SHARE FOUNDATION

SELECTING A MULTI-FACTOR AUTHENTICATION SOLUTION:

HOW TO ADDRESS THE HUMAN AND TECHNOLOGY CONCERNS

JUNE, 2023.

INTRODUCTION

The acceleration of digital transformation for all industries and sectors and the increased adoption of cloud-based technologies and hybrid work norms means that corporate and personal data are increasingly stored in dispersed cloud platforms. This data is also accessed by an expanding number of entities – apps, businesses, individuals, devices, etc.

The traditional brick-and-mortar corporate boundaries have diminished, rendering traditional approaches to security inadequate to protect our data. Identity has emerged as the new castle to defend; however, new security challenges related to identity protection have emerged. Organizations are investing in strengthening their access controls to combat this trend, moving toward a zero-trust cybersecurity model, and leveraging the power of multi-factor authentication (MFA).

This paper discusses the evolving identity and access management landscape and presents actionable considerations for addressing the human and technology concerns of effectively adopting multi-factor authentication.

THE CHANGING CYBER THREAT LANDSCAPE

The cyber battleground has shifted from protecting boundaries to protecting identities. Attackers have also evolved – access credentials (our identities) are the most sought-after asset in cyber-attacks. The Verizon 2022 Data Breach Investigations Report indicates that almost half of the data breaches involved compromised or stolen credentials. In addition, another 20% of the breaches began with a phishing attack aimed at our credentials.

Ransomware attacks increase in volume as the digital evolution of businesses continues. The efficacy to generate serious revenue for the attackers makes ransomware attacks popular amongst cybercriminals and a "must-have" in their toolboxes. Today it is considered the largest threat organizations face and a financial burden for all businesses.[1]

Attackers are also operationalizing their business – access-as-a-service or Initial Access Brokers facilitate associated criminal groups to penetrate systems and data by providing access to stolen or compromised credentials. The new business model criminals employ is evident in crime-as-a-service and ransomware-as-a-service operatives.

Ransomware-as-a-Service (RaaS), or human-operated ransomware[2], is driven by human intelligence and ends up in intentional business disruption and extortion. These criminals offer their services to others, establishing actual ransomware agreements in exchange for an agreed fee.

Microsoft mentions that the RaaS business model is similar to the traditional economy[3]: "In the same way our traditional economy has shifted toward gig workers for efficiency, criminals are learning that there's less work and less risk involved by renting or selling their tools for a portion of the profits than performing the attacks themselves."

1 2022 Cyber Claims Report, https://info.coalitioninc.com/download-2022-cyber-claims-report.html

2 https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

3 https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#DEV-0193

The Initial Access Broker (IAB) is one of the most significant links in the RaaS chain. The role of an IAB is vital for a ransomware attack's success since it provides initial access to the network and spares valuable time needed for target reconnaissance and intrusion strategy employment.

THE HUMAN ELEMENT OF CYBER THREATS

Although cybersecurity sounds more like a technology issue, it is all about humans. Humans are and will remain a critical component of cybersecurity. Individuals can unknowingly compromise sensitive information and systems through social engineering tactics or human error, highlighting the need for empowering people with proper technologies and awareness training.

Humans are the ones that mostly feel the ripple effects of a data breach. Personal, medical, and financial data are the most popular assets that criminals go after. Besides attacking the technology protecting our data, criminals are increasingly exploiting the inherent vulnerabilities of the human element.

According to the Verizon DBIR 2022 report, 82% of successful data breaches involve the human element in one way or another. In addition, human error is responsible for 13% of security incidents. Errors may include misconfigured apps in the cloud, email misdelivery, or employing weak password practices.

More companies are investing in providing security awareness training to empower their people. This training can help employees recognize and respond to potential threats, ultimately reducing the risk of a successful attack. It is crucial for companies to prioritize both technological and human-based security measures to protect sensitive data.

Equally important is for the individuals to educate themselves on basic cybersecurity practices and use tools such as password managers and two-factor authentication

to protect their personal information. Additionally, seeking out online resources and attending local workshops or events can help increase one's cybersecurity knowledge.

WHAT IS MFA AND ITS IMPORTANCE

Security agencies, national organizations, and businesses strongly suggest implementing multi-factor authentication to protect our digital identities and data better. MFA is an approach to strengthen the authentication process by requiring the user to present multiple elements in different categories, or "factors," as part of an authentication attempt. These factors, shown in the image below, are something you have, something you know, and something you are.

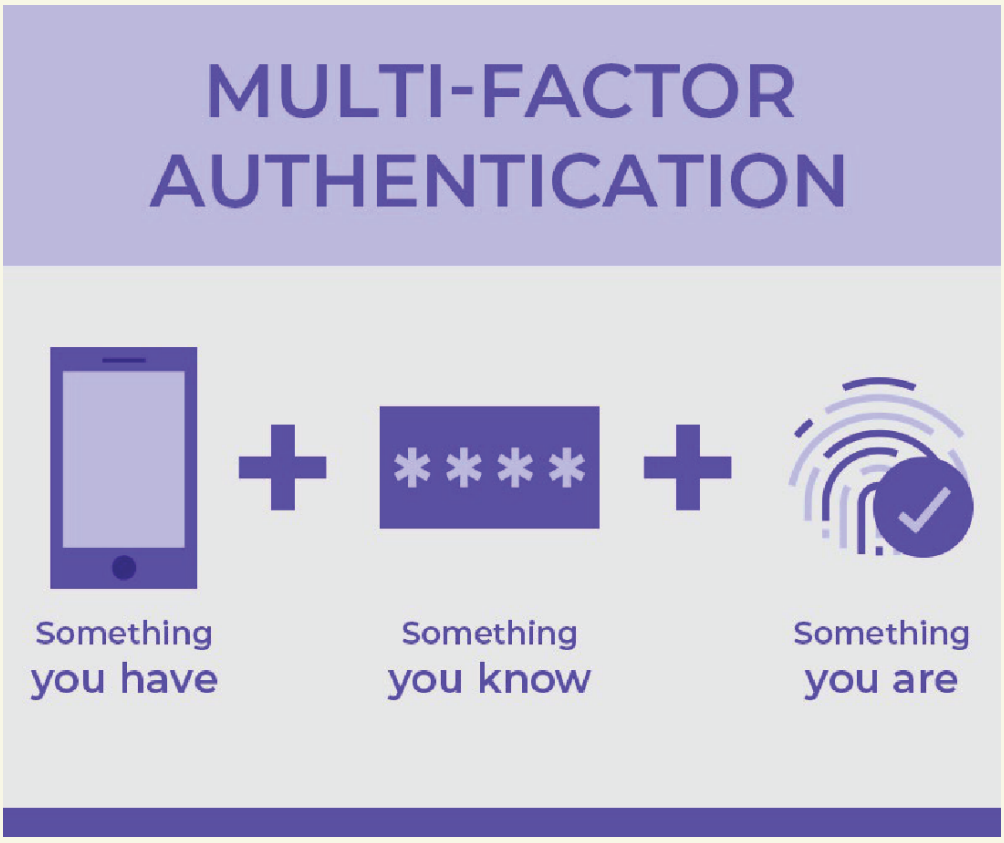

Figure 1: Multi-factor Authentication Factors. Source: CISA and NSA[4]

MFA incorporates more than one of the above factors into the login flow. Examples include:

4 CISA and NSA joint publication "Identity and Access Management: Recommended Best Practices for Administrators"

- Typing a password and responding to a push notification sent to a registered smartphone.
- Typing a password and providing a one-time code from a hardware authentication device.
- Using a biometric facial scan and/or passphrase to unlock a cryptographic credential stored on a registered device (i.e. phone, hardware token).

Authentication systems are the front doors to enterprise networks, applications, and data. As such, attackers are highly focused on finding and exploiting authentication vulnerabilities. Authentication systems are also high-volume user interfaces and are frequently seen as friction points between users and their ability to perform business functions. This combination of characteristics challenges systems engineers and implementers since they must be seamless and user-friendly yet strongly resistant to attacks.

MFA is a fundamental element of a strong access management policy. MFA is critical in preventing attackers from compromising our digital identities and penetrating our systems. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

MFA was created to address the shortcomings of passwords, including the fact that:

- Passwords can be shared with unauthorized users;
- Users can be tricked into giving their passwords to attackers through phishing; and
- Users often use the same or closely related passwords across multiple websites, services, and computer systems. A breach of one system allows an attacker to obtain usernames and passwords that can be used in other systems using techniques such as credential stuffing.

MFA mitigates common attacks against passwords, such as brute force guessing and credential stuffing[5], as well as common misuse practices, such as password sharing, by requiring the presentation of another factor besides the password. Knowing the password alone does not enable user impersonation unless an attacker can defeat the MFA authentication mechanism.

5 Credential stuffing is the automated injection of stolen credentials into login forms to fraudulently gain access to user accounts.

The US Cybersecurity and Infrastructure Security Agency (CISA) states that "MFA is one of the most important cybersecurity practices to reduce the risk of intrusions—according to industry research, users who enable MFA are up to 99 percent less likely to have an account compromised.[6]"

To understand the effectiveness of MFA, it is advised to look at a CISA security advisory, where the Agency mentions that "Multifactor authentication (MFA) prompts prevented the team from achieving access to one sensitive business system.[7]" The report was released following a pen-testing assessment that CISA conducted on a large critical infrastructure organization with multiple geographically separated sites.

NOT ALL MFA METHODS ARE EQUALLY SAFE

However, in the past two years, we have witnessed many attacks were criminals managed to bypass the MFA protection due to weaknesses in the MFA implementation. It is important to note that not all MFA solutions provide equal protection against authentication attacks, and there are critical implementation details that can impact the security and usability of an MFA deployment.

As cited in the National Institute of Science and Technology (NIST) MFA Update from February 2022[8], "All MFA processes using shared secrets are vulnerable to phishing attacks." This includes authentication methods that rely on memorized secrets, SMS-based push notifications, and one-time passwords (OTP).

---

6 CISA Alert (AA22-074A), https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

7 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a

8 https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_20Guidelines.pdf

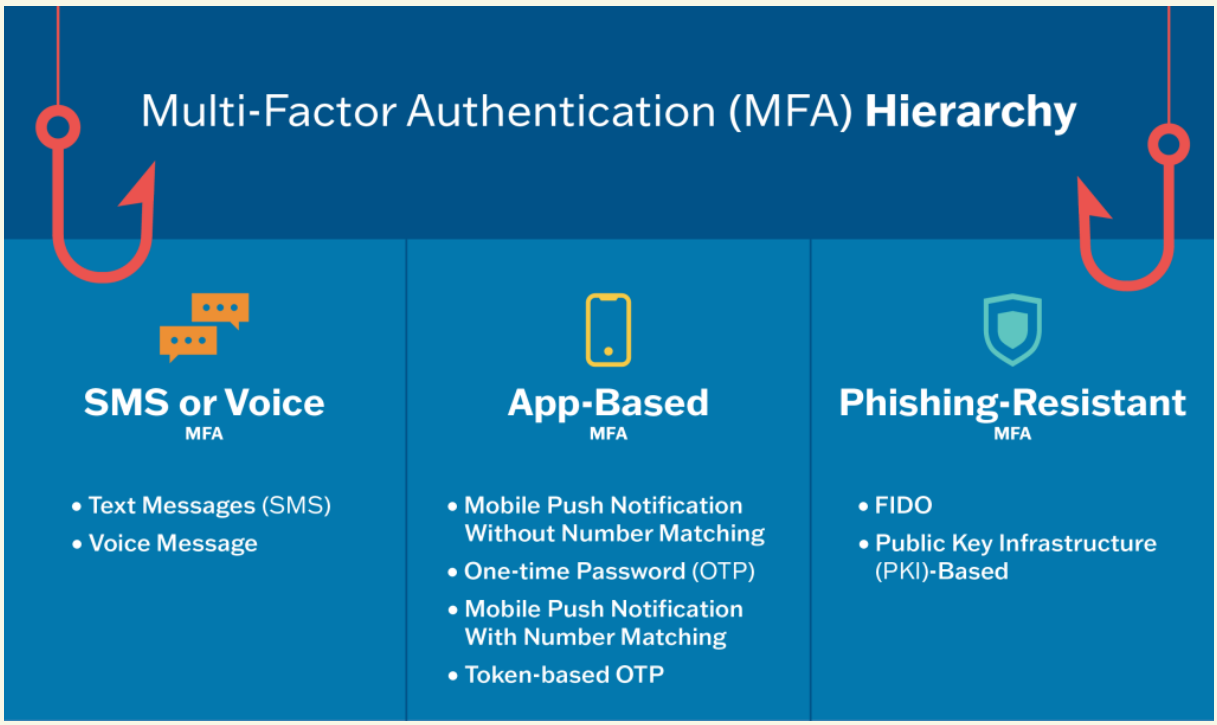

Figure 2: Weakest to strongest MFA methods. Source: CISA[9].

ONE-TIME PASSWORDS

Whether generated in an app or delivered through SMS or e-mail, one-time passwords do not protect against phishing. SMS is vulnerable because of either weaknesses in the architectural design of SS7[10] or SIM swapping attacks[11]. Because the user enters the one-time password into a login form, a phishing site can capture an OTP just as easily as a password and replay it to the legitimate site or application in real-time.

PUSH-NOTIFICATION AUTHENTICATION

Push notification-based authenticator apps that prompt users to approve login attempts do not generally protect against phishing. A phishing site can trigger a login attempt that will send a push notification to the user's registered device, and the user may have no way of determining whether the notification is legitimate. Some

9 https://www.cisa.gov/mfa

10 For more information on the SS7 vulnerability, see: https://www.techtarget.com/whatis/definition/SS7-attack

11 For more details on how SIM swapping attacks work, see https://www.enisa.europa.eu/news/enisa-news/beware-of-the-sim-swapping-fraud

attackers have had success rates simply triggering push notifications to users who are not even attempting to log in. Some push notification-based MFA solutions provide additional context about the authentication attempt, such as the location from which it originated, to aid the user in determining whether it is legitimate. If the login request came from a phishing site, the detected location of the login attempt should not match the user's current location. However, location can be spoofed, and the basic issue remains that the push notification is not strongly bound to a legitimate authentication attempt and the service to which the user is authenticating.

WHAT IS MFA FATIGUE?

When an organization's multi-factor authentication is configured to use 'push' notifications, the employee sees a prompt on their mobile device when someone tries to log in with their credentials. These MFA push notifications ask the user to verify the login attempt and will show where the login is being attempted.

An MFA fatigue attack is when a threat actor runs a script that attempts to log in with stolen credentials repeatedly, causing an endless stream of MFA push requests to the account owner's mobile device. The goal is to break down the target's cybersecurity posture and inflict a sense of "fatigue" regarding these MFA prompts.

In many cases, the threat actors will push out repeated MFA notifications and then contact the target through email, messaging platforms, or over the phone, pretending to be IT support to convince the user to accept the MFA prompt. Ultimately, the targets get so overwhelmed that they accidentally click on the 'Approve' button or simply accept the MFA request to stop the deluge of notifications they receive on their phone.

Many large and well-known organizations have become a victim of this tactic, includ-

ing Microsoft[12], Cisco[13], Uber[14], and Reddit[15].

THE NEED FOR A PHISHING -RESISTANT MFA

Considering the prevalence and success of these attacks, governments and agencies suggest using phishing-resistant MFA.

Phishing-resistant MFA is multi-factor authentication that is immune from attempts to compromise or subvert the authentication process, commonly achieved through phishing attacks, such as MFA fatigue. Phishing resistance within an authentication mechanism is achieved by requiring each party to provide proof of their identity and intent through deliberate action. The most common phishing-resistant protocol is FIDO (Fast Identity Online)[16].

In response to President Biden's Executive Order for Strengthening the US Cybersecurity, the Office of Management and Budget (OMB) issued a memorandum[17] that mandates all federal agencies use phishing-resistant MFA by the end of Fiscal Year 2024. The memo states that identity is one of the five pillars for zero trust security and that "Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks."

The European Union Agency for Cybersecurity (ENISA) released the guidelines "Boosting Your Organisation's Cyber Resilience[18]" which include provisions such as protecting all remotely accessible services with multi-factor authentication. Organi-

12 https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/

13 https://threatpost.com/cisco-network-breach-google/180385/

14 https://www.darkreading.com/attacks-breaches/uber-breach-external-contractor-mfa-bombing-attack

15 https://www.darkreading.com/risk/reddit-hack-shows-limits-mfa-strengths-security-training

16 https://fidoalliance.org/what-is-fido/

17 https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

18 https://www.enisa.europa.eu/news/enisa-news/joint-publication-boosting-your-organisations-cyber-resilience

zations should avoid using SMS and voice calls as authentication methods. Instead, they should consider "deploying phishing resistant tokens such as smart cards and FIDO2 security keys."

CHECKLIST FOR IMPLEMENTING MFA

However, these requirements do not imply that businesses must scrap their existing MFA implementations. They are, rather, a manifestation to better engage people with cybersecurity (in general) and selecting the proper MFA method.

Before deploying MFA, it is important to understand the full scope of use cases and scenarios the MFA solution needs to address. An ad-hoc approach can lead to incomplete coverage, multiple systems, and users needing to enroll multiple MFA mechanisms to access all the needed applications. Up-front planning and strategy definitions can help ensure a smooth, coherent implementation.

The following checklist can help businesses on how to select MFA per business needs.

CONSIDERATION	ACTIONS
Inventory users, devices, and user authentication journeys	**Consider the needs of different user groups to best determine how to handle MFA enrollment. Questions to consider include:** • What types of authenticators are suitable for each use case (mobile apps, security keys)? • What are the various devices your MFA solution needs to accommodate? • What are the potential device compatibility issues for both software and hardware MFA solutions (USB ports, Bluetooth, NFC, etc.)?
Assess the level of authentication assurance required	Some use cases, applications, or data types may require higher-assurance authentication than others. For example, privileged users with administration rights should have strong, phishing-resistant authentication. Other high-risk roles or functions may also require special protections if they involve the management of high-value assets or critically sensitive information.

CONSIDERATION	ACTIONS
Evaluate privacy and operational requirements	Many MFA solutions incorporate biometric authentication of the user, which can raise privacy concerns. Solutions that bind biometrics templates to a single device instead of storing them in a central database may help alleviate privacy concerns. Such is the case with FIDO-certified devices. Equity across demographic groups is another potential issue with choosing an authentication method. Aspects of your users' operating environment may impact the suitability of specific biometric modalities; gloves or masks, for example, may preclude facial or fingerprint authentication. On some factory floors, the use of mobile devices is forbidden.

EMPOWERING PEOPLE IN IDENTITY PROTECTION

Besides the sophistication of the attackers and the technical considerations of implementing an MFA solution, the real problem is how to inspire people at home and at work to use this security feature. Sadly, many reports indicate that businesses and individuals are NOT deploying MFA to the maximum extent possible.

- 56 of businesses say they have implemented MFA but only for privileged and remote employees[19].
- Only 8 of C-suite executives use MFA across most of their apps and devices[20].

However, the problem is not related only to business environments. Citizens using social media platforms do not employ best practices to protect their online accounts and personal data. For example, only 2.6% of Twitter users have activated MFA on their accounts[21].

Many reasons may justify this risky behavior:

- The technology is difficult to be implemented and integrate into daily busi-

19 https://cpl.thalesgroup.com/access-management-index

20 https://www.scmagazine.com/news/security-awareness/only-8-of-c-suite-executives-use-mfa-across-a-majority-of-apps-devices

21 https://transparency.twitter.com/en/reports/account-security.html#2021-jul-dec

ness workflows.

- The need for implementing MFA is not communicated effectively to businesses and societies.
- The misperceptions that people share about cybersecurity ("it will not happen to me" or "I have nothing to hide").
- Fear and uncertainty around cybersecurity alienate people from the industry.

Moving ahead, we need to realize that cybersecurity is not solely about technology or processes. Throwing more technology at people's faces will not ameliorate the situation. On the contrary, it will make things worse by introducing unnecessary complexities.

What we need to do is to empower people in cybersecurity and identity protection. For example, what have we done to educate people to recognize and report phishing attacks? The recent Reddit attack demonstrated most profoundly the limits of technology (and MFA) and the strengths of awareness training[22].

After entering credentials into the phishing site, the Reddit employee suspected something was wrong and contacted the IT department. That reduced the attacker's window of opportunity and limited the damage. It is time we stop looking at employees as a weakness and instead look at them as the strength they can be for organizations. Technology can only protect so far. Employees can offer the additional context required for detecting and stopping an attack.

Security awareness training should focus not only on "why" (the impact of a breach) but also on "why me?". Security awareness professional Jessica Barker notes[23] that organizations need to understand why certain behaviors are practiced (or not) for awareness to have a meaningful meaning. Understanding the cultural 'why' helps to explain the behaviors you seek to influence. There are no 'irrational behaviors', only behaviors we cannot explain due to the lack of awareness of the cultural context.

'Why' helps us frame cyber security in a more impactful way. But that is only half of what security awareness training is. The second half tackles 'why me?'. This provides the context, helping people understand not just why cyber security is relevant

22 https://www.darkreading.com/risk/reddit-hack-shows-limits-mfa-strengths-security-training
23 https://www.cygenta.co.uk/post/cyber-security-awareness-50000

but why it is relevant to them. Without this, it is hard to influence people's intrinsic motivation, which is key to influencing behavioral change.

Empowering and engaging people with cybersecurity is the best way to protect our digital identities in a highly interconnected world. Since every organization has a security (and organizational) culture, it is best to transform this culture into a positive and proactive one. One that is not based on blaming people for mistakes they do. One that rewards small wins.

We should consider the following five ingredients in building a positive, proactive security culture.

FORGET CLICK RATE	FOCUS ON REPORT RATE
Don't do long lists of don'ts	Motivate with key call-to-actions
Don't hide the message behind walls of text	Engage with bitesize videos
Break the shackles of fear and uncertainty	Build foundations of self-efficacy
Away with naming and shaming	Embrace a 'no blame' approach

Our businesses and societies will become safer and stronger only if we focus on all three domains of cybersecurity: people, processes, and technology.