO FACTOR AUTHENTICATION ADVANTAGES

The eventual reality of a BYOD program is that it can become a Bring Your Own Token where the smartphone or other device provides multiple authentication routes. Allowing users to not only carry their own personal token but determine the authentication method makes it more difficult for outside users to nefariously access your network.

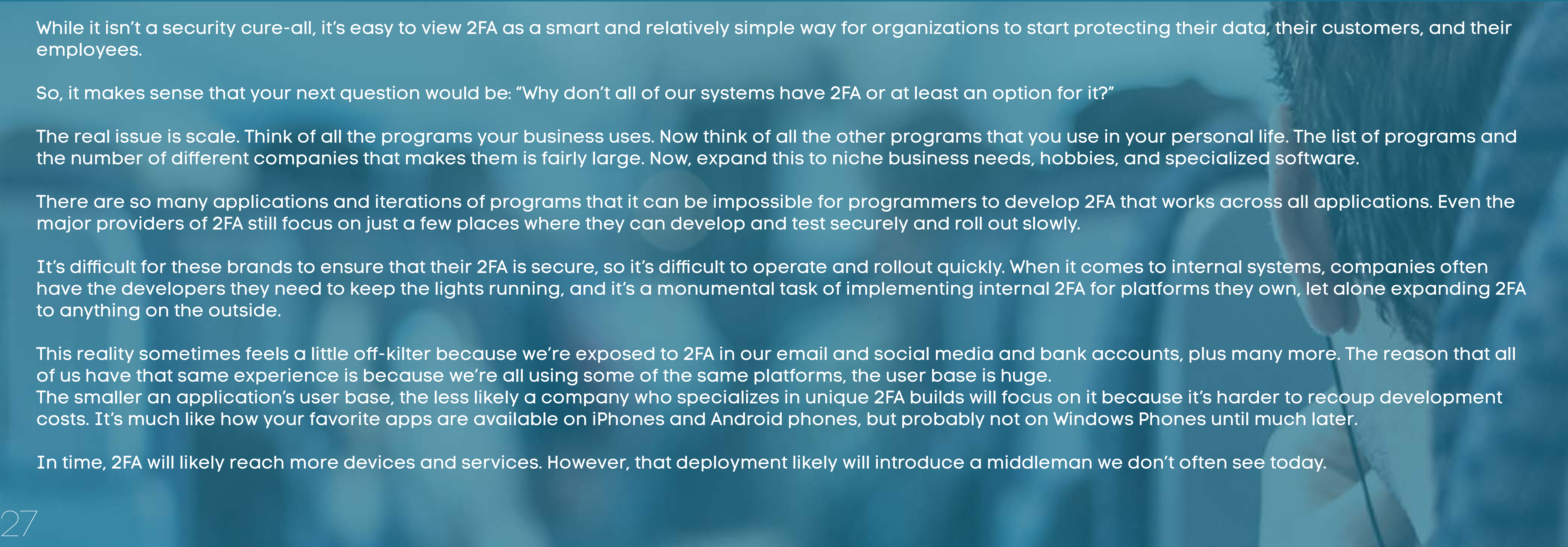
- Cross-platform support enabling access on the latest devices, even as users upgrade their own devices.

- Token savings with the employee/customer ab sorbing the cost of the device purchase as well as the replace ment.

- User control and choice, reducing demanding on IT.

- Faster access to the latest technologies, such as how fingerprint scanners arrived on devices before they were adopted by the average small or mid-sized business.

WHY IS TOTAL TWO FACTOR AUTHENTIFICATION ABSENT?



While it isn’t a security cure-all, it’s easy to view 2FA as a smart and relatively simple way for organizations to start protecting their data, their customers, and their employees.

So, it makes sense that your next question would be: “Why don’t all of our systems have 2FA or at least an option for it?”

The real issue is scale. Think of all the programs your business uses. Now think of all the other programs that you use in your personal life. The list of programs and the number of different companies that makes them is fairly large. Now, expand this to niche business needs, hobbies, and specialized software.

There are so many applications and iterations of programs that it can be impossible for programmers to develop 2FA that works across all applications. Even the major providers of 2FA still focus on just a few places where they can develop and test securely and roll out slowly.

It’s difficult for these brands to ensure that their 2FA is secure, so it’s difficult to operate and rollout quickly. When it comes to internal systems, companies often have the developers they need to keep the lights running, and it’s a monumental task of implementing internal 2FA for platforms they own, let alone expanding 2FA to anything on the outside.

This reality sometimes feels a little off-kilter because we’re exposed to 2FA in our email and social media and bank accounts, plus many more. The reason that all of us have that same experience is because we’re all using some of the same platforms, the user base is huge.
The smaller an application’s user base, the less likely a company who specializes in unique 2FA builds will focus on it because it’s harder to recoup development costs. It’s much like how your favorite apps are available on iPhones and Android phones, but probably not on Windows Phones until much later.

In time, 2FA will likely reach more devices and services. However, that deployment likely will introduce a middleman we don’t often see today.

WHERE IS **TWO FACTOR AUTHENTICATION** HEADED NEXT?

What we expect to see coming soon is middleware that allows an application to authenticate to a service. The middleware service then seeks out the two required identification tokens. When they are expected, it will then open the gate so the end-user can access the application.
This middleware platform will need to be a smart drawbridge that can not only store and understand a wide range of data, but it will need some semantic capabilities to look for nuance.

A potential option for this 2FA middleman could be a password remembering service or keychain program that creates unique, extremely long, and very complex passwords for the apps and software you use. You could use 2FA to get approval for the password service to authorize your current session, and it would consider your identity verified and then distribute passwords appropriately as you accessed apps and services.

This solution is being used for some small businesses, turning to software like LastPass , which requires a login to LastPass and then the second factor authentication with options for software support, hardware tokens, and mobile tokens.
LastPass provides authorization locally, typically being tied to a browser, so it can be susceptible to the main threat of smartphone-based authentication: access to the device. If a PC is left on and signed in to such a service, then it could remove the protection. Someone who can either physically or remotely access the device typically won't face another 2FA request at this point, creating a significant vulnerability.

RECAP

Small and mid-sized businesses continue to roll out cloud services and technology that expands their support for customers and employees anytime, anywhere. They're also contracting with more freelancers, marketing companies, virtual assistances, and remote workers than ever before because it saves on infrastructure costs.

These trends can lead to more significant threats to a company's data and systems, which in turn has most businesses looking for smarter protection options. Two-factor authentication is being touted as a future savior, but it might not be ready for primetime just yet.

Keeping sensitive information safe will require additional screening and security options that customers and employees are willing and able to use. The rise of consumer-facing 2FA techniques from ATM cards to email service verification will make enterprise adoption simpler and will slowly raise success rates.

However, in the near term it will likely be difficult to bring small and mid-sized businesses into the 2FA fold because of the high costs associated with the technology and the training. User administration needs, support staff, complex installations, and rolling out a user experience that is easy to navigate – if not easy to use – will all raise costs.

Many experts believe these costs will keep 2FA at bay until there is a major breach that pushes a significant amount of company data onto the more nefarious parts of the Web. We feel that Target may represent the most well-known breach that should be seen as a lesson on the importance of authentication.

Target's 2013 security breach that was caused by a small HVAC vendor who accessed its network has cost the business more than $110 million in settlements alone . The breach impacted nearly 40 million customers, and if it cost the brand just $1 per person to verify the data loss and contact the customer, that's an additional $40 million before we look at the cost of investigating the breach.

The future of 2FA is likely to be a commonplace effort that most companies use to limit outside access to the growing amount of data stored in the cloud. Identification and authentication are expected to focus on efforts that are harder to fake, such as biometrics, and place an emphasis on the BYOT model that limits company costs.

Cyber threats are increasing in frequency, complexity, and severity. Two-factor authentication represents a clear way that companies can start protecting their data, customers, and employees. While adoption hurdles exist, it can prove to be a smart addition when the rollout is able to balance security with ease of use.

It's time for companies to start researching and investing in 2FA even if they do not implement the program in the near-term because waiting carries a much greater risk.