SECURECYBER
Proven. Proactive. Personalized.

City of Huber Heights Ransomware Attack

Response and Recommendations

Presented to Ohio GFOA Conference September 26, 2024

Introductions

James Bell, *Director of Finance, City of Huber Heights*

Shawn Waldman, *CEO,* SecureCyber

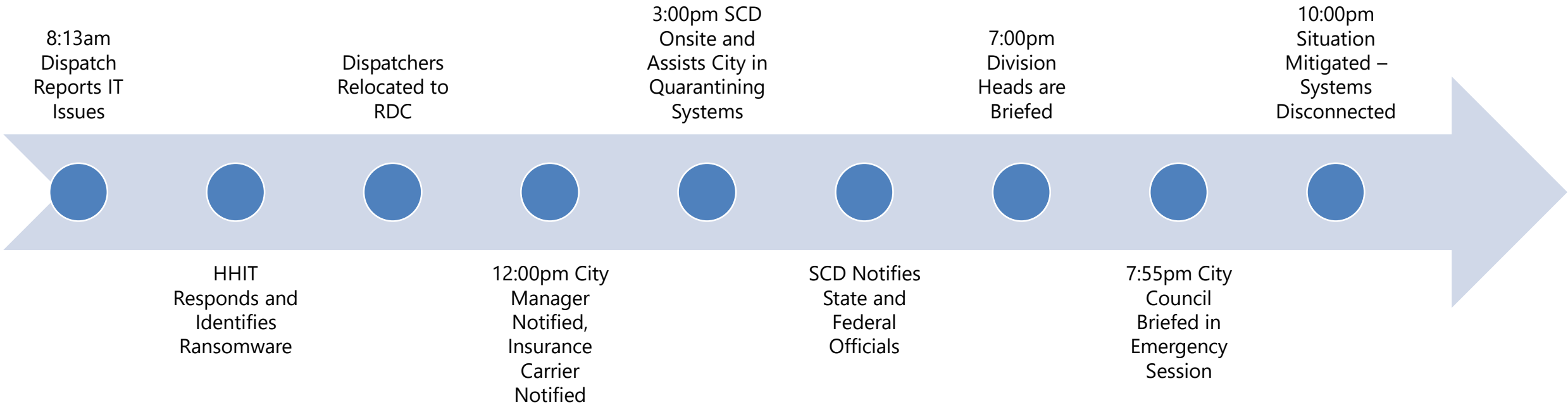
HUBER HEIGHTS

SECURECYBER

Background

- New City Manager was hired September 11, 2023.
- Huber Heights IT Director resigned effective November 3, 2023.
- Prior to his departure IT Director had completed Phase I of virtual local area network (VLAN) deployment.
- Phase II would have secured and isolated these VLANs, but was not yet been completed.
- City was preparing for a cybersecurity review and upgrade.
- From the beginning of the incident the ability for public safety to operate was unaffected.

Timeline – Sunday, November 12, 2023



Timeline – Monday, November 13, 2023

Insurance Carrier Engages Outside Legal, Forensic Investigation and Threat Negotiation Vendors

City Suspends all Late Fees and Utility Shut-offs. Critical Public Safety Services Unaffected.

4:00pm Kickoff Call Scheduled with Vendors

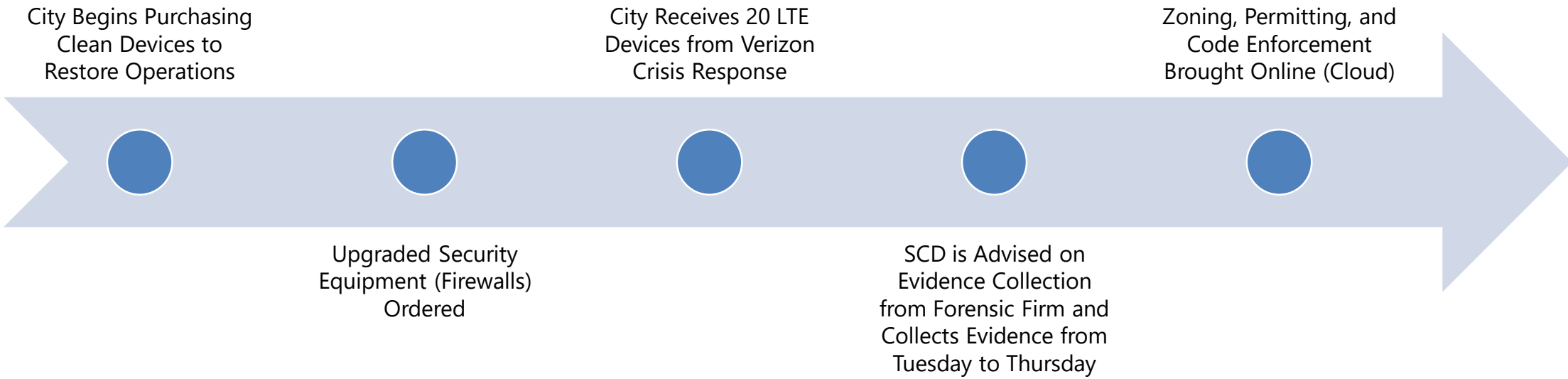
6:00pm Council Holds Regular Session, Passes Emergency Resolution, Authorizes City Manager up to $350,000 Spending Authority

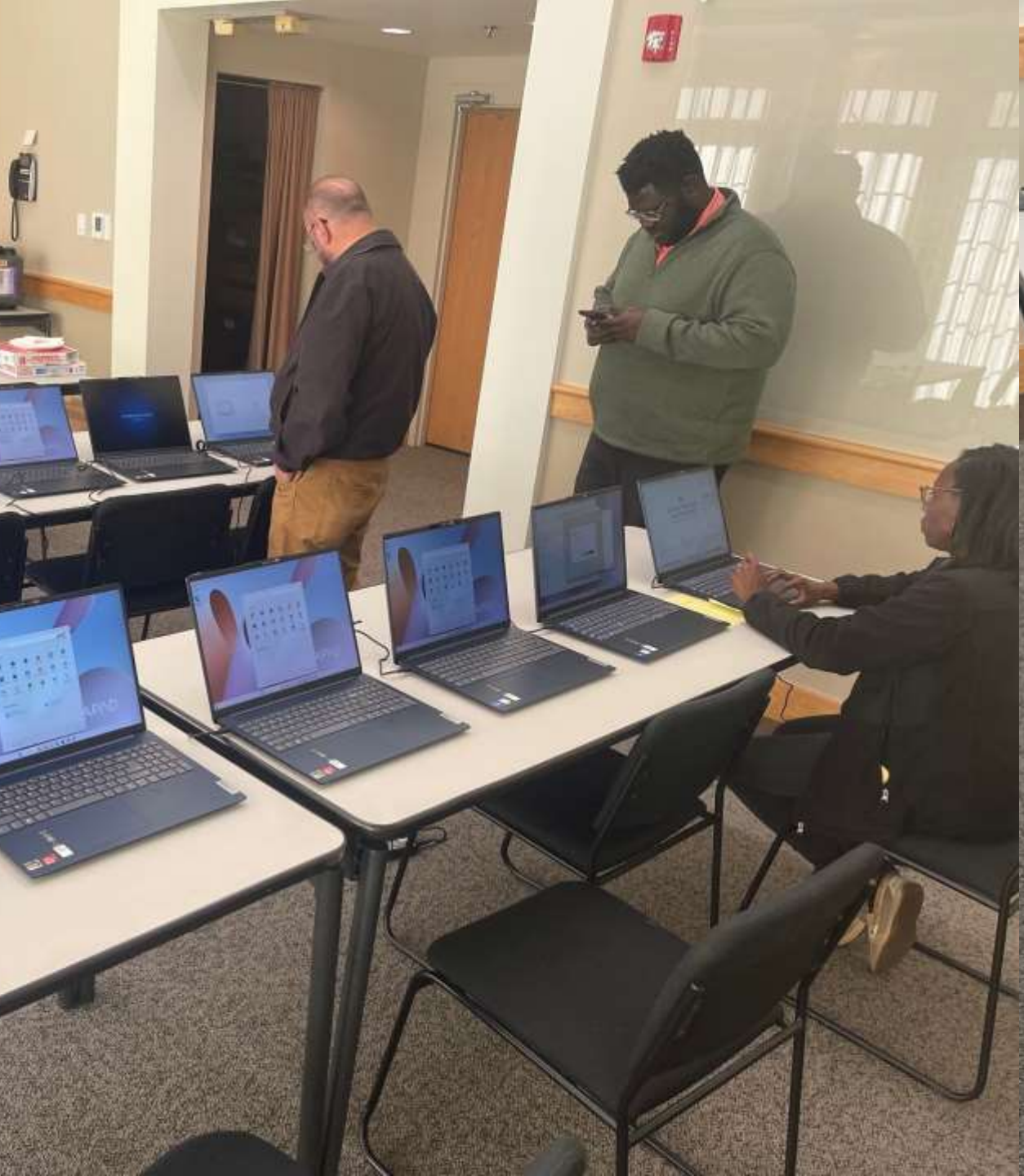
By EOD SCD had Validated all City Backups and Assessed Impacted Systems

City Begins Planning for Continuity of Government and Temporary Operations

SECURECYBER

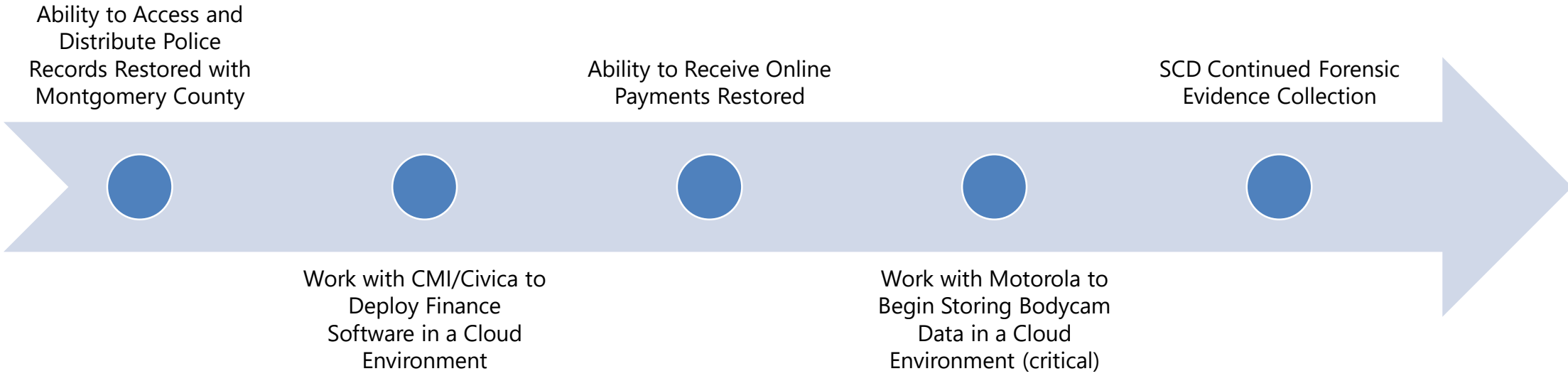
Timeline – Tuesday, November 14, 2023



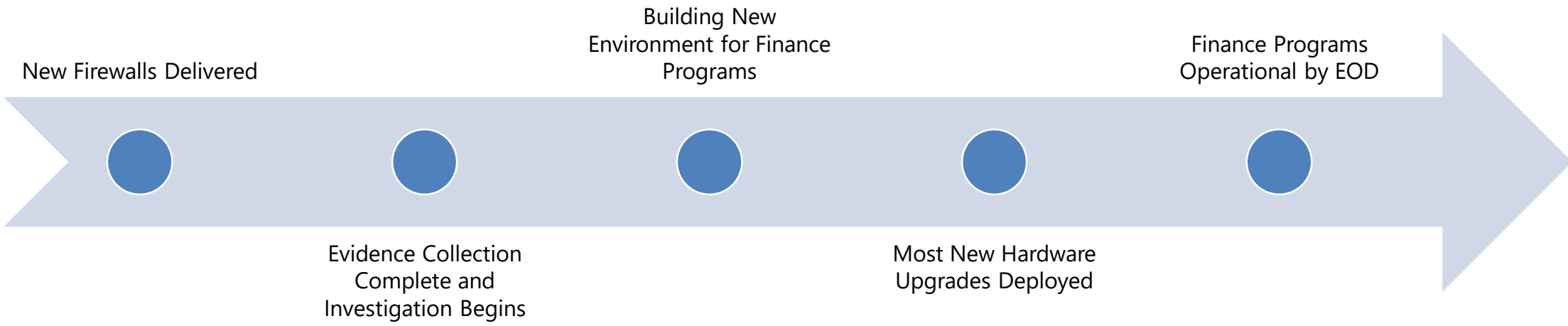



verizon response
Verizon Frontline
Crisis Response Team
1-800-981-9558
KANNUK

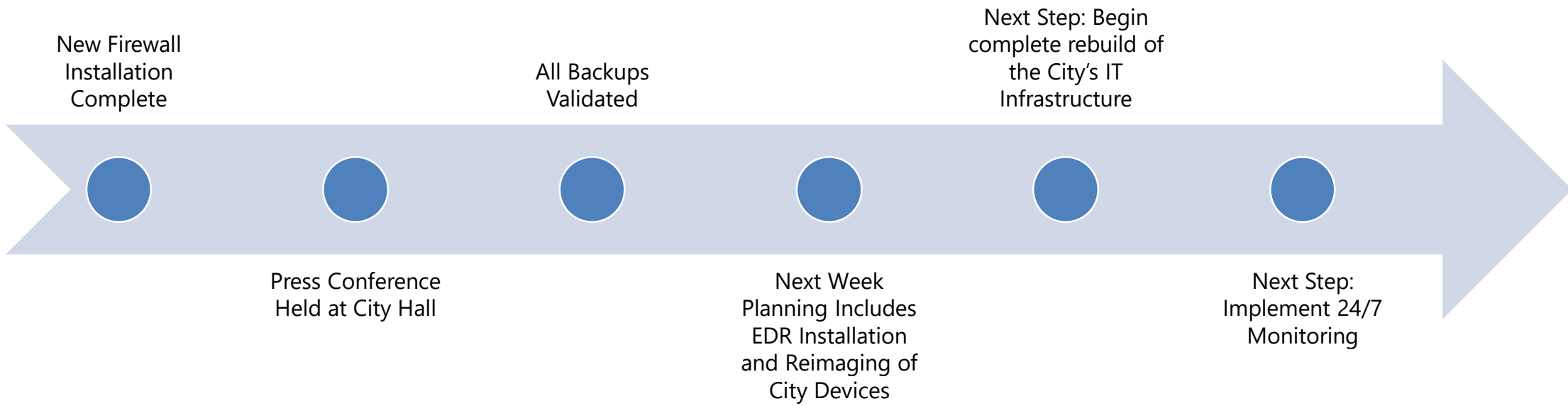
Timeline – Wednesday, November 15, 2023



Thursday, November 16, 2023



Friday, November 17, 2023



Items of Note

- All vendors and city personnel scheduled daily morning status calls for the first 3 weeks.
- AT&T/FirstNet operates a Crisis Response Program as well.
- Store bought computer equipment will lack some functionality versus enterprise devices (i.e. Home Edition).
- At some point in the first week it was identified that HHIT had previously connected the City's water plant to the City's unsecured network. This information was not shared publicly.

Staff Communications

- Weekly Staff meetings were focused on attack, set up additional staff meetings as necessary.
- Email and phone systems were cleared in first day making communications easier.
- Staff was advised to operate as closely to business as usual as possible. Advised to catch up on things not requiring technology (filing, etc.).
- Customer service was prioritized due to delays and difficulties for customers.

Public Information

- City started early by issuing a press release about the incident.
- City provided daily updates via the City website.
- City provided numerous print, radio and tv interviews.
- Culminated in Friday press conference.
- Ongoing updates until resolved.

Examples of all of this are provided in the appendix.

Media Recommendations

- Provide as much information as you can securely provide.
- Leave out vendors
- Leave out details about IT infrastructure
- Leave out issues that might create panic unnecessarily
- Don’t make promises you can’t keep.
- Okay to say maybe, we hope, or that the timeline isn’t certain
- If anything under promise and overperform
- Fully understanding the extent of personal information loss will take a long time…make sure everyone knows that from the beginning.

Finance Department Impacts

- Paper timesheets for 9 pay periods until timekeeping software restored
- Scanning documents to vouchers not available for 3 months
- Banking software approval setups changed to cell phones with 2 factor authentication
- No access to any network files for over one month (Word/Excel, etc)
- Daily backups corrupted back to November 1
- Data added to any spreadsheet Nov. 1-11 was lost, recreated in January
- 2024 Budget could not be completed and approved until January 2024

Water Department Impacts

- Lost remote access to SCADA system – manual staffing 24/7 for 45 days
- Disconnected from the city network to avoid further infection causing visual readings of tower levels and manual operation of booster stations
- Multiple weaknesses within Water Plant and Billing office identified
- Billing office unable to access billing software for over one month, no payment processing, no bills sent, no shut-offs, no new customer adds
- Billing office lost ability to use Word/Excel for 6 months resulting in delay for shut-offs and collection letters

Week Two – Thanksgiving Week

- Short week – priority was to bring all crucial systems up for the following week.
- Threat negotiator attempted to contact threat actor at the end of last week. All attempts to work with threat actor were unsuccessful due to inaccurate information from the threat actor.
- Think about this – What would happen if you had no backups and couldn't reach the threat actor to negotiate?

Week Three and After

- Worked closely with SecureCyber to facilitate the recovery of City systems.
- Continue to brief the media on progress
- Continue to work with insurance to figure who/exactly was impacted by the incident.

Ongoing

- Began cleaning and restoring devices.
- Obtained stolen data from dark web.
- Data mining company reviewed 198GB of stolen data.
- Insurance will make necessary notifications and provide credit monitoring.

Behind the Scenes – SecureCyber

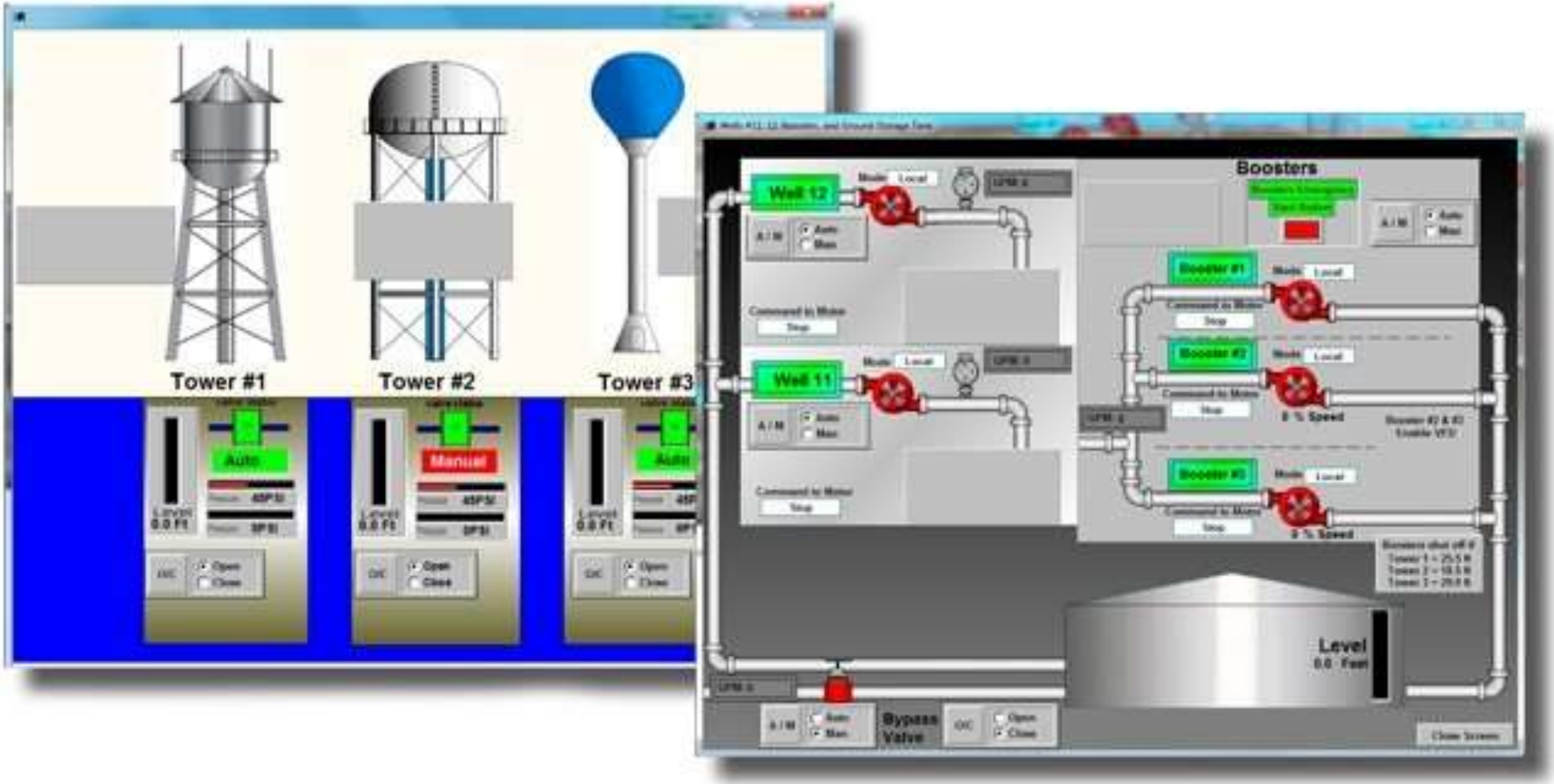
- Contacted Sunday afternoon, arrived around 4pm
  - Myself (Victim Advocate) and Senior Cyber Forensic Investigator – We act very much as first responders
  - Assess the scene, contain the incident (attempt to stop any bleeding), brief necessary resources, involve Federal LE, design the plan to move forward, assess additional staff required
  - Brief council, senior staff, assist with press releases and talk about continuity of Government
  - We know going in that an incident of this size is going to be many months of almost around the clock work

Behind the Scenes – SecureCyber

- Monday – Continue with isolation and containment
  - There is a lot to learn, we don't know the network, the applications etc. This has to be learned very quickly.
  - While we wait for insurance, we assess the backups and possible recovery paths. Continue to assess damage and what's been impacted
  - Assessed the water plant (more on this later)
- Tuesday – Insurance call, forensic gathering starts. This will end up lasting almost 5 days. At this point, PR folks just now show up, law firm has been secured. Daily calls start happening.

Behind the Scenes – SecureCyber

- Water Plant – Huber outsources the operation of water to Veolia. Waste water is handled through Tri-Cities.
  - The Water Plant had already been isolated off the network prior to our arrival
  - We took a forensic capture of the 2 Human Management Interfaces (HMI's) and found they were compromised by the threat actor
  - No water production was impacted, the plant operated normally with 24/7/365 coverage due to no remote access
  - Still working to recover fully the water plant, switch to updated components, new HMI's


Tower #1
Tower #2
Tower #3
Auto
Manual
Well 12
Well 11
Boosters
Booster #1
Booster #2
Booster #3
0 % Speed
Bypass Valve
Level
0.0 Feet

Behind the Scenes – SecureCyber

- At the same time as teams are gathering forensics, we're replacing the City firewall and installing new Endpoint Detection and Response. This connects the City to our 24/7/365 Cyber monitoring center in Moraine. This helps tremendously with long term recovery and places the City under constant monitoring.
- Moved many city resources to the cloud (Office365 wasn't impacted)
- Developed a recovery plan to rebuild authentication servers, contact vendors to rebuild key systems. Lots of work gathering vendors and getting them to move quickly. Getting updated documentation.

Behind the Scenes – SecureCyber

- Continue to fix network overhaul that was stopped mid-stream. At the same time, design an entirely new network with proper segmentation.
- The City's desire was to outsource Cyber and Network to SCD for the immediate future.
- About 2 weeks before Christmas we brought up the legacy network slowly and also helped facilitate the bringing back of the police dispatch center from the RDC.
- SCD placed an interim IT Director to help manage current staff and prioritize and facilitate day to day recovery tasks.

Behind the Scenes – SecureCyber

- AS OF TODAY – New networking equipment has arrived and we're beginning the plan to install the new updated equipment with the new design
- We're working with multiple Water Plant vendors to assist with the full recovery and ongoing protection of the plant itself.
- Installing new remote water plant resource communication equipment

Lessons Learned

- Prioritize cybersecurity and secure infrastructure.
- Ongoing, regular training with all staff about cybersecurity and phishing.
- Bring in 3rd party assistance early, preplan a vendor.
- Contact insurance early.
- Start issuing public information early.
- Invest heavily in IT infrastructure and staff.
- Institute multiple means for backup of files (onsite, cloud)

More Lessons Learned

- Implement imaging and logs of server systems.
- Do not delete anything prior to forensic investigation, simply quarantine systems.

Questions?

City of Huber Heights
6131 Taylorsville Road
Huber Heights, OH 45424

Phone: (937) 233-1423
Fax: (937)233-1272
www.hhoh.org

MEDIA RELEASE

City of Huber Heights – Ransomware Attack

FOR IMMEDIATE RELEASE – November 12, 2023

The City of Huber Heights was subject to a ransomware attack at 8:13 a.m. on Sunday, November 12, 2023. While public safety services are not impacted the following city divisions are affected: Zoning, Engineering, Tax, Finance, Utilities, Human Resources, and Economic Development. The Information Technology Department is coordinating with third parties as well as local, state, and federal law enforcement and is actively investigating the scope and severity of the issue. Public Safety Services continue to remain unaffected.

With the exception of public safety, the City of Huber Heights expects impacts to other City services for at least a week. Phones are currently operational, but residents are advised to access the City's website at www.hhoh.org to stay up to date on information. Updates will be made daily at 2:00 pm each day on the City website and Facebook. The City is taking every precaution to ensure the attack is isolated and to determine if any information was accessed. Anyone found to be impacted will be notified.

Contact: Rick Dzik, City Manager
(937) 233-1423
rdzik@hhoh.org

Appendix – Media Package

Initial Press Release sent on 11/12/2023 at 11:00 p.m.

Website News Flash

Facebook Post

Started list of FAQ's to address resident concerns on social media

SECURECYBER

Appendix – Media Package

- *Used Website Newsflash for Daily 2pm Updates 11/13/23 - 11/17/23*
  - *Posted until 11/22/23.*
- *11/27/23 - Issued media release update*
- *12/4/23 notice of closure for Water Division offices 12/5 - 12/7 posted on website and social media*
- *12/19/23 notice of delay/issues with water billing posted on website and social media*
  - *Posted until 1/1/24*

Appendix – Media Package

- *Coverage from media outlets:*
  - *https://www.daytondailynews.com/local/huber-heights-city-government-hit-by-ransomware-cyber-attack/4HAJD66AGJFTDDYSU4IQS3AJGY/*
  - *https://www.whio.com/news/local/local-city-experiences-ransomware-attack-what-residents-should-know/NCBLY5FXTBFIRPMT2VDY3DBCSM/*
  - *https://news.yahoo.com/local-city-experiences-ransomware-attack-045010413.html*
  - *https://dayton247now.com/news/local/huber-heights-investigating-following-ransomware-attack*
  - *https://www.energyportal.eu/news/several-services-impacted-after-ransomware-attack-hits-local-city/483352/#gsc.tab=0*
  - *https://dayton247now.com/news/local/several-city-services-impacted-after-cyberattack-on-huber-heights*

Appendix – Media Package

- *Coverage from media outlets:*
  - *https://www.wdtn.com/as-seen-on-2-news/what-is-ransomware-and-how-can-you-protect-yourself-from-it/*
  - *https://www.whio.com/news/local/really-frustrating-city-official-explains-how-recent-cyber-attack-impacts-residents/KPG5QT5HRFBWLPGAXPRJCG772Y/?fbclid=IwAR3utfWnfOjAPc8cqEtG1ToNxlyyZr8r09Fi4TAG09hapE7siO8F-pjBiHc*
  - *https://www.wyso.org/government-politics-news/2023-11-13/huber-heights-city-offices-attacked-by-ransomware-some-city-services-affected*
  - *https://therecord.media/huber-heights-ohio-ransomware-attack*
  - *https://www.cybersecurity-insiders.com/ransomware-attack-on-huber-heights-drives-it-into-emergency/*

Appendix – Media Package

- *Coverage from media outlets:*
  - *https://www.wdtn.com/news/local-news/huber-heights-declares-state-of-emergency-following-cyberattack/*
  - *https://www.whio.com/news/local/local-city-declares-state-emergency-after-cyber-attack-use-taxpayer-money-investigate/D4FZZXWYGZDEHFEUQRHMZHSJUA/*
  - *https://www.energyportal.eu/news/local-city-declares-state-of-emergency-after-cyber-attack-to-use-taxpayer-money-to-investigate/485724/#gsc.tab=0*
  - *https://news.yahoo.com/huber-heights-declares-state-emergency-030627055.html*
  - *https://www.wyso.org/news/2023-11-14/huber-heights-in-state-of-emergency-after-ransomware-attack*

Appendix – Media Package

- *Coverage from media outlets:*
  - *https://www.govtech.com/security/huber-heights-ohio-suffers-ransomware-attack-on-systems*
  - *https://www.daytondailynews.com/local/some-huber-heights-data-systems-remain-shut-down-following-cyber-attack/VCUJVRJKOBGIHI6JCFZOPRUWYQ/*
  - *https://www.scmagazine.com/brief/ohio-city-disrupted-by-ransomware-attack*
  - *https://www.whio.com/news/local/first-forensic-evidence-collected-after-local-ransomware-attack-city/IL74XLGSUBCWNGH75PQM42OILQ/*
  - *https://www.wdtn.com/video/huber-heights-declares-state-of-emergency-following-cyberattack/9170107/*
  - *https://www.daytondailynews.com/local/huber-heights-it-director-resigned-9-days-before-cyber-attack/NJMUSBJMEBH65MZYTNRVFUMED4/*

Appendix – Media Package

- *Coverage from media outlets:*
  - *https://www.whio.com/news/local/local-city-still-working-restore-services-after-ransomware-attack/3LTP4I63VBEDPKNA4JVLCITZAA/*
  - *https://www.whio.com/news/local/local-citys-it-director-resigned-9-days-before-ransomware-attack/YI24B43E2FHWLOEJNZ3RSBOGQU/*
  - *https://www.whio.com/news/local/city-huber-heights-hold-news-conference-today-following-ransomware-attack/RELVDFUENBDGVPNMGWGNVNSYQQ/*
  - *https://www.daytondailynews.com/local/just-in-kettering-to-consider-freeze-on-recreational-marijuana-businesses/V6N2ANRDXVFFTBJOTDCCSUWVGI/*
  - *https://www.wdtn.com/news/local-news/huber-heights-officials-to-give-update-after-cyberattack/*
  - *https://www.wyso.org/government-politics-news/2023-11-20/huber-heights-services-temporarily-restored-fbi-investigating-ransomware-attack*

Appendix – Media Package

- *Coverage from media outlets:*
  - *https://www.daytondailynews.com/local/huber-heights-still-doesnt-know-if-resident-data-was-hit-by-ransomware-attack/FKA2EEW5PNAJXDLIEQCDEXYEF4/*
  - *https://www.daytondailynews.com/local/huber-heights-able-to-process-city-payroll-but-still-solving-cyber-attack-issues/JITB7Z6YPJF2RPH3DCFN75FHSQ/*
  - *https://www.wyso.org/courts-crime-news-ohio/2023-11-28/huber-heights-ransomware-update-income-tax-online-water-billing-system-repairs-almost-completed*
  - *https://miamivalleytoday.com/huber-heights-gives-update-on-ransomware-attack/*
  - *https://www.whio.com/news/huber-heights-provides-update-cyber-attack-says-some-services-restored/16ee71ee-03d1-4574-a470-d85400f00dfe/*

Appendix – Media Package

- *Coverage from media outlets:*
  - *https://news.yahoo.com/huber-heights-provides-upate-cyber-213026879.html*
  - *https://www.daytondailynews.com/local/status-of-huber-heights-residents-personal-data-unknown-as-investigation-continues-into-cyberattack/2TSA2IRTUNHMZG7YVJQRMPTTJY/*
  - *https://www.daytondailynews.com/local/huber-heights-cyber-attack-city-functions-restored-350000-spent-personal-data-issue-in-limbo/M6VB74BTTFGRPKLWNX5K4KOS2Y/*
  - *https://www.whio.com/news/local/local-citys-functions-restored-350k-used-handle-ransomware-attack/UDJAU23EJNDBRDMXRUQX7WWNUM/*
  - *https://www.daytondailynews.com/local/huber-heights-cyber-attack-cost-hits-800k-resident-data-vulnerability-unclear/4GU6DAB7BVF3FITNGIGG7FUYUM/*