The 101:
Multi-factor Authentication. Unpacked.
Today’s Presenter

Kimberly Biddings
VP of Product
BIO-key International

• +10 years in cybersecurity
• Helped hundreds of customers understand & implement MFA
• Presented at:
  • NYSAC Legislative Conference – Cybersecurity Workshop
  • NACo CIO Forum & Annual Conference
  • NACo Tech Exchange webinars
Why are we talking about MFA?
The cybersecurity landscape

• **Every 39 seconds** there is a new cyberattack somewhere on the web

• **Over 4,000 ransomware attacks** take place around the world daily

• **A 300% increase in cybercrime reports** since the COVID pandemic was noted by the FBI

• **The average cyber insurance premium rose 25%** since 2021, with some policyholders paying over an 80% higher rate in 2022
Attacks on counties of all sizes

• **NJ county hit by ransomware** – marks the 22nd US state or local government hit by ransomware in 2022
  ~340,000 population

• Hackers accessed/acquired resident’s personal information from NY county services – residents told to check their credit reports closely
  ~1.5m population

• Services limited for 3 weeks, and county employee & resident data compromised after ransomware attack in CO county
  ~49,000 population

• In 2016, one of first ransomware attacks on TN county 911 call center had staff using pencil & paper for 3 days
  ~32,000 population
On September 16, 2022, the Department of Homeland Security (DHS) announced a first-of-its-kind cybersecurity grant program specifically for state, local, and territorial (SLT) governments across the country.

Current closing date for applications: Nov 15, 2022

**Required for DHS Cybersecurity Grant Program**

**Required Elements**

If there are any existing plans that meet the required elements, references to them may be used in lieu of incorporating them in their entirety. The Cybersecurity Plan must describe, to the extent practicable, how the state plans to address the below elements. The Cybersecurity Plan is a strategic document, looking broadly across the entire jurisdiction. The description should support the vision, mission and other strategic guidance set by the Cybersecurity Planning Committee.

1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below.

The following cybersecurity best practices under required element 5 must be included in each eligible entity's Cybersecurity Plan:

- Implement multi-factor authentication;
- Implement enhanced logging;
- Data encryption for data at rest and in transit;
- End use of unsupported/end of life software and hardware that are accessible from the internet;
MFA can prevent up to 90% of cyberattacks.

POLL QUESTION
Do you have MFA in place today?

We have MFA in place for:
A. All access
B. Some access
C. We do not have MFA
D. I’m not sure
What is MFA?
noun: **identity** ; plural noun: **identities**
1. the fact of being who or what a person or thing is.

noun: **authentication** ; plural noun: **authentications**
1. the process or action of proving or showing something to be true, genuine, or valid.

**MULTI-FACTOR AUTHENTICATION**

Using multiple authentication methods to prove you are who you say you are.
01 Something You ARE
- Fingerprint, Face, Palm

02 Something You HAVE
- Smart Card, USB Token, RFID Badge, USB Dongle, Phone, PC

03 Something You KNOW
- Password, PIN, Security Questions

Multi-Factor Authentication
E.g., PIN, Face, & ID Badge

Two-Factor Authentication
E.g., PIN and Face

E.g., PIN, Face, & ID Badge

Password, PIN, Security Questions

Smart Card, USB Token, RFID Badge, USB Dongle, Phone, PC
APPLICATIONS

Outlook

Domain/user name:

Password:

sign in

Hi, Michael

Accounts

Checking

$3,123.39
available

Transactions

YOUR TOWN CINEMA

$7.50

GREEN'S BIRD & PEAR

$87.50

YOUR TOWN CINEMA

$7.50

Servers

Here

There

Everywhere

Desktops
How do you implement MFA?
5 critical steps to implementing MFA

1. Assess Your Situation
   Cyber risk, users, & compliance/insurance

2. Pick Your Authentication Methods
   Give users enough choices & flexibility

3. Define Your Security Policies
   Down to the group, OU, or individual

4. Communication Strategy
   Change management at all levels

5. Phased Rollout & User Adoption
   Keep track of user satisfaction
How do you know what authentication you should use?

THE PERSON

HOW THEY WORK

WHAT’S REQUIRED

WHAT THEY ACCESS
Analyzed each method for:

- Security
- Convenience / Ease of Use
- Total Cost
- Effort of Implementation
- Ongoing Maintenance
- Phone-based or Not
Your cybersecurity policy outlines your guidelines and provisions for preserving the security of your county’s data and technology infrastructure.
Communication is key – use “Cyber Champions” to lead the way.
5 Steps to Communicating Effectively

1. Define your goals
2. Know your audience & their motivation
3. Focus messaging on the “why”
4. Have a clear Call-to-Action
5. Use an omnichannel approach
Cybersecurity is an ongoing journey with multiple chapters.
BIO-key PortalGuard
An award-winning platform to secure access for Employees, Citizens, & Suppliers

Multi-factor Authentication (MFA)
Wide range of authentication methods for flexible, powerful identity security

Identity-Bound Biometrics
Unique, centralized biometric identity that can be used to verify the person

Single Sign-on (SSO)
Reduce password prompts and secure access to all apps from single IdP

MobileAuth
Multi-factor authentication app that offers Identity-Bound Biometric authentication options & push tokens

Self-service Password Reset (SSPR)
Reduce password-related IT support calls by up to 95%

Hardware Devices
Offer a variety of devices including Microsoft-qualified Windows Hello USB fingerprint scanners & FIDO-keys
Learn more:

Ranking Authentication Methods eBook

Questions?

Try PortalGuard & MFA OR Contact Us to schedule a discovery call
Thank You

Kimberly.biddings@bio-key.com

www.BIO-key.com