
go
cyber
COLLECTIVE

June Announcements

Serving Our Communities

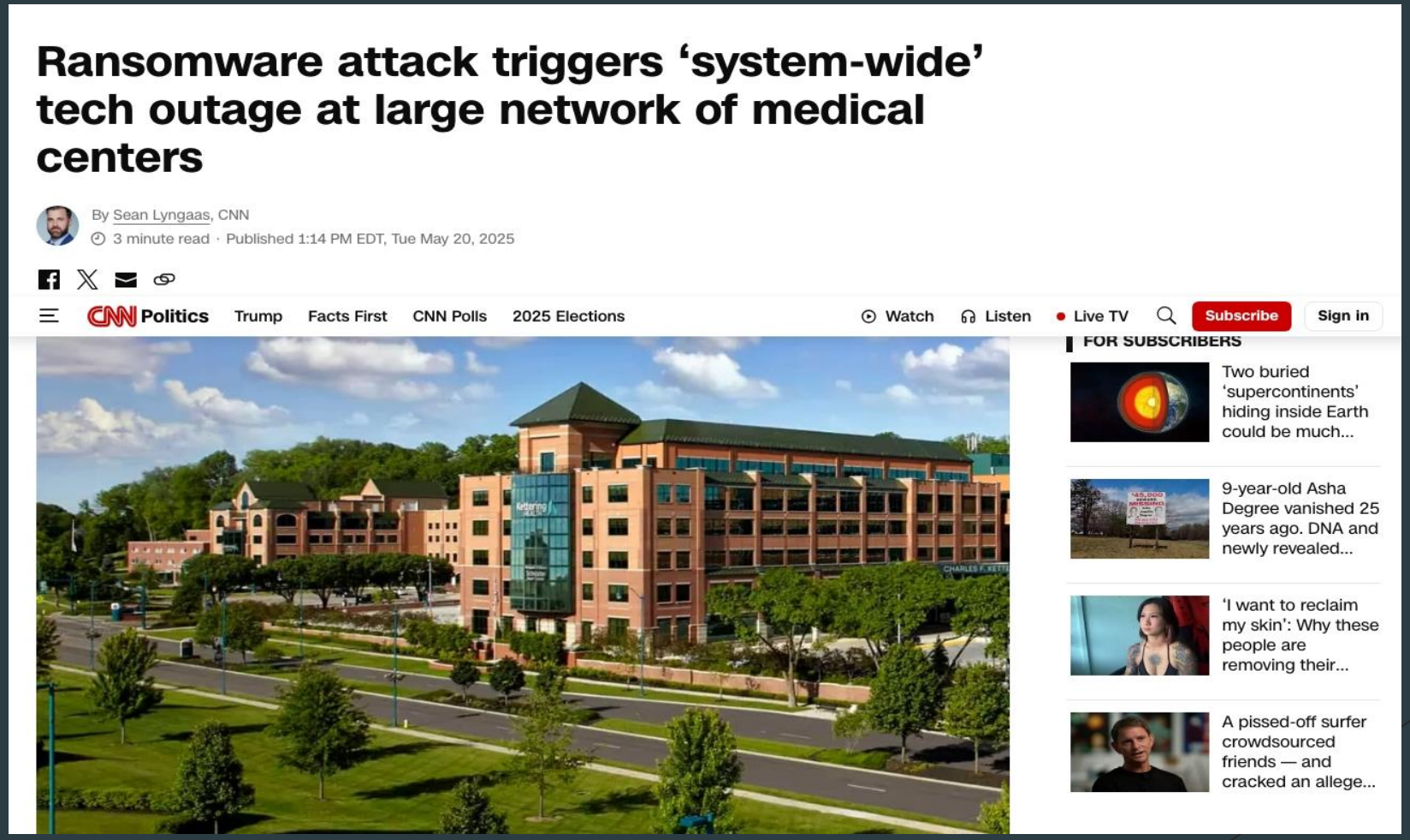
- Thank You, Fortinet!
- Congrats to Shawn Waldman for appointment to the Board of Voting Systems Examiners (BVSE)
- Road to Zero Trust a HIT! Thank you, Randy Hinders!
- HIPPA & LEADS workshops in the pipeline
- Municipal Cyber Summit 8/21

June Announcements

Serving Our Communities

- Incident Response Course (Two Day Workshop)
- Cympire as a service: Play inside the world's premier range
- Cyber 101 for Law Enforcement Sep. 9
- Sponsorship Committee
- *Safe Senior Surfing* and *Healthy Digital Families* are serving at-risk populations

Kettering Health Hit Making National Headlines



Ransomware attack triggers ‘system-wide’ tech outage at large network of medical centers

By Sean Lyngaas, CNN
3 minute read · Published 1:14 PM EDT, Tue May 20, 2025

CNN Politics | Trump | Facts First | CNN Polls | 2025 Elections | Watch | Listen | Live TV | Subscribe | Sign in

FOR SUBSCRIBERS

Two buried ‘supercontinents’ hiding inside Earth could be much...

9-year-old Asha Degree vanished 25 years ago. DNA and newly revealed...

‘I want to reclaim my skin’: Why these people are removing their...

A pissed-off surfer crowdsourced friends — and cracked an allege...

Cyberattack Vitals

-System-wide Technology Outage

-Procedures Cancelled

-KH claims to have not paid ransom. Interlock released data allegedly from cyberattack.

-Class-action lawsuit against KH seeking "Monetary damages, restitution, and/or injunctive relief."

June GoCyber Collective Keynote Speaker

- Eric Fisher
- District Technical Director - Mad River Local Schools
- Certified Education Technology Leader
- Leader of Education SIG (Special Interest Group)

THE TOTAL COST OF A CYBER INCIDENT

ERIC FISHER –TECHNOLOGY SUPERVISOR MAD RIVER LOCAL SCHOOLS

COMPANY INFORMATION

- 8 Schools, Maintenance, Transportation and Board of Education Offices
- 700 Employees, contractors, and Student Teachers/Interns
- Approximately 3600 Students from PK – 12
- Approximately 5100 Windows PC's
- Approximately 35 Windows Servers
- Approximately 40 Macintosh Devices
- Approximately 350 tablets (iPad and Android)
- Technology Staff (2 Full Time, 4 Part Time)

WHAT HAPPENED

1. Early Morning of August 29, 2019 Foreign actors downloaded the Malware
2. 6:30am that morning staff started to report internet not working
3. 7:45am first Technology staff arrived onsite to start working on figuring out the internet issue
4. 8am Technology staff found the Notification of the Malware on devices
5. 9am all Windows devices that were attached to internal network was encrypted with the Malware

WHAT NEXT….

1. **Initial thoughts of Technology Staff**
2. **Notification of complete damage to Senior Management**
3. **Steps taken after this to see what we could do.**
    1. Consult Fellow IT Professionals
    2. Consult Cyber Company
    3. Contact Insurance
    4. Contact Law Enforcement
4. **Next thoughts of Technology Staff and where to go next.**

RECOVERY PROCESS

1. **Work with Insurance provided Forensics**
2. **Work with USSS to start process to find threat actors and possible decryption key**
3. **Work on plan to restore the devices in the most secure process**
4. **Enlist help from staff to aid in a quicker recovery time**
    1. Senior Management
    2. Admin Assistants
    3. Teachers

IMPACT OF RECOVERY

1. **Total time before majority of items recovered**
    1. Phone systems – 1 Week
    2. Workstations for Staff – 3 weeks
    3. Servers – 8 weeks for 95% recovery.
        1. 3rd Party Vendor installs drug this out
    4. Printing 2 Weeks
    5. Network Operational
        1. Partial Capacity 5 days
        2. Full Capacity 4 Weeks
2. **School adjusting to limited technology for 4 weeks**
    1. Challenges for running with limited technology
3. **Financial Cost to Recover ~ $500K**

STAFF TIMELINE

1. **First Week – Understanding the Situation**
2. **Second Week – Frustrations Starting**
3. **Third Week – Questioning the Restoration Timeline**
    1. Why was the order chosen
    2. Why were they not higher priority
4. **Fourth Week – “Why Do We Need to Help Technology”**
5. **Fifth Week – Anger to Degraded Systems Still**
6. **Sixth Week – Extreme Anger to Requests to Help Fellow Staff**
7. **Beyond – Technology Doesn’t Really Have a Handle on This**

TECHNOLOGY HUMAN COSTS

1. **Stresses on the Technology Department**
    1. Feeling inadequate to defending your network
    2. Personal Toll on not being able to help and repair the network faster
    3. Coordinating all Recoveries, Insurance, LEO's, Staff Communications
    4. Staff Burnout on recovery from working long hours for weeks on end
    5. Personal Attacks from staff on issues involving them and not being able to correct their issues immediately
    6. Personal Family Hardships
    7. Physical Toll on Staff
    8. Relationships with other staff

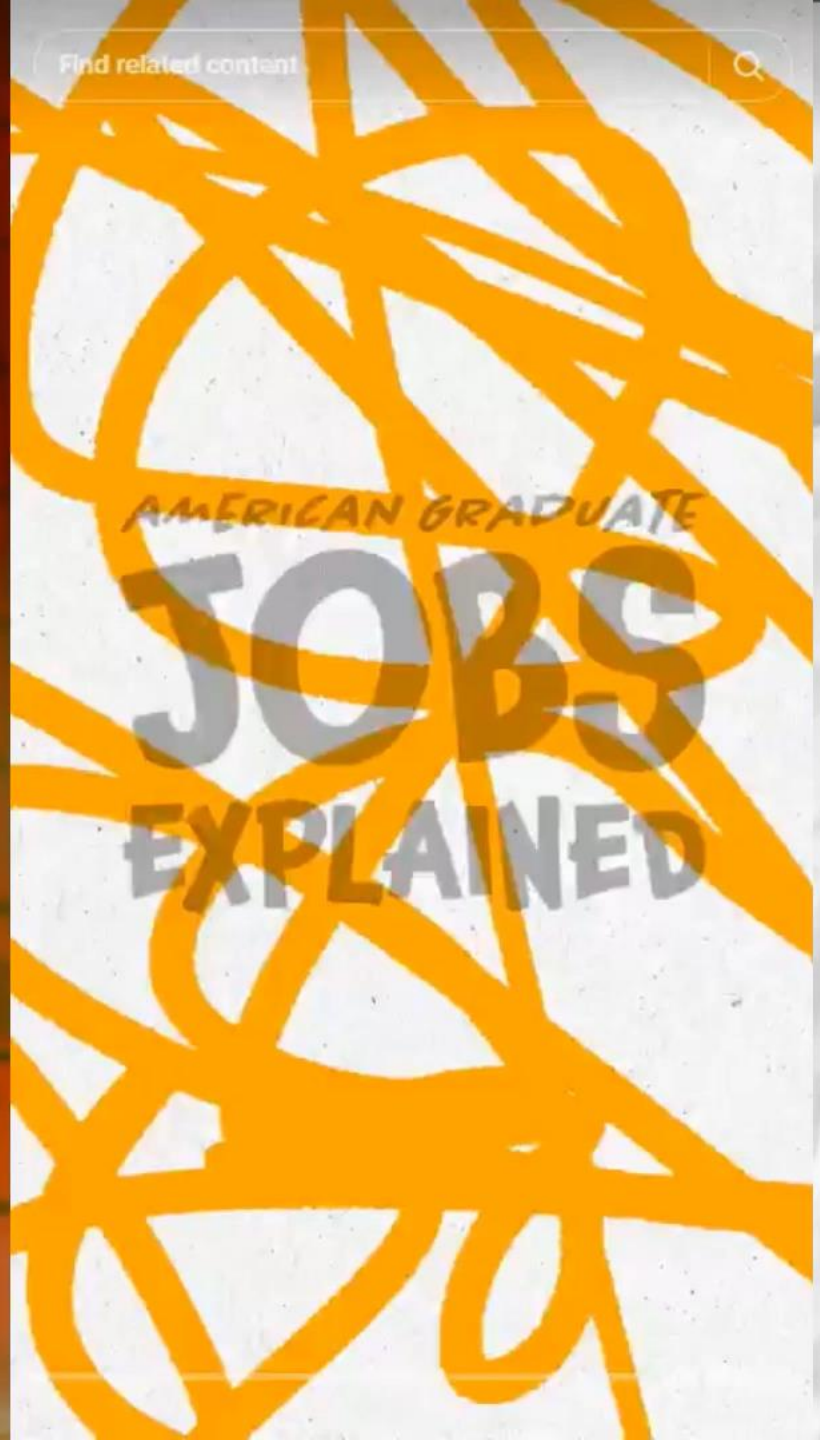
MOVING FORWARD

1. Trust with staff was severely damaged. How to recover the trust
2. Keeping items working while trying to bolster security
3. Educating staff on why security improvements are necessary
4. Explaining to staff why we will not release Patient Zero Identity
5. Building policies and procedures to minimize future threats
6. Working to spread the knowledge of what we learned during this process to others

June GoCyber Collective Spotlight Speaker

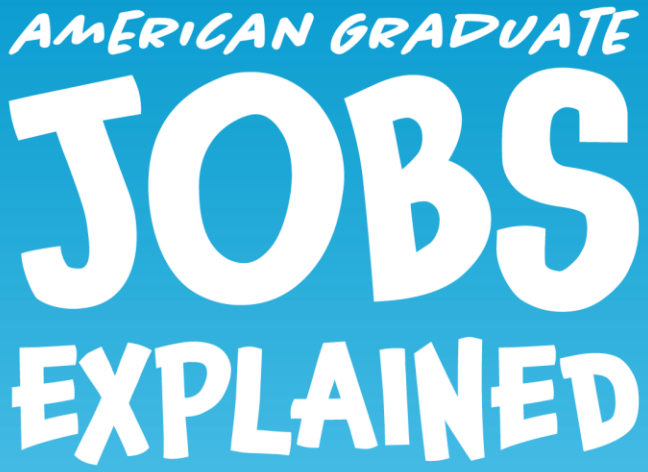
- Josie Masset
- ThinkTV Social Video Specialist – *American Graduates: Jobs Explained*
- Showcasing Jobs in Cybersecurity, Healthcare, etc.
- Connecting Local Youth to Education, Training and Job Opportunities


Find related content


Find related content
AMERICAN GRADUATE
JOBS
EXPLAINED

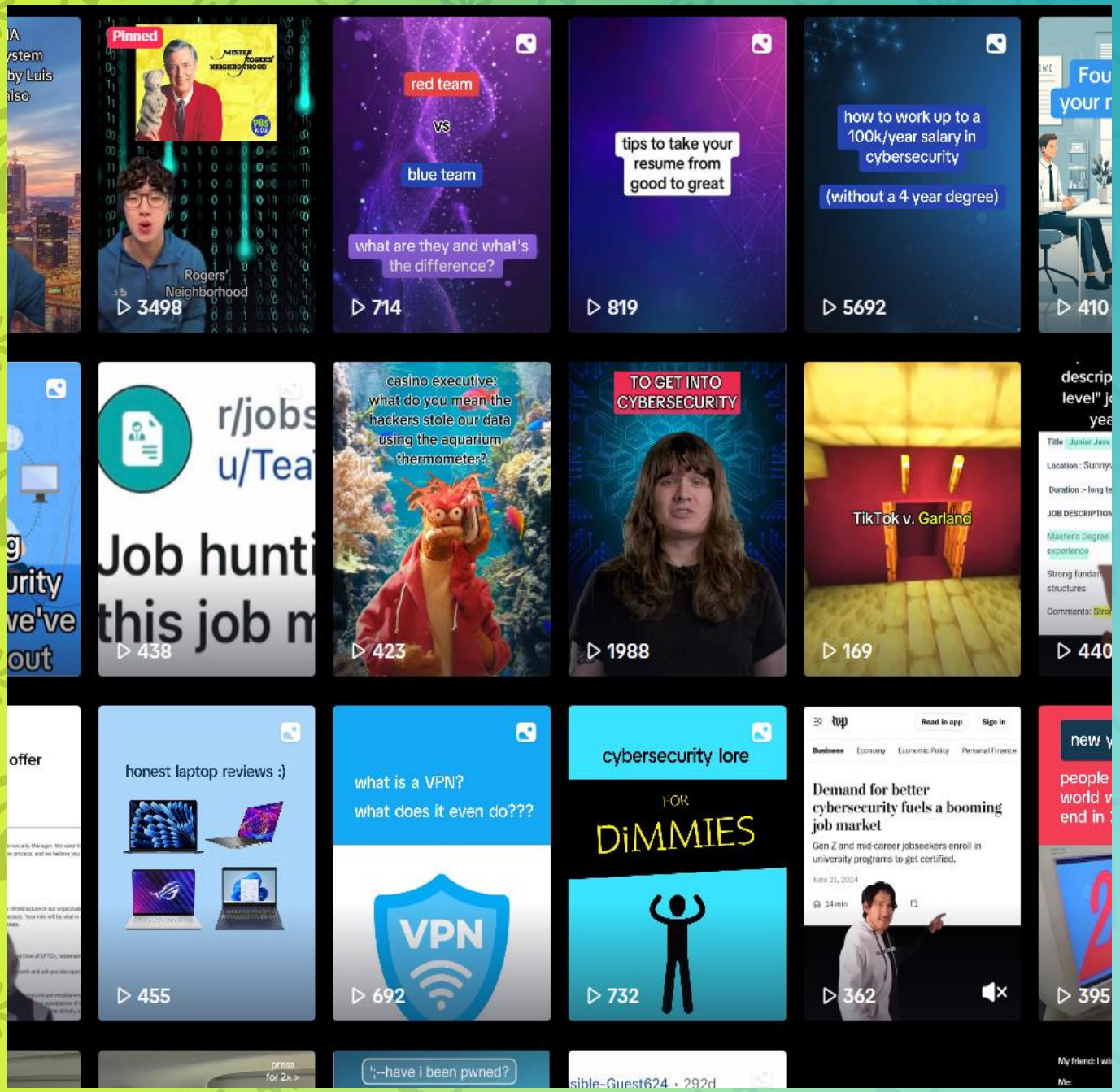

Find related content
"TELL ME ABOUT YOURSELF"
FORMULA
PRESENT
PAST
FUTURE
00:11/00:55

X



Jobs Explained Southwest Ohio

Connecting young people with in-demand jobs in their communities



What is it?

- Two-year partnership with *American Graduate: Jobs Explained*
- Digital initiative to educate young job-seekers on in-demand careers
- Short-form videos
- Focus on specifics and actionable information

Industries of Focus

- Cybersecurity
- Healthcare
- Hospitality

The Chase

- Pros across all fields
- Early in their career
- Interviews, shadowing, etc.
- Niche jobs
- Contacts

@jobs.explained

Business Advisory Committee

- Leading experts and leaders
- 6-8 Zoom meetings
- Guidance and feedback
- 8-12 hour total commitment

Connect with Us!

@SWOhioJobs_Explained

Scan to join
our contact list!

Josie Masset

ThinkTV

Social Video Specialist –
American Graduate:
Jobs Explained

jmasset@thinktv.org

(937) 220-1673

June Threat Briefing

- Jeff Boutell: Warren County Telecom Cybersecurity Analyst

June Threat Briefing

- AI-Powered Phishing Campaigns Exploiting Generative AI Platforms
- Zero-Day Exploits Targeting Chrome V8 Java PScript Engine (CVE-2025-12345)
- Ransomware and Botnet Campaigns Targeting Supply Chains

July Speaker
Mike Beagles – Mission Critical Partners

- Director of IT
- MCP's public safety and justice marketplace mission
- Risk assessment, vulnerability management and incident response
- Lessons Learned: Securing corporate enterprise

June Parting Shots

- Local Gov't/Public Safety SIG – Sun Watch Room
- Education SIG – Hawthorn Room
- Defense Contractor SIG – Wright Patt Room
- Sponsorship Committee
- Turn in your lanyards at the desk

Information

Email me at john@GoCyberCollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

You can register for future breakfast meetings from the website.

- GoCyberCollective.org

Event Sponsors

SECURECYBER™

Proven. Proactive. Personalized.

FORTINET®