ICONIC *Education*
Powering businesses through education.

MULTI-FACTOR AUTHENTICATION GUIDE

ICONIC IT
better together

CONTENTS

INTRODUCTION:
THE GROWING CYBER SECURITY THREAT

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, according to the latest studies, these gaps are being exploited at an ever-increasing rate.

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 intentionally by individuals or organizations looking to do financial harm to a company. They will try to take down a service, reduce consumer trust, steal company secrets, and steal records in order to use them to defraud customers.

Each client lost due to a breach increases 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 every day before the breach is caught and corrected will cost them more money. 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 multifactor authentication, or MFA. Multifactor 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. These secondary factors can include sending information to a device only the user has access to, the information the user knows inherently, or information about who they are, such as biometrics.

Because many of these authentication tokens have a physical aspect that limits access, security firms are presenting MFA as one of the top ways to protect a network against remote attacks and exploitation. 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 MFA, its standard deployments, benefits and weaknesses in its protections, adoption likelihood, and likely future developments.

WHAT IS MULTI-FACTOR AUTHENTICATION?

Multi-factor authentication, often listed as MFA 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 MFA 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 MFA 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 new-age MFA that pairs voice recognition with fingerprint or retinal scans, but the science of MFA is much older.

SIMPLE EXAMPLES OF MULTI-FACTOR AUTHENTICATION

One of the earliest cases of machine-based multifactor 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.

Of course, the ATM you use today has a couple of significant differences from the earliest version. While the first version didn't have a usage fee, it did use checks that had the radioactive isotope carbon 14. Otherwise, the concept of the old technology and the new is the same. They both use 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 acceptable platform for the token. You've probably seen with your email account. Enabling MFA in Gmail, for example, means that you'll have to sign into the account with your username and password, then receive a code on your phone via text, phone call, or mobile app.

Facebook also has a MFA option that sends a code to your mobile device. Both it and Gmail will request a verification code each time you log into a new, unrecognized device or if you select an option for the service to not "remember" that device.

Companies are currently using a wide range of MFA methods. There has been a recent push toward using a mobile device to help MFA because of the prevalence of consumer device and the fact that few people venture out without one. They meet a desired principal: the out-of-bond authentication. This is when your primary password and the second identifying factor use two different delivery mechanisms.

THE MANY DIFFERENT WAYS TO COUNT TO TWO

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 MFA option.

This option is easy to implement and can be rolled-out to all 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 forms of hacking represent about 55% of all data breaches.

BIOMETRICS

Biometrics are a common MFA method that uses something completely unique 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, biometrics are the most secure MFA 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 currently 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 scale 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. This may mean either locking out a customer or allowing someone who has a similar face or fingerprint to the user to access the account.

Think of a time where you've been at an ATM and needed to swipe your card multiple times. This is because time wears down the system's scanner. Now imagine trying to get device recognition to work when you have a new haircut or a significant weight loss or gain.

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 while lost or improperly disposed of devices account for another 6%, according to a report from BakerHostetler. Obviously, this creates a notable risk.

Also, tokens can be expensive to replace and IT tickets can take longer or be more complex, resulting in a huge inconvenience 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 MFA. 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 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. Cracking a USB and retrieving the data inside or using an advanced RFID reader to see what information is returned 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 using SMS protocols. This is common for banks, email accounts, and other consumer-facing controls. Whenever the MFA service wants to verify a connection or request, it simply sends out a new SMS passcode. Often the code is timed so that it must be entered within a few minutes or it becomes invalid.

A lost or stolen device is always a concern because it is a primary point of a breach. 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 sent to email, which is likely on an unprotected phone, and then use these credentials 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 MFA to be in place. 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 full notifications 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 MFA 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 that physical access to the device, not necessarily access to its data, is all that's required. This is a major security risk when using option one and allowing the callback to reach a smartphone.

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, you can have the call go to a specific desk or extension. This means that in most cases, the user must be physically present.

In virtually every scenario, the second option above is more secure. This MFA relies on "knowledge," such as a passcode, but additionally 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 multiple uses, from health insurance to tracking employees via GPS. Smart watches and other personal devices are also becoming 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 the security risks they pose. While they do make receipt of a token easier in many scenarios, their display settings may cause some security methods to be weakened simply because unlocking a device might not be required to see the MFA token.

The IoT device's current reliance on connection to a smartphone, relying on both access and needing to be in a close physical proximity to the phone, may mean that the risk won't be significant except under very specific circumstances such as internal corporate espionage.

THE STATE OF MULTI-FACTOR AUTHENTICATION

Though not used too often, another system can be to physically call the user on a specific phone to ensure verification. This MFA 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 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 MFA relies on "knowledge" section listed above but specifies an unusual method of providing the knowledge token.

TRAINING AND USER EXPERIENCE

The hardest part of any new security element is training your employees to use 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 are placed to 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 MFA.

For MFA, 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 MFA 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 MFA 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 means training your entire staff or a core IT team to help each individual user to properly set their credentials. Fingerprints, for instance, require placement on a specific location to be properly scanned, which makes positioning important. If the scanner is dirty during the initial scans, it can adjust the biometric in a way that makes it nearly impossible to recreate in the future.

COST AND 5 THINGS YOU CAN DO RIGHT AWAY

There's no clear MFA 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 be affordable for companies.

This 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? Does your small business control everything you use, or do you need to rely on other services that supply MFA? Those can be difficult questions, especially when you're trying to balance growth with security. Here are a few thoughts on how small businesses can make the most out of MFA:

1 Because your staff or users are less likely to lose smartphones and tablets, stick with these first. This is also useful because, according to MFA brand Duo, the cost of tokens can approach more than $100 per user. Additionally, the lifespan of a token is three years while damage, malfunctions, loss, and theft can mean absorbing the token cost again and again.

2 Start off with an app. They can be safer than SMS because you have more control over who can log in when MFA tokens or notifications are sent. 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 may arise due to trouble tickets relating to unauthorized access, lost tokens, and broken access points.

4 Turn to secondary systems that already offer MFA. The good news is that there are utilities, payment options, email, communications, hosting, and much more already offering the services.

Here's our favorite site to check your options or see if the platform you want to use offers MFA: 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 ultimately look for vendor support. 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 cover in the following section looking at the evolution of "BYOT," or Bring Your Own Technology.

DOES MFA 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.

Multifactor authentication is also a bit like those old cartoons except that, in the moment right before our wolfish hacker snatches a pie off of a windowsill, the MFA rolling pin flashes to thwart their greedy appetite. Try as they might, there's almost no getting past it.

That's not to say that MFA 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.

The good news is that in most cases the hackers will need access to the physical token or will have to search for cookies and tokens that are placed on a device by the authentication mechanism. The bad news is that this can occur via phishing attacks, malware, or account recovery services. This means your employees should be properly educated about the risk of cyber-attack.

As attempted breaches become more commonplace, MFA is becoming increasingly more secure. The industry is learning how hackers are attempting to infiltrate the network and are beginning to address those security gaps.

3FA is an additional layer of security **beyond your password.**

****

BYOD AND MOBILE
MULTI-FACTOR AUTHENTICATION

For most MFA 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.

While adding MFA makes it much harder for any illicit access to take place, internal systems look at the personal smartphone with greater skepticism.

The Bring-Your-Own-Device push varies in success by industry. For MFA, we've seen minimal interest in BYOD on its own because of the cost it takes to lock down devices and platforms.

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

As businesses grow, they tend to start looking at BYOD as a more cost-effective solution to ensuring employees have proper cloud access. Consequently, the industry will need to start focusing on the smartphone as the MFA element of choice.

Adoption of BYOD does have a benefit: people tend to notice sooner when their personal devices are lost or stolen. Most mobile platforms also have options for remote locking or even the wiping of a phone's database when it's stolen, making the user able to render it useless as soon as it is noticed to be missing.

The future of mobile MFA 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, it can notify the user immediately when any authorization attempt is made. This gives the user the ability to flag an inappropriate login attempt and adding another layer of security.

MULTI-FACTOR AUTHENTICATIONS
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 to also 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 absorbing the cost of the device purchase as well as the replacement.
- User control and choice, reducing demanding on IT.
- Faster access to the latest technologies, such as fingerprint scanners appearing on devices before they were adopted by the average small or mid-sized business.

WHY IS TOTAL MULTI-FACTOR AUTHENTIFICATION ABSENT?

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

It makes sense that your next question would be: "Why don't all of our systems have MFA 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. Next, expand this to cover business needs, hobbies, and specialized software.

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

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

This reality sometimes feels a little off-kilter because we're exposed to MFA in our email, social media and bank accounts, plus many more. The reason we all share the same MFA experience on various apps is because we're all using the same platforms. The user base is huge.

The smaller an application's user base, the less likely a company who specializes in unique MFA builds will focus on it. It's much harder to recoup development costs for smaller user bases. It's much like how your favorite apps are available on iPhones and Android phones, but probably not on Windows Phones until long after their initial release.

In time, MFA will likely reach more devices and services, but that deployment will most likely introduce a a middleman we don't often see today

WHERE IS MULTI-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 accepted, the middleware service will open the gate so the end-user can access the application.

This middleware platform will not only need to be a smart drawbridge for storing and understanding a wide range of data, it will need some semantic capabilities to look for nuance, too.

A potential option for this MFA 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 MFA to get approval for the password service to authorize your current session, and it would consider your identity verified. It would then distribute passwords appropriately as you accessed apps and services. This solution is being used for some small businesses, using software like LastPass or 1Password, which requires a login to the initial application followed by 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, it would completely remove the protection. Someone who can either physically or remotely access the unlocked device typically won't face another MFA request at this point, creating a significant vulnerability.

RECAP

Small and mid-sized businesses continue to roll out cloud services and technology that expand 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. Multifactor authentication is being touted as the next big thing in security, 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 MFA techniques from ATM cards to email service verification will make enterprise adoption simpler and will slowly raise success rates.

In the short term, however, it will likely be difficult to bring small and mid-sized businesses into the MFA 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 user-friendly will raise MFA costs.

Many experts believe these costs will keep MFA in the sidelines 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's breach should be a lesson on the importance of authentication.

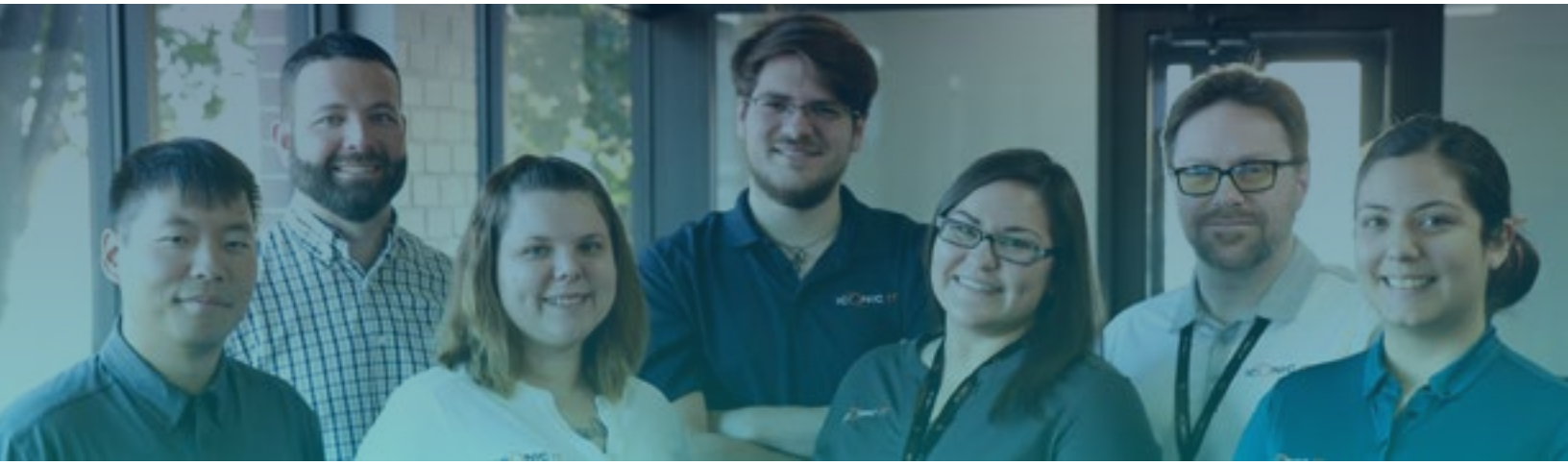
Target's 2013 security breach was caused by a small HVAC vendor who accessed its network. It cost the big retailer more than $110 million in settlements alone.

The breach impacted nearly 40 million customers. If it cost the brand just $1 per person to verify the data loss and contact the customer, that's an additional $40 million, and that's before we even look at the cost of investigating the breach itself.

MFA is most likely going to become commonplace for most companies to 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 hack, such as biometrics, and place an emphasis on the BYOT model that limits company costs.

Cyber threats are increasing in frequency, complexity, and severity. Multifactor authentication represents a clear way that companies can start protecting their data, customers, and employees. While adopting MFA can seem like a daunting task, it can prove to be a smart addition when the application balances security with ease of use.

Companies need to start researching and investing in MFA, even if they do not implement the program in the near future, because waiting carries a much greater risk.



WHO IS ICONIC IT?

We're a one-stop shop for all your managed IT services needs. We look out for you so you don't waste time trying to figure out why your technology isn't working, or spend money recovering from a breach that could have been avoided. With the right partner, you can get back to running your business and leave the rest to us.

We believe every business has the right to technology that works for them when they need it. We're here to remove the hurdles, keep your equipment proactively updated, and offer your network top-notch protection so you can sleep easy knowing that you, your employees, and your clients are taken care of.

WHY CHOOSE ICONIC IT *as your Partner?*

When it comes to security, you can't pick and choose which areas to focus on and which to ignore. Combined, all the services an MSSP offers provide you with a comprehensive security package that affordably safeguards your entire company.

If IT and security issues are draining your resources, or if your team is overwhelmed by fixing gaps in your system, consider starting with a network audit and security assessment from Iconic IT or call us at (817) 575-6230. You'll receive an unbiased evaluation that's easy to understand and can point you toward your next steps in security.

CONTACT US TO SEE IF YOU QUALIFY