

The Geauga County Data Board met on Thursday, April 13, 2023, at 12:00 pm at 231 Main Street in the Auditor's Appraisal Conference room and via Microsoft Teams for an Emergency meeting. Members present: Chuck Walder, County Auditor; Scott Hildenbrand, County Sheriff; Joe Cattell, County Engineer; Sheila Bevington, County Clerk of Courts; Jim Flaiz, County Prosecutor; Michelle Lane, Board of Elections Director; Scott Daisher representing Nora McGinnis, Board of Elections Deputy Director; Tim Lennon, County Commissioner and Celesta Mullins, County Recorder. Also present: Pam McMahan, Deputy Auditor; Ron Leyde, Chief Deputy Auditor; Frank Antenucci, Chief Deputy Administrator; Allen Keener, Chief Technology Officer; Gail Roussey, League of Woman Voters of Geauga; Adam Litke, Health Department; Kate Jacob, Auditor's Chief Compliance Officer; Andy Haines, ADP; Zach McLeod, ADP; Elise Von Gunten, Chagrin Valley Tines; Diane Jones; Katie Taylor, Engineers Human Resources and Fiscal Officer; Nick Gorris, Water Resources; Mike Kurzinger, Water Resources; Steve Oleic, Water Resources; Brian Doering, Maple Leaf; Nina Lalich, League of Woman Voter of Geauga; Joe Camino, CSJ Technologies; Gerry Morgan, County Administrator and Jim Dvorak, County Commissioner.

Absent: C.P. Hitchcock, County Treasurer.

CrowdStrike Critical Threat Escalation on Water Resources Exchange Server

Chuck summarized the sequence of events as we currently know:

On Wednesday 04/12/23, we estimate in the early morning hours around 4:00 am CrowdStrike Falcon noticed possible nefarious activity on the Water Resources server. CrowdStrike Falcon is an endpoint cyber security product installed on all county workstations touching the network by ADP.

Shortly before 8:00 am ADP staff received serious high-priority alerts from CrowdStrike which appeared to be a persistent and significant threat on this Water Resources server. CrowdStrike observed what appeared to be nefarious activity trying to access the server. Given the persistent nature, CrowdStrike upgraded it to critical and automatically blocked execution, isolated the services, and put in motion a procedure for ADP to further isolate and protect the County's network.

ADP personnel immediately notified Water Resources of the attack, blocking all inbound WR domain traffic, removing WR from all shared ISP switches, and began a deep scan of all county systems to ensure the county's environment under ADP's control was secure and unaffected.

It appears the WR server in question is an end-of-life, end-of-support server operating Microsoft Exchange for WR which is not properly serviced and patched. This vulnerability likely permitted the exploitation of an outside actor to externally penetrate the server through Exchange and attempt to run a series of tasks or commands through a power shell script.

The server was ultimately powered off by WR staff which prevented any further analysis by ADP and CrowdStrike. As of now, there is no indication that the attack reached beyond WR, and they remain offline awaiting remediation. CrowdStrike and ADP were successful in containing the attack with no disruption to other county services or systems under ADP's control. Since the penetrating server was not under the control or oversight of ADP, the board's emergency meeting was called to discuss the issue.

Who will speak for WR? Steve Oluic advised he had no e-mail access currently. He stated he received an email at 8 o'clock the day prior after WR was shut down. Jim Flaiz said the server is WR's and he would expect WR to come to this meeting and explain what is going on. Mike Kurzinger said that CrowdStrike is a very good product when it sees an

attack it will go in and shut that server off from any other access. Mike went on to say he made many attempts to speak to Frank and ADP to find out how to remediate the problem and did not get an answer. Frank said he communicated via email.

Jim Flaiz asked why Water Resources is running its own exchange server and not converted to Microsoft 365. Mike said they were running the exchange server since they began operations, and he was told by Gerry Morgan during the mediation not to convert to 365. There was a Purchase Order opened for Microsoft 365 but during mediation it stopped. Chuck asked what in mediation had anything to do with running email. Gerry said he would love to discuss the subject, but they are under a gag order that everyone signed during mediation. Chuck said what part of the lawsuit you filed had anything to do with email from Water Resources. Tim said it was the direction of what the future of Water Resources interaction was going to be whether it was fully under the umbrella or another option. Chuck said the lawsuit itself had no mention of WR. Tim said not in the lawsuit but in mediation. Chuck said being under a gag order you are taking action that is resulting in mediation to stop people from migrating from Exchange to the Cloud.

Chuck asked what version the operating system of WR is. Joe Camino replied 2016. Zach McLeod clarified they have a 2012 Microsoft version server and a 2016 Exchange. Joe introduced himself as having worked with Water Resources for 30 years providing support and working with Mike. Chuck said a 2012 server is an obsolete, non-supported version. Joe said everyone (WR) agreed to move to 365 back in February 2022 but there was a debate on who was going to pay for it. The first attacks Joe continued started happening with that version of the server and WR can only do what was approved whether they came under ADP or the County or if they were going to stay on their own. Jim asked if all the patches were up to date. Joe said up until what happened. Chuck said the operating system is at the end of its life, end of support, and the 2016 Exchange server was not currently being properly patched as CrowdStrike indicated. Tim asked if someone did get through and if there was a report. Chuck said there were three reports from CrowdStrike that have been forwarded to WR three high priority and one critical. Frank said others cannot access the CrowdStrike infrastructure but the initial writeup indicating what the threat level was everyone received.

Jim asked if there were any indications the WR exchange server had any vulnerabilities prior. Joe Camino answered other than Windows updates and patches there were no issues. Jim asked if there was ransomware or other attacks. Joe and Mike both answered no. Jim asked if any of WR's vendors or partners have had any ransomware issues. Mike answered no not at this point. Jim followed up with the question of whether in the last year any. Mike then answered Joe did. Joe then replied yes, his company's email servers got the same type of attack in December 2022. Chuck asked what the remediation was. Joe replied the server was taken offline, and all their emails are now on 365 as of December 2022. He went on to say forensic people were hired, he dealt with the ransom guys, paid the ransom, and recovered their emails. Jim asked if there was any link between his servers and Water Resources. Joe said no link at all. Frank then asked if Joe had the ability to remotely access to get into the WR's servers. Joe asked what all the questions were for as it sounded to him like there was a link trying to be established. Jim asked why he came to the meeting if not to answer questions. Joe asked what do his servers have to do with what happened the other day at WR. Frank responded you are telling us your Exchange server was hacked in December and now Water Resources was hacked, and you are asking what it has to do with that. Chuck said you represented yourself as being WR's IT expert and there was an Exchange server that was not properly patched. Joe said with third -party software he could remote into WR servers but had not done so for over a year.

Jim asked Joe if he told WR that his server was hacked. Joe said yes. Jim asked Mike if he did anything when he found out Joe's server was hacked, and Mike said he checked theirs as a precaution. Chuck asked if Joe's hack was due to the vulnerability of a patch. Joe said yes, they came in through OWA which is an online web access vulnerability. Chuck said that is exactly how they got into WRs. Joe responded there was a patch applied in June but to fully replace that server and to upgrade to Exchange was not in the budget. Chuck said patching it with the current patch does not cost anything but the labor to do so. Chuck asked if Water Resources were subscribed to Microsoft patching, and if they were they would have received a notice. Mike said they are but did not receive a notice. Mike said if ADP would share their notices WR would get them as well. Chuck said if WR was under the County ADP then they would not have to share them. Allen Keener interjected every Tuesday is patch Tuesday with Microsoft where you can set your servers for automatic updates, and you will get those notifications.

Mike said the email that was circulated did not say the server was not patched it said to ensure the patch was applied and he cannot ensure that if he cannot open the server. Tim asked what the resolution was and if there was damage done. Chuck responded WR shut the server off and once it was shut off CrowdStrike cannot get access or go any further the instruction CrowdStrike gave was to reboot the system. CrowdStrike is on all workstations in the County and protects the environment. If CrowdStrike detects a severity that is high enough it locks that box out from communicating. Chuck said the instruction from CrowdStrike in the email that was sent was to reboot and then CrowdStrike looks to see if the scripts are running again.

Jim said before we discuss solutions the ADP Board should understand the progression of the incident. In September 2021 ADP started the process with WR to migrate to Office 365 they were asked for the PO to proceed with migration in October 2022. Chuck said October 18th, 2022, they were using Expert IT to do their migration on 6/6/2022. WR amended the plan and timeframe. ADP initiated the contact with Expert IT to do the work. Late fall they got a PO made out to Expert IT and work was to be done the first week of February on February 2nd. WR told ADP to stand down and not proceed per Gerry Morgan he had instructed Steve and himself (Mike) not to proceed with the migration and they have been running their Exchange server ever since. Jim said the migration could have started in October 2022 and then in December 2022 WR's IT vendor gets ransomed with the same type of attack. WR does not patch their Exchange servers properly and they are out of date. The only way ADP knew about the attack was by the installation of CrowdStrike which is running 24/7 on all County equipment including WR and that saved it not going beyond their Exchange server, which is currently shut down, so they do not have email.

Jim asked Gerry if he was going to allow the 365 migrations now and Gerry responded yes, he talked to Water Resources about proceeding. Jim asked Gerry if he remembered sitting in front of the ADP Board two years ago and saying that Water Resources was coming under ADP. Gerry said yes and they were working towards that. Jim said when that has not happened for two years, he considers it lying.

Chuck said ADP was applying O365 to the rest of the County, but he did not want to subject the ADP staff to implement WRs because of all the difficulties ADP has had with them and did not want to put the staff in harm's way. Expert IT will have to be contacted again. Steve asked what harm's way meant. Chuck went on to explain Gerry's command to get ADP staff to the McFarland plant 7 employees were sent when it shut down because IT passwords were changed. The implication ADP was getting was that changing passwords caused the plant to shut

down. Steve said no one knows what happened and the County spent \$50,000.00 on Dragos not to remediate the problem but to do forensics on it. Jim said the Commissioner's Office blocked funding finalizing the Dragos investigation. Chuck said Gerry spoke to his staff after an ADP meeting when the incident was first discovered at McFarland that the next day, he would transfer \$50,000.00 to pay for Dragos. Twenty-four hours later Gerry sent an email saying Water Resources would pay the \$50,000.00 and WR staff said it would take about four weeks to get a purchase order, so Chuck asked why you are worried about remediation.

Jim said to Steve you should understand why ADP employees are a little gun-shy. Steve said he understood the dynamics. Jim continued that Gerry illegally filed a lawsuit against ADP employees to which Gerry interjected he did not the BOCC did. Jim asked what meeting that action was approved in and Gerry responded it did not have to be in a meeting and did not have to be approved. Jim asked who signed the complaint and Gerry replied he did, and Jim asked in what meeting did the BOCC authorize him to sign the complaint. Jim said that Gerry illegally sued ADP employees so that is why an outside vendor was hired to perform this project.

Gerry asked if Water Resources could migrate to Office 365 themselves. Jim said Gerry should read the revised code ADP does IT. Gerry said what he is asking is if WRs can transfer to O365 themselves and then later convert over to what ADP has with regards to that. Chuck said why would we do a later date as ADP Board has waited two and half years for the migration of WR supposedly into ADP. Gerry said to solve the issue since you do not know when the vendor is available.

Jim said WR is not going to be standalone, they are not running their own email, and that is according to the revised code ADP runs IT unless the Board permits you to do otherwise. Gerry said there is also another section in the ORC that says the BOCC can hire for services. Jim said WR is not the Commissioners and if Gerry felt so confident in the law, he should not have dismissed his lawsuit after wasting \$60,000. Gerry said the lawsuit was dismissed for the BOCC to come before the ADP Board with possible options to move this forward. Chuck said I accept that you made a request to the ADP Board, but it was for two items the Mission product and key card access nothing about emails. He went on to say if the two things you requested were addressed this email issue would never have been resolved as it was not on the table.

Tim said he is ok and comfortable moving WR under the ADP umbrella as he knows they have been working outside of ADP for the last 35-40 years, but WR IT still needs the ability to operate their hardware out in the field and have 24-hour access. Tim went on to say he proposed to move WR toward the new O365 as soon as possible. Joe Camino said he wanted to be clear that O365 was never presented at WR originally it let ADP migrate the mail and then it was taking over the servers, the users migrated to GCOADP, and taking over administration of all the user accounts and passwords it was a lot more then emails or it would have been done a year ago. Chuck found an exception with that statement and asked Joe how many ADP meetings besides today have you been to. No response.

Chuck said what was preventing Joe as their IT vendor or WR from putting in a service patch on an Exchange server that is free. Joe replied the operating system was also outdated and he agreed. Gerry asked as being over WR as County Administrator if moving WR over to Office 365 only moved the mail. Chuck said if it requires a domain change because it is coming under the County any other changes needed to make it happen will be done. Frank said the point is to do the least amount of work possible to migrate the email if ADP must

migrate the domain to do so then they will. Jim spoke about how his migration took a month since his Prosecutor's Office domain had to be changed and Tim said that is what should be done in this case as well.

Tim asked if the WR server gets turned back on could it be saved with a patch and if it could not interact with the County could it interact with others outside. Chuck responded it will begin to communicate with CrowdStrike. Chuck asked Joe Camino if his server was able to back up and go after his ransomware or was the backup infected. Joe replied his backup was infected but they were able to recover all the data from the backup. Frank asked why to pay the ransom then. Joe said because there was other stuff infected that was going to take longer to retrieve and build that server and migrate 1600 mailboxes that he had to import and export. Chuck said it is irresponsible to put a system in place that is vital to wastewater treatment plants that is outdated, unsupported, and unpatched.

Motion: by Jim Flaiz, seconded by Chuck Walder, to authorize ADP to immediately commence performing the migration of Water Resources email to Office365 and perform any other services necessary to get Water Resources operational. Any cost incurred will be covered up front by Water Resources. ADP will attempt to recover historical Water Resources email data if possible

Voice votes: 9 ayes, 1 absent, 0 abstain. Motion carried.

Tim suggested because there is a communication issue that ADP and Water Resources designate persons that are comfortable talking together and working together to communicate to not spiral back down. Mike Kurzinger volunteered to be the contract. Frank objected based on history and suggested Adrian Gorton and Steve said no to that suggestion. Chuck said it is very difficult to volunteer a pointed person that works for you who could become subject to being named in a lawsuit. Jim said ADP had a baseless police complaint made against them and they were illegally sued so he could understand why they are reluctant to work with WR. Chuck said he has never heard of a County naming a person in a lawsuit and Tim said that was beyond the discussion. Jim said the BOCC sued individual employees and it was classless and uncalled for and it was vindictive by Gerry (who got up and left the meeting). Tim said then let us not communicate and keep it going. Chuck said to Tim you are either part of the problem or part of the solution. Tim said he brought up the subject of starting communication and Chuck said no, and Chuck responded he told him why. Tim then motioned to adjourn, and Chuck responded the ADP Board usually takes public comment but if the meeting is adjourned the public does not get the opportunity. Tim said go ahead and take public comment.

Mike Kurzinger asked if WR can get back in operation with the email server down. Steve asked if WR could open up CrowdStrike and figure it out. Tim asked if there was a way, WR could communicate with CrowdStrike to which Mike said ADP will not provide access for them. Chuck said ADP employed CrowdStrike ADP will be the single source of communication to CrowdStrike and he not going to open up CrowdStrike for anyone to call and ask them all kinds of questions that could be contrary to ADP's direction. Chuck said Zach McLeod is the single point of contact and if there is a question for CrowdStrike it needs to be directed to him.

Chuck asked WR staff if all the rest of their servers are current and currently patched. Mike said yes. Chuck said that BOE was one wire away from having a potential threat due to the WR issue. Andy Haines said as soon as CrowdStrike gives the all-clear on the servers being up to date the WR servers can be turned back on. Mike said he wanted their servers turned back on

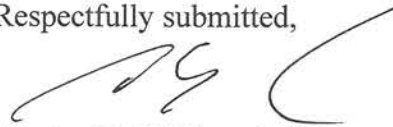
first and Steve mentioned he wanted email to come first. Chuck said what do you want first you are saying two different things. Chuck said all the servers must be current and then email.

Public Comment

Elise asked for the motion to be reconfirmed. Jim said Pam will email it out.

BEING NO FURTHER BUSINESS TO COME BEFORE THE BOARD, Celesta Mullins motioned to adjourn.

Respectfully submitted,




Charles E. Walder, Auditor
Secretary/ADP Board

Michele Lane
Board of Elections Director




Sheila Bevington
Clerk of Courts




Celesta Mullins
Geauga County Recorder



Scott Hildenbrand
Geauga County Sheriff




Nora McGinnis
Board of Elections Deputy Director



Joe Cattell
Geauga County Engineer

Christopher Hitchcock
Geauga County Treasurer

Tim Lennon
Geauga County Commissioner



Jim Flaiz
Geauga County Prosecutor