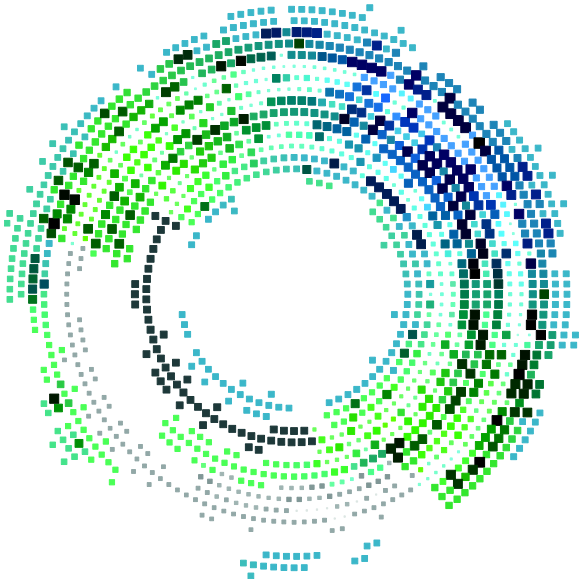
Deloitte.



Multi-factor authentication: A technology whose time has finally come

Raising the hurdles to cyberattacks

Major retail chains, banks, health insurers, major media companies, state and federal government agencies: All are recent victims of data breaches putting at risk confidential information in core operations, including the personal, health, or credit card information of millions of customers and citizens. Some 90% of today's data created in just the last two years,[1] and most companies and organizations know that the incentives to break into their data vaults will only increase with the continued rapid expansion of data created by mobile computing, cloud-based technology, big data and analytics, and the Internet of Things. The breaches can total millions of dollars per incident for both the immediate costs of repair and the less tangible costs to reputation, consumer confidence, credit ratings, and business operations that unfold over time.[2]

Though many organizations are aware of the high risks of cyber breaches, most are less aware of another key vulnerability they share: The majority of confirmed breaches are due to weak or stolen passwords.[3] Often overlooked is the need to fortify this front line of defense. The password is nearly ubiquitous as the primary access control to sensitive data, but its common failings are taken for granted as a part of the daily routine. Weak passwords, password sharing, and the reuse of passwords across multiple accounts make them an especially ineffective sentry at a time when critical data is ever more susceptible to attack. But a relatively simple and cost-effective fix is available today: The addition of a second, different credential to gain online access via multi-factor authentication (MFA). Given the high risks of attack and the availability of this mature solution, implementing MFA should be considered a priority for organizations.

MFA, by which users proffer at least two forms of identity to gain access, is not new. Yet, the time is ripe for widespread adoption. Smartphones and other technologies make it easier now to supply a second authentication factor. Indeed, with the widespread use of mobile devices, user-friendly, declining technology costs, and greater availability of skilled technical support, MFA should be a core part of enterprise cybersecurity strategy.

MFA can help companies meet their strategic priority of securing the critical information at the heart of their business value. No technology today will provide a 100% fail-safe system, but

MFA can significantly raise the obstacles for would-be attackers, thereby making your company a less attractive target. Strong authentication through MFA can also enhance the confidence of various corporate stakeholders and—most important—customers, consumers, partners, investors, and regulators.

Multi-factor authentication: more widespread, less costly

MFA is already familiar to many, whether for business or personal use. Forms of MFA include a password combined with authentication apps, the use of facial recognition, or fingerprint readers, for example. As consumers, many may already use MFA with online banking and other transactions. The user may type in his/her username and password on a laptop, for example, and then the bank sends a separate one-time code via text, voice call, or mobile app to his/her phone to enter on the laptop. Two-step verification, especially if performed over two separate devices, imposes a hurdle on any cyber attacker, who would have to have access to the user's phone, in addition to his/her password.

In the past, many enterprises refrained from adopting MFA due to the costs associated with an older generation of MFA technology. Issuing employees passcode-generating USB keys, for example, entailed the expense of the hardware itself, as well as the administrative costs of dealing with lost tokens. Today, most employees already carry a second device—a smartphone—over which a second authentication factor may be sent via authentication apps, helping to lower the costs of MFA. Moreover, less expensive software solutions can replace hardware tokens. Instead of each receiving a USB fob, for example, employees could just download a phone app to generate one-time passcodes. Indeed, the costs of cyberattack may result in significant, if not catastrophic, loss of business, productivity, and trust among key stakeholders for small, medium, and big businesses alike.

Multi-factor authentication: stepping up from username and password

Today, most consumers and workers use a password to gain online access to their accounts and networks. They often use the same password for multiple accounts, share passwords, and misuse them in other ways, compromising security. Instead, using two or more types of factors to provide credentials for online access, referred to as "multi-factor authentication," can provide stronger security.

An extra layer of protection comes when the two factors required for authentication are delivered over two separate devices, such as a laptop and a smart phone. The factors can take the form not only of something you know, such as a password, but also something you have, such as a token, or some aspect of who you are, such as a fingerprint or iris pattern. Some examples follow on the next page.

Avoiding pitfalls in implementation

Implementing any new technology involves challenges. For MFA, the technology, for the most part, is mature and tested; the greater hurdles lie instead in user acceptance and system design that fails to anticipate user needs and potential aggregate costs. Careful strategic planning prior to implementation can help enterprises avoid these traps. Below are some issues to consider:

Winning hearts and minds: Users want a seamless online experience. Many view even the use of the password as a time-consuming annoyance to access the online databases they want at their fingertips. The request for a second credential may be viewed as bothersome. With MFA, choosing authentication technologies that are intuitive and easy to use by the target user is essential, such as the familiar fingerprint swipe. In addition, educational outreach to users ahead of implementation on the importance of data security, the advantages of MFA, and usage instructions can help pave the path for a more successful uptake.

Tailoring to users' needs: Matching the type of MFA authentication technology to the actual needs of an organization's users will help boost acceptance. For instance, sales people on the road requiring access to their corporate databases may find authentication apps via smartphones a convenient solution, while a doctor accessing a database during a patient visit may not have time to pull out a smart phone and instead may prefer a quick fingerprint swipe.

Containing costs: Though newer MFA options such as authentication apps, fingerprint readers, and software solutions, are less costly than earlier generations of hardware solutions, expenses can still snowball if organizations do not take care in the design of the new systems. Texting can cost just one cent per use, but multiplied several times a day over thousands of users, the expense grows quickly. Thus, organizations benefit by taking a risk-based approach, identifying the most critical databases requiring stronger security, such as those containing strategic business, financial, and personally identifiable information, and implementing MFA for access to those areas. In contrast, they need not require MFA for users to access to non-sensitive information, such as the company holiday calendar or public press releases.

Protecting privileged users: Companies can take the risk-based approach one step further to provide more security even more cost-effectively by implementing MFA for a subset of users such as

What You Know

Passwords, used since ancient times:

Pythagoras, the great mathematician, employed passwords to distinguish true followers from political foes. Prohibition-era speakeasies required passwords for admission. The first documented computer password was used at the Massachusetts Institute of Technology's time-sharing system in 1963.

What You Have

Hardware and software tokens:

Hardware USB keys enable workers to log on by entering their user name and password and then a random passcode generated by the fob at set intervals of time. Software tokens operate similarly, where an app downloaded on a smart phone, for example, generates the codes.

Who You Are

Biometrics, such as fingerprint, face, iris, and voice recognition:

For time-pressed workers, biometrics is fast and convenient. Rather than remembering and entering a complex password, users merely present something that is part of them, whether a quick fingerprint swipe, gaze into the computer camera, or vocal instruction to the computer voice recorder.

administrator-level users. Such users, equipped with elevated access privileges to the most critical databases, are a prized target of hackers. These users have the authority to alter and remove data, access transactions data, change user privileges, and other powerful functions, and their accounts provide a gateway for attackers to navigate more easily throughout the network, potentially causing catastrophic damage. Converting privileged users to MFA can be an end goal in itself or a first step in a phased plan to implement MFA across the board.

With cyber breaches on the incline and ever more critical data at risk, companies and organizations cannot afford to ignore solutions, such as multi-factor authentication. Where password vulnerability is a leading cause of breaches, requiring a second credential for access to key databases helps fortify one of the weakest links in data security. That the technology is tested and available at relatively manageable costs means MFA is at the ready to protect companies and organizations that have the know-how to put this solution to best use.

[1] Åse Dragland, "Big Data--For Better or Worse," Sintef, May 22, 2013, accessed June 3, 2016, http://www.sintef.no/en/latest-news/big-data--for-better-or-worse/
[2] *Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts*, Deloitte 2016.
[3] 63% of confirmed data breaches involved weak, default, or stolen passwords, according to *2016 Data Breach Investigation Report*, Verizon, 2016, 20.

Take action today!
Request a briefing.

Deloitte Advisory Contacts

Emily Mossburg
Principal | Deloitte Advisory
Deloitte & Touche LLP
emossburg@deloitte.com

Mike Wyatt
Managing Director | Deloitte Advisory
Deloitte & Touche LLP
miwyatt@deloitte.com

David Mapgaonkar
Principal | Deloitte Advisory
Deloitte & Touche LLP
dmapgaonkar@deloitte.com

Rahul Kohli
Managing Director | Deloitte Advisory
Deloitte & Touche LLP
rahkohli@deloitte.com

Secure.Vigilant.Resilient.™

To grow, streamline, and innovate, many organizations have difficulty keeping pace with the evolution of cyber threats. The traditional discipline of IT security, isolated from a more comprehensive risk-based approach, may no longer be enough to protect you. Through the lens of what's most important to your organization, you must invest in cost-justified security controls to protect your most important assets, and focus equal or greater effort on gaining more insight into threats, and responding more effectively to reduce their impact. A *Secure.Vigilant.Resilient.* cyber risk program can help you become more confident in your ability to reap the value of your strategic investments.

BEING SECURE means having risk focused defenses around what matters most to your mission.

BEING VIGILANT means having threat awareness to know when a compromise has occurred or may be imminent.

BEING RESILIENT means having the ability to regain ground when an incident does occur.