Cybersecurity Domain and Data Defense

Anthony Wayne Local Schools

Chris Hamady
Director of Technology

Devin Filip
Technology Supervisor

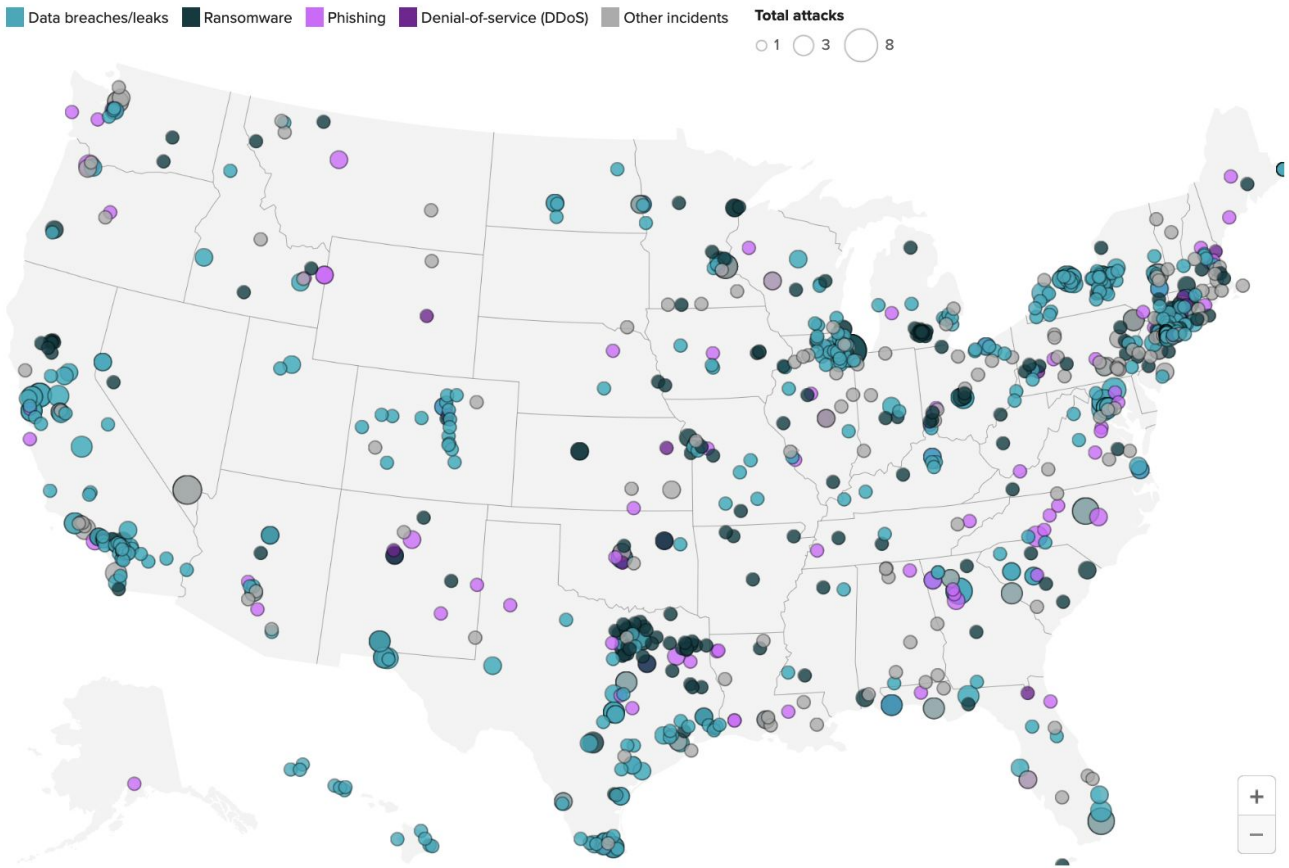
K12 School Attacks Are Increasing

Background- Why is this important?

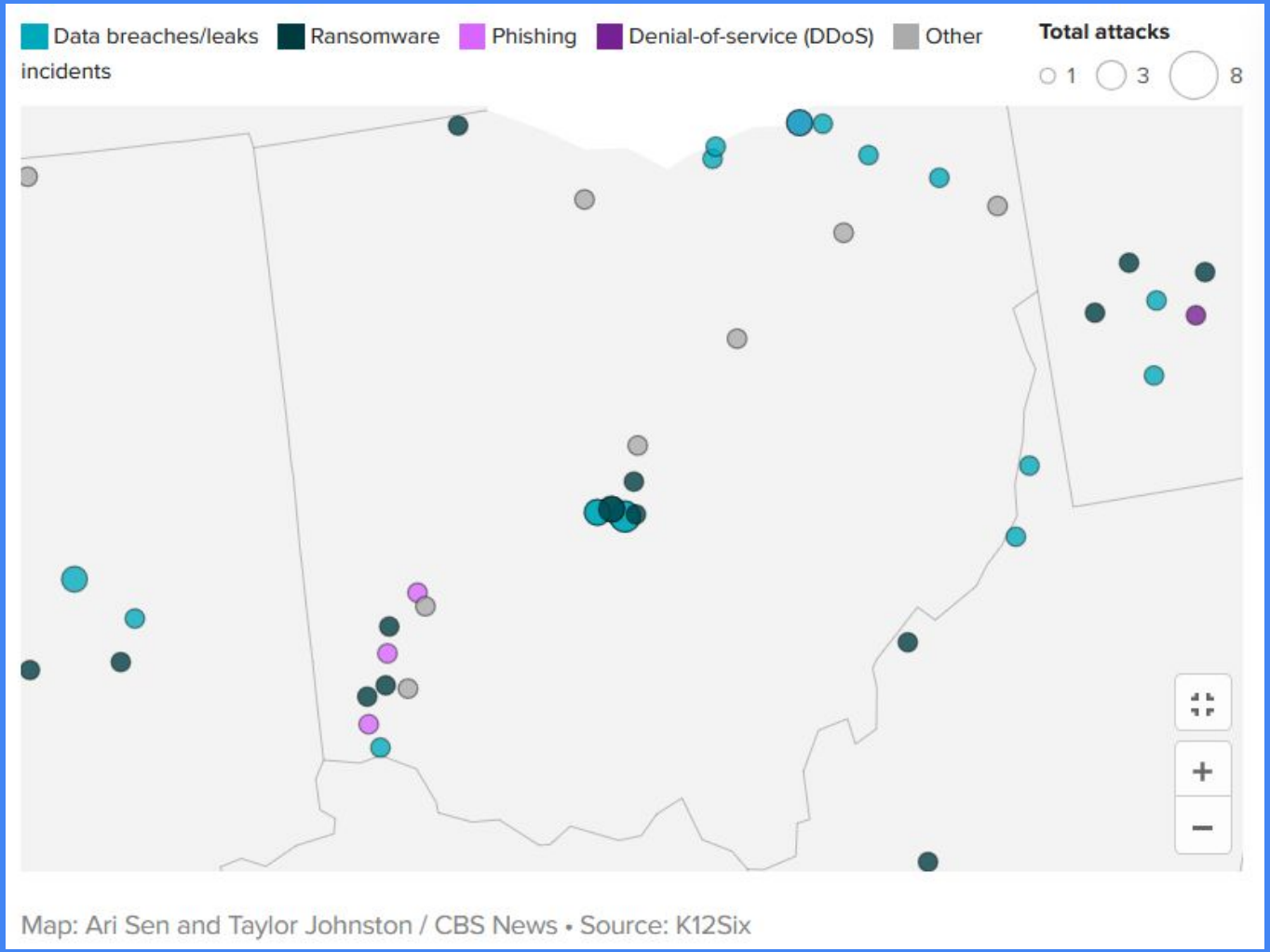
- Increases of data thefts
- Increases of ransomware attacks
- Increases of identity thefts
- Increases of phishing attacks (gift cards)
- Insurance requirements

Cyberattacks on school districts

Between April 2016 and November 2022, K12Six recorded over 1,600 cyberattacks targeting school districts across the U.S.



Map: Ari Sen and Taylor Johnston / CBS News • Source: K12Six


Data breaches/leaks
Ransomware
Phishing
Denial-of-service (DDoS)
Other
incidents
Total attacks
1
3
8
Map: Ari Sen and Taylor Johnston / CBS News • Source: K12Six

Usability vs Security

- We must balance security with usability.
- We are compelled to take action for the sake of security best practices, and also from mandates by insurance companies.

Insurance Questionnaires:

8:	If you have any end of life or end of support software, is it segregated from the rest of the network (for example VLANS)?	Yes ☐ No ☐ N/A ☐
9:	Do your users have local admin rights on their laptop / desktop?	Yes ☐ No ☐
10:	Can users run MS Office Macro enabled documents on their system by default?	Yes ☐ No ☐
11:	Do you perform vulnerability scans? If so are they carried out on:	Public Facing IP addresses ☐ Internal IP addresses Both ☐ No ☐
12:	Do you conduct Information Security risk assessments at least annually?	Yes ☐ No ☐
13:	Do you conduct penetration testing at least annually?	Yes ☐ No ☐
	If yes to any of questions 11-13, are there any outstanding critical	
14:	Do you encrypt portable media devices (e.g. laptops, smartphones, tablets, etc)?	Yes ☐ No ☐

Our Action Plan:

- Vet online instructional resources
- Enable device encryption
- Choose secure directory authentication
- Leverage single sign on with multi-factor authentication (PowerSchool and web resources)
- Configure secure device authentication along with multi-factor authentication
    - -Windows
    - -Mac
    - -Chromebooks
- Anti-virus (savings)
- Updates and patch management
- Backups, backups, backups!
- Device End of Life (EOL) plans
- Disaster recovery drills

For Your Home Defense...

- Physical Security
- Passwords
- Browser Choice
- Use Multifactor Authentication
- Recognize and Report Phishing
- Software and Device Updates
- Keeping Yourself Informed
- Freeze Your Credit
- Have I Been Pwned
- NPD Breach

Physical Security #1

- Your home
- Your car
- Your computers
- Your tablets
- Your phones
- Your passwords

CISA Password Recommendations:

Encourage Strong Passwords in the Workplace

Create a safer workplace by establishing smart employee password practices.

1. Require strong, unique passwords.

Keep your networks secure by enforcing strong password policies. Strong passwords are:

- **Long**—at least 16 characters long (even longer is better).
- **Random**—like a string of mixed-case letters, numbers and symbols (the strongest!) or a passphrase of 4 –7 random words.
- **Unique**—used for one and only one account.

Passwords

- Make them Long (16+ characters)
- Make them Random (numbers, symbols)
- Make them Unique (never reuse)
- Avoid identifying information in its entirety
  - Birthdays
  - Pets names
  - Kids names
  - Anniversary year
- How will I remember them?
- How do I store them?
- Password manager?
- Browser password managers?

Passwords


LastPass
Try Business for free
Blog
Recent
Industry News
LastPass For Admins
LastPass Labs
Product Updates
Tips And Tricks
PRODUCT UPDATES
12-22-2022: Notice of Security Incident

Passwords

root- Eber Lassie 2025

CoeberStlassieCo2025$6 (Costco)

WaeberLmlassieArt2025$6 (Walmart)

HueberNtlassieIngton2025$10 (Huntington)

Passwords

Eber Lassie 2025

CoeberStlassieCo2025$6 (Costco)

WaeberLmlassieArt2025$6 (Walmart)

HueberNtlassieIngton2025$10 (Huntington)

Browser Choice

- Some browsers are more secure than others.
- Brave browser
- Firefox browser
- Some browser extensions can help
  - Ublock Origin

Turn on Multi-Factor Authentication (MFA)

What is MFA??

- Adds a layer of security to your account
- Combines something you *know (username/password)* with something you *have (your phone)* or something you *are (fingerprint, face)*
- Makes it harder for someone to impersonate you
- Protects against security breaches and leaked credentials

Turn it on!

- Each website or service you use will have its own method to turn on MFA
- Sometimes it's required, most times it's optional
- Look for it in the website settings
- You may receive your MFA code via email, text message, or by using an authenticator app on your phone
- Start with your most sensitive data and then enable it everywhere

Recognize and Report Phishing

What is Phishing?

- Phishing occurs when criminals try to get us to open harmful links, emails or attachments that could request our personal information or infect our devices.
- The “bait” usually comes in the form of an email, text, direct message on social media or phone call.
- Messages from a trusted person or organization, to get us to respond.

Recognize, Resist, and Delete!

- Look for the signs
  - Urgent or emotionally appealing language
  - Requests to send personal and financial information
  - Incorrect email addresses or links
  - Poor grammar or misspellings
- If you are unsure DON’T CLICK IT!
- Contact the organization in a known trusted method of communication
- Report if possible, and then delete

Recognize and Report Phishing

New Phishing Methods

- QR Code manipulation
- Can embed a phishing site into the QR code
- Can insert a link to a malware site that downloads malware or pulls data from your device

Stay up to Date

Keeping your software updated

- Watch for update notifications
- Install the updates as soon as possible
- Turn on automatic updates
- All your electronics use software
  - Computer
  - Phone
  - Watch
  - Thermostat
  - TV
  - Home network router
- Avoid cheap IOT devices

Keeping yourself up to date

- Security is always changing
- Look for new security settings on your phone or service that you use
- Read the notifications from services that have your data
- Stay informed
  - CISA.GOV
  - have i been pwned?
  - NPD Breach

Have I Been Pwned

https://haveibeenpwned.com

NPD Data Breach

https://npd.pentester.com/

Freeze your Credit

- A credit freeze restricts access to your credit report. If you suspect your personal information or identity was stolen, placing a credit freeze can help protect you from fraud.
- It's 100% free
- You can do it online
- You can unlock it whenever you need to
- Protects against identity theft
- https://www.usa.gov/credit-freeze
- Experian, Equifax, TransUnion
- YouTube

What else can I do?

- Standard user accounts on computers without admin access
- Firefox or Brave + Ublock Origin.
- Don't open email you weren't expecting
- Don't install software that you aren't 100% sure is legitimate
- Don't click links in email.
- Ignore phone calls from strangers.
- Can you really trust voicemail?
- Confirm anything financially related by calling parties directly.
- Don't allow people to use your computer or phone.

CISA

https://www.cisa.gov/secure-our-world

Questions?

Thank You