Government Business Council

STATE OF ALERT

MULTIFACTOR AUTHENTICATION AND THE FUTURE OF DATA

INTRODUCTION

Multi-factor authentication (MFA) is quickly becoming a key component of many government cyber security defense strategies. State and local government security teams are constantly looking to outpace malicious actors, who are mounting data breaches that are both increasingly sophisticated and exponentially expanding. An estimated 11.1 billion records have been lost or stolen since 2005, costing about $1.66 trillion nationwide.1 In an effort to beef up security, governments are instituting increasingly rigorous two-factor and multi-factor authentication. These layered security protocols are meant to ensure that the right people (and only these people) are accessing the right applications and data at the right time. MFA has become especially crucial recently as telework and hybrid working has significantly increased the need for state and local government employees to securely access applications and data from their homes. Moreover, the rise in personal information being submitted to state benefits agencies increases the threat surface for hackers and other bad actors, making effective security protocols for employees and constituents a significant goal for state and local agencies.

11.1 BILLION
RECORDS GONE

=

$1.66 TRILLION
LOSS NATIONWIDE

WHY IT MATTERS

State governments are repositories of troves of sensitive and personal information, including Social Security numbers, driver's licenses, and credit card information. When state security protocols are violated, either through a cyberattack or human error, this can have serious consequences for the privacy and security of state residents. Poor experiences with government can erode public confidence and data theft can have lasting consequences for individuals who are victimized.

THE BIG ISSUE

Data security is always a critical component of government services and increasingly innovative hacks and data breaches demonstrate that a username and password is no longer enough to protect against phishing attacks and account takeovers. MFA is increasingly crucial to ensure continuity of government, and should be deployed as a first step in securing data and application access for both state employees as well as citizens. The future of data security may include getting rid of passwords altogether.

WASHINGTON STATE:
1.47 MILLION RESIDENTS IMPACTED

On Christmas Day, 2020, unauthorized access to files of the Office of the Washington State Auditor exposed the personal information of over 1.47 million state residents. The data, which included names, Social Security numbers, bank information and places of employment, originated from the Washington State Employment Security Department, and belonged largely to residents who had filed for unemployment claims in 2020. The Auditor's office blamed a legacy system that had not been updated, but the state was widely criticized for not doing more to protect the secure data of its citizens — among them, those hit hardest by the pandemic.[2]

WHAT IS MFA?

Multi-factor authentication is a method of controlling data security through conditional access — essentially ensuring that the user is who they say they are, and are entitled to see the data they're asking to access. This takes various forms, typically involving a password and a secondary item that is separate from the system (often a phone). This secondary device, whether a hardware security key or mobile-based authenticator app, or even biometric data like a thumbprint, reduces the likelihood that an adversary will be able to successfully impersonate an authorized user. Even if the system is compromised, this second round of authentication is more likely to keep the data secure.

The rise of remote and hybrid work has put credential-based access in the crosshairs of bad actors. Passwords are a notoriously weak system of security, prone to being lost or forgotten by users and easily hackable (TeleSign reports that 54% of consumers use 5 or fewer passwords for all of their accounts). Compromised passwords are responsible for 81% of hacking-related breaches.[3] Consequently, both industry and state and local governments are looking for solutions that may leave passwords in the past.

THE MULTI - FACTORS[4]:

SOMETHING YOU KNOW

password, PIN, challenge question

SOMETHING YOU HAVE

hardware or software token

SOMETHING YOU ARE

biometric data

MFA EXAMPLES

- Hardware Security Key
- App-based Authentication
- SMS Authentication/Mobile Passcode
- Biometric Authentication

NIST

The National Institute of Standards and Technology (NIST) has the following guidelines for choosing an MFA solution[5]:

GUIDELINE 1

Does the solution protect the authenticator from common exploitation techniques?

GUIDELINE 2

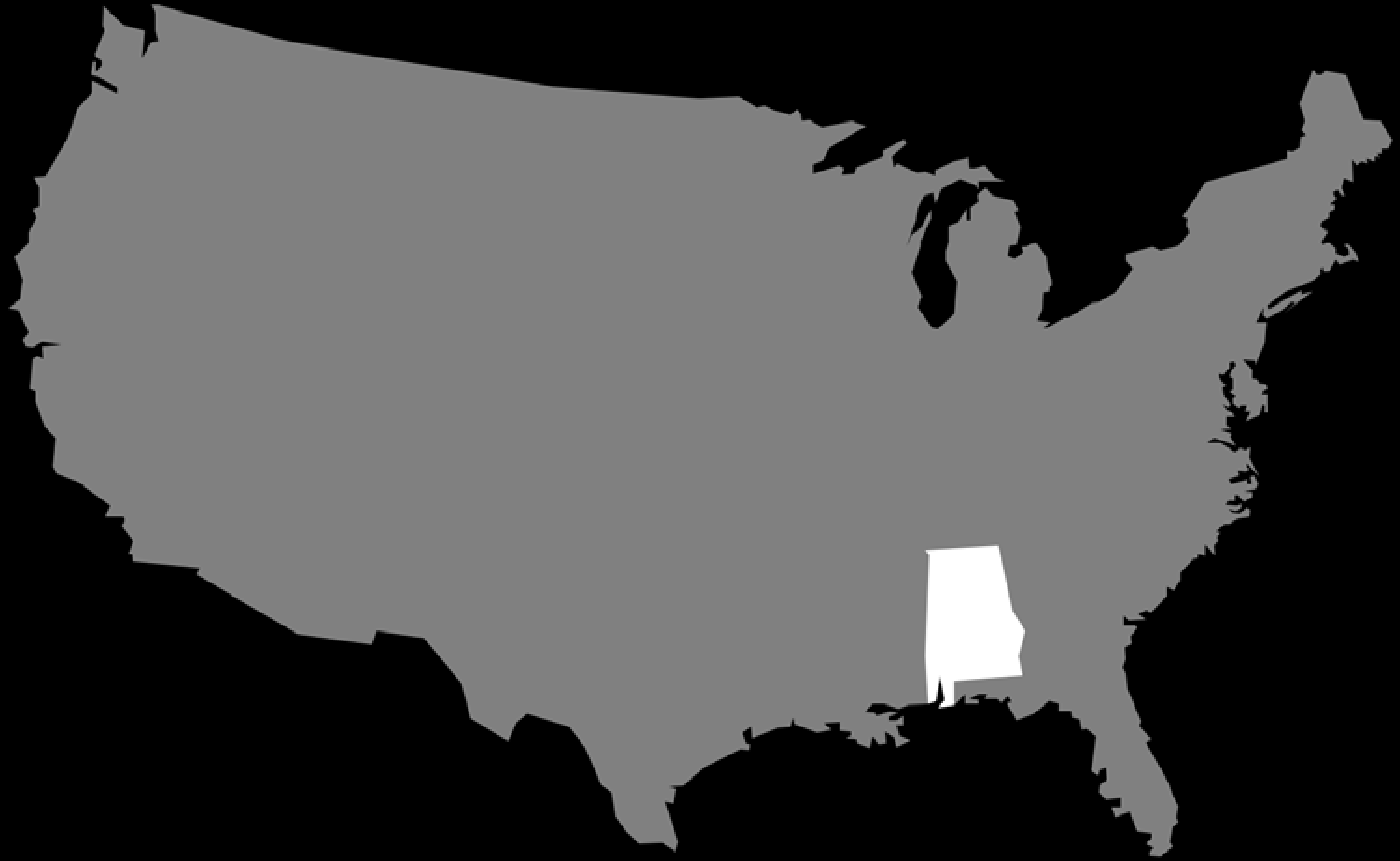
Does the solution protect the verifier from common exploits and make sure that the request for access is from the correct user?

GUIDELINE 3

Are communications between the parts of the authentication system protected?

GUIDELINE 4

Does the solution support maintaining the lifecycle of digital identities?



ALABAMA
HOSPITALS UNDER ATTACK

In October of 2019, three hospitals in Tuscaloosa fell victim to a Ryuk ransomware attack, knocking all of their systems offline and halting operations related to patient care. All but the most critical patients had to be transferred out of these hospitals to other institutions, and medical staff were forced to track patient data with pen and paper. The hospitals eventually had to pay the hackers for the decryption key to restore access to locked systems. Attacks like these are becoming increasingly common. In 2020 alone, 600 clinics, hospitals, and other healthcare organizations were targeted by cyberattacks, costing an estimated $21 billion in damages.[6,7]

PAIN POINTS

SECURITY

Multi-factor authentication is recognized as a security priority, but not all multi-factor authentication processes are created equal. Mobile-based authentication, for example, is fairly common, but is susceptible to malware, SIM-swapping, and man in the middle attacks.

USABILITY

State and local agencies have a diverse group of employees as well as a diverse constituent base, some of whom may not have a smartphone or those who live in an area without reliable cell coverage that would enable them to use some forms of MFA. Compliance issues or union restrictions may also prevent employees from using personal mobile devices for work. Users who don't have this kind of access still need a secure authentication. Without it, there may be gaps in state and local governments' security postures that increase the risk of account takeovers.[8]

COSTS

State and local governments work with tight budgets, and the COVID-19 pandemic tightened some belts even further — state budget shortfalls for fiscal years 2020 - 2022 are estimated to be $555 billion.[9] Agencies have to do more with less while simultaneously facing a higher threat landscape. These organizations will have to choose their multifactor authentication methods accordingly, as some MFA solutions put agencies on point to reimburse employees for related costs.

INCREASING THREATS

Thousands of workers logging in remotely creates an ongoing opportunity for bad actors to access sensitive information. Since 2017, reported cyberattacks on state and local governments went up by at least 50% — in reality, that number is likely much higher. Ransomware is the most commonly used method of attacking municipalities, often demanding exorbitantly high amounts to return or unlock data. Government computers are not the only ones targeted: third-party payment processors, land operations at ports, nuclear systems and power generator equipment settings have all been past targets in multiple municipalities. Concerns about cyberattacks also fray public trust in election results, cause delays in receiving state benefits, and disrupt health information campaigns.

BALTIMORE: ROBBINHOOD AND $18 MILLION

In 2019, hackers calling themselves RobbinHood exploited a gap in the City of Baltimore's remote access system, seizing the city's voicemail, email and parking fines database, as well as the system used to pay water bills, vehicle citations and property taxes. They held the city hostage for two weeks, demanding ransom in Bitcoin and keeping major systems offline. Baltimore didn't pay the hackers, but ended up paying around $18 million in damages and remediation, including the cost of rebuilding government systems. This was Baltimore's second attack in 15 months; a previous round of ransomware knocked out their emergency 911 system for 17 hours.[10]

MOVING TOWARD A “PASSWORDLESS” FUTURE

Even multi-factor authentication can pose problems. Malicious actors have been known to use SIM-swaps (switching target mobile phone number to a new phone, allowing them to access confirmation codes), malware (such as Cerberus, which stole Google Authenticator codes from Android devices in 2020) and social engineering (such as posing as the target’s bank).[11]

Is the next step to eliminate passwords altogether? Some certainly think so. Passwordless systems and touchless authentication solutions may be the next big thing in cybersecurity. Passwordless logins are exactly what’s on the box — providing a secure authentication experience without requiring a password during login. Passwordless systems use a cryptographic pairing of a private and public key. The private key is local to the user, such as a fingerprint or PIN, and is paired with a public key through the online system the user wants to access. This alleviates the need for users to remember passwords as well as the need for agencies to store and manage them. In some places, this is already in use. Smartcards are common across federal government agencies, but the scalability and infrastructure may not be feasible for state or local governments.

A newer take on passwordless comes from the FIDO2 and WebAuthn authentication protocols. These modern authentication protocols use user gestures (such as PINs, touch, or biometrics), which stays central to the user. This validates a signature that’s held on the web (the public key). But unlike passwords, which are sent over the web, both keys stay firmly in their domain. This makes this kind of service impervious to phishing or man-in-the-middle attacks. Only an end user with the FIDO2 private key can successfully authenticate to a service. This solution may be more attractive to state and local governments, as it requires little infrastructure, is highly secure, and uses common devices. Not to mention that users don’t have to remember their password.

CONCLUSION

State actors have both a responsibility and an opportunity to lead nationwide movements for secure data access to ensure that their constituents' data remains secure and protected. They are uniquely positioned to serve as gatekeepers and champions, thinking creatively about how to safeguard their citizens' data. Increasing options for multi-factor authentication offers tailored solutions that can address problems of cost and access — and protect against an increasingly threatening cyber-environment. The advance of a "passwordless" future, while still developing, may herald a new age in which access is safer, our data is more secure and bad actors see their window of opportunities slam shut.

> "[State actors]... are uniquely positioned to serve as **gatekeepers** and champions, thinking creatively about how to safeguard their citizens' data."

INDUSTRY PERSPECTIVE

THE BRIDGE TO PASSWORDLESS

Balancing security and usability has always been a challenge for state and local governments. Software authentication, including passwords, sms and mobile apps are all increasingly vulnerable to malware and hackers. And the more secure hardware authentication solutions are difficult to use and deploy. Yubico, a global authentication leader, is helping many state and local government agencies with strong authentication and their journey to passwordless. Yubico's flagship product, theYubiKey, is a hardware-based authentication solution that is FIPS 140-2 validated, Department of Defense OCIO approved, and provides superior defense against phishing and account takeovers.

The YubiKey offers strong authentication with support for multiple protocols, including FIDO U2F, PIV (smart card authentication), OpenPGP, one-time password, and WebAuthn/FIDO2, the new open web standards enabling the replacement of weak password-based authentication with public key cryptography. The YubiKey is easy to use, fast and reliable, and is proven at scale to significantly reduce IT costs and eliminate account takeovers -- crucial for agencies who are trying to do more with less.

The YubiKey works across the full range of passwordless implementation options—across legacy and modern environments, using smart card, FIDO2/WebAuthn, or even in conjunction with identity and access management solutions such as Azure Active Directory, Okta, Ping and Duo. In a world where state and local government cybersecurity is threatened more than ever, Yubico can help you bridge to passwordless.

THE YUBIKEY

> Passwordless is where the industry is headed, and state and local governments are starting their journey now for a passwordless future by taking the following steps - strong MFA for all, and ensuring adaptability to the new standards like FIDO2 and WebAuthn that enables the move to passwordless when ready."
>
> **Jeff Phillips** | *VP Public Sector, Yubico*

yubico

Government
Business
Council

ABOUT GBC

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research analysis.

EMAIL GBC

yubico

ABOUT YUBICO

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts. As a global authentication leader, Yubico is helping federal, state, and local government agencies with strong authentication and their journey to passwordless. Yubico's flagship product, the YubiKey, enables one single security key to access computers, phones, networks and online services—all in a simple touch. With its unique multi-protocol support, the YubiKey delivers strong hardware protection across any number of IT systems and online services—all with just a simple touch. Founded in 2007, Yubico is privately held, with offices in USA, Sweden, UK, Germany, Australia, and Singapore.

LEARN MORE

ENDNOTES

1. IBM. “IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years.” July 23, 2019. https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years
2. GeekWire. “Data breach exposes 1.6 million Washington State residents who filed unemployment claims in 2020.” February 1, 2021. https://www.geekwire.com/2021/data-breach-exposes-1-6-million-washington-state-residents-filed-unemployment-claims-2020/
3. IRS. “Multi-factor Authentication Implementation.” https://www.irs.gov/privacy-disclosure/multi-factor-authentication-implementation.
4. NIST. “Security and Privacy Controls for Information Systems and Organizations.” https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
5. TeleSign. “TeleSign Consumer Account Security Report.” https://www.telesign.com/resource/telesign-consumer-account-security-report.
6. Gizmodo. “Alabama Hospitals Pay Out in Ransomware Attack Amid FBI Warning of More to Come.” October 19, 2019. https://gizmodo.com/alabama-hospitals-pay-out-in-ransomware-attack-amid-fbi-1838826293
7. Becker’s Hospital Review. “Ransomware attacks on healthcare organizations cost nearly $21B last year, study finds.” March 12, 2021. https://www.beckershospitalreview.com/cybersecurity/ransomware-attacks-on-healthcare-organizations-cost-nearly-21b-last-year-study-finds.html.
8. StateScoop. “State agencies look to multi-factor authentication to augment security.” https://statescoop.com/briefs/multifactor-authentication-security-state-agency-report/
9. Center on Budget and Policy Priorities. “States Continue to Face Large Shortfalls Due to COVID-19 Effects.” July 7, 2020. https://www.cbpp.org/research/state-budget-and-tax/states-continue-to-face-large-shortfalls-due-to-covid-19-effects.
10. GovTech. “For Second Time in a Year, Baltimore Hit with Ransomware Attack.” May 7, 2019. https://www.govtech.com/security/For-Second-Time-in-a-Year-Baltimore-Hit-With-Ransomware.html.
11. Computer Weekly. “Two-factor authentication is broken. What’s next?” April 6 2020. https://www.computerweekly.com/news/252481189/Two-factor-authentication-is-broken-What-comes-next