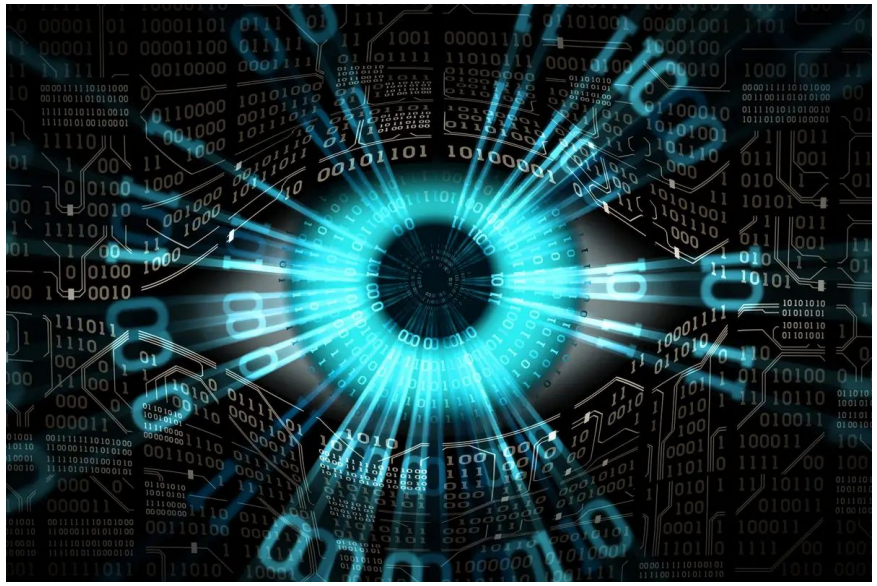
Life of a Cyber Attack from the Eyes of the Superintendent & Tech Director



This presentation is to be informative and not to promote specific products, services companies, etc. Illinois ASBO Sponsored Programs are permitted to promote products and services in accordance with the Service Associate Ethics Policy and Code of Conduct.

2024 ANNUAL CONFERENCE

#iasboAC24

INVEST IN YOURSELF IGNITE OTHERS

Introductions

Name: Andrew D. Johnson
Role: Speaker
- *Superintendent, Effingham Unit #40*

Name: Emily Flach
Role: Speaker
- *Technology Director, Effingham Unit #40*

Name: Jan Bush
Role: Moderator

Effingham Unit #40: At a Glance

- PreK-12 School District
- 2400 students
- 6 school buildings + 4 support buildings
- Technology Environment (not a Chromebook district!)
  - PreK and K: iPads
  - 1st-5th: Laptops stay in classroom carts
  - 6th-12th: Laptops go home nightly
  - Teachers: Issued a laptop, a desktop, and a smart display

Food For Thought

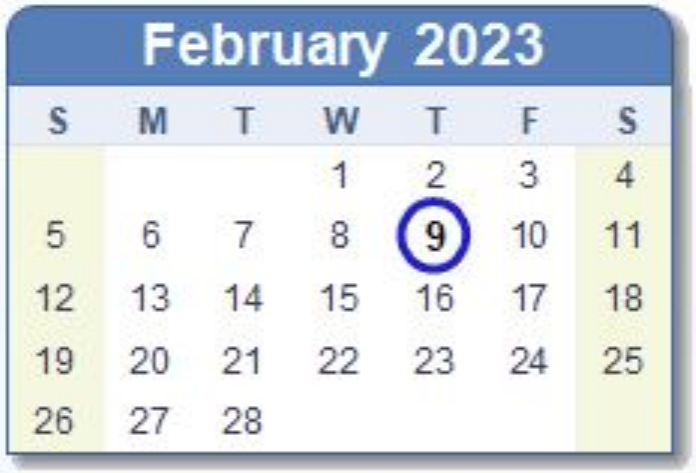
Cybercriminals come for schools — and schools aren't ready

Cyberattacks have become a growing threat to school districts across the country in recent years, with cybercrime gangs viewing school systems as soft targets because of their lack of cybersecurity infrastructure. While many school districts are starting to take steps to secure that infrastructure, there's still a long way to go, according to experts.

https://hechingerreport.org/cybercriminals-come-for-schools-and-schools-arent-ready/

The news…


6:15


February 2023
S M T W T F S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28

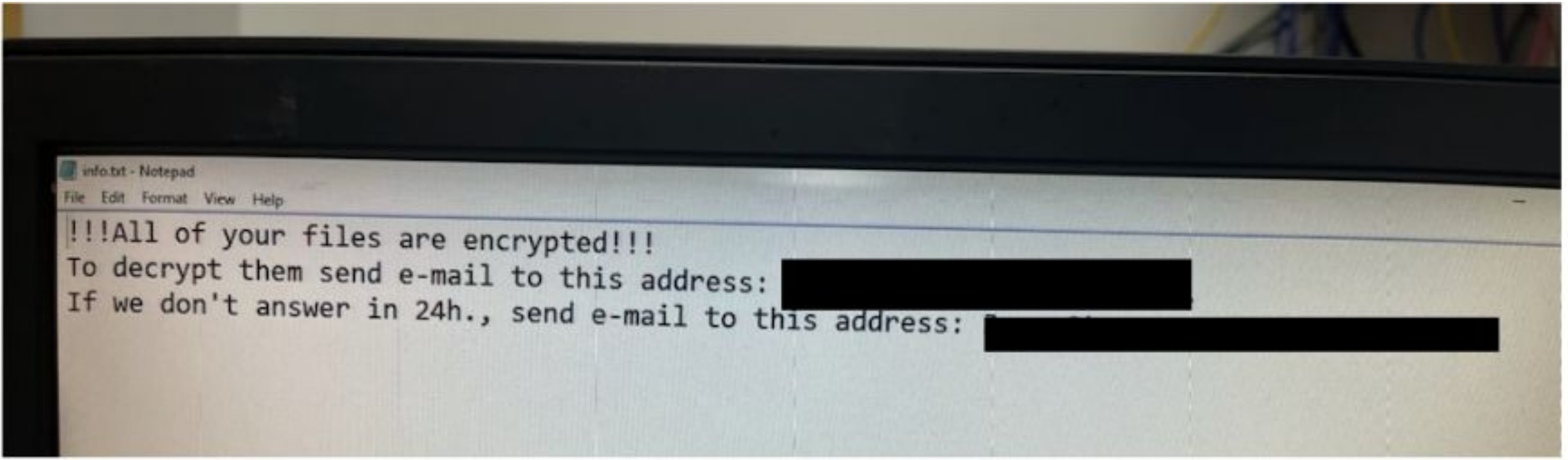
“We’ve been hacked.”

“It’s bad.”

“Somehow it got the servers.”

“We are in trouble.”

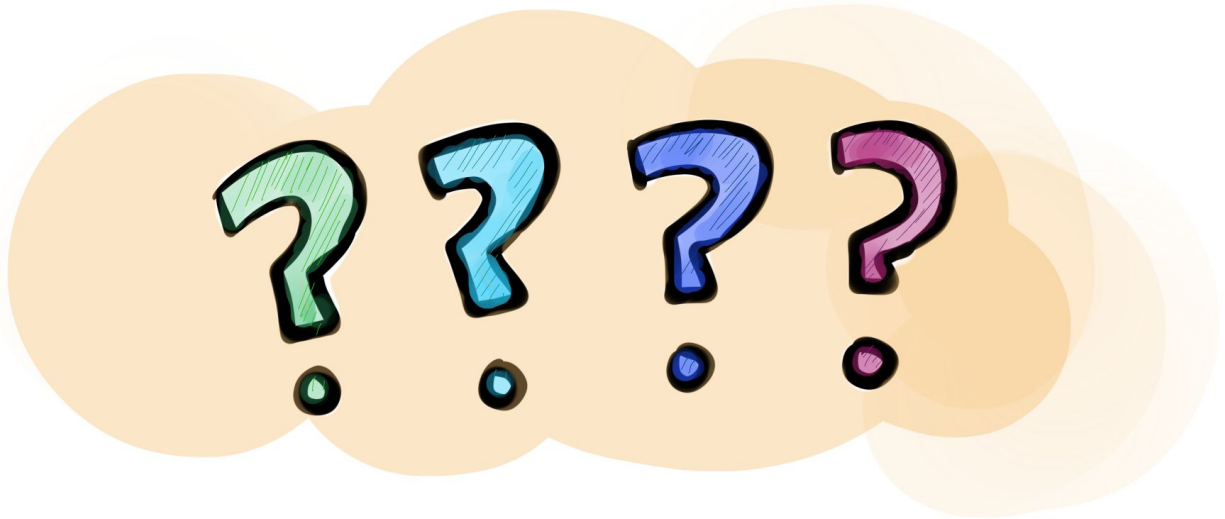

encrypted
All your files have been encrypted!
All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail [redacted]
Write this ID in the title of your messag[redacted]
In case of no answer in 24 hours write us to this e-mail: [redacted]
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.
Free decryption as guarantee
Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 4Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)
How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to regster, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/
Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.


info.txt - Notepad
File Edit Format View Help
!!!All of your files are encrypted!!!
To decrypt them send e-mail to this address: [redacted]
If we don't answer in 24h., send e-mail to this address: [redacted]

Thursday, 2.9.23

- Triage
- Travis Roundcount/Billy Rockey at Mt. Zion
  - Mt. Z was hit 2/6/2019
- Disconnect the network! Too soon?
- Garrett Discovery Inc (GDI) in Champaign, IL
  - On property pulling machines and data by 2pm
  - NDA for all initially involved
- Effingham PD and FBI
- Notified our lawyer
- 5:00PM: Voice message sent for a school closure on Friday, 2.10.23

Unknowns and Questions on Thursday, 2.9.23



Friday, 2.10.23 at 3:51 AM

#iasboAC24

2024 ANNUAL CONFERENCE

INVEST IN YOURSELF IGNITE OTHERS

Friday, 2.10.23

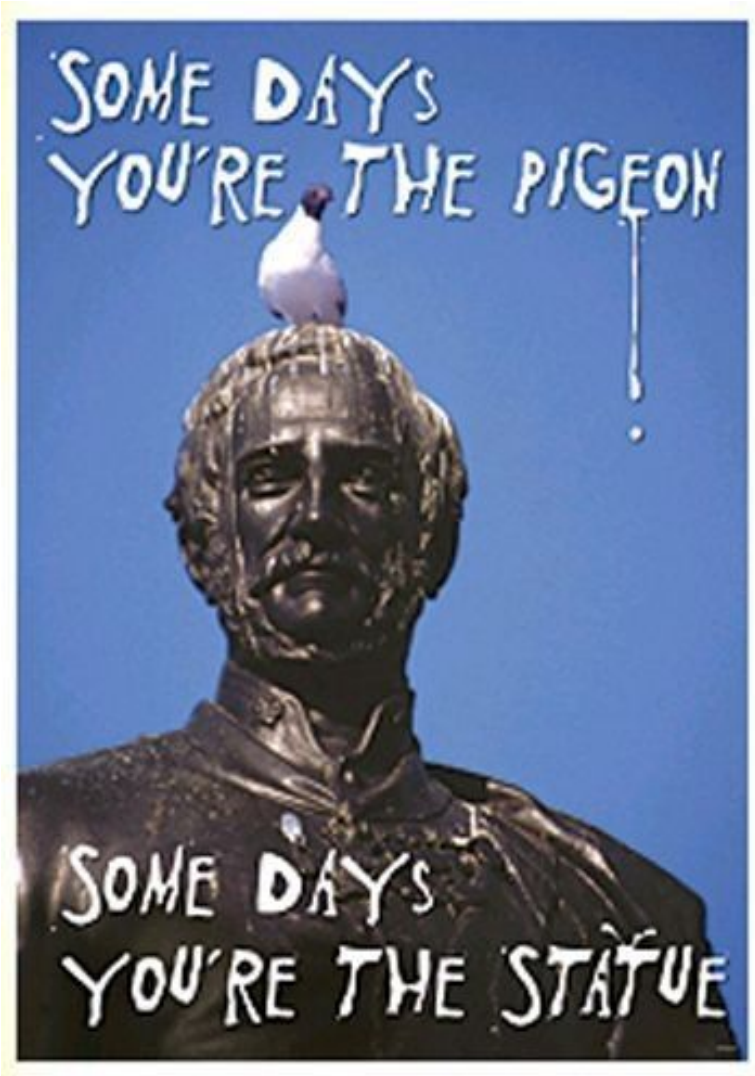
- Investigation continues
- Worked on getting data back
- **12:30am**
  - Outlined mission critical systems and identified what we HAD to get back & estimated costs

Saturday, 2.11.23

- **10:00am**
  - Met with cabinet in-person
  - Questions on all day-to-day operations

Saturday, 2.11.23

1:00pm



Super Bowl Sunday 2.12.23 at 5:08pm

#iasboAC24

Monday, 2.13.23

- Teacher Institute Day
- Debrief on situation
- Time to shift to teaching without ANY technology
  - Contrast to the times of covid
- Priorities for us:
  - Offices up and running
  - Copiers (disconnected from the network) available with toner and paper

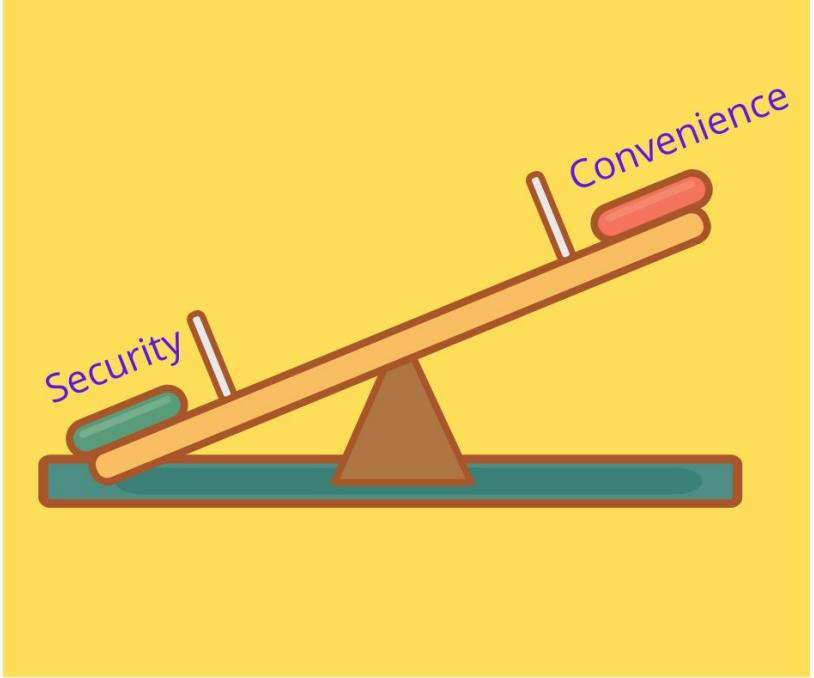
Communication During the Incident

Communication During the Incident

- Coached to call it a “Cyber Incident” or “Network issue” for security
  - Don’t draw attention to your district or situation
- Updates to public at same time every day (5pm)
- How to Update Staff Without Email
  - Our answer: Big chart paper
- Suggestion: Have cell phones for each building AND with the numbers readily available
- “Don’t bother tech staff!”- important to say and stress
- Enforced & tightened chain of command

8 Things to Secure Your Digital Environment

1. Upgrade/Update to Software
2. Research Antivirus Software Options
3. Keep your Network Secured
4. MFA/2FA/Two-Step
5. Cyber Insurance
6. Train your staff and students
7. Plan for Day-To-Day Operations with No or Limited Technology
8. IT-Minded Security Measures



The things I never heard in a ransomware presentation but wish I had …

Actionable Items You Can Also Do NOW

- Prioritize your staff for return of access/technology
- Identify digital vs hard copy curriculum
- A plan for Standardized Testing (IAR, ISA, Access) on **PAPER**
- Outline Cloud-Based vs Non-Cloud Based Systems
- How will you keep track of who is “up and running”

CAN'T PREPARE FOR…

- Psychological Impact-
  - Paranoia and suspicions will be FIERCE
- Emotional toll
- Staff fear they caused it
- Unrelated issues blamed on the incident
- Lack of understanding of how technology works
- Software sales reps
- Won't be thinking clearly due to late nights and donut diet

2024 ANNUAL CONFERENCE

#iasboAC24

INVEST IN YOURSELF IGNITE OTHERS

Encounters & Decisions During the Event

Network & Devices

Teaching and Learning

Finances/Financial System

Celebrations from Our Experience

- Cost to our district was minimal
- We never missed a payroll
- Retain your technology staff
- Staff and student data was not breached that we are aware of
- Educators CAN educate without technology
- Our staff, students and our community were amazing and supportive

Questions and Answers

We thank you for your time!

Presenters:

PANELISTS INFO:

Andrew D. Johnson, Superintendent; Effingham Unit #40
(217) 540-1500; johnsona@unit40.org

Emily Flach, Technology Director; Effingham Unit #40
(217) 994-2617; flache@unit40.org

Extra Resource Slides

Return of Services Timeline (2.9.23)

The following table outlines the approximate dates that our systems returned to "normal" use after our cyber incident.

Service/Equipment	Timeline
Phones	February 13th - February 20th
Security Cameras	February 13th - February 20th
Payroll and Admin Accounting Functions	February 13th
Security Access/Badges (always accessible)	February 13th
Access to Google Accounts (only after 2FA has been set up)	February 13th - No End Date
One Device per Staff	February 13th - March 13th

Return of Services Timeline (2.9.23)

Printers and Copiers	February 13th - March 13th
HVAC	February 2023
Teacher Interactive Panels (Displays) Without Wifi	February 28th - March 13th
Food Service Software	February 28th - March 24th
Student Labs	March 13th - March 24th
Wifi Access	March 17th - August 2023
Teacher Laptops: 2nd Device for Most Staff	February 24th - May 2023

Return of Services Timeline (2.9.23)

Employee Access to Financial System (on network only)	February 2023 - May 2023
Guest Wifi Configured and Procedures Established	July 2023
Wifi Access for Interactive Panels (Displays)	May - August 2023
Student Laptops	May - August 2023
iPads	May - August 2023
District Online Assessments	August 2023
State Mandated Assessments (IAR, ISA, Access, DLM, etc)	Will be available when state testing windows open (the first opens January 2024)