

The Geauga County Data Board met on Monday, April 17, 2023, at 1:00 pm at 12611 Ravenwood Drive in the 3<sup>rd</sup> Floor 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; Nora McGinnis, Board of Elections Deputy Director; Caroline Mansfield, representing C. Hitchcock, County Treasurer; Celesta Mullins, County Recorder and Tim Lennon, County Commissioner. Also present Pam McMahan, Deputy Auditor; Ron Leyde, Chief Deputy Auditor; Frank Antenucci, Chief Deputy Administrator; Allen Keener, Chief Technology Officer; Shelly Lewis, League of Woman Voters of Geauga; Katie Taylor, Engineers Office; Kate Jacob, Auditor's Chief Compliance Officer; Zach McLeod, ADP; Corey Thompson, ADP; Andy Haines, ADP; Jim Dvorak, County Commissioner; Tom Huff, Court IT; Paul Pestello, Auditor's Office; Rob Bushman, ADP; Mike Adams, ADP; Joe Birli, ADP; Carol Benton, League of Woman Voters of Geauga; John Karlovec, Maple Leaf; Brian Doering, Maple Leaf; Gerry Morgan, County Administrator; Diane Jones; Amy Patterson, Maple Leaf; Nick Gorris, Water Resources; Mike Dorka, ADP; Scott Daisher, BOE and Elise von Gunton, Geauga Times Courier.

Discussion of additional issues regarding the cyber-attack on Water Resources Exchange server  
Chuck asked Zach McLeod to explain what the current standing was on the Water Resources incident. Zach explained that CrowdStrike, a third-party vendor, reported that they saw exchanges in the logs where a network request was made between the Water Resources server and somewhere in Russia and the server remains in network containment. There has been no additional malicious activity after the server was put in containment. The attack was on the exchange server for email. Jim Flaiz asked Zach to address rumors from Water Resources employees saying they have been told the attack was made up by ADP and the people running ADP. Zach reiterates that CrowdStrike is a third-party vendor that brought the detections to ADP and alerted them. CrowdStrike was able to identify the exact type of malware that was used it is not something ADP could duplicate particularly the connection going to Russia.

Chuck then asked Allen to go over the issues found in the Water DNS that were found after reviewing programs because of the malware attack. Allen explains that DNS is Domain Name Service so when you type in a website it looks for an IP address, so humans don't have to remember numbers, just names. When ADP began the process to convert Water Resources over to Office 365, they found the DNS was being controlled by a third-party company. ADP had to have the service transferred over to the Network Solutions account which is the Water Resources account to which ADP has access and worked with Network Solutions to make sure the service would be available immediately. Frank said Mike Kurzinger was asked by ADP if he had access to the Buriel account, to which Mike replied he thought Allen or Joe Comino had access but neither did so ADP found another way to proceed.

Corey Thompson explained the process of setting up the tenant for the M365 email accounts. ADP had to do an internal admin takeover since they did not have access to the tenant that was previously set up for Water Resources. The delay of the internal admin takeover caused the email setup to take an extended period. Expert IT is currently setting up the emails for M365 and they will be ready shortly for Water Resources to use. Frank said he asked Mike Kurzinger who had the credentials for the account, and Mike replied he was unaware of a tenant being set up by WR in the past. When ADP got into the tenant, ADP found out the only user established in the account was Mike Kurzinger no one had accessed it in the last thirty days and ADP has control of it currently. Frank explained how ADP requested an email list from Water Resources, but Water Resources did not provide a list, so ADP used a previous payroll submitted by Water Resources and with that, an email list was able to be produced. It was not confirmed if Water Resources had any type of backup that could provide the information requested by ADP. Frank stated he had asked Mike Kurzinger twice for the WR backup database and he got the impression

Mike thought he was harassing him, so he assumed it is either not functional, doesn't exist or Mike just did not want to provide it.

Mike Adams gives the status of the other IT servers. The other servers have been patched. The servers were shut off several times over the weekend.

Andy explained what a firewall is and what it does. The Water Resources firewall expired on February 17<sup>th</sup>, 2023, and it was no longer doing the comprehensive security it is designed to do. Mike Kurzinger provided ADP with the firewall credentials to access the old firewall. It is still a basic firewall but missing some of the more advanced protection that is typically offered. A firewall was brought from McFarland to 470 to use instead of the firewall that was not up to date. The firewall brought over had been powered on and updated but was not currently being actively used by WR. Andy said the firewall is ready to go and ADP just needs physical access to the site. Andy stated the password for the firewall had been changed in the last year and has now been updated to a more secure password.

Zach explained the ADP Board Multifactor Authentication policy. A long complex password is needed as well as a second or more form of authentication other than just the password. The current password policy of 25-character passwords is a minimum across the board, but other things have higher minimums like service and admin accounts. ADP is currently looking at implementing three-factor authentication on administrative accounts. Machine or service accounts need to be protected at a higher rate because they can have very high permissions on the network. After a dive into the Water Resources passwords, there were passwords that were far under the recommended number of characters for a "strong" password. Different passwords should be used for different accounts for which WR was overlapping their passwords. ADP does not feel comfortable putting the servers back online with the current passwords. Frank explained that changing the Water Resources server password is a short-term problem because of consolidation using M365 so the servers will not be operational. Until then, having the servers running operational with short passwords is incredibly dangerous. Jim asked if the server's files could be extracted from the servers without them being lit. Frank explained what is possible without reconnecting the servers to the network. Jim stated WR is under ADP and WR should be following the Boards policies.

Gerry stated that the information on the server was needed immediately for customers that need the data who have their own water and wastewater plants and the results of their tests from the lab need to go to them. Frank said that waiting for the server to be connected wouldn't work since the information was needed and changing the passwords to restart the servers would be the better approach. Gerry commented they would like the passwords to be changed and the servers to be started immediately but has fears there could be issues. Chuck brought up the idea of having an OT vendor on site or on call to be supported if something was to go wrong and have a method to control the outcome. Chuck continues that if the passwords were changed to higher credentials and WR has the plant staff on notice if something goes wrong it could revert to the prior passwords.

Chuck gave a brief introduction to the Wonderware relocation. It is a storage box for archived historical data in a SQL server database. This box is integral to the compromised servers making the box a problem as to where it is housed. Frank explained that it had been discussed for roughly one year that Water Resources needed to leave the 470 location. Chuck suggested the board vote to authorize Water Resources to deploy an OT company to move the Wonderware server to McFarland. There is a maximum of \$25,000 up for a vote to hire a third-party vendor to move the Wonderware server and it will also be off the County network.

Approval of Water Resources hiring outside vendor to move Wonderware Server

Motion: by Chuck Walder, seconded by Jim Flaiz to approve Water Resources to hire any necessary outside vendor to move the Wonderware server from 470 to McFarland in an amount not to exceed \$25,000.00.

Voice votes: 10 ayes, 0 absent, 0 abstain. Motion carried.

Zach from ADP explains the end-user patching and vulnerabilities. The scans are showing the workstations are not up to date and are not being regularly updated. ADP would like to move all workstations minus the ones that touch the OT system to the weekly regular update schedule. Frank mentioned that there are four total workstations that would not be moved over to the regular update schedule, one at the county office building that is Mike Kurzingers, two at McFarland, and one at the shop. These are the only four stations that are touching the OT system. Chuck explained to the board that when a station is connected to the OT system, you do not want to do automatic updates because there are collisions that can happen. If a new patch comes down, you must wait for a release to put the patch in place and then load the update. The box at the County office building is touching the network which is where there could be an issue with not patching that workstation. Chuck believes it should be cloud-based so you don't need to run the software on the box.

Approval of ADP Password Policy for all under the authority of ADP

Motion: by Chuck Walder, seconded by Tim Lennon to move all passwords under the authority of ADP to the policy that has already been approved by the Board as soon as possible considering that with a select few servers that should be done in a controlled manner.

Voice votes: 10 ayes, absent, 0 abstain. Motion carried.

Chuck asked if the Board was willing to pass a resolution for the end-user patches and vulnerabilities. ADP needs to push the latest version of the workstation revisions to each workstation in Water Resources before they come back onto the network. The motion would cover all workstations except for OT workstations at McFarland and the shop.

Approval of ADP Resolution for Water Resources Workstation Update

Motion: by Jim Flaiz, seconded by Chuck Walder to approve taking all WR patching to current to eliminate vulnerabilities minus any OT workstations at McFarland and at the shop.

Voice votes: 10 ayes, absent, 0 abstain. Motion carried.

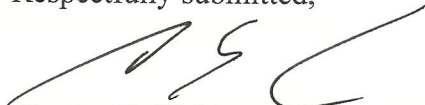
Frank brought up the firewall and the need for physical access to WR at 470. There is a potential of doing a "go live" and switching the firewall. Chuck requested that these are done one at a time to see the effect. A 3:00 PM meeting time was set to meet at 470 to perform the firewall switch Gerry will arrange access for Andy to begin the process. Tim asked if there was any more equipment from 470 that can be moved. Chuck said yes after the OT component is done the rest can be moved. The plan is for the Mission equipment to go to McFarland.

Public Comment

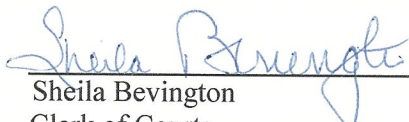
None.

BEING NO FURTHER BUSINESS TO COME BEFORE THE BOARD, Tim Lennon motioned to adjourn.

Respectfully submitted,

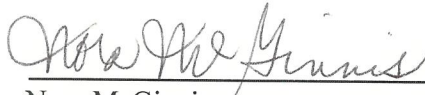
  
Charles E. Walder, Auditor  
Secretary/ADP Board


  
Michele Lane  
Board of Elections Director

  
Sheila Bevington  
Clerk of Courts

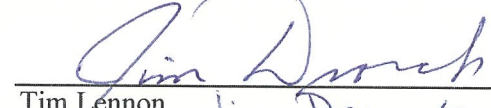
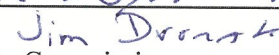
  
Celesta Mullins  
Geauga County Recorder

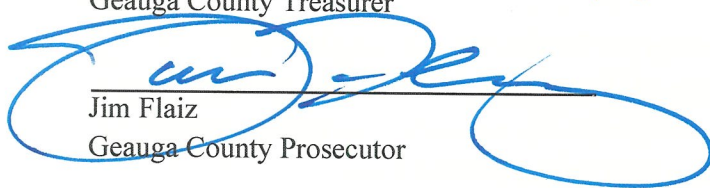
 Foe.  
Scott Hildenbrand  
Geauga County Sheriff

  
Nora McGinnis  
Board of Elections Deputy Director

 Alternate  
Joe Cattell  
Geauga County Engineer

\_\_\_\_\_  
Christopher Hitchcock  
Geauga County Treasurer

  
Tim Lennon   
Geauga County Commissioner

  
Jim Flaiz  
Geauga County Prosecutor