FEBRUARY 2017

STRONG AUTHENTICATION IN CYBERSPACE

8 Key Principles for Policymakers

CONTENT:

INTRODUCTION

It's hard to find a major cyberattack over the last five years where identity – generally a compromised password – did not provide the vector of attack.

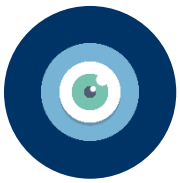
Target, Sony Pictures, Anthem, the Democratic National Committee (DNC), the U.S. Office of Personnel Management (OPM) – each was breached because they relied on passwords alone for authentication. We are in an era where there is no such thing as a "secure" password; even the most complex password has fundamental weaknesses as a security tool.

In response to the increased frequency of authentication-based cyber-attacks, governments around the world have been crafting policies, initiatives and regulations focused on driving the adoption of more secure, multi-factor authentication (MFA) solutions that can prevent password-based attacks and better protect critical transactions, data, communications and infrastructure.

As they tackle this issue, however, governments face a number of challenges. At the core of them is the fact that all MFA is not the same. Rather, MFA represents a wide variety of technologies that vary in three key areas:

Security. New attack methods mean that the threat against authentication technologies has also gotten more sophisticated, with some types of MFA emerging as much more resilient than others. Governments thus need to craft any new rules carefully, lest they mandate or promote adoption of authentication technologies that are outdated.

Usability. Today, there is a veritable explosion of innovation in the authentication sector, marked by the arrival of next-generation authentication solutions that are not only more secure than first-generation solutions which first hit the market in the 1990s, but are also easier to use. This is important, given that the market has largely rejected first-generation MFA solutions that degraded the overall user experience. Governments need to craft policies that incent use of the "right" kind of MFA that can overcome these barriers.



Privacy. Some authentication technologies offer enhanced security at the expense of privacy, or create new privacy risks that must be mitigated. Others are designed to improve both security and privacy, with no tradeoff between the two.

Against this backdrop – it is important that governments crafting policies or regulations around the use of strong authentication take into account the ways that both the threat has evolved, as well as how the market has evolved to address it. Policies that are written for yesterday's technologies and threats are certain to fail.

This paper will:

1. Lay out the current state of threats associated with inadequate authentication
2. Provide an overview of the types of technologies available on the market today to address these threats
3. Outline eight key principles for governments to consider as they craft authentication policies and initiatives.

WHY AUTHENTICATION IS IMPORTANT

As the table below demonstrates, it's hard to find a major cyberattack over the last five years where inadequate authentication – generally a compromised password – was not the vector of attack.

Breach	Date	Attack Vector
Oracle/Micros	August 2016	Compromised Password
Democratic National Committee (DNC)	July 2016	Compromised Password
Yahoo	December 2016	Multiple – Target was passwords and answers to authentication "security questions
OPM (2 Breaches)	May 2015	Compromised Password
Anthem	February 2015	Compromised Password
IRS	May 2015	Inadequate Authentication (Compromise of Knowledge-Based Questions)
JP Morgan Chase	July 2014	Compromised Password
Target	December 2013	Compromised Password
Apple iCloud	August 2014	Compromised Passwords
Home Depot	September 2014	Compromised Password
Sony Pictures	December 2014	Compromised Password
Heartbleed	April 2014	Compromised Password
1.2B Passwords (Russian CyberVor Hacker Gang)	August 2014	Multiple – Target was passwords to be used for other potential attacks

Outside of these high-profile breaches, Verizon's annual Data Breach Investigations Report (DBIR) has also helped to make this point clear. The 2016 DBIR found that "63 percent of confirmed data breaches involve using weak, default or stolen passwords." No other attack vector comes close.[1]

The reasons for this are simple: passwords are "shared secrets" that – once compromised – can be used to break into many systems and bypass other forms of security.

Indeed, attack after attack has shown that adversaries use passwords to bypass traditional perimeter defenses that create virtual "fortresses" around cyber assets; with passwords, they can simply walk through the front door. A 2015 report from Secureworks[2] highlighted how attackers were moving away from sophisticated malware-based attacks, noting: "In nearly all of the intrusions in the past year…cyber criminals utilized the target's own system credentials and legitimate software administration tools to move freely throughout the company's networks infecting and collecting valuable data."

There are myriad ways for an attacker to compromise systems protected by a password. These include:

- Phishing attacks that trick someone into sharing their password
- Brute force attacks that can quickly crack passwords
- Keyloggers or other malware that capture passwords while they are being entered
- Default passwords such as "admin" or "1234" that are never changed on many machines and devices
- Reuse of passwords between accounts

This last point is worth expanding on in more detail: Because stolen credentials are so useful, passwords themselves are often the most valuable treasure for attackers to steal, given how many people reuse passwords between accounts. A September, 2016 article Ars Technica drove this point home, detailing how the breach of a White House contractor was facilitated by him reusing the same password on his Gmail account that was revealed in the Adobe breach of 2013.[3] This problem is widespread: a study from Telesign illustrated just how common password reuse is – showing that 71% of accounts are protected by a password that is being reused across multiple accounts.[4]

When passwords are reused across sites, even so-called "strong" passwords become weak, as the compromise of one account can lead to the compromise of others.

The last few years have made clear that the guidance experts give people to change their password after every breach – or add more characters to their password – is not effectively thwarting attackers. If they were, we would not be seeing these kinds of attacks continue. Increasingly, industry and governments have realized that passwords must be augmented with at

[1] http://news.verizonenterprise.com/2016/04/2016-verizon-dbir-report-security/
[2] http://www.darkreading.com/analytics/stealing-data-by-living-off-the-land/d/d-id/1322063
[3] http://arstechnica.com/security/2016/09/hacked-e-mail-account-of-white-house-worker-exposed-in-2013-password-breach/
[4] https://www.telesign.com/wp-content/uploads/2016/11/TeleSign-Consumer-Account-Security-Report-2016-FINAL.pdf

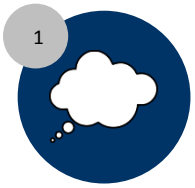
least a second factor of authentication, or ideally, replaced with technology that is fundamentally more secure.

In the United States, for example, the Commission on Enhancing National Cybersecurity called out inadequate identity solutions as a major problem, noting "we are making it far too easy for malicious actors to steal identities or impersonate someone online," and declaring:

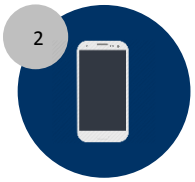
"An ambitious but important goal for the next Administration should be to see no major breaches by 2021 in which identity—especially the use of passwords—is the primary vector of attack."

FUNDAMENTALS OF AUTHENTICATION

As policymakers look to improve authentication, it's important to consider the different kinds of technologies used in authentication solutions. While there are many types of authentication technologies, they commonly fit into three categories, or "factors":



Something you know: such as a password, or the answer to a "security question" (i.e., what elementary school did you attend?)



Something you have: such as a smart card, token, or mobile phone

Something you are: typically, a biometric, such as fingerprint, face, or iris recognition

Best practices for MFA implementations dictate that a solution combine at least two of these types of factors – for example, requiring that a knowledge-based factor such as a password is augmented with additional security by layering on one of these other factors.

Beyond these three categories, however, there is another way to split authentication technologies:

1. Those that are "shared secrets" – meaning that they are known by both the user trying to authenticate and the service provider requiring authentication. Passwords fall into

this category, but so do other "stronger" methods of authentication, such as SMS codes or One Time Password (OTP) tokens and apps.

2. Those that are not – instead requiring that each party have part of the solution needed to authenticate. This latter category generally relies on asymmetric, public-key cryptography

A fundamental tenet of authentication is that solutions that rely on shared secrets are less secure than ones that do not. This is because a shared secret can be compromised in ways that solutions using asymmetric approaches cannot.

SMS and OTP are both increasingly vulnerable today, as adversaries develop attack methods to compromise the technologies. Google is one of several firms who have recently flagged the extent of the problem, noting that these days, a "phisher can pretty successfully phish for an OTP just about as easily as they can a password" and noted their shift to hardware-based solutions using the FIDO Alliance specifications as the way to stop these targeted phishing attacks.[5]

Likewise NIST has proposed to deprecate use of SMS authentication in its latest version of SP 800-63-3, "Digital Authentication Guidance," due to a variety of documented weaknesses in use of SMS as a second factor.[6] For example, SMS texts can be redirected by malware, or by attacks on the SS7 network itself. Additionally, "SIM swap" attacks are increasingly being used to take over mobile phone accounts, with a key focus being to compromise the authentication codes sent out by many online service providers.[7]

The takeaway: any authentication solution that relies on the use of a "shared secret" – even one that is only good for a short time – is vulnerable to increasingly common and effective attacks. The market needs to move away from shared secrets toward other solutions. And as policymakers look to incent adoption of strong authentication, they need to make sure they are focusing on the right kind of strong authentication.

[5] Speech at 2015 Cloud Identity Summit, see https://www.youtube.com/watch?v=UBjEfpfZ8w0 Note that Google had previously tried to drive two-factor login by offering OTP through both SMS and a free OTP app based on the OATH protocol; these comments reflect their experience with this technology.
[6] See: http://nstic.blogs.govdelivery.com/2016/07/29/questionsand-buzz-surrounding-draft-nist-special-publication-800-63-3/
[7] https://www.wired.com/2016/06/even-ftcs-lead-technologist-can-get-hacked/

EIGHT KEY PRINCIPLES FOR POLICYMAKERS CONSIDERING AUTHENTICATION

With so many different types of authentication technologies – and so much churn in the marketplace – how should policymakers approach efforts to drive adoption of strong authentication? There are eight policy principles that, if followed, can help to ensure the success of authentication policy initiatives:

1. **Have a plan that explicitly addresses authentication.**

   While a sound approach to authentication is just one element of a proper approach to comprehensive cyber risk management, any cyber risk management initiative that does not include a focus on strong authentication is woefully incomplete.

   As this paper has documented, there simply is no other attack vector that matches the password in frequency or impact – a point made clear by the near-monthly news of a major breach caused by passwords causing major economic, security and privacy harm. Authentication needs to be explicitly called out as an area needing attention.

2. **Recognize the security limitations of shared secrets.**

   All MFA is not the same, and the problems with MFA solutions that rely on shared secrets for both authentication factors are becoming more apparent each year. Policymakers should understand the limitations of first-generation technologies that rely on shared secrets and look to incent adoption of more secure alternatives.

3. **To gain widespread adoption, authentication must be easy to use.**

   As a 2010 study detailed, "Poor usability of IT security presents a serious security vulnerability which can be exploited to compromise systems that are otherwise secure."[8]

   Poor usability has presented a particularly notable challenge with many first-generation authentication solutions, in that they required a user to "break stride" to log in – forcing them to not only enter a password, but then find another device – such as a mobile phone or hardware token – read a code off of it, and then enter that code in an application. These sorts of solutions degrade the user experience, and have the effect of dissuading people from using them. When presented with a poor user experience, users look to find ways around it.

   History has shown that when mandates are issued for authentication solutions that degrade the user experience, they tend to fall short of their goals, as implementers choose solutions that sacrifice security for usability. For example, a 2006 effort in the United States by the Federal Financial Institutions Examination Council (FFIEC) to drive use of stronger authentication recommended a number of highly secure MFA options, but also permitted

[8] http://folk.uio.no/josang/papers/APAJ2010-ICITIS.pdf

some simpler technologies that offered less security.[9] Nearly every U.S. bank chose these options instead of MFA.

There is good news on this front: the emergence of new, next-generation MFA solutions that are more secure than passwords – and also simpler to use – creates incentives for people to adopt them. Policymakers should focus on incenting use of these next-generation solutions that address both security and user experience.

4. **Understand that the old barriers to strong authentication no longer apply.**

Historically, some governments have shied away from efforts to require strong authentication, given concerns about the costs and burdens imposed by the technology.

For example, in 2015, the U.S. Department of Health and Human Services (HHS) chose to avoid setting new requirements for use of MFA in health systems, citing a commenter who "pointed out that current approaches to multi-factor authentication are costly and burdensome to implement."[10] While this statement may have been accurate when discussing "first generation" strong authentication technologies, the market has responded to address them. Today, there are hundreds of companies delivering next generation MFA that is stronger than passwords, simpler to use, and less expensive to deploy and manage.

There are two themes here at play:

1. Advances in product design that have helped to address the security vs. usability tradeoffs common to first-generation authentication – described in the principle above.

2. A move by most major computer and device manufacturers to embed new security capabilities as standard features in their products. These include:
   - Trusted Platform Modules (TPM) – embedded into most commercial laptops available today that run Windows
   - Trusted Execution Environment (TEE) – embedded into most Android phones
   - Secure Enclave (SE) technology – embedded into Apple smartphones

Each of these technologies serve as a hardware root of trust – isolated from the rest of the device – that can be used to generate cryptographic key pairs to authenticate to online service providers. This is a game-changer: it means that policymakers can begin to assume a world exists where most of the users in entities they oversee will have a COTS device in their hands or at their desks that can be used to deliver strong authentication without creating extra burdens on those users.

One industry initiative that has been key to delivering these solutions – and changing the old authentication paradigm – is the Fast Identity Online (FIDO) Alliance – a consortium of more than 250 members across the globe, including Microsoft, Google, PayPal, eBay, all major

[9] https://www.ffiec.gov/pdf/auth-its-final%206-22-11%20(ffiec%20formated).pdf
[10] https://www.regulations.gov/document?D=HHS_FRDOC_0001-0602

payment card networks, several major banks and health firms, and dozens of security vendors.[11]

The FIDO Alliance was launched in 2013 with a mission to change the nature of online authentication by developing open, interoperable specifications to supplant passwords and other first-generation authentication technologies with new solutions offering more security, privacy and usability.

FIDO standards were specifically architected to take advantage of these new embedded security features in devices, ensuring a simple, consistent authentication experience for users, regardless of device or platform.

In a typical deployment of these standards, a user swipes a finger, speaks a phrase, or looks at a camera on a device to login, pay for an item, or use another service. Behind the scenes on that device, the biometric is used as an initial factor to verify the user is the same person who registered the FIDO credentials with the service, then this verification unlocks the second factor used to communicate with the online service: a private cryptographic key that works “behind the scenes” to authenticate a user to the service by cryptographically "signing" the authentication request sent to the user's device.

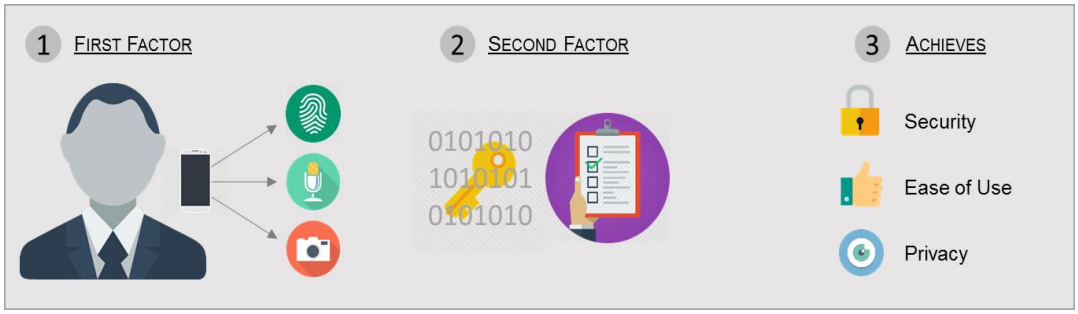


Figure 1: FIDO biometric-based deployment

The result of this innovative solution, already codified in emerging industry standards, is a truly multifactor authentication from a single user gesture. Since biometrics and cryptographic keys are stored on local devices and never sent across the network – eliminating shared secrets – user credentials are secure even if service providers get hacked, thereby eliminating the possibility of scalable data breaches and ensuring the privacy of the user's biometric information.

FIDO solutions can alternately be deployed via a standalone “security key” token that contains a chip similar to the secure hardware embedded in devices. With the security key architecture, a user can use a single token across several different devices and online services, leveraging common interfaces such as USB, NFC and Bluetooth.

[11] https://fidoalliance.org/

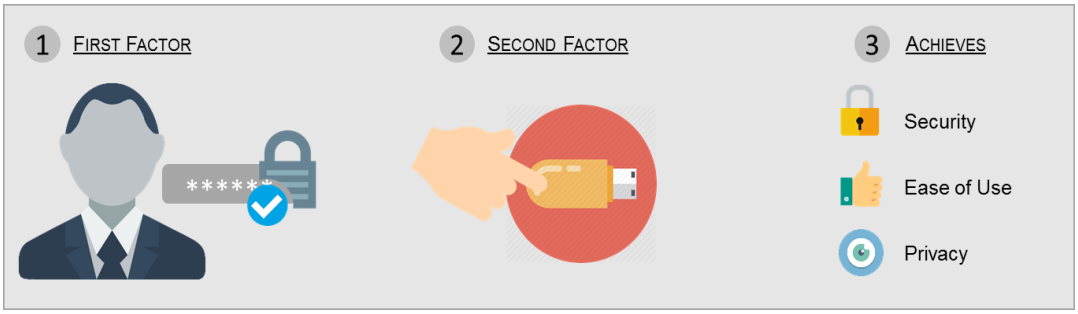


Figure 2: FIDO "security key" deployment

FIDO standards are currently being used to enable simpler, stronger authentication in offerings from Google, PayPal, Bank of America, Facebook, NTT DOCOMO, BC Card (Korea), Dropbox, GitHub, eBay, Samsung and other leading firms. In addition, Microsoft has designed its Windows 10 "Hello" product for passwordless login around FIDO standards. In each of these deployments, consumers and businesses do not have to know how the authentication works or why it's more secure – they are getting login experiences that are easier to use, with great security baked in behind the scenes.

The FIDO approach has been embraced by the World Wide Web Consortium (W3C), who is expected to finalize a formal "Web Authentication" standard built on FIDO specifications in 2017.[12] The emergence of this new standard, combined with the wide industry and government support of the growing FIDO ecosystem, makes it an important tool in efforts to improve authentication.

The FIDO approach is gaining plaudits from governments such as the United Kingdom, Germany, and the United States; its approach to authentication is also being recognized by entities such as the European Banking Authority (EBA), who, while not calling out FIDO by name, highlighted the combination of biometrics paired with a protected cryptographic key as an example of the type of solutions that will be permitted for authentication under Europe's new Payment Services Directive 2 (PSD2).[13] The EBA specifically focused on concerns around the "independence" of authentication elements inside a multi-purpose device such as a smartphone, laying out how "the implementation of separated trusted execution environments inside the multi-purpose device" could be used to ensure "that the breach of one of the elements does not compromise the reliability of the other elements."

The work of FIDO and industry efforts to embed better security capabilities directly in devices also features prominently in the United Kingdom's 2016 National Cyber Security Strategy.[14] The strategy focuses, in part, on ensuring that future online products and services coming into use are "secure by default," ensuring that users don't have to go to great lengths in order to enjoy strong protection.

[12] https://www.w3.org/Submission/2015/02/
[13] See the Directive 2015/2366 of the European Parliament and Council on Payment Services in the Internal Market at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366
[14] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Authentication plays a central role in the strategy, which states:

> *"[We will] invest in technologies like Trusted Platform Modules (TPM) and emerging industry standards such as Fast IDentity Online (FIDO), which do not rely on passwords for user authentication, but use the machine and other devices in the user's possession to authenticate. The Government will test innovative authentication mechanisms to demonstrate what they can offer, both in terms of security and overall user experience."*

5. **Authentication solutions must support mobile.**

The market is in the midst of a major shift where more and more consumer and enterprise transactions take place on a mobile device instead of a desktop. Consider:

- Mobile web adoption is growing 8 times faster than web adoption did in the 1990s and early 2000s.[15]
- By the end of 2017, over two billion mobile phone or tablet users will make some form of mobile commerce transaction.[16]
- By 2018, 25% of corporate data traffic will bypass the corporate network and flow direct from mobile device to the cloud.[17]
- 84% of people have experienced difficulty completing a mobile transaction.[18]
- 62% of "checkout abandonments" in mobile commerce happen due to friction in the login process.[19]

The impact of this on authentication is notable, as technologies and models that work well in desktop settings often do not translate well to the mobile environment. Thus, any policy which does not optimize use of MFA in the mobile environment will fail to adequately protect transactions conducted in that environment.

The good news is that mobile creates opportunity: the explosion of mobile devices is enabling many new ways to deliver strong MFA – often using technologies in the devices themselves. The increasing ubiquity of mobile phones containing both embedded hardware roots of trust (TPM/TEE/SE) and embedded biometric sensors means that the primitives to enable strong MFA are now baked in to these devices at the manufacturer.

For example, a smartphone that contains a secure hardware element can be used to generate cryptographic key pairs to authenticate to online service providers in a highly secure manner, protected from any malicious software that may have been installed on the phone by a remote attacker. Users can then use their biometric as a second factor to unlock access to those keys, with solutions that leverage the FIDO standards enabling interoperability across the ecosystem. Combined, the biometric and the cryptographic key allow for the delivery of

[15] http://resources.mobify.com/50-mobile-commerce-stats.html
[16] http://www.invespcro.com/blog/mobile-commerce/
[17] https://twitter.com/gartner_inc/status/481528221054169088
[18] http://www.outerboxdesign.com/web-design-articles/mobile-ecommerce-statistics
[19] http://resources.mobify.com/rs/946-QEC-409/images/Q3-2016-Mobile-Insights-Report.pdf

multiple, independent authentication elements in a single device, usable by a single user gesture – without a need to enter a password.

In the United States, the Commission on Enhancing National Cybersecurity highlighted the importance of FIDO to addressing mobile authentication challenges, noting: "FIDO specifications are focused largely on the mobile smartphone platform to deliver multifactor authentication to the masses, all based on industry standard public key cryptography," and highlighting that "today, organizations complying with FIDO specifications are able to deliver secure authentication technology on a wide range of devices, including mobile phones, USB keys, and near-field communications (NFC) and Bluetooth low energy (BLE) devices and wearables."[20]

6. **Privacy matters.**

Authentication solutions can vary greatly in their approach to privacy. Some embrace approaches that track or monitor a user's every move, or leverage centralized databases of biometric information. While these types of solutions may be appropriate for certain use cases, they also create privacy and security risks that must be mitigated.

Other solutions are architected with a "Privacy by Design" approach, delivering robust authentication without linking or tracking, and enabling transactions that offer both excellent security, as well as the possibility of anonymity or pseudonymity. Apple, for example, designed its Touch ID system so that biometric data is only stored on the device and cannot be exported to a central server. Likewise, solutions leveraging the FIDO standards are architected to ensure:

- No third party in the protocol
- No secrets on the server side
- Biometric data, if used, never leaves the device
- No link-ability between services or accounts

Privacy is not just a matter of risk management; privacy also weighs on the minds of consumers when considering which solutions to adopt, and can dissuade people from using stronger security. Thankfully, privacy and security do not have to be at odds with each other in authentication; standards such as FIDO are architected to improve both. Policymakers should look carefully at different authentication approaches to ensure that privacy is not unnecessarily degraded in the name of security.

7. **Biometrics are making authentication easier – but must be applied appropriately.**

The near-ubiquity of biometric sensors in mobile devices and laptops – such as fingerprint sensors and cameras (which can be used for both face and iris recognition) – is a boon to efforts to drive used of strong authentication. For years, any organization wanting to use biometrics – a "something you are" authentication factor – had to purchase a stand-alone biometrics solution, which created additional acquisition and integration costs and required

[20] https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

the enterprise to solve the problem of how to distribute these software capabilities to all their users' devices. But enterprises today can leverage the capabilities that are built in directly to all standard compliant devices with just one integration of standard compliant software within their infrastructure.

Biometrics alone do not provide multi-factor authentication, however. For this reason, biometrics are best used as one layer of a multi-factor solution. This approach ensures that if a biometric is somehow compromised, there are other layers of protection behind it.

For example, biometric solutions designed around FIDO Alliance standards use the biometric only as an initial factor to then unlock a second factor, in this case a private cryptographic key that is used to authenticate to a system through public key cryptography.

With FIDO, biometrics are only stored and matched on the device – and cannot be exported outside of the device – avoiding the need to address privacy and security risks associated with systems that store biometrics centrally. And by using biometrics as just one layer of a multi-factor authentication solution, implementers mitigate risks should an adversary look to steal biometrics or try to spoof a biometric system.

8. **Don't prescribe any single technology or solution – focus on standards and outcomes.**

The authentication industry is going through a wave of innovation, with dozens of novel new technologies hitting the marketplace each year. While some are better than others, the progress driven by innovation is a net positive for the industry. Moreover, it is clear that the state of the market today will not be state of the market five years from now.

For this reason, governments should focus on setting a principles-based approach to authentication policy that does not preclude the use of new technologies or modalities that were not anticipated at the time a policy was written.

An excellent case study demonstrating the problems with mandating specific technologies for authentication is the experience of South Korea. In 1999, South Korea created a policy mandating that any person who wants to use online financial services or payments had to obtain a digital certificate tied specifically to use of Internet Explorer and ActiveX controls.[21] At the time of its creation, the strong link to Internet Explorer was not a concern, given the dominance of that browser in the marketplace. But as the market evolved, South Korea quickly found itself locked into a platform that was not only limiting – given interest in using other browsers and platforms – but that also created notable cybersecurity risk.

South Korea has since found a way to migrate off of this platform; the Korean Internet Security Agency (KISA) has since embraced the FIDO specifications as part of a broader way to get to a more modern, vendor-neutral approach to authentication.[22] However, the country's lock-in to a single technology – as opposed to vendor-neutral solutions rooted in standards – meant that efforts to migrate to a more modern solution took many years and introduced significant levels of complexity.

[21] http://www.zdnet.com/article/south-korea-takes-another-step-to-activex-liberation/
[22] http://www.slideshare.net/FIDOAlliance/bioauthentication-fido-and-pki-trends-in-korea

In contrast, authentication policies that embrace the principles above will be flexible enough to ensure security and privacy are protected while also allowing innovation to flourish.

CONCLUSION

No technology or solution can completely eliminate the risk of a cyberattack, but adoption of modern, standards-compliant, multifactor authentication is one of the most impactful steps that can meaningfully reduce cyber risk.

Governments looking to drive more widespread adoption of MFA by embracing a principles-based policy approach – informed by the eight principles above – that offer better security and privacy, while also achieving the results of adoption without major burdens. Such as approach will ensure the best results in protection of consumers and businesses, as well as government systems, at a time of great innovation and technological change.

ABOUT THE CHERTOFF GROUP

The Chertoff Group is a premier global advisory firm that provides risk management, business strategy, and merchant banking advisory services. We apply our insights into technology, threat, and policy to help our clients improve their resiliency, build competitive advantage, and accelerate growth.

With a particular focus around security and technology, The Chertoff Group provides a broad array of professional services to help our clients at every stage of the business lifecycle. We leverage our deep subject matter knowledge around important policy matters and security operations to build and execute effective strategies that enable companies to capture new opportunities and create lasting competitive advantage. For those organizations that require tactical security support, we work hand-in-hand with clients to better understand today's threats and assess, mitigate and monitor potential dangers and evolving risks in order to create more secure environments for their business operations.

Headquartered in Washington D.C., The Chertoff Group maintains offices in Menlo Park and New York City. For more information about The Chertoff Group, visit www.chertoffgroup.com.