CPIM

Center for Public Investment Management

A Program Brought to You By:

Robert Sprague

Ohio Treasurer

Cyber Security: Data Breaches
It Can Happen to You

Stacey Russell, CPA, CPFO

Muskingum County Library System

Headlines

- *Cyber Attack Cripples Licking County Government* – January 2017
- *Hackers Seizing Ohio Government Systems* – February 2017
- *Cyber Attack Against Ohio Government Websites May Not be Over* – June 2017
- *Ohio Cities Face Increasing Ransomware, Cyber Attacks* – June 2018
- *Akron Systems Mostly Mended Following Cyberattack* – February 2019

- Background information:
  - Medium Size Library serving all of Muskingum County. Annual budget of about $4.75 million with 6 locations
  - 2 Accounting staff members, 1 full time and 1 part time

ACH Fraud

What Happened?

- Tuesday, March 19th we ran payroll and uploaded direct deposit to our bank
- Monday, March 25, 2013 we were notified by our bank via phone that they felt we had some fraudulent activity on our account
- 3 ACH transactions that were not initiated by the Library on March 21, March 22 and March 25 totaling $144,743
- The bank immediately took steps to “recall” those transactions

What Happened?

- Library IT staff disconnected both Accounting PCs from the internet and called our Technology Consultant
- Based on the Tech Consultant's advice, Library IT staff erased & re-formatted both Accounting PCs
- Zanesville Police were called and a report was filed
- We closed our existing bank accounts and opened new ones with new log on information
- We notified staff of a possible security breach and contacted the Board of Trustees

What Happened?

- AOS was involved and information was shared with the FBI via AOS
- Our insurance carrier was notified and a claim made
- By April 25th, 2013 $54,910 was recovered
- We settled with the bank regarding the remaining loss of $89,833
- Both the loss and the settlement were shown on our financial statements along with a footnote explanation.

Mistakes Made

- Our ACH Originator Agreement required us to notify the bank of direct deposit uploads; when we were trained by the Bank, we were told to disregard that requirement
- IT should have not erased and reformatted hard drives
- We should have pushed harder with local law enforcement

What we are doing differently

- Switched back to our regional bank
- We have a stand-alone PC that is only used for online banking
- We have requested that online access be granted from only 1 IP address.
- We purchased a cybercrime policy
- We revised our Banking RFP to include a section regarding online banking security minimums

Ransomware

- March 2017, Accounting server was not working
  - Local IT Staff investigated and accounting software provider was called to double check for any changes they might have made
  - Text File was found on the server

KEY BACKUP.txt - Notepad

MCLS-KVS01

File Edit Format View Help

Hi!

If you're seeing this file, then all your FILES have been LOCKED with the most strongest military CIPHER.

All your important data - documents, photos, videos - everything in CRYPTED.

The only way to recover your files - contact us via restoreserver@yandex.com

I stored the crypted data in your hard disk.

If you want to become your data back, send me an email containing your ip adress.

Your ip adress: 66.213.91.13

Next Steps

- Called our CyberRisk Risk Policy and made a claim
  - CyberRisk Policy put us in touch with a company that specialized in breaches – the goal was to minimize liability by following the law and protect the library and any affected parties
- Report was filed with the Internet Crimes Division of the FBI

Next Steps

- New server was created for the accounting system and accounting software reinstalled – with only data from the backup
- All staff were contacted and offered a help line and credit monitoring since it could not be determined if payroll data was breached.
- Instituted on-going end-user training for all staff.
- Upgraded Malware protection
- Expanded the use of Deep Freeze to include office computers.

Cost to the library:

- Accounting was down for approximately 1 week
- Over $36,000 to the library

CPIM

Center for Public Investment Management

A Program Brought to You By:

Robert Sprague

Ohio Treasurer

Cyber Security: Data Breaches
It Can Happen to You

Dusten Kohlhorst

IT Director

Ohio Treasurer of State

Local and state governments are facing an increase in threats and attacks.

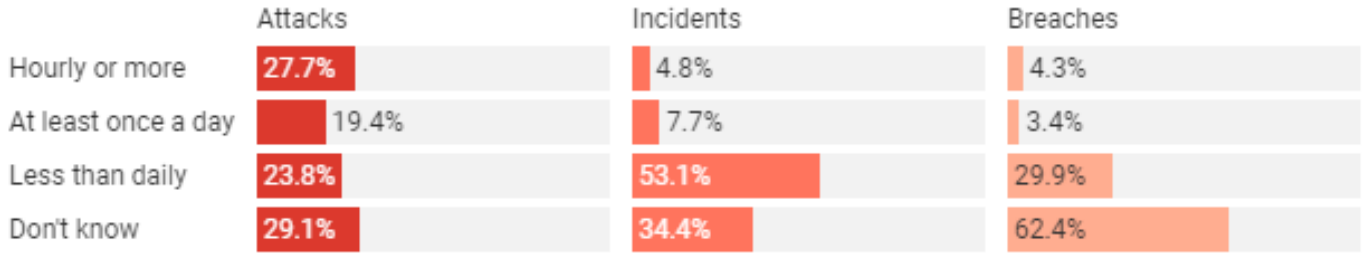
- 1/3 of all attack are ransomware
  - According to the FBI the top local attacks:
    - Ransomware
    - Payroll Account Hijacking
    - Unauthorized Wire Transfers
    - Illicit access to Internet of Things & Insider Threats
- 38 % of local governments are relying on technology that is at least one generation outdated
- Under 50% have purchased cybersecurity insurance

"It hasn't happened to me, so we must be secure."

"Oh, thank goodness it happened to them, I'm not sure what we'd do."

How frequently are local governments under cyberattack?

While many local governments know how often they're being targeted, a surprising number do not.



Attacks are attempts to gain unauthorized access to cause mischief or do harm. Incidents are events that compromise confidentiality, integrity or availability of a computer system. Breaches are incidents that result in confirmed disclosure of information to an unauthorized person.

Chart: The Conversation, CC-BY-ND • Source: University of Maryland, Baltimore County • Get the data

Do local governments know who's attacking them?

Most local governments said they cannot determine the types of attackers that attack their systems.

Chart: The Conversation, CC-BY-ND • Source: University of Maryland, Baltimore County • Get the data

Why aren't local governments practicing better cybersecurity?

Many of the barriers to better cybersecurity in local governments have to do with money – including to pay salaries and hire and train enough staff.

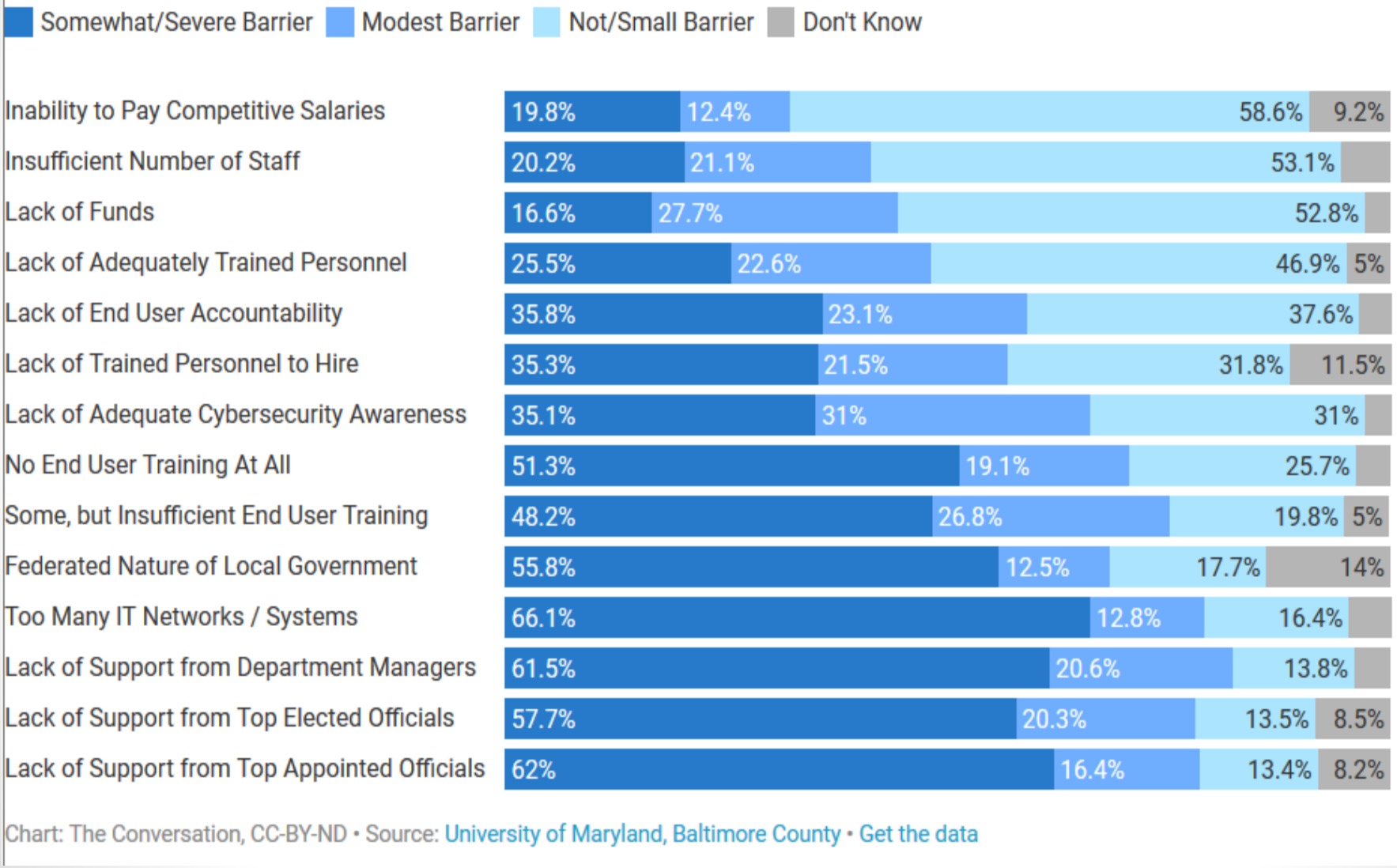
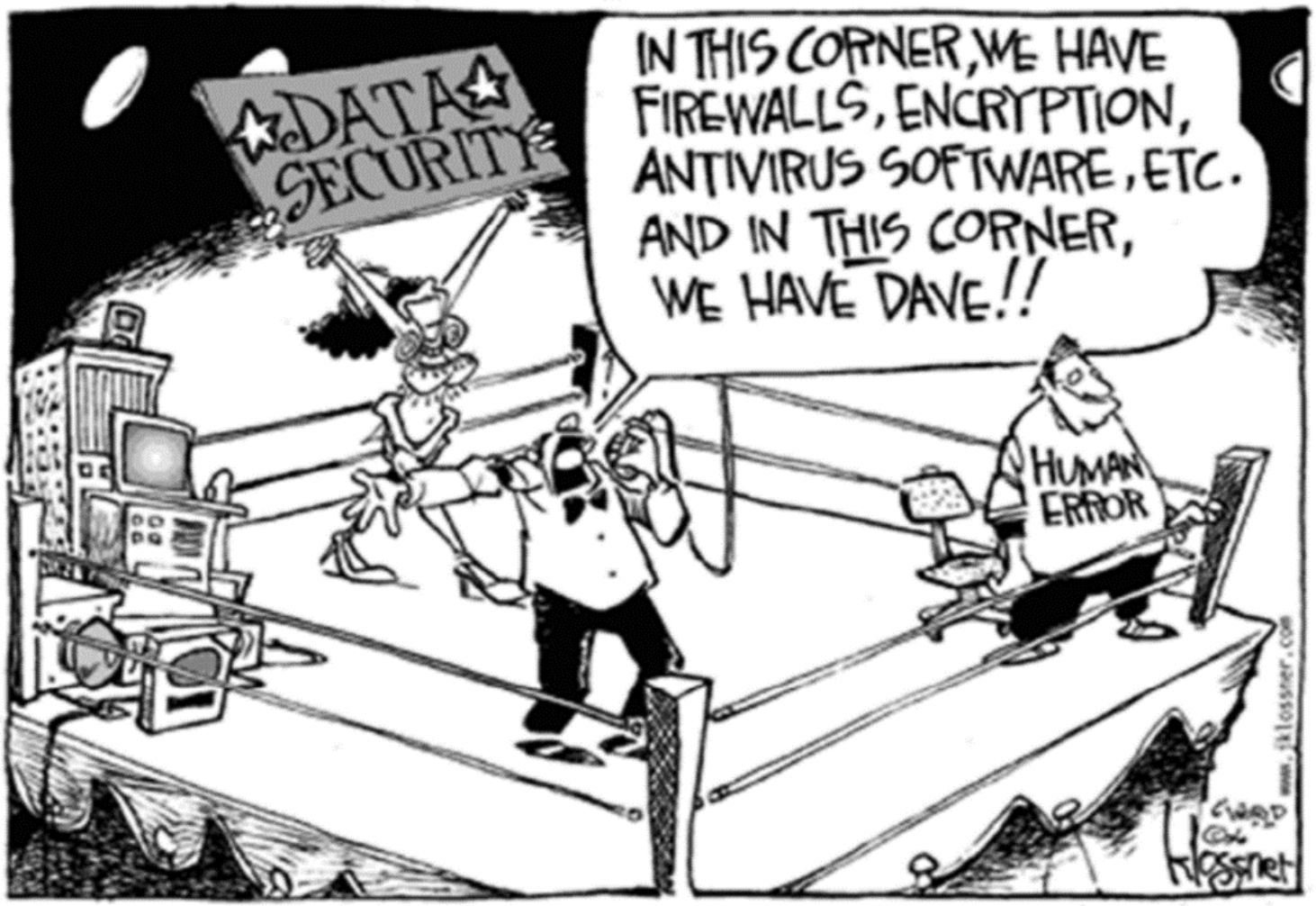


Chart: The Conversation, CC-BY-ND • Source: University of Maryland, Baltimore County • Get the data

Biggest risk:



How to help/stop Dave

- Give Dave only the permission he needs to do his job.
  - Do NOT make him a local administrator
- Backup Dave's data
  - Have a regularly scheduled backup of all of his important data
  - Test the restore of the backup at least quarterly
- Install antivirus/malware on his desktop/laptop
  - Make sure it's up to date
- Set his computer to automatically install patches from Microsoft.
- TRAINING: He should have regular cyber security training.
- HELP: He should know who to contact if…

Staff Education: Best protection

- A robust education program that all staff MUST complete
  - Email & phishing attacks:
    - Spear & Whale phishing attacks
    - Imbedded URLs
    - Attached Files
  - Sensitive personal data requests
  - Safer Web browsing
    - Pop-ups
    - Click-bait
  - WiFi & mobile security
  - Social Engineering
  - Physical Security
    - USB/Device safety (phone)

Ransomware: Best Protection

- Staff education
- Email awareness
- Minimum User Rights
- Antivirus/malware on all computers
- Regular Backups
- Security Patching
  - All computers, servers, switches, firewalls, etc.
- Limit connections/ports that are open to the world
- Use development best practices (no applications connecting directly to internal databases)
- Dual Factor Authentication

NOTE: Current Ongoing Attack

- Payroll officers: Being targeted with request by “higher ups” to change payroll deposit account.
- Has been very successful.