Geauga County Automatic Data Processing Board
Department of Information Technology

Charles E. Walder, Chief Administrator
Courthouse Annex, 231 Main Street, Suite 1A, Chardon, OH 44024-1293

(440) 285-2222, 834-1856, 564-7131 Ext. 4357
Direct Line: (440) 286-4357 FAX: (440) 279-2184
Web site: http://www.co.geauga.oh.us/departments/adp/index.htm

WATER RESOURCES PRE-MIGRATION ISSUES

ABSTRACT

For the last 30 years, Geauga County Water Resources has operated its own staff for both Operation Technology and Information Technology. As described in the Ohio Revised Code Section 307.84, all county IT operations must be maintained or approved by an ADP Board. Up until now, this section of the ORC had been ignored by the Commissioners' office regarding the Department of Water Resources. While OT will continue to be operated by Water Resources staff, IT operations must be moved to ADP. The process of moving control and management of Water Resources IT to ADP has already begun, and many the issues mentioned later in this document have been remediated, which is why this document is being released in this form.

PURPOSE

Described below are various issues encountered by ADP technicians while remediating the April Water Resources incident. Primarily, this document focuses on issues that could compromise the security of the Water Resources system, but also includes details about barriers that hindered the remediation of the incident and other minor general issues or bad practices in the Water Resources system that needed to be brought up to industry standards.

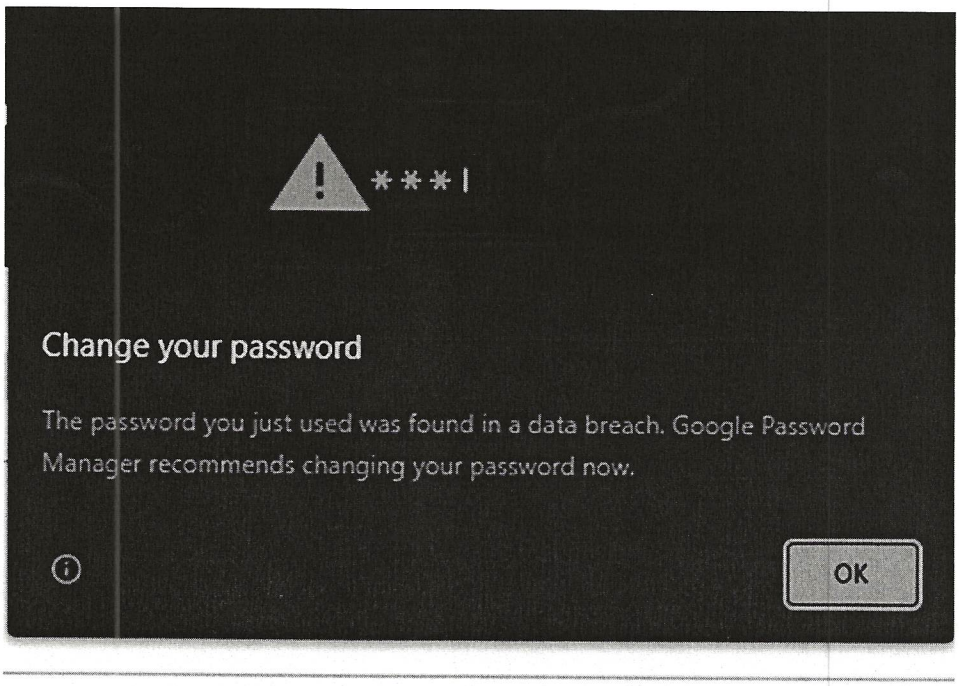
DISCOVERED SECURITY ISSUES

As ADP remediated the April incident with Water Resources, ADP Technicians discovered many security issues, both major and minor, at all levels of the Water Resources network. These security issues and bad security practices leave the system at a much greater risk of successful future cyber-attacks. It was especially relevant to address these issues as soon as possible, as it is likely that cyber-attacks on Water Resources will come more frequently, be more forceful, and be more skillfully executed after the April incident.

PASSWORDS

- Regarding the domain administrative password that give full access to all the Water Resources computers, said password was woefully under-secured. The password was only seven characters long, a password length that would be instantaneously brute forced with modern techniques. The password was also reused for other applications, and a bad actor who cracked this password could have used it to access these applications.
- The password for the local administrator accounts on every single machine under Water Resources was incredibly unsecure. This password was even shorter than the previously mentioned domain admin password and would also be cracked instantly with modern techniques. The password was also easy to guess by any human without access to these techniques, as it was merely the word "image". This was not only an insecure password because of its nature as a common English word but was also insecure because the term is used in IT management of network endpoints and is a word an attacker is likely going to try at the very start of a brute force attack. This simple password would have given bad actors access to the entire operating system of any computer in the Water Resources system. As described later in this document, this access would have given said actor a terrifying amount of control over the Water Resources network, all from such a simple password. Due to the simplicity and ubiquity of this password, it is likely that it had not been changed in some time, possibly dating back decades. Due to the potential length of time between the password's creation and retirement, the scenario where the password was not exploited for malicious purposes in that time is staggeringly improbable.
- Mike Kurzinger's main login password was only eight characters long, and with modern techniques, this password length can also be cracked instantly. This was one of the biggest security flaws in the system, as any bad actor gaining any physical access to any of the Water Resources computers could brute force his password and wreak havoc on the network with administrator privileges.
- The printer admin console's password prompted the following popup from google chrome while ADP was still remediating the issue. Getting this popup implies that Google's database of leaked passwords includes the password being used for

the Water Resources printer admin console.



- Old users that have left the department have their accounts retained, with full permissions, including users that had administrative access to the computers. There was no policy in place to remove old users or even disable their account.
- Regarding passwords for other users, many of said passwords are stored physically on pieces of paper throughout the office, and anyone with physical access to the space would be able to log into any of these accounts. Also, some of the passwords for these users were stored locally in their browser, which can be easily scraped with one of the many exploits in those browsers, most of which can be done without the user's knowledge.
- The password for Water Resources' main New World Systems login is a weak 8-character password. This password would be cracked immediately with modern techniques and would give access to much of the financial information of the department. This would also allow bad actors to make practically anonymous changes into the program.
- Mike Kurzinger's NWS password is written down in a notepad file on WRO-Data. If a malicious actor were able to get into this computer with Mike Kurzinger's simple password, they could make changes in the NWS program as Mike Kurzinger.

CROWDSTRIKE

- Ever since the program was installed, Crowdstrike had consistently been picking up massive number of vulnerabilities of varying severities from Water Resources computers and servers. Suspicious internet traffic has been coming and going from multiple international IP addresses, including specifically IP addresses from Russia and China. Pictured below is data collected from a report from Crowdstrike showing these IP addresses and their country of origin, in this case all being from Russia.

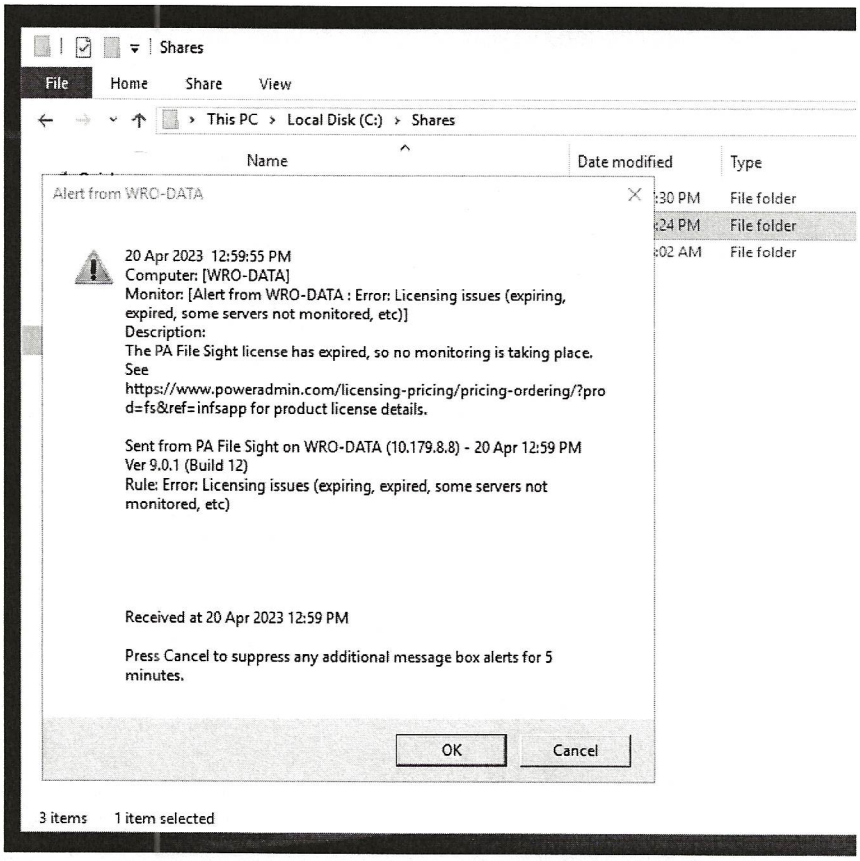
Computer	Date	IP Address it went to	Country	Whois Lookup
WRL-LAB2	10/28/22-10/31/22	77.88.21.90, 87.250.250.90, 93.158.134.90	Russia	Yandex
WRO-DESIGNENGIN	10/31/2022	93.158.134.90, 87.250.250.90, 213.180.204.90, 213.180.193.90, 77.88.21.90	Russia	Yandex
WRO-JAMIE	10/31/2022	213.180.204.90, 87.250.250.90, 77.88.21.90, 213.180.193.90, 93.158.134.90	Russia	Yandex
WRO-MIKE	10/31/2022	213.180.204.90, 87.250.250.90, 213.180.193.90, 77.88.21.90, 93.158.134.90	Russia	Yandex

CAMERAS

- All of the cameras in the Water Resources system are either out of date or nonfunctional. All cameras in the system are fed back to an antiquated DVR setup. The poor maintenance of this system poses a significant risk to the physical security of the Water Resources system. ADP recommends a complete overhaul of the camera system and at least twenty more cameras across the various locations in the Water Resources security system.
- At the Lab, one camera is not working, and the camera overview is not working for the office manager and has not for some time.
- At the McFarland plant, at least one camera is not working and the same camera overview is not working for the plant's office. There are not nearly enough cameras to cover the whole plant.

SHARED DRIVES

- The shared drives used by Water Resources before the migration to SharePoint were extremely unsecured and poorly designed. Most of these problems originate from the permissions that controlled access, which were very poorly maintained.
- The folders in the shared drive were not created or maintained in a way that promoted good security practices. For example, many files that pertained to administration, engineering projects, lab results, payroll, and IT files were casually placed in the folder labeled "User shared files". Any users that had access to this folder, which was most users, as this is the folder where each user's file share was stored, could see these files.
- There was no security to prevent users from accessing data in the file share that they should not be able to view. For example, any main office employee in the Water Resources domain could view and edit payroll documents in the Users shared files folder, which contained most of the administrative folders. Outside of just the potential legal ramifications of unintended users accessing payroll or administrative documentation, this made it so that bad actors did not even need to get access to an account that should have permissions to this data to be able to read or write to it, any account in the main office would have given them access to it. This was likely the greatest security vulnerability to the Water Resources system.
- Long before ADP began assisting WR, a program called PA File Sight logged whenever any user accessed any file in the share, so a record of the user's access would be available to Water Resources IT. While this would, in theory, be a possible solution to track a user accessing files they should not, it did not prevent access to these files in the first place, giving malicious actors access where it should be denied. In addition, at some point the license expired and the program is no longer logging this information. Water Resources does not appear to have made a move to renew the license at this time. Pictured below is the error message an ADP technician discovered that led to the discovery of the PA File Sight program, its use, and this whole file share practice.



- Notably, this read and write access given to every user would also include permissions to delete any file in the shared drives. While these files could be restored if discovered, as soon as the files fall outside backups, they would be gone without method of recovery and a weak trail of evidence. A bad actor that gained access to this folder through almost any user's account could, for example, covertly delete payroll documentation that isn't regularly in use and wait for it to fall out of retention, and the data would be unrecoverable.
- In the shared drive, there was an unencrypted excel document held every user's passwords as they were generated by Water Resources IT, including login passwords, timesheet access passwords, and fuel card access passwords. This increases the risk to the WR network to an almost unfathomable level, only to be compounded by the fact that none of these passwords were required to be changed by Water Resources IT policies. Because of the lack of policy on changing passwords, many of the passwords stored in this document were the same passwords that the users were using to log in. Because of this document, any user in the WR domain could log in as any other user, without their knowledge. They could log into the fuel system as anyone in the department. That is only the tip of the iceberg of this particular issue. The potential ramifications of someone acting on the data stored in this document are staggering and are only amplified by the access issues posed by the shared

drive itself.

POOR SECURITY PRACTICES

- As stated above, there was no policy in place to remove old users from the system, including users with administrative permissions. While the passwords to these accounts were changed, they were not changed to a secure password, merely "Admin". Since this is a common password on poorly managed IT, bad actors are likely to try it first in a brute force attack. In addition, this insecure password makes it much easier for any employee that once worked for the Water Resources department to maliciously log into the system and make changes. This puts the system at a greater risk than average to cyber-attacks that rely on the permissions or information on previous employees.
- Users occasionally leave their computers unlocked when they leave their desks, even when going on lunch. Gatekeeper should be preventing this, as it will automatically lock as it stops detecting the token, but if the user leaves it at their desk, it will stay unlocked. This is much worse than leaving their computer unlocked before Gatekeeper was implemented, as the password manager will be unlocked as well, giving anyone with physical access to both the Gatekeeper and the unlocked computer full access to that user's account and permissions. Cyber-attacks become trivial if a bad actor gets physical access to the Water Resources office space.
- Users in Water Resources accessed a shared New World through a shared computer login, called "Counter", due to the computer it is usually accessed from being at the front counter. Due to many users needing to use this account, the password was incredibly simple, the exact same name as the shared login. This password would be cracked instantly with modern techniques if the attacker could not guess it on their own.
- As addressed in the section on passwords, the shared New World account is also accessed with a remarkably simple password, but that, surprisingly enough, was not the most concerning issue with this account. Due to there being no log of which user accessed the account and what changes they made, there was no way to determine said information. Due to New World's nature as a software that manages transactions and financial information, data on what changes were made and what individuals made those changes is vital to protecting against fraud.
- The printer at the McFarland plant had a public IP address, meaning it could be seen by anyone inside or outside the network. Any computer connected to the global internet could ping the IP address and attempt to reach it. A public IP makes attacks that utilize that IP much easier to execute, as they do not require any physical access to the device in question.
- Phishing emails were not responded to with any urgency or perceived threat. A couple of weeks into the remediation, a user clicked on a phishing link. When

informed, Mike Kurzinger perceived the incident as funny, rather than an urgent matter that threatened his network's security. He joked about the incident to ADP technicians who were assisting in another issue. This lax reaction to what could become another major network incident is a significant risk to the Water Resources network. Even if all the technology is patched, those patches will do nothing to protect a network if its most vulnerable aspect, its end users, is bypassed. IT's response to incidents like this is vital to protecting the county's data from breach or ransom by attackers, and a serious attitude is an important first step to response.

REMOTE ACCESS SOFTWARE

- Water Resources used LogMeIn and TeamViewer to allow its users and vendors to remotely control their office workstations, specifically during the 2020 Covid pandemic and resulting lockdown order. Unlike the county's more secure methods of remote connection, such as a securely set up VPN, this software is not managed by either ADP or Water Resources IT. Without managing the connections that can be made directly, there is a larger risk of a bad actor exploiting credentials to gain remote control of a Water Resources computer.
- Certain alternate methods of remote connection are allowed on county machines while the machine is physically monitored by ADP and only if a vendor needs to remotely control a computer. This access is granted sparingly, such as when a vendor needs to preform manual maintenance to the devices or software they are providing the county. Water Resources computers had LogMeIn installed on them by Mike Kurzinger some time ago and the software was not removed for the end user's and WR IT's convenience.
- Water Resources IT would often learn about vendors connecting to a user's computer to fix certain issues after it had already happened. Even with a trusted vendor, it is best practice to have IT monitor the vendor's remote session to prevent malicious actions from being taken. End users generally do not have the experience necessary to identify malicious actions being taken, which is why it is imperative that IT be the point of contact and supervising agent in these scenarios.
- A known feature of some remote software, possibly including LogMeIn, was the ability to return to a previous remote session without the user's permission. A "recent connections" tab on the vendor's side would allow them to resume full control over the system, often without prompting the end user for the second time, leaving the end user and IT none the wiser.
- LogMeIn is particularly dangerous to keep on county systems because while installed, it regularly sends logs to some undisclosed location on the internet, even when not in use. Without knowing where this data is going and what parties may be privy to it, ADP must assume that it is being sent to malicious parties. Due to this assumption, ADP cannot allow the software on county systems at all.

- ADP asked Kurzinger to remove the software some time last year. Months later, the software was still on the Water Resources systems. Kurzinger claimed the software had been "disabled" and that because of that, the software did not have to be uninstalled. The ADP Board convened and formally asked for the software to be removed again. Kurzinger and other Water Resources technicians removed the program from most of the computers in their network. However, LogMeIn was still installed on two computers when Mike Kurzinger was placed on administrative leave.
- Since this software was connected to the county's network for so long, it is entirely possible that attackers could have discovered that vulnerability, exploited it, and were able to control the computers remotely.

BARRIERS TO REMEDIATION

Detailed below are various unnecessary obstacles encountered by ADP technicians in their work remediating the Water Resources incident, while migrating Water Resources away from the antiquated GCDWR domain, and while migrating Water Resources to Office 365. While these were only temporary setbacks, most had to be worked around so that the remediation could continue as planned and added many hours of unnecessary work to the remediation and migration.

DIRECT BARRIERS

- When converting to Office 365, most of the email backbone needed to be rebuilt from scratch, and this could have been prevented if the data were retrieved from the exchange server through a physical connection by Water Resources IT.
- In addition, many emails that should have been attached to a user's inbox were not attached in that way. In the rebuilding process the technicians needed to manually add the emails back to the user's inbox
- Throughout the remediation and migration process Mike Kurzinger has not been completely forthcoming or timely with his responses to ADP's questions and requests. For example, when being asked for a list of email addresses to make the migration to Office 365 much easier, he called said request, and previous requests, "intentional harassment" and ADP temporarily ceased further communication. After this brief pause in communication, ADP attempted to reach out again with relatively simple requests and Kurzinger still did not respond in a timely manner. This lack of communication forms a barrier that completely prevents ADP from continuing to work on the Water Resources network, specifically in the remediation effort, until Kurzinger responds.
- Water Resources seems unaware of the true scope of their network. They were unsure whether some servers were physical servers or virtual machines. This creates a created a situation where ADP was forced to either wait for Water Resources to confirm details about their own network or do unnecessary additional work to probe the network to get its true scope and determine which servers are virtual machines.
- Mike Kurzinger, likely due to not understanding how Gatekeeper works, deliberately told employees to leave Gatekeeper tokens at their desks. Doing this would leave those user's computers unlocked unless deliberately locked by the user. In addition, it makes it so that an attacker who can either gain physical or remote access to the computer only needs the 4-digit pin to log in, even though they should need both the Gatekeeper and the pin or the 25-character password. While this misinformation may have come from a fundamental misunderstanding of Gatekeeper's functionality, this specific misinformation drastically reduces the number of users who understand how the Gatekeeper works and how to keep the network secure with it. Additional training was required for all these users. ADP is not confident these users will listen to ADP's advice in the long term, as

the users are more likely to trust Mike Kurzinger's original statement or will find it more convenient in the long run.

- Windows Firewall was enabled on all computers across the GCDWR domain. While in theory this would improve the network's security, it also made it impossible for vendors to remote into the system to make necessary changes to continue remediation. ADP has tools in place that both prevent bad actors from getting into the network in that way and still allowing outside vendors to operate when necessary. Due to these tools, Windows Firewall does not add any additional security and only serves to hinder remediation efforts.
- The scanner at the main office is controlled by a tablet that was added to the GCDWR domain when initially set up. The admin password required to add it to the domain had been lost at some point, without Water Resources IT's knowledge. When attempting to help a vendor update software on the tablet, Water Resources attempted to find the password, to no avail. While ADP was able to work around this, it took more than two hours of unnecessary work.
- When some Water Resources users were having issues with their shared files, Nick Gorris began changing user permissions in the shared drive, accidentally deleting everyone's access to the folder, including his own. There are major security concerns with a non-trained user having the ability to change file access permissions. In addition, there are also concerns over the fact that Nick took it upon himself to fix user permissions, without contacting ADP until he had broken the sharing permissions. The following remediation took over 2 hours of research and work.
- Therefore, a scanning software used by Water Resources, was primarily controlled by Mike Kurzinger. When he was placed on administrative leave, there was no one in the department who knew how to function as an administrator for the software. Joe Birli's old login was still active, long after he left the Water Resources department. While Using this old login, ADP was able to set up Nick Gorris as an administrative user and trained him how to manage they system.
- The keycard control system for the Shop, Lab, and McFarland plant only had one account that could manage it, Mike Kurzinger's account. When Kurzinger was placed on administrative leave, no one could log into the software to make changes. While this has since been resolved, the system was inaccessible to WR IT for at least a month and a half.

CLIENTELE NOTIFICATION

- It appeared that Water Resources failed to notify clientele of the incident, including the EPA, OUPS, and the general public, until the delay in their services almost prevented them from meeting an EPA guideline and they asked ADP to have scanning to email ready so they may meet that deadline.

MDM MIGRATION

- All work smart phones are currently managed by Water Resources, and nothing can be installed without Mike Kurzinger's permissions through MDM. While this

does increase network security, this does hinder the remediation effort as the easiest way to set up Multi-Factor Authentication is through an authenticator app.

- Since Mike Kurzinger was the only person with access to the MDM, when he was placed on administrative leave, no management could be done on any of the Water Resources phones, and a separate training with Verizon on how to manage the MDM software and the various phones throughout the department had to be held. ADP was needed to be present for this remediation.
- The Apple Business Manager still has Joe Birli's old Water Resources phone as the authentication method. The location of this phone is currently unknown and may have been seized in the federal authorities' investigation.
- Many of these phones are not up to date with the latest security patches and present a possible vector of attack. Education of the users on the importance of regular patches would assist in management, as the users would be less likely to delay patches indefinitely because of the minor inconvenience patching would cause.
- The contact lists of the Water Resources work cellphones were controlled by the MDM through Exchange, and when the Exchange server was decommissioned, all contacts on the phones were deleted. The nature of the contact list was not communicated with ADP, and remediation of this issue has not begun.

OTHER MINOR ISSUES

Detailed below are minor issues that do not fall into the categories above but are still worth detailing. Also included in this section are bad practices that do not decrease the overall security of Water Resources system but should be addressed to bring them up to industry standards.

DISTRIBUTION GROUPS

- Distribution groups only contain 1 or 2 users which is not the best use case for a distribution list.

SPECTRUM PHONES

- At the Lab, the Spectrum phones managed by Water Resources IT stopped working for over a month and were not able to receive phone calls. These phones are not managed by ADP but instead by Water Resources IT department.

SERVER-SIDE PERMISSIONS

- Server-Side permissions should be delegated through groups but are instead being delegated by directly adding users to security folders.

MANUALLY BYPASSING THE SPAM FILTER

- Until placed on administrative leave, Mike Kurzinger had been manually allowing blocked emails through the Barracuda spam filter for several employees on a weekly basis. This had been going on for an unknown amount of time. This process defeated the purpose of the spam filter, if those emails were getting blocked by the filter's settings but were not malicious, the filter's settings should have been changed to accommodate.

DOCUMENT CHANGELOG:

Updated By:	Date Updated:	Version:
Zachary Molseed	5/19/2023	Version 2.0