MINNESOTA ASSOCIATION OF DEVELOPMENT ORGANIZATIONS

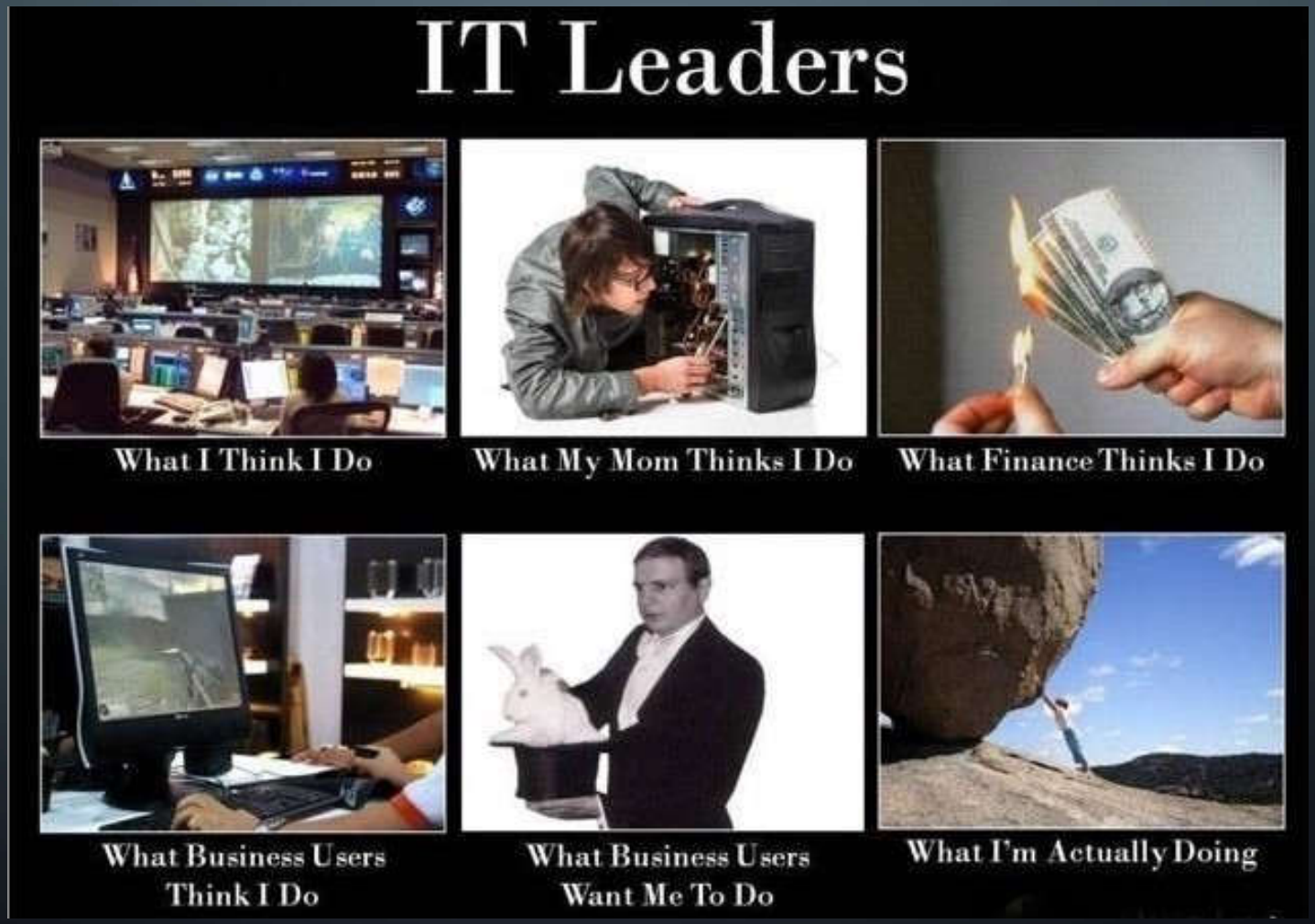
DEVELOPING A PRACTICAL CYBER HYGIENE MODEL

"…The next Pearl Harbor that we confront could very well be a cyber-attack…"

Leon Panetta, 2011 Senate confirmation hearing for Secretary of Defense

*** Positions held: Secretary of Defense, CIA Director, White House Chief of Staff, Director of Office of Management and Budget, Congressman*

DEVELOPING A PRACTICAL CYBER HYGIENE MODEL



DEVELOPING A PRACTICAL CYBER HYGIENE MODEL

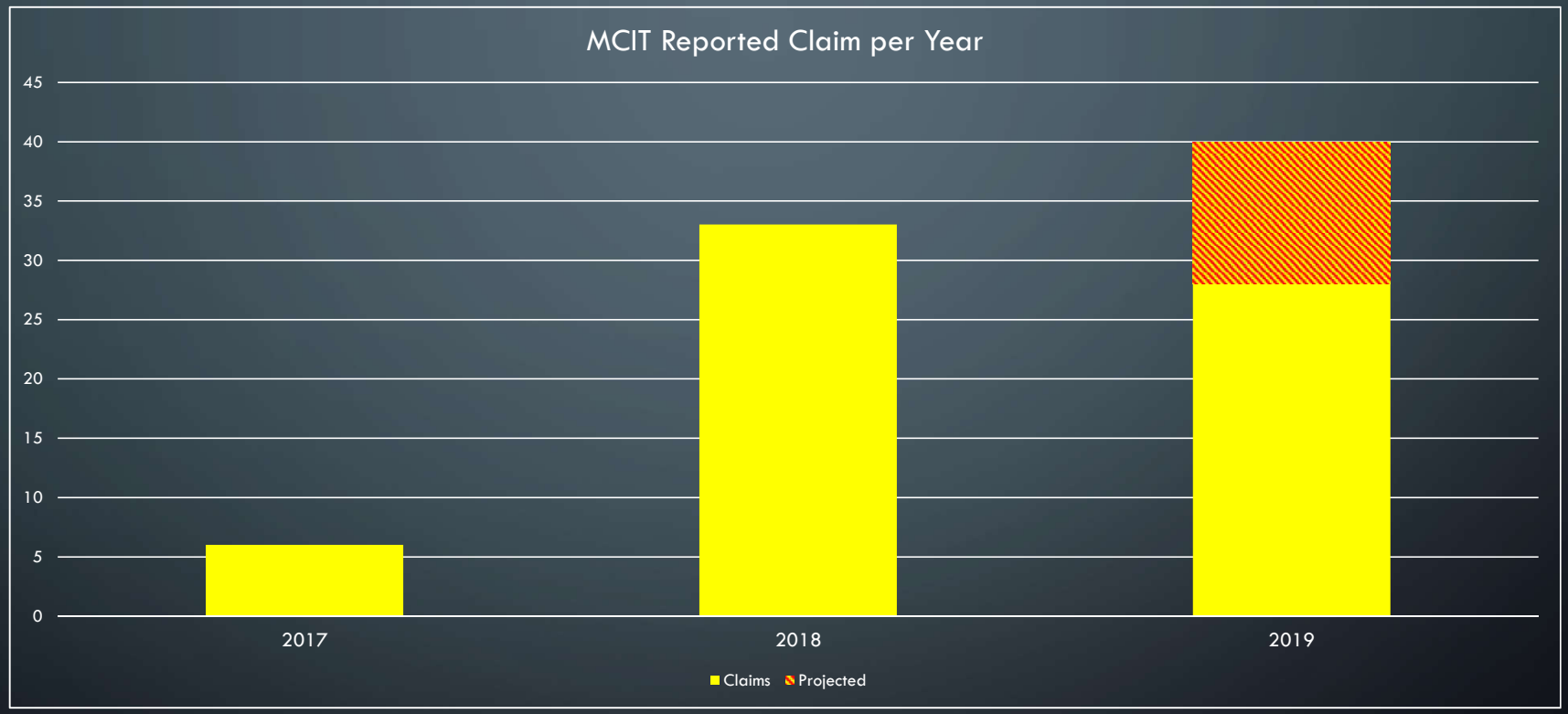
WHY DOES OUR MOST USEFUL BUSINESS TOOL HAVE TO BE SO COMPLICATED?

- What are you hoping to get out of today?
- What are your top five concerns about cybersecurity?
- Has anybody been a victim of a cybersecurity incident?
- Do you spend as much time thinking about cybersecurity at home as you do at work?

HOW REAL IS THE THREAT?

- Dakota County (2/2019): One email box hacked, affecting over 1,000 citizen's private data.
- MN DHS (3/2019): One email box was compromised, eventually leading to 11,000 citizen's being affected.
- Mayor Minneapolis (9/2019): Email hacked. Threat contained quickly.
- MN DHS (9/2018): One email box was compromised, eventually leading to 3,000 citizen's being affected.
- City of Albert Lea (8/2018): Email phishing attack with malicious link. 330 current and former employee private and confidential data including social security numbers (employee records including payroll and W2 information)
- City of Minneapolis (8/2018): Unreported
- Hennepin County (8/2018): Email phishing attack with malicious link. About 20 email accounts exposed, including historical emails and attachments stored in email folders. Originated from State of Minnesota email phishing leak, which originated from City of Minneapolis email phishing leak
- Ramsey County (8/2018): Similar to Hennepin County, 28 county email accounts were hacked leading to 118,000 citizen's data being breached.
- Becker County (8/2017): Ransomware discovered on the network. Approximately 3 days of downtime.
- Stearns County (7/2017): County website hacked and redirected to malicious site
- Crowwing County (9/2016): Ransomware discovered on the network. Discovery was quick and stopped with minimal damage and downtime.
- City of Wadena (7/2016): Virus isolated to city hall computers
- City of Prior Lake (7/2016): Computer virus affected PCs and city's HVAC system

HOW REAL IS THE THREAT?

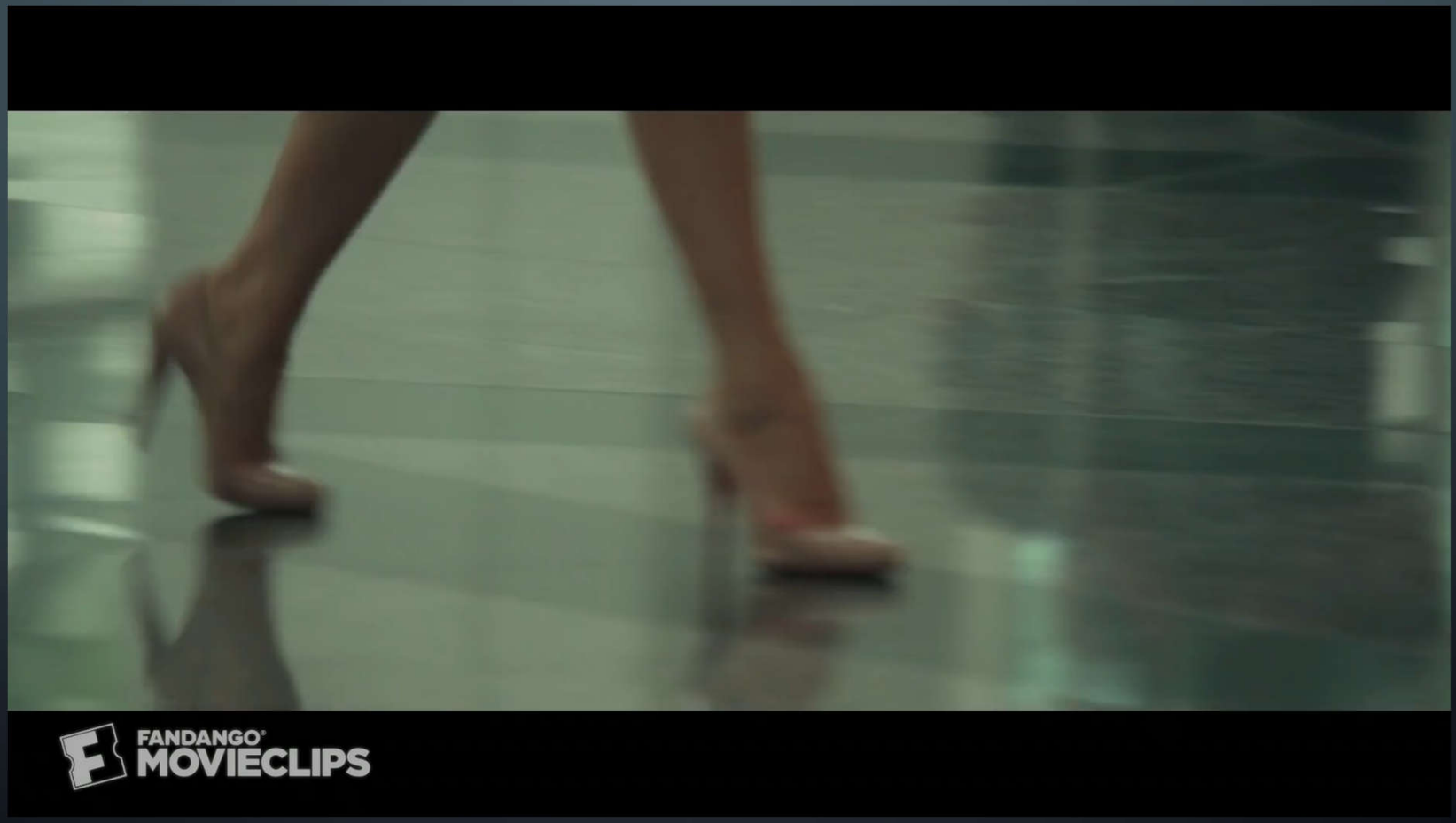


CYBER SECURITY: "GUARDING THE PERIMETER"

TYPICAL CYBER SECURITY MODEL:

- Technology department imposes security policies and procedures
- Top down mentality
- Firewall, anti-virus software, software patching and updates
- Accountability and responsibility falls on the technology department or vendor
- Stereotypical "guard the perimeter" protection
- Relying on your neighborhood watch and local police instead of teaching your family members to lock doors and windows.

WHO IS THE REAL THREAT?



CYBER HYGIENE: A WHOLISTIC APPROACH

WHAT IS CYBER HYGIENE?

Cyber Security PLUS:

- User participation through training, buy-in, and ownership
- Accountability and responsibility is shared across the whole organization
- Situational awareness by all users around all data
- Workspace security (i.e. closing offices when employees are not present)
- Relying on your neighborhood watch and local police, locking your doors and windows, and training your teenagers to choose wisely which friends to trust in your house.

BUILD BUY-IN AND OWNERSHIP

- Practical and Interactive Training
- Include training for personal use
  - Social media security
  - Credit card security
  - Parent/Child education
- Schedule training at least annually
- KnowB4 or SANS with testing modules (*discounts through one of your county seats?*)
- Purchase a password manager and allow/encourage personal use (LastPass, 1Password, KeyPass)

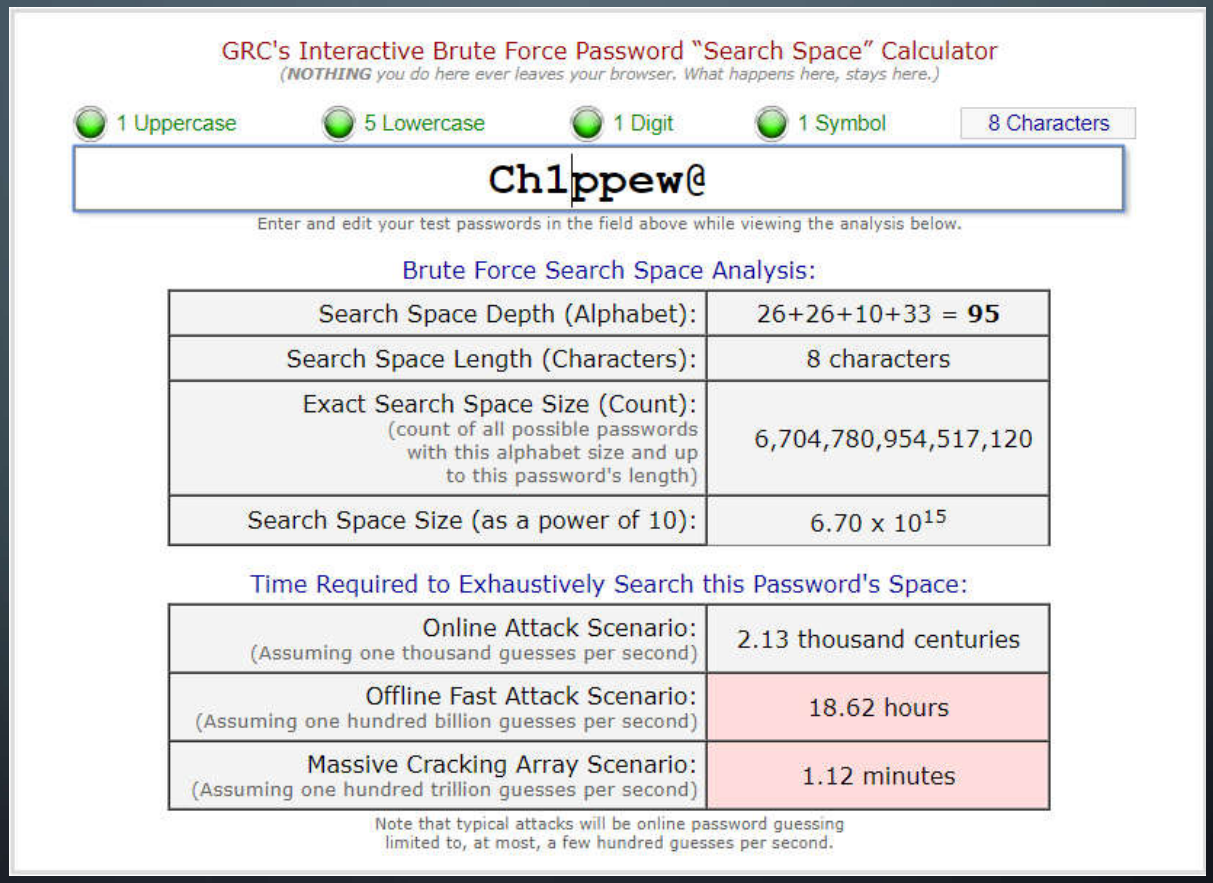
MOBILE DATA PROTECTION

MOBILE DEVICE SECURITY

- Extension of your office or cubicle
- Close the lid or lock your screen when you walk away.
- Family members may be trustworthy, but is it appropriate to share your device?
- VPN with multi-factor authentication to access office resources
- Multi-factor authentication to access cloud resources
- Passwords, PIN or biometrics on phones and laptops
- Switch to pass phrases instead of passwords
  - Use a password crack timer: https://www.grc.com/haystack.htm
  - Password sentences are easy to remember and very complex

MOBILE DATA PROTECTION

COMPLEX PASSWORD EXAMPLE:



GRC's Interactive Brute Force Password "Search Space" Calculator

(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)

1 Uppercase | 5 Lowercase | 1 Digit | 1 Symbol | 8 Characters

Ch1ppew@

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10+33 = **95**
Search Space Length (Characters):	8 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	6,704,780,954,517,120
Search Space Size (as a power of 10):	6.70×10^{15}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	2.13 thousand centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	18.62 hours
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.12 minutes

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

MOBILE DATA PROTECTION

PASSWORD SENTENCE EXAMPLE:

GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

1 Uppercase | 10 Lowercase | 1 Digit | 6 Symbols | 18 Characters

My dog spot is #1.

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10+33 = **95**
Search Space Length (Characters):	18 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	401,440,002,697,135,760, 758,578,320,767,017,120
Search Space Size (as a power of 10):	4.01×10^{35}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	1.28 hundred billion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.28 thousand trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.28 trillion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

MULTI-FACTOR AUTHENTICATION

WHAT IS MULTI-FACTOR AUTHENTICATION?

Something you know:
Username & Password

Something you have:
Mobile Device

Something you are:
Confirm you are human with fingerprint, face ID, answer the phone, type a PIN or challenge question

BACKUP PLAN

BACKUP YOUR DATA

- How often should you backup your data? Weekly, daily, hourly?
- What data should you backup?
- Is “cloud data” a reliable backup solution?
- Where should your backup be stored?
- Test your backup regularly (configure email notifications for backup)

PRACTICAL SOLUTIONS

SMALL OFFICE CYBER SECURITY

- Small office firewall with VPN
  - Protects access to on-site data, servers, or resources
  - Entry point devices can start uner $200
  - Cisco, Sonicwall, Fortinet, Ubiquiti offer affordable small business options
- Anti-virus software:
  - Built in Windows 10 Defender is ranked as one of the best by several independent reviews
  - No matter what you use, keep it updated frequently
- Email/Cloud data protection:
  - Office365 and G-Suite both offer basic, built in cloud data protection against virus, malware, ransomware, and some spam or phishing email
  - Consider advance security optional add-ons for deeper protection

PRACTICAL SOLUTIONS

DATA STORAGE

- In-Office Shared Storage
  - Synology, Drobo, QNAP
  - No server required
  - File sharing in the office
  - Employee files synchronize or cloud client to work remotely
  - 12TB business storage solutions start around $1,000
- Cloud Storage:
  - Purchase Government Cloud licenses
    - Less expense
    - Separated from general public data
    - Data store on servers
  - Office365 with OneDrive
  - G-Suite with Google Drive
  - Both offer file sharing inside or outside of organization
  - Auto synchronize employee data to cloud storage
  - Versioning Control allows restoring file versions

PRACTICAL SOLUTIONS

BACKUP SOLUTIONS

- In-Office Storage
  - Server with professional software with external hard drive or tape (expensive)
  - Synology, Drobo, QNAP network storage devices offer client backup software
  - Synchronize two devices for offsite backup
- Cloud Storage Backup:
  - Office365 and G-Suite offer versioning control
    - Keep multiple versions of user documents in case or errors or virus
    - OneDrive or Google Drive auto synchronize from employee device to cloud
  - Synology offers Office 365 backup on site to keep a copy of data locally

PRACTICAL SOLUTIONS

SIMPLE OFFICE SOLUTION

- CyberSecurity training: KnowB4 (MnCCC or County partner) $15/yr
- Small office firewall (all brands below would work well)
  - Ubiquity: $127
  - Cisco: $350
  - Sonicwall: $240
- Office 365 Government Cloud Office Software
  - G3 user licenses ($204/yr)
    - Email, Microsoft Office, Skype, several collaboration features
    - Add Advanced Threat Protection option for $24/yr
  - Multi-Factor Authentication built in
  - Use OneDrive sync with version control to keep 10 versions
  - Share files using OneDrive
- In-Office Storage and Backup:
  - Two Synology 5-Bay drives (3 year warranty)
    - 12TB of storage = $2,200 (five 3TB drives each)
    - 20TB of storage = $3,000 (five 5TB drives each)
    - Two devices allow you to synchronize to an off-site location (county data center)
  - Synology offers Office 365 backup on site to keep a copy of data locally
  - Use Synology free cloud software to work remotely and keep files synchronized to the office
  - Share files with office employees

RESOURCES

- CyberSecurity/Data Breach insurance: MCIT offers basic $100,000 per incident coverage with $250k, $500k, $1M options
- MCIT online resources
  - Tips on cyber security and training documents: https://www.mcit.org/quick-takes-on-safety/
  - "Essentials of Data Security for Public Entities" handbook: https://www.mcit.org/data-security/
- FCC tips for small businesses https://www.fcc.gov/general/cybersecurity-small-business
- Talk to your IT support:
  - Don't be afraid to ask for explanations or analogies in simple terms (English)
  - Find a *partner(s)* not just tech support: Proactive solutions vs Reactive repair