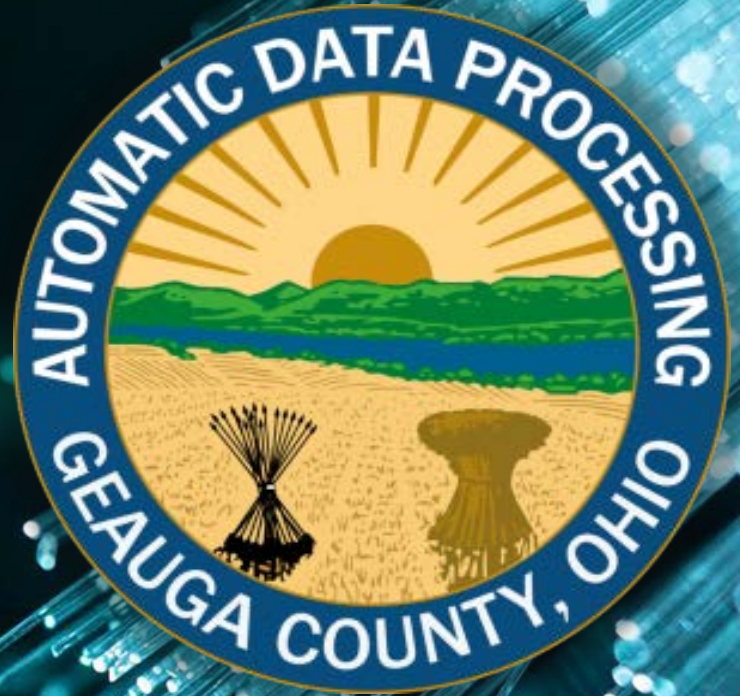


Intentionally left blank

Geauga County, Ohio
Cybersecurity Acceleration

Practical Cybersecurity Improvements

What We Have Done, and
What You Can Do Too



ABSORB what is useful
DISCARD what is not
ADD what is uniquely your own

- Bruce Lee



Geauga's View of Security – CIA Triad

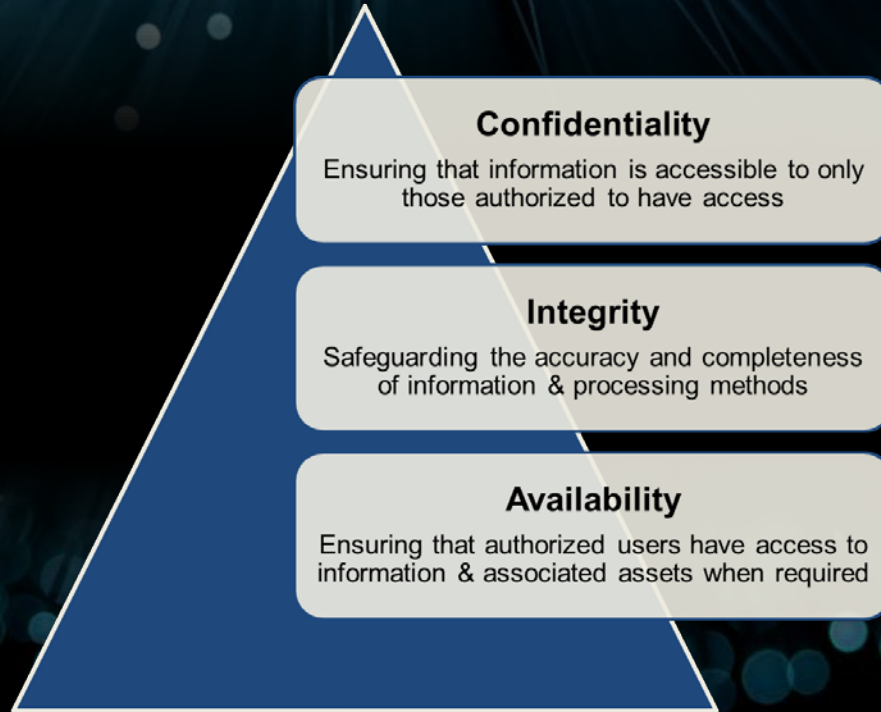
Confidentiality

Integrity

Availability

This is How We Look at Information Security

Confidentiality – Integrity – Availability



Confidentiality

This principle addresses the need to protect sensitive, private information from unauthorized access.

This may include, but is not limited to, financial records, business plans, personally identifiable information (PII) such as Social Security Number (SSN) or date of birth, password-protected records, email records, payment information (including credit/debit cards) and protected health records.

You must segregate your data, limit access, and actively prevent unauthorized users from accessing data.

Some of the methods used to manage data confidentiality include access control lists, role-based access control (RBAC), volume/file encryption, file permissions, encryption of data in process, in transit and in storage, remote wipe capabilities, and education and training for all individuals with access to protected data.

<https://www.unitrends.com/blog/cia-triad-confidentiality-integrity-availability>

Integrity

This component of the CIA triad ensures the data is correct, authentic and reliable.

In other words, it ensures that the data has not been tampered with and therefore can be trusted.

Data must be protected while it is in use, in transit and when it is stored, regardless of whether it resides in a laptop, storage device, data center or in the cloud.

You must ensure your data is protected from both deletion and modification by an unauthorized party, and in such a way that when an authorized individual makes changes in error, those changes can be reversed.

Data integrity can be preserved through encryption, hashing, digital signature, digital certificate, intrusion detection systems, auditing, version control, authentication and access controls.

<https://www.unitrends.com/blog/cia-triad-confidentiality-integrity-availability>

Availability


This principle ensures systems, applications and data are available and accessible to authorized users when they need them.

Networks, systems and applications must be constantly up and running to ensure critical business processes are uninterrupted.

Availability of your data systems can be impacted by human error, hardware failure, software failure, network failure, power outages, natural disasters and cyberattacks.

Some of the methods used to ensure data and application availability include redundancy (servers, networks, applications and services), fault tolerance (hardware), regular software patching and system upgrades, maintaining backups and backup copies, and disaster recovery.

<https://www.unitrends.com/blog/cia-triad-confidentiality-integrity-availability>



Transition to Methods
to Achieve the CIA Triad

Starting with Cloud Computing

What is the “Cloud?”

I Will Let You in on a Major Industry Secret



There is no cloud
it's just someone else's computer

Cloud Computing Simply Put

Simply put, The Cloud is a series of servers in a datacenter over the Internet—more specifically, it's all of the things you can access remotely over the Internet. When something is in the cloud, it means it's stored on internet-connected servers instead of your computer's hard drive.

This is the colloquial name for a datacenter managed by a vendor that shares its computing resources among that vendor's many clients. Because the data and processing is “in the cloud” and not on a single computer or a client's server; setup, maintenance, and costs are notably lower for a cloud-based solution.



Cloud Computing Described

A **Server** is a specialized computer that, rather than being operated directly by a user, is interacted with through other computers. Servers are used to host network files and applications, which need to be accessed by many computers, but that would be taxing or redundant to have on each computer individually.



Datacenters Described

Datacenters are rooms where many servers are stored and operated.

The servers are generally stored in server racks, which can house, power, and provide networking to the servers.

Cloud Computing for Applications

Wellsky and New World Systems

We are currently in the process of moving various applications to the cloud:

- This lessens the number of servers we need to spend time and money managing.
- This also places the services out of reach of failures to our own system.

Wellsky's move to the cloud has been finished and MVP, ArcGIS, and NWS are currently in progress.



Cloud Computing for Applications



We are currently migrating our Payroll Systems and preliminary researching our Help Desk software to for cloud-based moves. Payroll is being moved to ADP INC. Help Desk is preliminarily being reviewed for a move from the current system through ManageEngine ServiceDesk to BMC Helix IT Service Management.



Move to Cloud – Move As Much Off Premise As Possible – In Progress



WellSky
~ Completed



New World
Systems
~ In Progress



MVP Tax
~ In Progress



ArcGIS
~ In Progress



Web
Modernization
~ In Progress



Move to Cloud, HRIS From Paper – In Progress

What is HRIS?

HRIS stands for Human Resources Information System. Basically, an HRIS is a software solution that maintains, manages, and processes detailed employee information and human resources-related policies and procedures. As an interactive system of information management, the HRIS standardizes human resources (HR) tasks and processes while facilitating accurate record keeping and reporting.



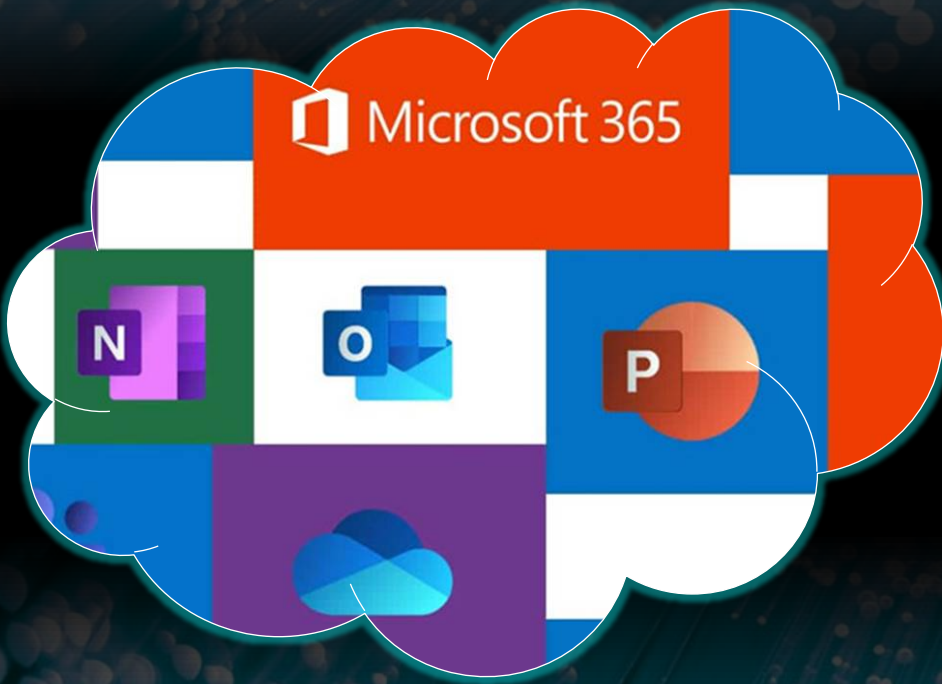
Microsoft 365

Microsoft 365, previously known as Office 365, is a replacement for the commonly-used Microsoft Office Applications. M365 is hosted by Microsoft in the cloud, rather than relying on the end user's computer or server.

Benefits over the previous iterations include an expanded suite of applications, easier access on more devices, reduced maintenance required from IT, and easy portability.



Microsoft 365 Use In Our Environment



Microsoft 365 offers a cloud-based alternative to Microsoft Office, which solves some of the main issues ADP has with on-prem Exchange. Notably, this allows us to decommission our old Microsoft Exchange servers and make the process of licensing and management easier.

Microsoft 365 Use In Our Environment

In addition, it gives the entire county access to more Office applications, with Microsoft Teams being the highlight program. SharePoint is also particularly noteworthy for its ability to remove many of the currently-in-use network drives.



The background features a dark blue gradient with numerous thin, bright blue light rays emanating from the top center, creating a starburst effect. Scattered throughout are various sized, semi-transparent blue circles, some appearing as bokeh or lens flare effects. The overall aesthetic is clean, modern, and tech-oriented.

Transition from Cloud Servers to On-Premises Servers Security

How We Secure Our Local Servers, Physically



Local servers are physically secured in server rooms with limited access. When necessary, they are also locked in locking switch cabinets.

All digital access to the servers are controlled in a few ways. Access is only given to specific users at specifically the level of access they need. This both prevents non-administrator users from making changes to the server and prevents users from accessing data they should not have access to.

How We Secure Our Local Servers, Digitally

Unless a server specifically needs to connect to any device in the county, access is restricted to specific devices. When connecting to external IP address is necessary, vulnerability scans are performed.

Servers are kept up to date to prevent bad actors from exploiting old updates.

In addition to these server-specific levels of security, CrowdStrike is installed on all the servers in our network, and if it detects suspicious activity, it will alert HelpDesk and if need be, quarantine the machine.



Why We are Moving From In-House To Hosted Servers



ADP currently manages all of the servers utilized by the county. While some of the management for these servers is reduced by making them virtual machines, there is still a lot of upkeep and management that could be offloaded to cloud-based services that provide the same solution. While this does give cyber-attackers another vector from which to approach the network, the burden of security does not fall as heavily on ADP.

In addition, by utilizing hosted servers, if one of the vendors undergoes a cyber-attack that renders their network and servers unavailable, it only prevents the county from using that specific service, rather than the whole network.

What We Moved From In- House To Cloud-based “Hosted” Servers for File/ Print

We have migrated a number of entities from in-house servers to SharePoint, but we are also migrating our printing and scanning to cloud-based through vendors.

Print servers, in particular, are cumbersome and typically the last remaining on-premises servers entities maintain.

Cloud-based print management is a way of managing and controlling a corporate print environment from a cloud-based application, and also enhancing security.



PHAROS
Secure Cloud Printing





Transition to Leveraging
IT Vendors with In-House IT Staff

Best Practices For In- House IT Staff/ Leveraging Vendors

All work that falls under the scope of daily operation of the county's networking is done by ADP staff, this includes user and endpoint management, phones, on-premises server maintenance, website creation and updates, and security management.

Work that falls outside of that scope, such as web or application hosting, nonstandard equipment installation and management, security database management, or end user training, is being partially or fully outsourced to outside IT staff.

By outsourcing part of this work to the cloud, ADP staff can have their full attention on daily operations and incident response, as well as researching new solutions.



Vendor Leveraging

Sampling of Vendors Leveraged



DotNetNuke
(DNN) to
WordPress
Websites



On-
Premises
Exchange to
M365



On-
Premises
Cisco
Phones to
Kinetic Mitel

Best Practices For In- House IT Staff

Training, training, training.

By outsourcing longform trainings to Cybalt, KnowB4, and Microsoft 365, technicians can focus on helping the presenter and helping tailor the trainings to our network and users, rather than focus on making the training itself.

Training is Mandatory for all Users, IT Staff, and Cybersecurity Personnel.

Dictated by Policy.

Annual Requirements:

1. End Users – 30 to 60 minutes
2. IT Professionals – 4 hours
3. Cybersecurity Personnel – 8 hours



The background is a dark blue gradient with a bokeh effect. Numerous thin, light blue lines radiate from the top center, creating a starburst or sunburst pattern. Scattered throughout the image are various sized, out-of-focus circular light spots in shades of blue and white, giving it a digital or network-like aesthetic.

Transition to Endpoint Security/ Management

Endpoint Protection Described

Endpoints are the devices where a network is accessed, specifically the computers and servers. Users primarily interact with endpoints. A network is built to support sending and receiving data between endpoints and the wider internet.



Endpoint Protection Described



● **Traditional Antiviruses** are programs that protect against malicious programs by blocking their download, preventing them from running, and running scans to see if the programs are installed on the computer.

● **Managed Antiviruses**, such as CrowdStrike, take a different approach. CrowdStrike's main goal is to monitor a system for any strange activity, regardless of program, and quarantine it if need be. From quarantine, CrowdStrike's team can extract malicious programs safely.

Endpoint Protection

CrowdStrike (CRWD) is our primary software for use in endpoint security. After extensive vetting we chose CRWD because it is a “managed” antivirus program that has the capability to quarantine computers acting suspiciously, even if that activity is at a very low level.



CROWDSTRIKE

Endpoint Protection

The increased power of CrowdStrike over previous solutions like Sophos and Kaspersky allows ADP to not only prevent cybersecurity incidents, but also remediate incidents more quickly and thoroughly. In addition, ADP can gather data about the nature and potential origin of these incidents, increasing chances that future incidents would be prevented.

Sampling of Prevented Malicious Activity

User Credential Hacking on the Dark Web

End-user Clicks on Popups/Malicious Software Installation

Browser-based Addons

Exchange Server Attack

Endpoint Management



Endpoint Central is the primary program used to manage county computers. The software allows technicians to remotely control the computer in almost any way. Updates, software installations, and commands can be run in the background, as well as direct remote control of the machine.

Why Endpoint Management?



With Endpoint Central, you can

- ✔ Automate patch management
- ✔ Manage and monitor mobile devices
- ✔ Deploy software in a few clicks
- ✔ Image and deploy operating systems
- ✔ Troubleshoot systems remotely and securely
- ✔ Enforce compliance measures across your organization
- ✔ Secure your device, applications and data
- ✔ Manage endpoints on the go using our mobile app

Geauga's Use of Endpoint Management

Search and Eradicate End of Life/End of Support Operating Systems



Kill Windows 7 Operating Systems

Nothing personal – but Microsoft has not provided any patching for bugs and security updates since 2020, and any Windows 7 OSs are highly vulnerable to intrusion and attack. Windows 7 is End of Support/End of Life.



Strategy (least best): isolate Windows 7 Machines

Strategy (better): upgrade to Windows 10

Strategy (best): upgrade to Windows 11

Network Protection

SIEM PROCESS FLOW



SIEM – Security Information and Event Management

At its core, SIEM is a data aggregator, search, and reporting system. SIEM gathers immense amounts of data from your entire networked environment, consolidates and makes that data human accessible. With the data categorized and laid out at your fingertips, you can research data security breaches with as much detail as needed.

SIEM Use in Geauga County

Currently Geauga County uses SIEM only for our Board of Elections Environment and is Intending to Expand to a full SIEM in 2023.



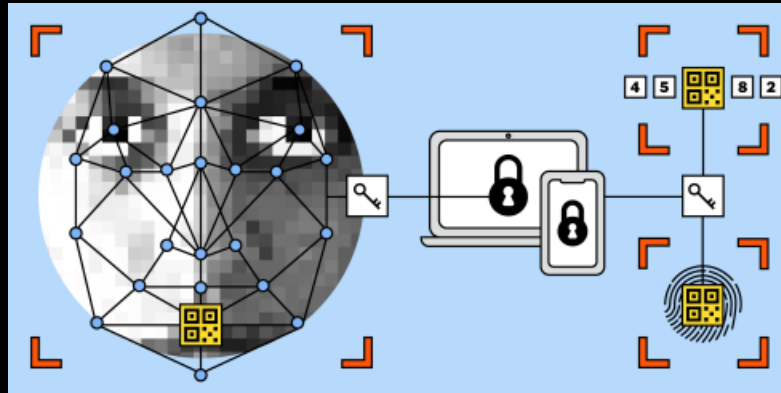
The background features a dark blue gradient with numerous thin, bright blue light rays emanating from the top center, creating a starburst effect. Scattered throughout are various sized bokeh circles in shades of light blue and white, giving the impression of distant stars or data points.

Passwords, Multifactor Authentication, and Security

Passwords

Wall Street Journal Article by Christopher Mimms from October 2022

“In the Future, There Will Be No Passwords—Because You Keep Giving Yours Away”



NY Times Article by Thorin Klosowski from January 2023

“RIP, Passwords. Here’s What’s Coming Next.”

Passwords are Passe

Microsoft, Apple, and Google are working together – yikes – on a password replacement. This concept is called a “passkey.”

What is a passkey? Essentially, this is much like how some of you unlock your Apple phones. You look at it! The phone is using biometrics and cryptography to skip the password process, but still permit the access.

In Geauga County, we are still using passwords. But we have also included passkeys which provide both passkey cryptography and multifactor authentication. More on that in a bit.

Password Best Practices For All Passwords

Basic user account Passwords are required to be 25 characters long, and be a combination of uppercase letter, lowercase letter, numbers, and special characters. Information relating to a user's account, such as their first name, last name, and their date of birth are not allowed to be included in the passwords.

Higher level administrative passwords have the same complexity requirements but are also required to be a minimum of 100 characters long.

Password cracking with modern techniques and hardware is just easy now. The barrier to entry as a hacker is incredibly low. The longer a password is, the longer it takes, exponentially, to brute force.

The recent jump in our password requirements from a minimum 12-character passwords to 25-character passwords was an attempt to get ahead of the ever-shrinking cracking times that newer, more powerful hardware and techniques will provide.

Password Best Practices For All Passwords 20 22 Edition

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

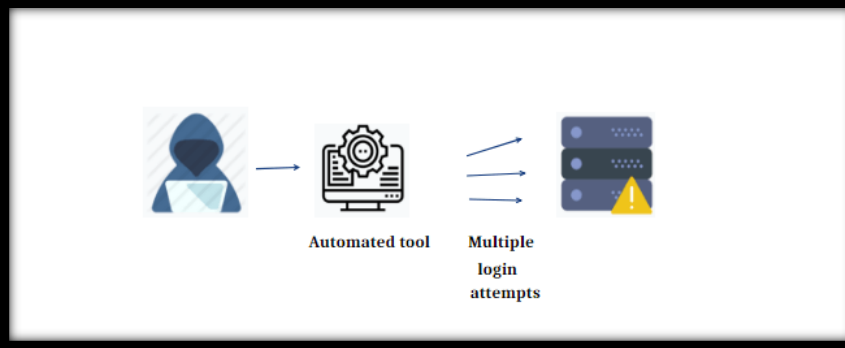


**TIME IT TAKES
A HACKER TO
BRUTE FORCE
YOUR
PASSWORD
IN 2022**

Password Brute Force Attack

A brute force attack uses a trial-and-error approach to systematically guess login info, credentials, and encryption keys. The attacker submits combinations of usernames and passwords until they finally guess correctly.

Once successful, the actor can enter the system masquerading as the legitimate user and remain inside until they are detected. They use this time to move laterally, install back doors, gain knowledge about the system to use in future attacks, and, of course, steal data.



Most Common Brute Force Attack

Simple Brute Force

A simple brute force attack uses automation and scripts to guess passwords. Typical brute force attacks make a few hundred guesses every second. Simple passwords, such as those lacking a mix of upper- and lowercase letters and those using common expressions like '123456' or 'password,' can be cracked in minutes. However, the potential exists to increase that speed by orders of magnitude. All the way back in 2012, a researcher used a computer cluster to guess up to 350 billion passwords per second.

Dictionary Attack

A dictionary attack tries combinations of common words and phrases. Originally, dictionary attacks used words from a dictionary as well as numbers, but today dictionary attacks also use passwords that have been leaked by earlier data breaches. These leaked passwords are available for sale on the dark web and can even be found for free on the regular web.

Credential Stuffing

Over the years, more than 8.5 billion usernames and passwords have been leaked. These stolen credentials are sold between bad actors on the dark web and used in everything from spam to account takeovers.

A credential stuffing attack uses these stolen login combinations across a multitude of sites. Credential stuffing works because people tend to re-use their login names and passwords repeatedly, so if a hacker gets access to a person's account with an electric company, there is an excellent chance those same credentials will provide access to that person's online bank account as well.

Multifactor Authentication Described

Multifactor Authentication, or MFA, is a more secure method of sign-in that relies on more than one form of “authentication” which is a method of proving identity.

For example, rather than requiring just a password, a password and a One-Time-Passcode would be required to sign in.

MFA can be enabled by a system administrator to require users to create and maintain a second form of authentication, usually in the form of a One-Time-Passcode. Another common form of authentication is detecting a physical object, one intended for the user to always carry to prove identity.

Wireless 2FA and Password Manager

Login with your presence,
not password.



Multifactor Authentication as One Time Passcodes

One-Time-Passcodes, or OTPs, are single-use passwords that are automatically generated by a specialized authenticator app. This passcode is regenerated roughly every 30 seconds, and must be retrieved each time the user attempts to log in. Because they can't be written down and saved for later, they are inherently very secure as a form of authentication.



Multi-Factor Authentication (MFA)

Multifactor authentication is required throughout the county system. Users must log in with MFA, no exceptions, and software used throughout the county must be capable of MFA.

Currently the primary forms of multifactor authentication are the Microsoft Authenticator and Gatekeeper.

Microsoft Authenticator is the most convenient authenticator for anyone with a county phone, as the app is easy to use and is more secure than SMS authentication.



Multi-Factor Authentication (MFA)



Gatekeeper was chosen for its proximity-based multifactor authentication, allowing the additional security MFA provides without as much risk of tokens being lost as other, USB-based solutions. In addition, the built-in password manager allows users to create, manage, and securely share passwords.



Two Very Common Attack Points Email and Payroll Scams

Malicious E- Mail Protection

Our Barracuda spam filter does much of the heavy lifting in blocking easily detectable malicious emails, but some phishing emails still make their way through the filter. In addition, it will block any domain we specify, so its capabilities are constantly improving.



Malicious E-Mail Protection

Outlook also has some spam filtering and will catch some emails that Barracuda missed. This is not our primary form of malicious email protection but adds an extra layer of protection.

Our last line of defense is the end user's judgement. Trainings have been conducted to educate users who have failed our phishing campaigns or clicked phishing links in the past. Future trainings and campaigns are being planned.



Payroll Scams

Payroll scams are becoming more and more common. These scams are usually spear phishing emails pretending to be an employee wanting to change their bank account information. These phishing emails are then sent to users who deal with payroll to either get the user to change the bank account information directly or click on a malicious link.



Payroll Scam Example

----- Message -----

From: Timothy Grendell <privatemail0725@gmail.com>

Sent: Thursday, April 25, 2023 9:06 AM

To: Walder, Charles <cwalder@geauga.oh.gov>

Subject: INSTITUTION OF PAYROLL

Good Morning Charles.

Unfortunately, I recently changed banks and would like my paycheck deposited into my new account. Would you be able to make the change for me if I sent you the details? Due to the switch in banks I recently made.

Thanks,

Payroll Scams

We specifically held a county-wide training day to educate users who deal with financial and payroll data on the various types of phishing emails and payroll scams that they may encounter. Our training features known cybersecurity specialist Kevin Mayo from Cybalt, based out of Texas.

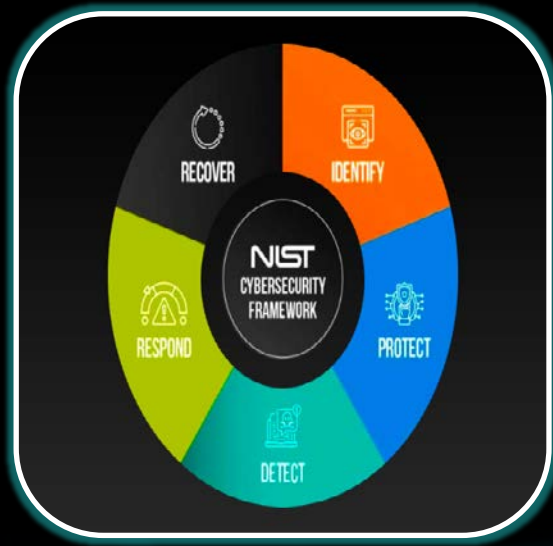




Policy

Policy Development

The following policies are currently in place:



- Acceptable Use Policy
- Cybersecurity and Social Engineering Awareness Policy
- Multi-Factor Authentication and Password Policy
- ADP Restricted Area and Access Control Policy
- ADP Backup Tape Rotation Procedures
- Privileged Account Policy
- Software Management and Approval Policy
- ADP Backup Tape Rotation Procedures
- ADP Approval Policy
- Electronic Door Access Controls Policy
- Security Response Plan Policy

Policy Development

The following policies are currently in place:



- Information Technology Risk Assessment Policy
- Data Breach Response Policy
- Router, Switch and Device Hardening Policy
- Data Destruction and Sanitation Policy
- Remote Access and VPN Policy
- Email Security Policy
- Clean Desk Policy
- Guest Wi-Fi Acceptable Use Policy
- Continuity of Government Policy
- Vulnerability Management Policy
- Data Classification Policy

The background features a dark blue gradient with numerous thin, bright blue light rays emanating from the top center, creating a starburst effect. Scattered throughout are various sized bokeh circles in shades of light blue and white, some appearing as soft, out-of-focus spots and others as sharper points of light.

Domains and Program Blocking

Email Domains Described

An email addresses' **Domain** is the section of an email address after the @ symbol
For example:

user1@domaingoeshere.com

An email domain can be purchased, and the owner may create email addresses in that domain. (admin@domaingoeshere.com would be available to them as well)



Domain Blocking



Due to the recent uptick in phishing emails and scams, we have needed to block a larger volume of emails to better shield ourselves against nefarious attackers. To prevent emails all coming from the same domain, we block phishing and spam emails in the Barracuda spam filter, so that we are unable to receive emails from those domains. As an additional layer, we also blacklist these domains on Office 365 through Outlook.

Domain Blocking

Blocking a domain only prevents emails originating from that domain, and domains are easy enough to obtain that some bad actors can purchase them in mass quantities for relatively cheaply. Also, if we block a domain, it may stop some of the emails sent by that bad actor for a bit, but they will likely catch on quickly and use another domain we have not blocked to send the same emails.



Program Blocking

Programs known to be malicious or to be carriers of other malicious programs are important to remove from county machines as soon as possible and block from future installs, when possible.

Notable malicious programs we have encountered are the Wave Browser, OneLaunch, and Clear Browser.



Wave
Browser



OneLaunch



Clear
Browser

Program Blocking

CrowdStrike is the primary program that allows us to block malicious programs. If a program is detected by CrowdStrike, the antivirus stops the malicious program from running and quarantines the system. From there, the malicious program can be extracted, and the computer can run as normal. CrowdStrike then adds the program to their database of programs to look out for in the future.

If one of these known programs isn't actively running on the user's computer but is discovered by a technician, it can be added to CrowdStrike's database. From there, whenever it is detected on a system, CrowdStrike can send an alert and quarantine the system.

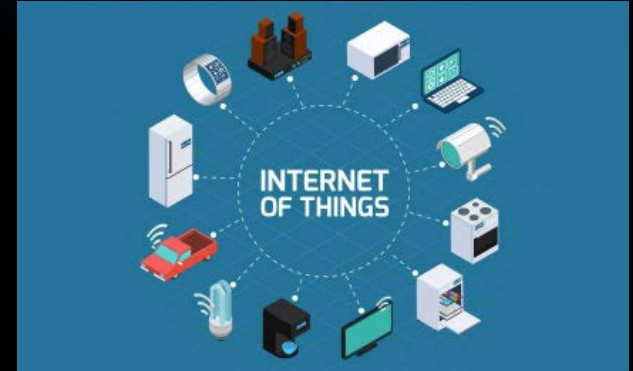


The background features a dark blue gradient with numerous thin, bright blue light rays emanating from the top center, creating a starburst effect. Scattered throughout are various sized bokeh circles in shades of light blue and white, giving the impression of a digital or networked space.

Transition to Internet of Things Discussion

Internet Of Things Overview

Generally, the term Internet of Things, IoT encompasses physical things connected to the internet – like objects that "talk" to each other. The IoT can be thought of as devices – from simple sensors to smartphones and wearables – connected together through the Internet. Great examples of IoT devices that effect governments are security cameras, door access controls, and security systems.



Internet Of Things Security – Security Cameras



Cameras are a crucial component to physical security in a network. ADP currently covers all Geauga County government buildings with a camera infrastructure.



Internet Of Things Security – Access Controls

Digital Access Controls to the doors in the county's various buildings is important for the physical security of the County's network. With these controls properly in place, no employee will have access to areas outside of what they need.

Access to the buildings can be granted on an employee's hiring, and more access can be granted as the employee's position changes. If an employee leaves or an access card is misplaced, access can be revoked immediately.



Internet Of Things Security – Firearm Detection

Zero Eyes is a program that scans a camera feed and uses AI to identify firearms. If it identifies a firearm, it sends the footage to Zero Eyes to review. If Zero Eyes determines the alert to be legitimate, they send an alert to local authorities. This program increases the physical security of the buildings in the county.



Zero Eyes Firearm Detection

Alerts sent to 911 Dispatch and Critical Contacts within 5-8 Seconds of Detection



The background features a dark blue gradient with numerous thin, white light rays emanating from the top center, creating a starburst effect. Scattered throughout are various sized bokeh circles in shades of white and light blue, some appearing as bright points of light and others as soft, out-of-focus circles.

Transition to Disaster Recovery

Disaster Recovery Planning

What is a disaster recovery plan?

A disaster recovery plan (DRP) is a documented, structured approach that describes how an organization can quickly resume work after an unplanned incident.

Why have a disaster recovery plan?

Because Natural Disasters, Hardware Failures, Human Errors, Threat Actors, and Data Corruption happen.



Data Backups 3, 2, 1 Rule

Master the 3-2-1 Rule

Or, the 3-2-1-1-0 Rule...

3

Different copies
of data



2

Different media



1

of which is off-site



1

Is offline



0

No errors after
backup recoverability
verification



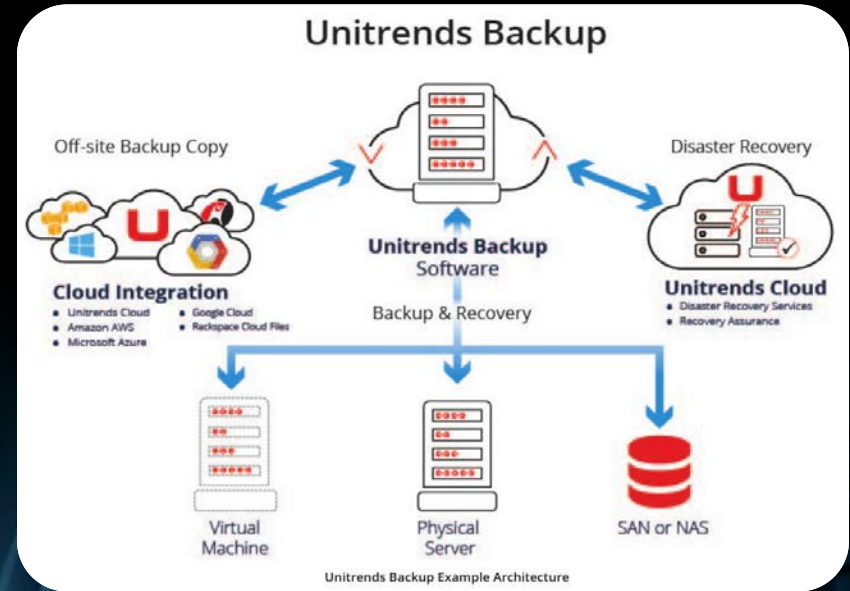
Data Backups – Tapes

Backups allow the county to maintain information that would have otherwise been lost due to user error, data breaches, or system-wide failure. They also allow us to comply with data retention laws for the purpose of public record.



Data Backups – The Cloud

Unitrends Backup software, is a prepackaged virtual appliance with fully integrated, backup, replication, deduplication, archive and instant recovery.



Data Backups – On- Premises Storage

We also have on-premises appliances which hold data for long term cold storage. These are Synology Appliances and hold a combined 150 terabytes.

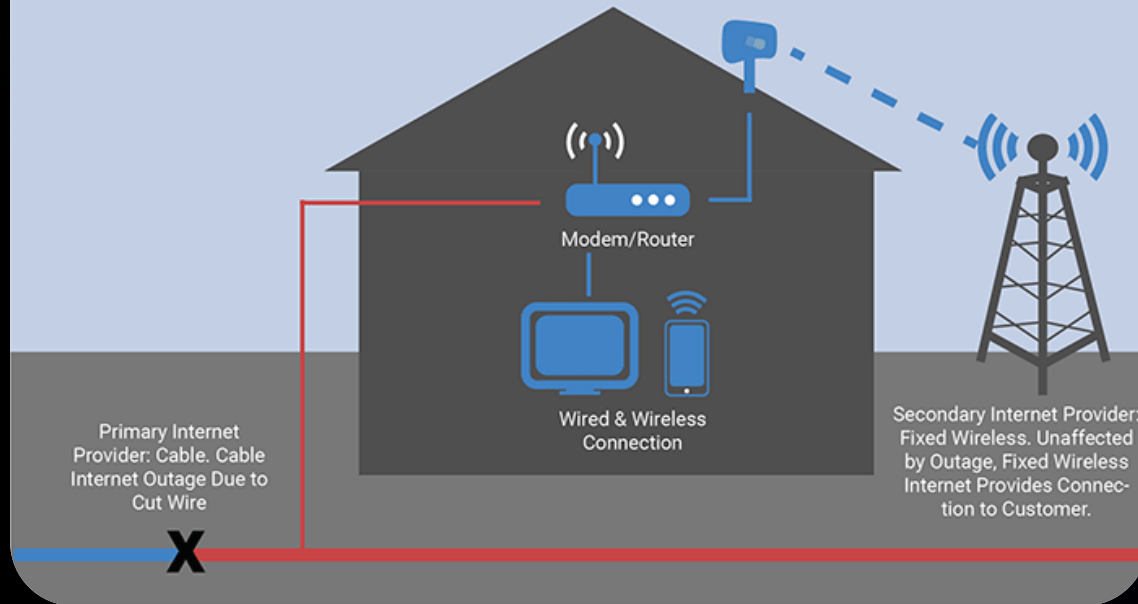




Transition to
Communications
Redundancy

Internet Redundancy With Cellular

Redundant Internet Supply



Internet Redundancy With Cellular



At Geauga's main government campus, the internet is redundant through FirstNet's cellular antenna. FirstNet's solution was chosen for the first-responder priority it gets over civilian signals. FirstNet's wireless signal is being used by Illuminati Labs, allowing for a boosted 4G LTE and 5G signal in the building.

The background is a dark blue gradient with light blue rays emanating from the top center, creating a starburst effect. There are also several light blue bokeh spots scattered across the image, particularly concentrated at the bottom.

Actionable Takeaways for You!

Immediate Security Takeaways

Ensure Long Passwords

Add in Some Kind of Multifactor Authentication

Kill All Windows 7 Operating Systems

Consider Hiring an Information Security Firm for an Assessment

Develop, Institute, and Utilize Policies

Immediate Security Takeaways

Patch Operating Systems

Don't Buy Chinese Made Technology

Subscribe to DHS CISA Alerts and Updates

Review Cybersecurity Insurance

Train End Users – Awareness is Key!

The background is a dark blue gradient with light blue rays emanating from the top center. There are several bright white and light blue circular bokeh spots scattered across the image, particularly near the top and bottom edges.

Movies, Podcasts, and Books

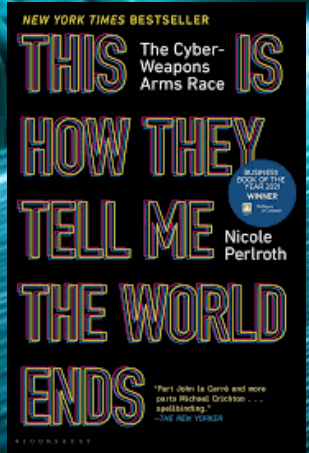
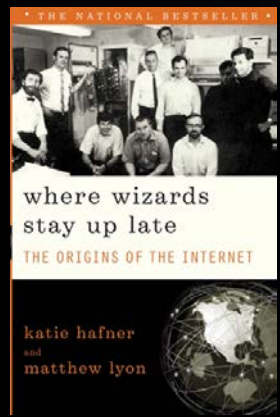
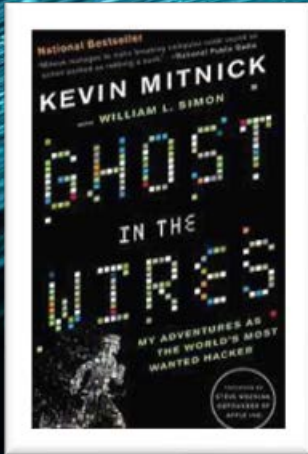
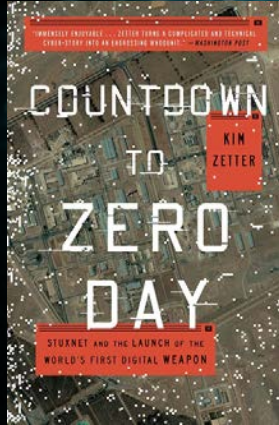
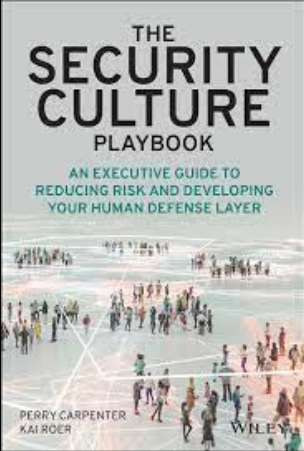
Movies



Podcast Suggestions

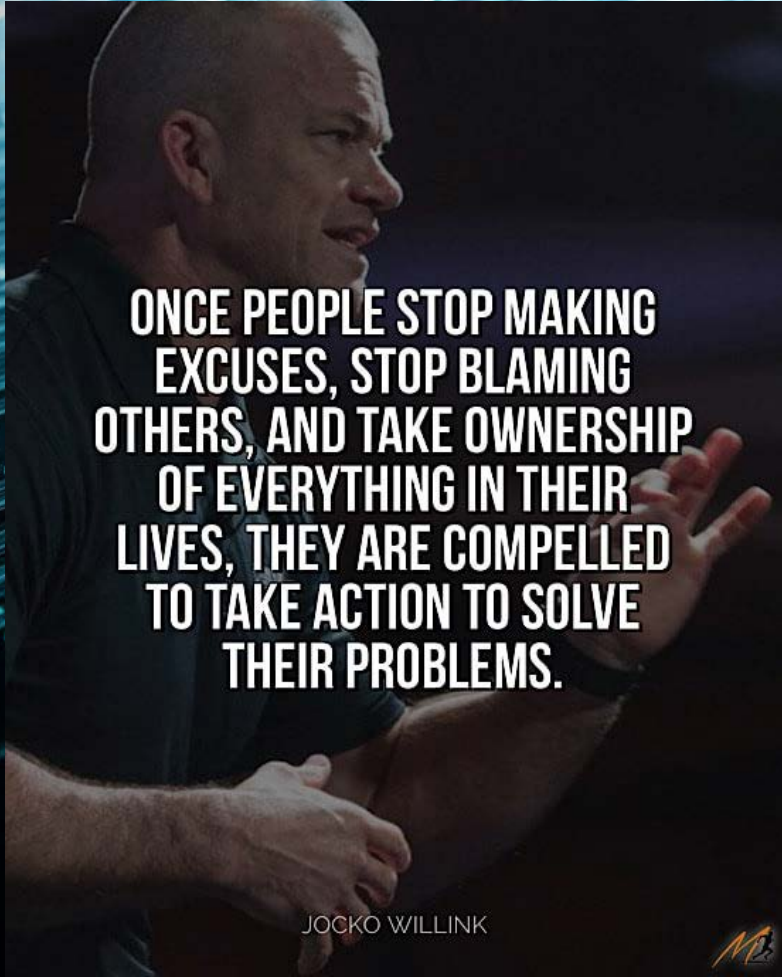


Book List



Take Ownership

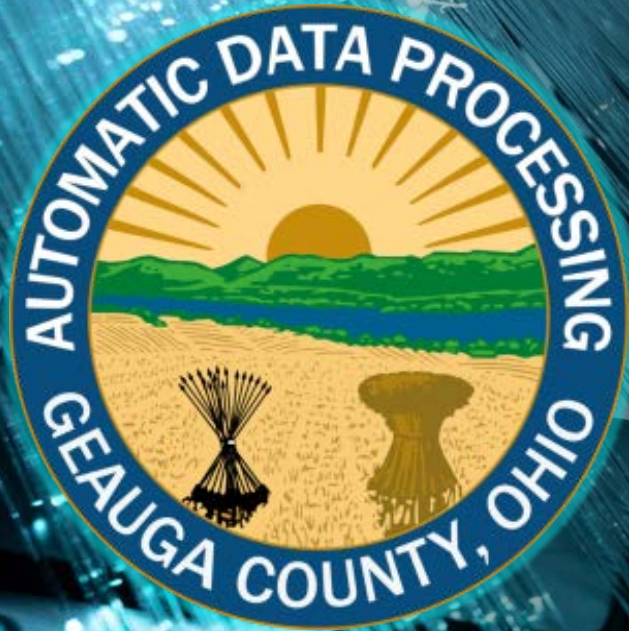
Questions and Attempts at Answers



**ONCE PEOPLE STOP MAKING
EXCUSES, STOP BLAMING
OTHERS, AND TAKE OWNERSHIP
OF EVERYTHING IN THEIR
LIVES, THEY ARE COMPELLED
TO TAKE ACTION TO SOLVE
THEIR PROBLEMS.**

JOCKO WILLINK





Thank You

ADP

Department of Information
Technology

Chief Administrator

Charles E. Walder

Geauga County Auditor
CWalder@GCAuditor.com

O: (440)279-1602

Specific questions about this
presentation can be sent to
fantenucci@geauga.oh.gov