Surviving a Hack

Hello!

Michael Rosenberg

Project & Communications Coordinator

Western Arkansas Planning & Development District

Overview

- About WAPDD

- So, What Happened?
- Our Old Structure
- Restoring the Data
- The Move
- Going Forward

Who is WAPDD?

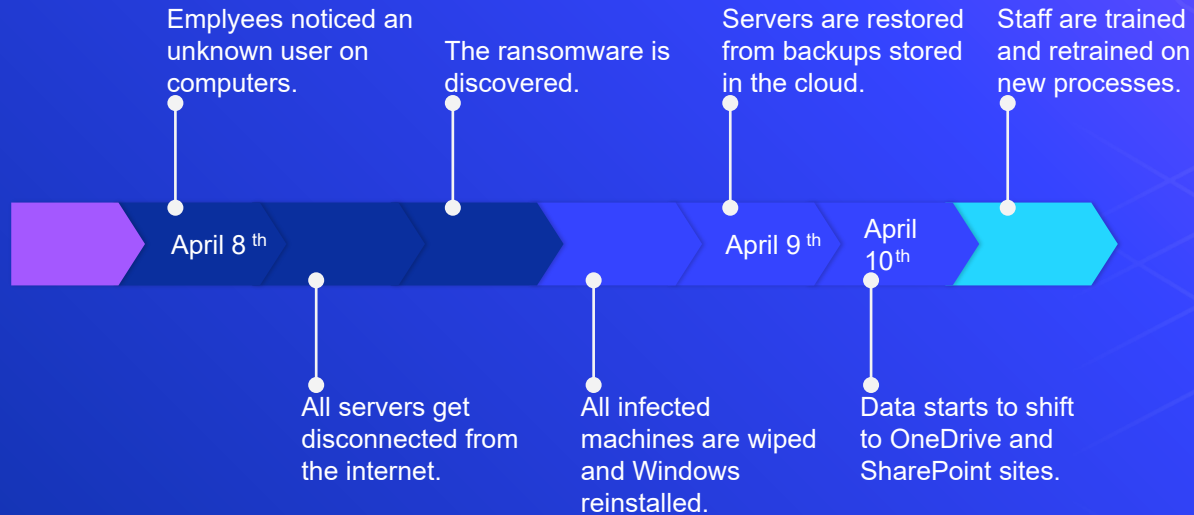Western Arkansas Planning & Development District

Where we are located…

Departments

- 911/Geographic Information Systems (GIS)
- Community Development
- Economic Development
- Frontier Metropolitan Planning Organization (MPO)
- Workforce Development
- Western Arkansas Intermodal Authority (WAIA) Contract

So what happened??

Timeline

Emplyees noticed an unknown user on computers.

The ransomware is discovered.

Servers are restored from backups stored in the cloud.

Staff are trained and retrained on new processes.

April 8 th

April 9 th

April 10th

All servers get disconnected from the internet.

All infected machines are wiped and Windows reinstalled.

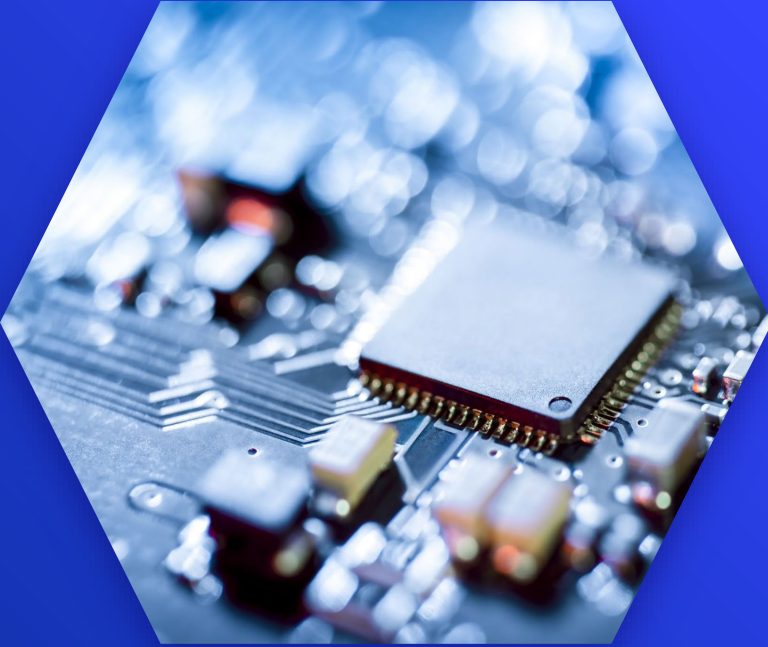Data starts to shift to OneDrive and SharePoint sites.

8

Our Old Structure

How we were doing business pre-hack.

How we stored data

- NAS (Network Attached Storage)
- Cloud Backup
- Most users not using OneDrive, etc.

IT Infrastructure

- ⬡ Locally managed users
- ⬡ Email has been migrated to Microsoft 365 (non ‑profit)
- ⬡ Data stored locally with a cloud backup
- ⬡ Few employees using OneDrive

How did we restore the data?

Backup off -site

- Most data was recovered up to the day before the attack.

- Some backed updata was corrupted and had to be destroyed.

Users already on OneDrive

- Users retained all data.

- Any corrupted data was rolled back to the hour before it was infected.

12

The Move

Taking our data to the cloud.

Migrating to the cloud

- Utilizing Teams/SharePoint for shared resources
- OneDrive Backups
- Azure Active Directory

Going Forward

Embracing the

Microsoft 365 Platform

Microsoft 365

Azure Active Directory

- Cloud Based
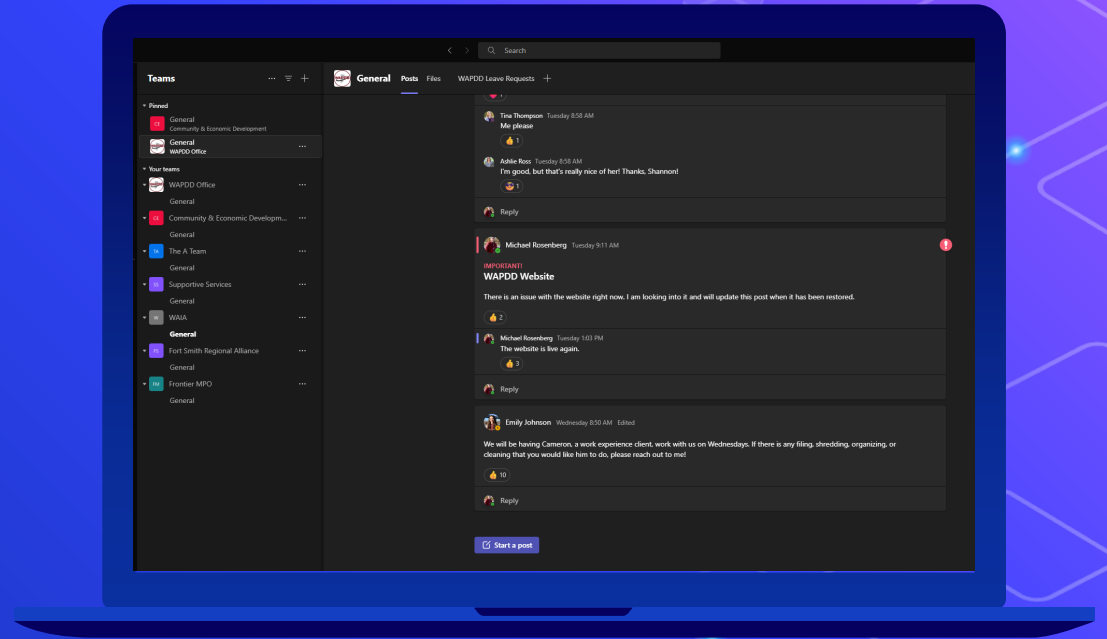- Single Sign -On
- Multi -Factor Authentication

Teams/SharePoint

- Collaboration Platform
- Centralized location to communicate and collaborate
- Improved efficiency
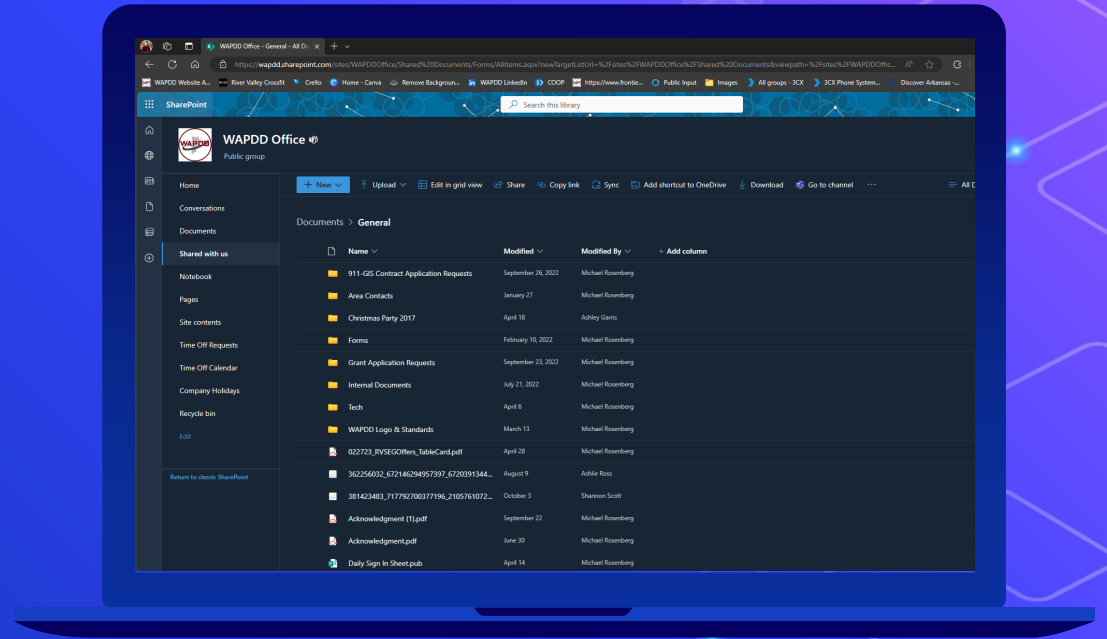- Has enabled the development of in - house PowerApps

OneDrive

- Cloud based secure storage
- Employees can access their data anywhere
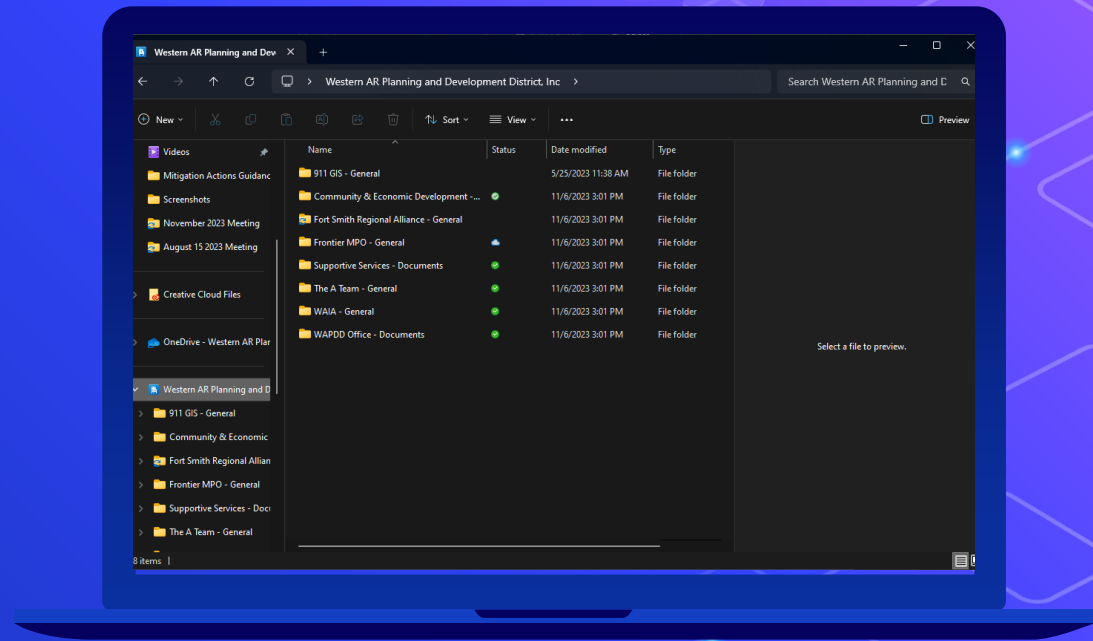- Works with all other Microsoft 365 services

Microsoft Teams

Office

SharePoint

File

Structure

Custom PowerApps

" Times of adversity often bring about the best changes. "

Thanks!

Any questions?

You can reach me at:

mrosenberg@wapdd.org

CYBER CASE STUDY

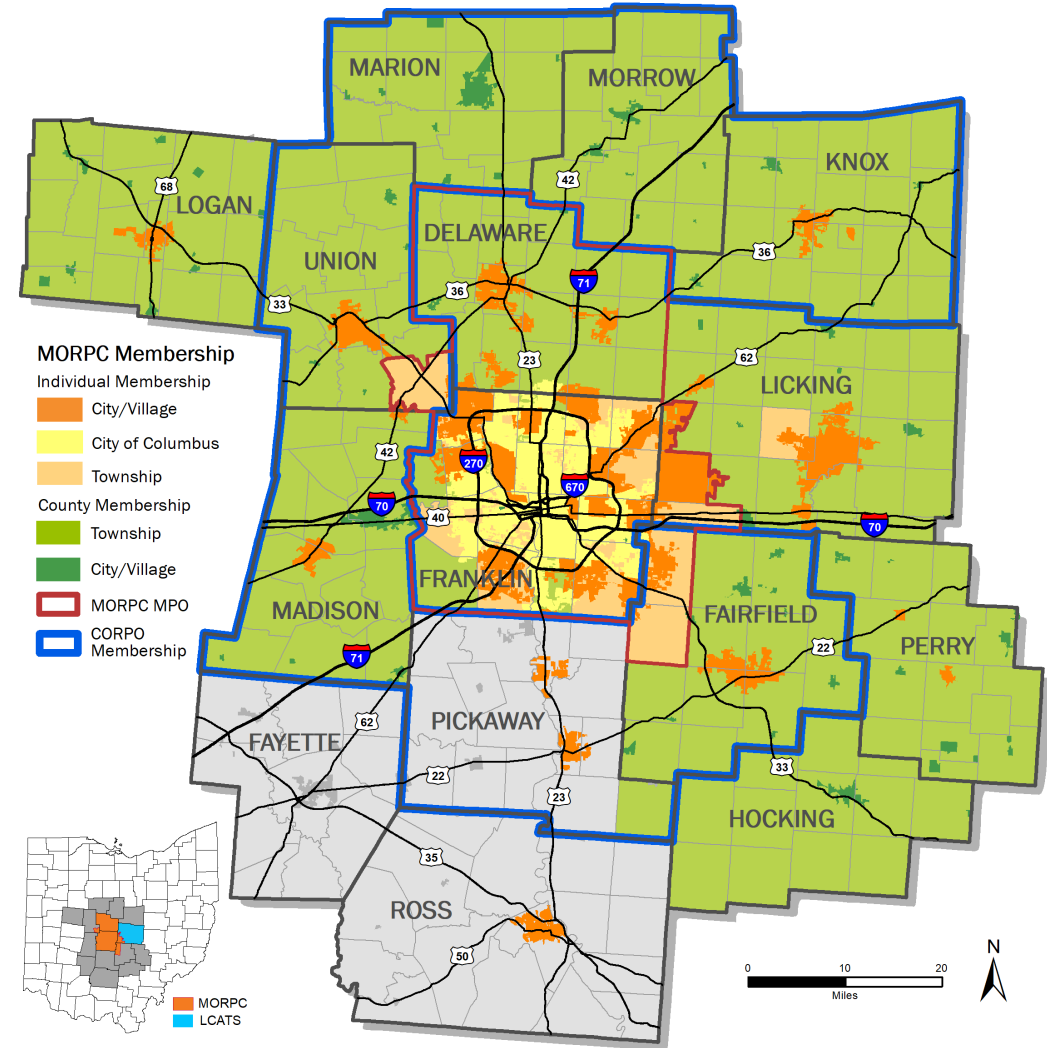Shawn Hufstedler, Chief Operating Officer

MID-OHIO REGIONAL
MORPC
PLANNING COMMISSION

ABOUT MORPC

- 85 members across 15 counties

- Drives the future prosperity and sustainability of the Central Ohio region

- Provides nonpartisan data analysis, community resources and long-range planning

MORPC

THE EVENT

- Sophisticated ransomware cyber attack

- Network penetration through compromised employee credentials

- Traditional ransomware approach – capture data and encrypt.

THE GOOD

Cyber Insurance

Most data is public

Backups

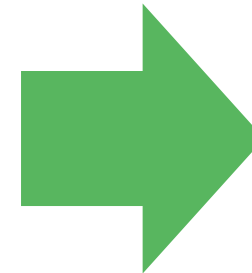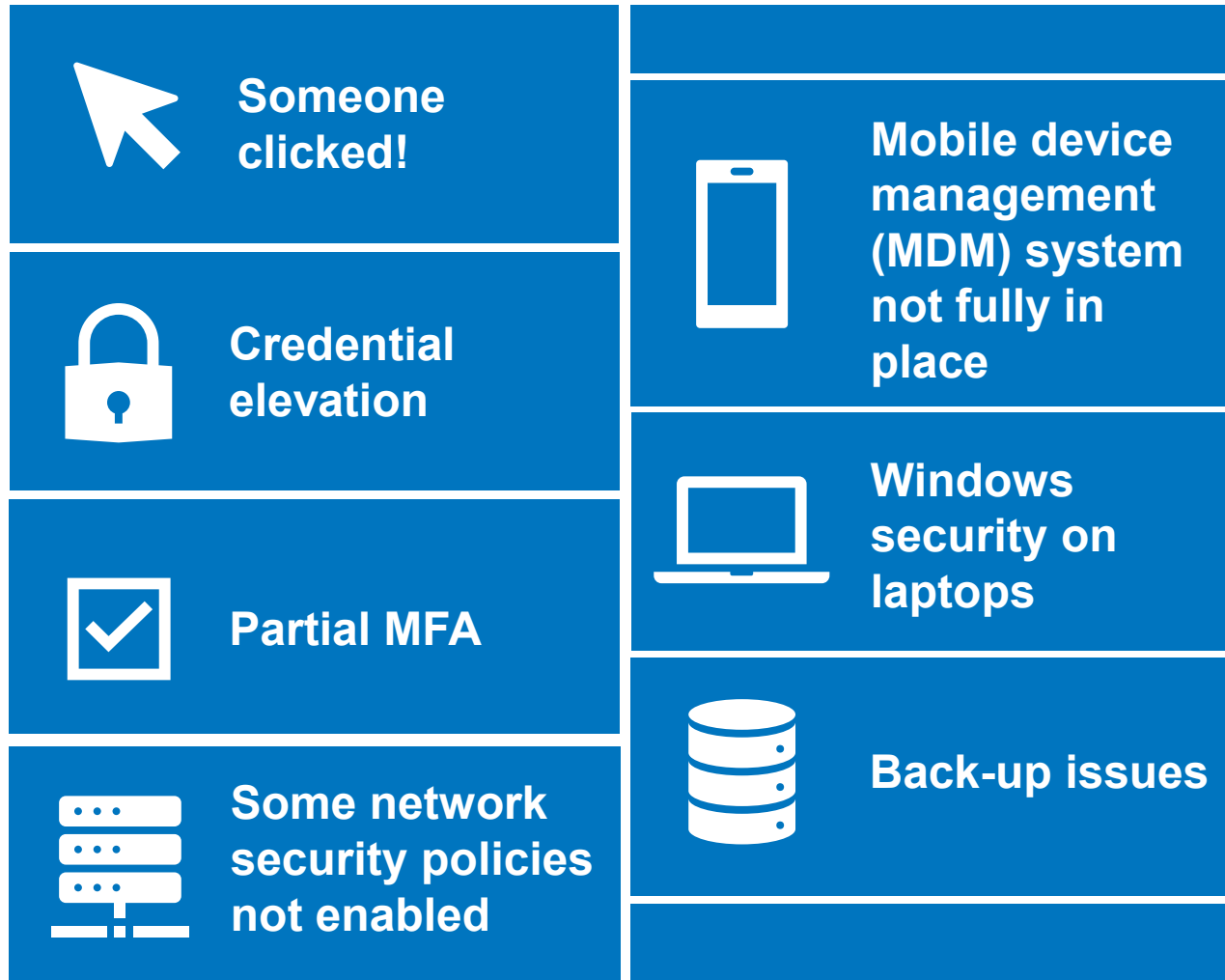**End-point protection**

Cloud-based software

Progressive network improvement over the years

Ability to continue the majority of work

THE BAD

Someone clicked!

Credential elevation

Partial MFA

Some network security policies not enabled

Mobile device management (MDM) system not fully in place

Windows security on laptops

Back-up issues

Productivity Loss

Ransom

More Risk

MOVING FORWARD

- Full MFA and additional Microsoft security policy implementation.
- Upgrades and enhancements
- 3rd party IT service – monitoring; testing
- End Point protection upgrade
- IT focused alerts and dashboards
- Microsoft Intune (MDM for mobile devices)
- Enhanced/restructured IT Team
- Actively engaging with state and local security experts
- Enhanced all staff cybersecurity training and internal communications
- More focus on cybersecurity
- Continued cyber-insurance

SHAWN HUFSTEDLER, CPA, CGFM, CTA

Chief Operating Officer

Mid-Ohio Regional Planning Commission

T: 614.233.4136

shufstedler@morpc.org