CYBERSECURITY THREATS:
Companies Need Multi-factor Authentication to Keep Employees Safe

Payroll Network℠
Simplifying Human Capital Management

Authors: Nick Holcomb and Eric Whisenhunt

While the migration of business applications to cloud-based platforms has been a boon for businesses, exposure to cybercrime has spiked dramatically. Employees have vastly better access to systems and data, and at the same time, hackers are developing more sophisticated schemes to steal whatever they can get their hands on.

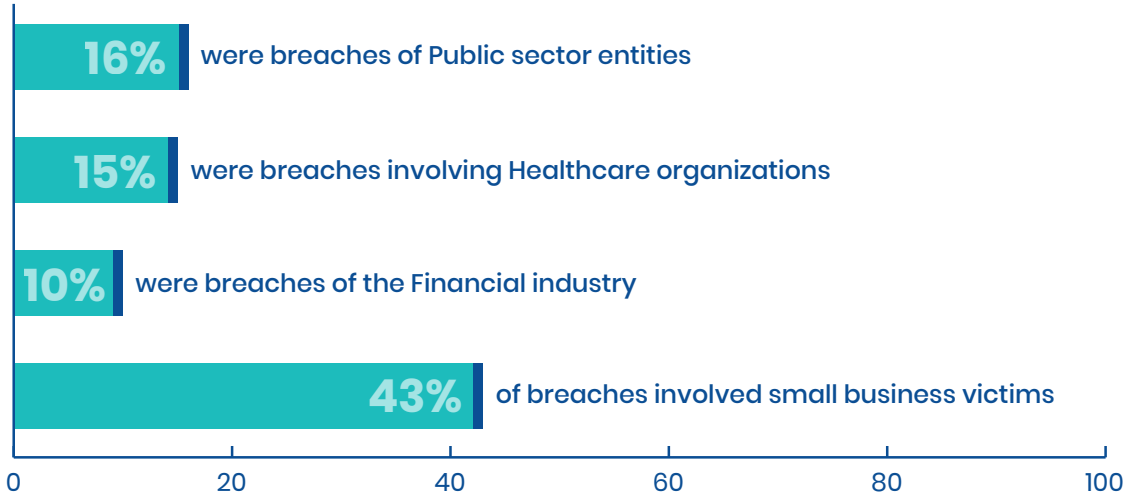
Companies have significantly reduced capital investment requirements and ongoing maintenance for IT infrastructure. Server-based local area networks are fading into history for small and medium-sized businesses (SMBs). Organizations whose IT systems are entirely cloud-based are becoming the new norm.

Easier accessibility, less maintenance, no upfront costs – these are the benefits that are driving the migration to cloud-based applications. So, what's the downside? Vulnerable IT security.

IT SECURITY BREACHES SPIKE

Most organizations have already conducted their cost/benefit analysis and decided to move forward with cloud-based systems. The major adjustment, often unexpected by business owners, is the increased need for better IT security. Data breaches continue to make headlines around the world. It is striking that no matter what defensive measures security professionals put in place, attackers circumvent them. No organization is too large or too small to fall victim to a data breach. According to the 2019 Verizon Data Breach Investigations Report,[1] 43% of data breaches in 2019 involved small business victims.

Who are the IT Security Breach Victims?



Don't Be a Data Breach Victim

No industry vertical is immune from attack. Regardless of the type or amount of your organization's data, there is someone out there trying to steal it. Having a sound understanding of the security threats you face, how they have evolved and which tactics are most likely to be utilized, can enable you to prepare to manage these risks more effectively and efficiently. Today's online environment calls for additional layers of verification, and multi-factor authentication (MFA) is where it begins.

What is Multi-Factor Authentication?

MFA is a method of logon verification where at least two different factors of proof of identity are required, such as when employers ask for a photo ID and Social Security Number during the hiring process. MFA protects your data (email, financial accounts, health records, assets, etc.) by adding an extra layer of security. Once a user enters their username and password, the online system prompts the user for a second form of authentication.

3 Types of Multi-factor Authentication

There are three recognized types of authentication factors, according to Global Knowledge[2]:

- **Type 1 – Something You Know** – includes passwords, PINs, combinations and code words. Anything that you can remember and then type, say, do, perform, or otherwise recall when needed falls into this category.
- **Type 2 – Something You Have** – includes all items that are physical objects, such as keys, smart phones, smart cards, USB drives and token devices.
- **Type 3 – Something You Are** – includes any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans and voice verification.

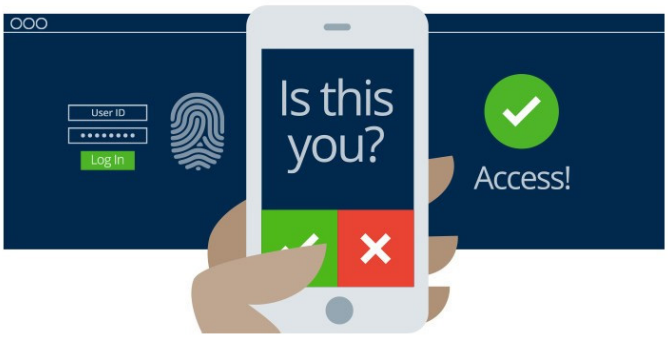
Multi-Factor Authentication Methods

The most common form of secondary authentication is a 6-digit code that is sent as a text to the user's phone. Another option is to use a phone-based Authenticator App that generates a code every 30 seconds. The code must be entered on the login screen to gain access.

The idea behind MFA is that even if someone accidently falls for a phishing attack and unwittingly gives away their username and password to an application, such as email, the hacker cannot access the online application by only possessing the stolen credentials. They must also be in possession of the compromised user's mobile phone.

This second step in the authentication process drastically reduces the success rate of hacking attempts of online applications. But it is not foolproof.

To make their apps more user friendly, authenticator apps have alternative ways to be configured instead of having to input a 6-digit code. One method is to send a text that allows the user to select "Approve" directly from the phone app. Another method is an automated voice call is made to the user. They can approve the login request by pressing the pound key (#). This saves the time and hassle of entering the code directly into the online application.



Sounds like a good idea, right? However, what if the end-user is multitasking and receives a notification to approve access to an online application, and they are not paying close attention? They then press the approve button or pound key. Now the hacker has access to the online account. Whoops! That's not what developers of Authentication Apps had in mind!

Be sure that your MFA is configured so that the user is required to input their authorization code on the login screen. This will prevent them from inadvertently approving an authorized login request.

OPTIMIZING MICROSOFT OFFICE 365

In addition to setting and forgetting MFA for cloud-based email, the following features can be modified in Microsoft Office 365 by an administrator to strengthen security.

1. **Disable MFA App Notifications.** By default, Office 365 allows MFA to occur via app notification. The issue with this method is that it does not require the end-user to input authorization codes. Requiring users to key in the code versus simply approving an app notification is more secure. The ability to send notifications can be disabled for the Microsoft authenticator app.
2. **Disable Web Access to Email.** Do your employees need it? If not, browser-based email access can be completely disabled. It can also be disabled for most users and allowed only for a select few who actually use the feature and benefit from it. Disabling online access to email, combined with MFA, is a strong barrier to prevent hacking. Almost all email hacking is conducted by hackers accessing the compromised email account via a web browser. By closing this access method, breaching the system becomes significantly more difficult.
3. **Lock Down Email in Azure AD.** For Microsoft Azure AD users, a policy can be created to lock down email access. If a device isn't recognized by Azure AD, which would be the case for a hacker using their own device, that's the end of the line. This policy combines device and identity security to provide maximum protection. For example, access could be restricted to only company issued equipment and pre-approved mobile phones.

BEYOND MFA FOR OTHER ONLINE APPLICATIONS

For other types of cloud-based applications beside email, your best bet is to check with the application provider to learn more about other levels of security available to implement. In addition to user authentication, ask about device authentication or geographical restrictions. Remember, the goal is to combine multiple levels of user authentication with other types of authentication. For example, if you don't need access to an application outside of North America, ask about restricting geographical access. If there is a way to restrict access based on device authentication, that is a feature you want to consider enabling.

Conclusion

According to *Harvard Business Review*[3], the big picture here is that no single method of authentication will always be suited for every situation. Sooner rather than later, companies should adopt a risk-based approach that uses MFA, taking into account location, behavior analytics, and numerous other indicators of identity. Another type of authentication gaining momentum is biometrics. The most common types of biometric authentication include fingerprint scans, facial or retina scans and voice recognition. As technology advances, and attackers get more aggressive, organizations must be vigilant and utilize MFA to protect both employees and assets.

Nick Holcomb is the Chief Technology Officer for Payroll Network, a premier HCM provider that brings together key workforce functions in one robust, easy-to-use platform. Nick has more than 20 years background in cybersecurity and 15 years of payroll/HR industry experience.

Eric Whisenhunt is a Principal with Computer Showcase, an IT solutions provider offering strategic consulting, managed services, and cloud solutions. Eric has been helping organizations embrace new technologies to improve capability, efficiency, and data security for more than 25 years.

1 https://enterprise.verizon.com/resources/reports/dbir/
2 https://hbr.org/2017/11/companies-need-more-than-two-factor-authentication-to-keep-users-safe
3 https://www.globalknowledge.com/us-en/resources/resource-library/articles/the-three-types-of-multi-factor-authentication-mfa/