Let’s Talk Multi Factor Authentication

Benjamin Hendricks

IT Director, Wood County

What is Multi Factor Authentication (MFA)?

Multi-factor authentication (MFA) is a security mechanism that requires someone to provide two or more forms of identification before accessing an account or system. This is done to ensure that the person is who they claim to be and to prevent unauthorized access.

MFA can be implemented in various ways, you may already be familiar with a password and a fingerprint (smartphone), a password and a one-time-passcode (secure banking/credit card), or a password and facial recognition (smartphone).

Today, passwords can be easily stolen. We are becoming all too familiar with social media posts like “my account got hacked” or random emails with “Invoice attached” from someone you know. If someone does gain access to your password, they still need the additional MFA information to gain access to an account.

What do you need to implement MFA?

Technology to manage MFA when accessing protected resources. This could be a centralized system connected to your accounts, or it could be as simple as licensing to enable MFA on accounts you already have. Here are some key providers:

Microsoft, BIO-Key, DUO, RSA, Okta, Yubikey, etc…

Some acceptable MFA technologies that can work with the following are recommended:

Biometrics (fingerprint or facial recognition)
Smartphone App – Google Authenticator, Microsoft Authenticator, DUO, etc…
Keychain one-time-passcode (OTP) token device
Yubikey or similar USB device connected to the computer
ID Badge or key fob device used on secure doors
Pattern (weaker option than above)
Question/Answer (weaker option than above)

What do you need to implement MFA? (cont’d)

What about the text messaging? Why is that not a valid option? I use it today with my banking/credit card website.

The communication between your phone and the cell tower is not secure, which would allow for someone to intercept that text and use it. There are some insurance carriers today that may not accept that method as a good option.

The key is to an acceptable MFA solution is to use methods that are difficult to guess, impersonate, or copy.

Wood County’s MFA Project…

One major hurdle to a successful MFA system is employee acceptance. Some employees may not permit the use of an app on their personal smartphone, or they didn’t own a smartphone.

Via a Request for Proposal (RFP) process, Wood County selected a managed authentication provider that could accommodate a mix of MFA methods.

Biometrics (fingerprint or facial recognition)

Smartphone App – Google Authenticator, Microsoft Authenticator, DUO, etc…

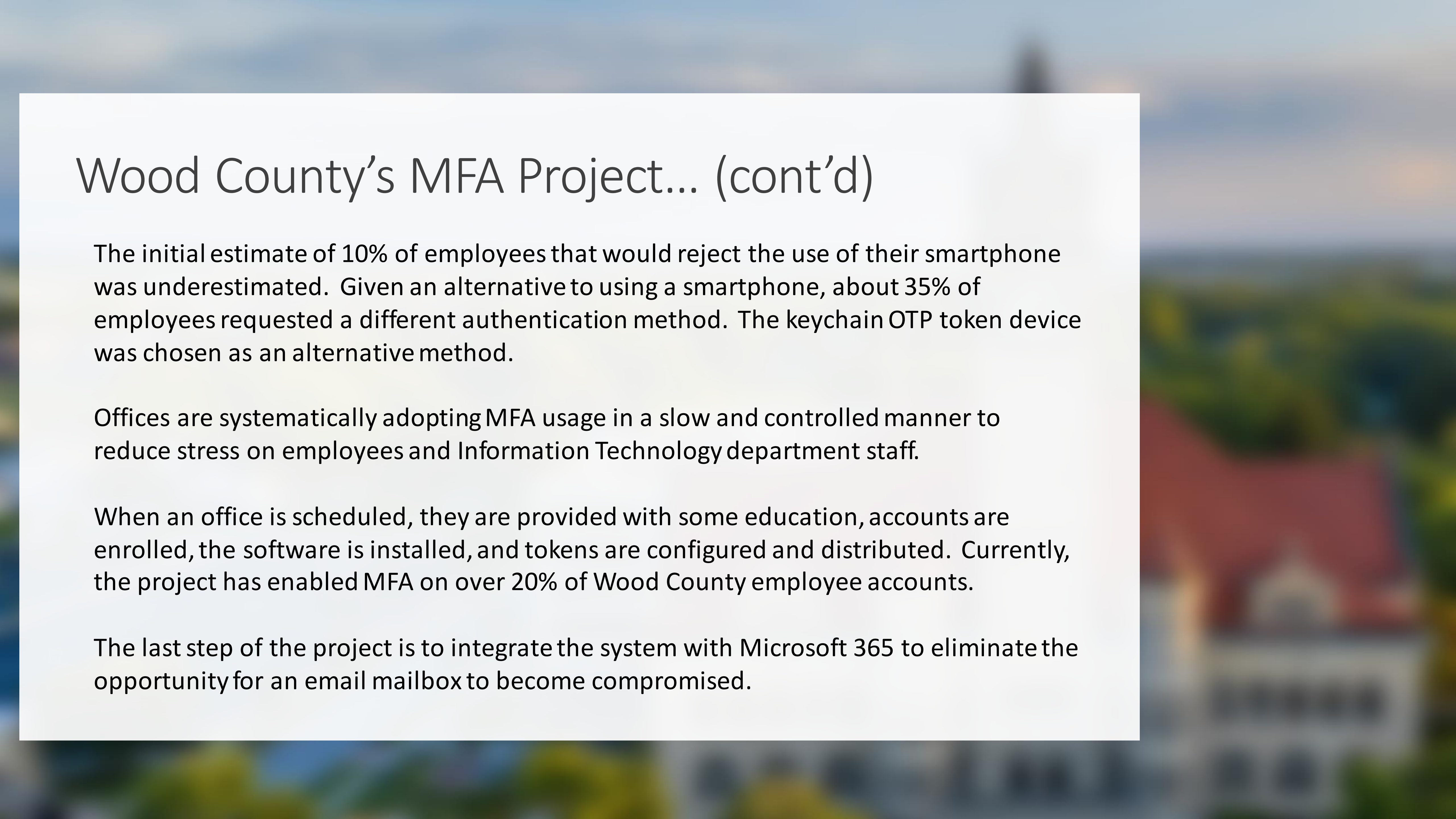
Keychain one-time-passcode (OTP) token device

Yubikey or similar USB device connected to the computer

ID badge or key fob device used on secure doors

Pattern (weaker option than above)

The system also needed to monitor an account’s last known location. That eliminates the ability for a stolen smartphone, door fob, or keychain OTP token from working.



Wood County’s MFA Project… (cont’d)

The initial estimate of 10% of employees that would reject the use of their smartphone was underestimated. Given an alternative to using a smartphone, about 35% of employees requested a different authentication method. The keychain OTP token device was chosen as an alternative method.

Offices are systematically adopting MFA usage in a slow and controlled manner to reduce stress on employees and Information Technology department staff.

When an office is scheduled, they are provided with some education, accounts are enrolled, the software is installed, and tokens are configured and distributed. Currently, the project has enabled MFA on over 20% of Wood County employee accounts.

The last step of the project is to integrate the system with Microsoft 365 to eliminate the opportunity for an email mailbox to become compromised.

Questions?