City of Ripon

259 N. Wilma Ave. • Ripon, California 95366
Phone 209 599-2108 • Fax 209 599-2685
www.cityofripon.org

December 14, 2022

Honorable Michael D. Coughlan, Presiding Judge
Superior Court of California, San Joaquin County
180 E. Weber Ave, Suite 1306J
Stockton, California 95202

Dear Judge Coughlan,

The City of Ripon welcomes the opportunity to respond to the 2021-2022 San Joaquin Grand Jury Case #0321 Report (the "Report") regarding Cybersecurity. The City of Ripon always welcomes independent review of its information technology systems, and thanks the Grand Jury for its efforts.

The City of Ripon has reviewed the Report and implemented many of its recommendations. The City of Ripon would also like to take the opportunity to address the Report's specific findings and recommendations.

By way of background, the City of Ripon's IT Department experienced a significant amount of turnover over the last couple of years. Prior to the beginning of the information gathering stage by the Grand Jury, the City's only full-time Information Technology Technician that had been in this position for 15 years had resigned. During the information gathering stage, the City had just filled the full-time Information Technology Technician position, but unfortunately this individual resigned shortly after the completion of the information gathering stage because of a lack of the technical skill level and experience to function in this position.

Since the completion of the Grand Jury investigation and as part of the Fiscal Year 2022-23 budget, the City has created a second full-time Information Technology Technician position so there would be overlap in the understanding of department operations in the event an individual resigns in the future. The City is confident that these measures will address the areas of concern outlined in the Report.

Grand Jury Findings and City Responses:

In responding to the Grand Jury's Findings, we note each finding and the City of Ripon's response follows.

F6.1 It is unclear in the City of Ripon's Organizational Chart where responsibilities for IT and IT security lie, creating confusion over who is responsible to act in a disruptive event.

The City of Ripon respectfully disagrees with this finding for the reasons set forth below.

The IT Department is organized into Information Technology Technician level I and II, with the tier II technician reporting directly to the Lieutenant of the Ripon Police Department. The Police Department's organizational chart (see attached) depicts the relationship between the two IT positions and the Lieutenant. In a disruptive event it is clear that the technicians within the IT Department, as well as all identified vendors and contractors, respond to, preserve and reinstate functions at the City of Ripon, under the supervision of the Lieutenant.

At this time, both Information Technology Technician positions are filled and both employees have been fully briefed as to the organizational structure.

F6.2 The City of Ripon has a rudimentary network diagram outlining the City's router and firewall relationship with networks used, but the diagram lacks detail, leaving uncertainty about data security.

The City of Ripon respectfully disagrees with the finding. The City of Ripon has contracted with Waypoint Network Solutions for the last 15 years to assist in creating very detailed diagrams of network structure including documentation on router and firewall settings. Both of the City's Information Technology Technicians understand these diagrams and work with Waypoint Network Solutions as updates are periodically needed when improvements are made to increase the security of the City's network.

F6.3 Although the City of Ripon met expectations in the areas of data confidentiality and security, lack of IT staff and leadership leaves these areas vulnerable to cyberattack.

The City of Ripon has addressed this Finding as to staffing following the information-gathering phase of the Report. The City of Ripon has created a second full time position as part of the Fiscal Year 2022-23 budget. The City has filled both full-time positions since the completion of the information-gathering phase.

The City of Ripon respectfully disagrees with the finding regarding lack of leadership. The IT team leader reports directly to the Lieutenant of the Ripon Police Department for status updates and administrative decisions.

F6.4 The City of Ripon Lacks a Business Continuity Plan, rendering the City relatively unprepared to restore essential services in a disruptive event.

The City of Ripon has addressed this finding following the information-gathering phase of this Report. The City of Ripon has drafted a formal plan for business continuity as part of the City's Network Security Plan (see attached) that was approved by the City Council on December 13, 2022.

F6.5 The City of Ripon does not have a Disaster Preparedness Plan, leaving the City at risk for significant delay and cost to restore IT systems in the event of a disaster.

The City of Ripon has addressed this finding following the information-gathering phase of this Report. Many of the disaster response measures were already in place prior to the information-gathering phase. To avoid the confusion of utilizing multiple plans in the event of a ransomware attack, the City of Ripon has drafted the elements of the disaster preparedness plan as part of the City's Network Security Plan.

F6.6 The City of Ripon does not have a formal policy or procedure to address ransomware attacks. This absence of policy could cause confusion, delay and greater loss of security in the event of an attack.

The City of Ripon has addressed this finding following the information-gathering phase of this Report. Many of the measures to address a ransomware attack were already in place prior to the information-gathering phase. To avoid the confusion of utilizing multiple plans in the event of a ransomware attack, the City of Ripon has incorporated the elements of the ransomware attack response as part of the Network Security Plan.

Grand Jury Recommendations and City Responses:

In responding to the Grand Jury's recommendations, we note each recommendation and the City of Ripon's response follows.

R6.1 By January 1, 2023, the Ripon City Council develop and make public an updated City Organizational Chart showing details of the City's IT functions, including all IT positions.

The City of Ripon has updated its organizational chart to show the changes made to our current staff positions (see attached).

R6.2 By January 1, 2023, the Ripon City Council develop and adopt a detail Network Diagram to decrease system vulnerabilities.

The City of Ripon already has developed and adopted highly detailed networks diagrams that are kept confidential and secure internally. The City of Ripon recognizes the importance of maintaining network documentation and will continually maintain its network documentation consistent with the Grand Jury's recommendation.

R6.3 By January 1, 2023, the Ripon City Council obtain a third-party security review of the City's IT department assets, positions, and policies and an evaluation of data confidentiality, security systems and protocols.

The City of Ripon has obtained the third-party firm "Resolute Guard" to perform an independent review of the City's IT department assets, which has been completed. The City of Ripon's IT department has incorporated the recommendations of this third-party review into the operations of the IT department, consistent with the Grand Jury's findings.

R6.4 By January 1, 2023, the Ripon City Council develop, adopt and implement a formal Business Continuity Plan.

The City of Ripon has conducted an internal review of its network and developed the elements of the business continuity plan as part of the City's Network Security Plan that is accessible to the IT department and relevant Response Team Members. This plan was adopted by the City Council on December 13, 2022 and will be continually reviewed and updated to stay current and effective with evolving technologies.

R6.5 By January 1, 2023, the Ripon City Council develop, adopt and implement a formal Disaster Preparedness Plan.

The City of Ripon has conducted an internal review of its network and incorporated the elements of the Disaster Preparedness Plan as part of the City's Network Security Plan previously described.

R6.6 By January 1, 2023, the Ripon City Council develop, adopt and implement a formal internal policy and procedure for response to a ransomware attack.

The City of Ripon has conducted an internal review of its network and incorporated the elements of responding to a ransomware attack as part of the City's Network Security Plan previously described.

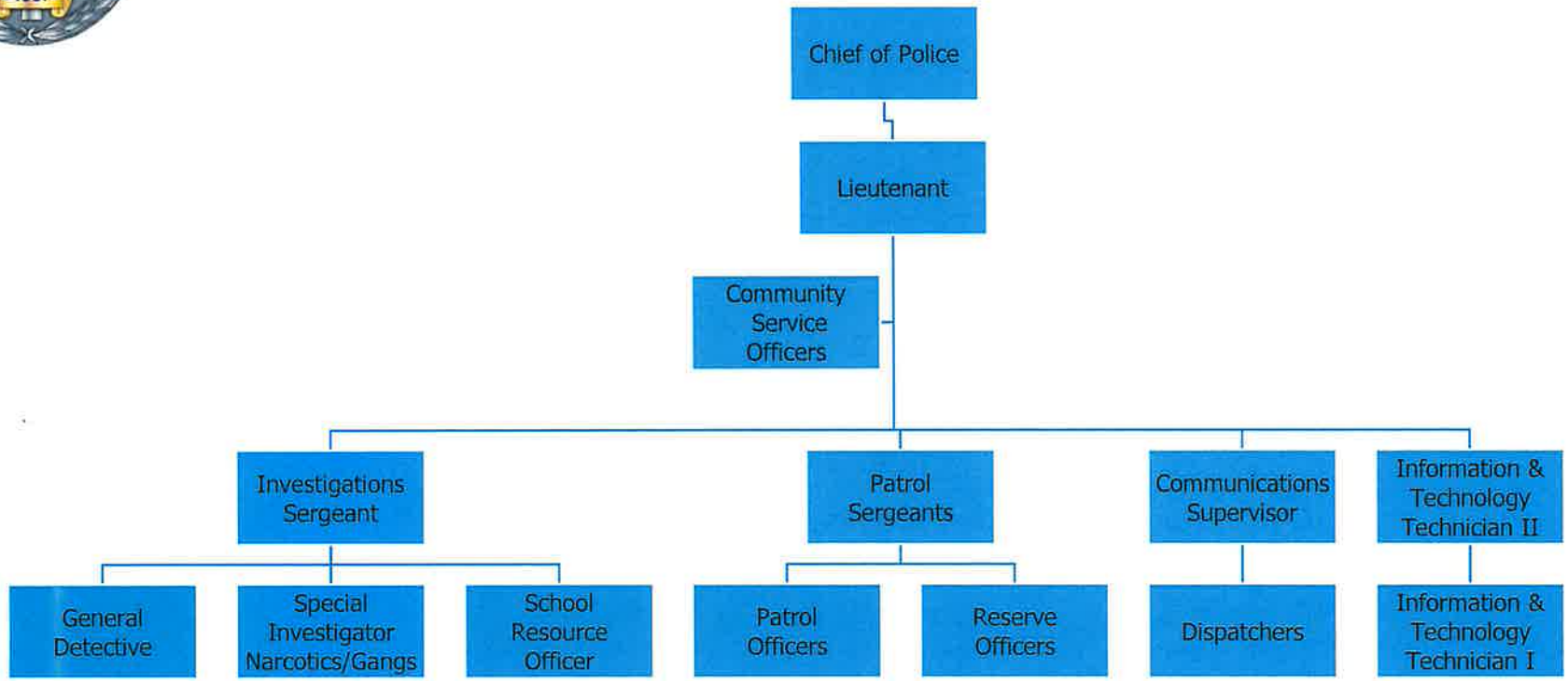
The City of Ripon would like to once again thank the Grand Jury for its effort in their review of the City's security posture. The City of Ripon agrees that it is vital that all local municipalities implement sufficient safeguards to protect their information systems and continue to supply vital resources to their constituents.

Please contact Kevin Werner, City Administrator at (209) 599-2108 or kwerner@cityofripon.org if there is anything further that you require.

Michael Restuccia, Mayor

Ripon Police Department

Organizational Chart



NETWORK SECURITY PLAN

City of Ripon

Network Security Plan

Version History

Version	Date	Author	Reason/Comments
1.00	October 2022	Hunter Crosby	Document Origination
1.1	October 2022	Hunter Crosby	Specific Team Details Added

Table of Contents

Introduction

There are several threats that could impact the City of Ripon's Information Technology Network resulting in lapses in the City's ability to conduct the "business" of the various City departments. The purpose of the document is to provide a framework for the efforts to prepare for these threats, and if realized, how to respond and recover.

Definitions

Below are the definitions of threats that are considered as part of the plan:

Standard Event

Any abnormal observable loss of service or accessibility occurrence in system, network, environment, process, workflow or personnel. Events may be negative in nature.

Adverse Event

Events with a negative consequence. This plan only applies to adverse events that are caused by factors beyond the resolution capabilities of the computer Incident Response Plan (IRP). Examples of adverse events outside of the scope of the IRP are natural disasters, power failures, ransomware or other malicious software attack, etc. and will be covered by the Network Security Plan.

The intent of the document is to provide a framework for the policies of the City of Ripon related to a standard or adverse event, which includes the following:

Part Contents

I Business Continuity Plan

II Disaster Preparedness Plan

III Ransomware or other Malicious Software Preparedness Plan

Audience

This document addresses several groups within the City of Ripon central administration with differing levels and types of responsibilities for network security, as follows:

- Administration
- Management Team
- Support Teams
- External Organizations

It should be emphasized that this document is addressed particularly to the members of the Network Security Team, since they have the responsibility of preparing for, responding to, and recovering from any disaster that impacts the IT functions of the City of Ripon.

Business Continuity Plan

Purpose

The increasing dependency on computers and telecommunications for operational support poses the risk that a lengthy loss of these capabilities could seriously affect the overall performance of the City of Ripon. A risk analysis identified network systems in two categories:

> Category I – those functions whose loss could cause a major impact to the City of Ripon within 72 hours of an outage; and
>
> Category II – those functions whose loss could cause a major impact to the City of Ripon within 2 weeks of an outage.

This risk assessment process will be repeated on a regular basis to ensure that changes to our processing and environment are reflected in recovery planning.

The Management Team recognizes the low probability of an event that results in severe damage to the network system, but understands the importance of preparing for such an event in order to reduce the impacts to the City's operations by limiting the damage during an event and being prepared to restore the lost data.

The City of Ripon's Business Continuity Plan is designed to focus resources on the restoration of the critical functions of the City based on the previously identified categories. This is accomplished by identifying responsibilities of the Business Continuity Management Team during an adverse event.

Assumptions

The Business Continuity Plan is predicated on the validity of the following three assumptions:

- The situation that causes the disaster is localized to the data processing facility within the City of Ripon network; or to the communication systems and networks that support the functional area. It is not a general disaster, such as an earthquake or hurricane affecting the entire region.

  It should be noted however, that the Business Continuity Plan will still be functional and effective even in an area-wide disaster. Even though the basic priorities for restoration of essential services to the community will normally take precedence over the recovery of an individual organization, the City of Ripon 's Business Continuity Plan can still provide for a more expeditious restoration of our resources for supporting key functions.

- The Business Continuity Plan is based on the availability of the hot sites or the backup resources. The accessibility of these, or equivalent backup resources, is a critical requirement.

- The Business Continuity Plan is a document that reflects the changing environment and requirements of the City of Ripon. Therefore, the Business Continuity Plan requires the continued allocation of resources to maintain it and to keep it in a constant state of readiness.

Development

The City of Ripon 's Information System Network Administrator, with assistance from key City of Ripon support areas, is responsible for developing the City of Ripon 's Business Continuity Plan.

Maintenance

Ensuring that the Business Continuity Plan reflects ongoing changes to resources is crucial. This task includes updating the Business Continuity Plan and revising this document to reflect updates; testing the updated plan; and training personnel. The Information System Network Administrator is responsible for this comprehensive maintenance task.

The Management Team ensures that a formal review is initiated whenever there is a significant change required for the Business Continuity Plan or at least completed annually.

Testing

Testing the Business Continuity Plan is an essential element of preparedness. Partial tests of individual components and recovery plans will be carried out on a regular basis. A comprehensive exercise of the Business Continuity Plan capabilities and the designated recovery facilities will be performed on an annual basis.

Contact Information

Updated October 2022

The following is a list of roles to be referred to in a disaster recovery event.

Name	Title	Role	Contact Information	Escalation (1-3)*
City Administrator	Business Continuity Manager	BC manager	(209) 599-0235	1
IT Tech II	Infrastructure Manager	IR Manager	(209) 599-0277	1
Chief of Police	Communications Manager	BCT member	(209) 599-0259	2
City Attorney	Legal	BCT member	(209) 599-0214	3
IT Tech II	Risk Manager	BCT member	(209) 599-0277	3
City Clerk	HR Representative	BCT member	(209) 599-0217	3
Chief of Police	Physical Security Representative	BCT member	(209) 599-0259	3
Consultant – Way Point Network Solutions	3rd Party Support		(209) 581-6789	2
Alliant	Cyber Insurance Provider			3
City Council	Regulatory/Government Reporting Body			3

*Escalation level determines order in which notification should occur:

1. Notify first, required on all incidents
2. Required on all moderate or high-severity incidents
3. Involve as needed

Processes and Procedures

The processes and procedures explained below pertain specifically to a disaster disabling the main data center. This functional area houses the servers and infrastructure devices needed to support the City of Ripon's administrative applications. Especially at risk are the critical applications designated as Category I systems. The Business Continuity Plan provides for recovering the capacity to support these critical applications within 72 hours. The subsections below detail the framework set in place to restore the business functions of the City in response to an adverse event:

1. Detect and determine a disastrous condition.
    a. The detection of an adverse event that could negatively affect information processing systems at the City of Ripon is the responsibility of the IT Team, Physical Security Representative, or whoever discovers or receives information about an emergency developing in the data center or other areas housing major information processing systems or about the communication lines leading into the buildings.
    b. The Infrastructure Manager evaluates the initial status of the damaged area and isolates the event, to the best of their ability, such that other areas are not damaged.
    c. The IT team will estimate the salvageability of the remaining equipment. The assessment of the damage is reported to the Business Continuity Manager.
    d. The Business Continuity Manager will notify the City Council of the issue and continue to provide updates through all phases of the event.
2. Notification of Personnel Responsible for Recovery.
    a. When a situation occurs that could result in interruption to major information processing systems on sites, the Infrastructure Manager must be immediately notified.
    b. Based on the evaluation by the Infrastructure Manager and resources needed to evaluate, isolate, and eventually restore the impacted infrastructure, the Business Continuity Manager will contact additional resources, including the City of Ripon's consultant to assist.
    c. Other resources will be notified to assist with the functions of the Business Continuity Plan, as determined by the Business Continuity Manager.
3. Activate the designated hot site.
    a. The responsibility for activating any of the designated hot sites or backup resources is delegated to the Infrastructure Manager. Within 24 hours of the occurrence the Infrastructure Manager, or designee, will determine the prognosis for recovery of the damaged data center or network infrastructure through consultation with the Consultant, as needed.
    b. If the estimated occupancy or recovery of the damaged data center cannot be accomplished within 72 hours, the usual occupants of the backup site are notified of the intention to occupy their facility.
4. Disseminate Internal and External Information.
    a. The Infrastructure Manager is responsible for relaying estimates and updates regarding the status of the recovery process to the Communications Manager (external communication) and HR Representative (internal communication).
    b. The Communications Manager is responsible for directing all meetings and discussions with the news media and the public, and in conjunction with the IT Team, personnel not actively participating in the recovery operation.

c. The Communications Manager will notify the public and the media of the City of Ripon business functions that are impacted by the event and the duration of the expected outage.
d. The HR Representative will communicate with the City Department Heads regarding the impacts to those various departments and any interim operating plans they will need to implement, based on the impacts from the event.

5. Emergency Phase
    a. The emergency phase begins with the initial response to a disaster. During this phase, the existing emergency plans and procedures are implemented for direct efforts to protect life and property. Security over the area is established as local support services such as the Police and Fire Departments are enlisted through existing mechanisms. The Infrastructure Manager is alerted and begins to monitor the situation.
    b. If the emergency situation appears to affect critical facility or services, either through damage to data processing or support facilities, or if access to the facility is prohibited, the Infrastructure Manager will closely monitor the event, notifying the Business Continuity Team Members as required to assist in damage assessment. Once access to the facility is permitted, an assessment of the damage is made to determine the estimated length of the outage. If access to the facility is precluded, then the estimate includes the time until the effect of the disaster on the facility can be evaluated.
    c. If the estimated outage is less than 72 hours, recovery will be initiated under normal Information Systems operational recovery procedures. If the outage is estimated to be longer than 72 hours, then the Infrastructure Manager, activates the Business Continuity Team Members and notifies the Communications Manager and HR Representative that the Business Continuity Plan is activated. The recovery process then moves into the backup phase.
    d. The Business Continuity Management Team remains active until the recovery is complete to ensure that the organization will be ready in the event the situation changes.
    e. The Infrastructure Manager is responsible for establishing voice and data communications between the affected site and the remainder of the City of Ripon departments.
    f. The Infrastructure Manager along with the appropriate team members will evaluate the initial status of the damaged functional area and estimates both the time to reoccupy the facility and the salvageability of the remaining equipment.
    g. Following the assessment of damage the Infrastructure Manager is responsible for salvaging equipment, data, and supplies following a disaster; identifying which resources remain; and determining their future utilization in rebuilding the data center and recovering from the disaster.
6. Backup Phase
    a. The backup phase begins with the initiation of the appropriate Business Continuity Plan for outages lasting longer than 72 hours. In the initial stage of the backup phase, the goal is to resume processing critical applications. Processing will resume whether at the main data center or at the designated hot site, depending on the results of the assessment of damage to equipment and the physical structure of the building.
    b. In the backup phase, the initial hot site must support critical (Category I) applications for up to 4 weeks and as many Category II applications as resources and time permit. During this period, processing of these systems resumes, possibly in a degraded mode, up to the

capacity of the hot site. Within this 4-week period, the main data center will be returned to full operational status, if possible.

c. However, if the damaged area requires a longer period of reconstruction, then the second stage of back up commences. During the second stages, a shell facility is assembled and equipment installed to provide for processing all applications until a permanent site is ready.

7. Recovery Phase
    a. The time required for recovery of the data center and the eventual restoration of normal processing depends on the damage caused by the disaster. The time frame for recovery can vary from several days to several months. In either case, the recovery process begins immediately after the disaster and takes place in parallel with backup operations as soon as possible.
    b. The Business Continuity Manager will contact the carrier notifying them of the event and the City of Ripon submitting a claim.
    c. The Physical Security Representative is to investigate the event and work with the City Attorney, as needed.
    d. The Business Continuity Manager will assign the task of updating the Business Continuity Plan, and other related plans, with the lessons learned from the most recent event to the most appropriate team member(s).

Disaster Preparedness Plan

Disaster Preparedness is a constantly evolving field, and as such, the City of Ripon's IT Team will continue to constantly re-evaluate the various systems and procedures in place to respond to a major adverse event. The section below provides an overview of the steps that the IT Team has or plans to put into place to maximize Disaster Preparedness.

1. Documentation
    a. The City of Ripon's IT Team maintains a database of constantly updated documents that detail the Information System Network in place at the City of Ripon. These documents consist of detailed network maps and copies of infrastructure configuration settings.
    b. In the event of a major adverse event, highly detailed network maps will assist with isolating any potential issues as well as assist in rebuilding the network.
2. Routine BackUp
    a. The City of Ripon utilizes a robust backup system that completes a backup of all servers within the Data Center no more than every 24 hours.
    b. Critical applications marked as Category I are routinely backed up on a schedule of no more than every 12 hours. Category I servers are also replicated, so that a working copy of the service can be brought up within minutes as long as the replication is available.
    c. Active databases are backed up separately, keeping a spare copy of the database available for restoration in the event of disaster.
3. Hot Spares
    a. The City of Ripon stores hot spares of important infrastructure that can be put in place of non-functioning equipment in the event of a failure.
4. Training
    a. The City of Ripon's IT Team is continuously training and revising recovery strategies to ensure that the procedure put into place is best practice. In a major adverse event, the IT Team is prepared to react quickly to restore Category I systems and minimize downtime.

Ransomware and Malicious Software Attack Plan

Instances of malicious software breaches are becoming more prevalent as businesses become more technology dependent, making cybersecurity an area on concern. The City of Ripon will continually re-evaluate its network to find vulnerable areas that can be bolstered to prevent against Malicious Software Attacks (MSA).

The City of Ripon embraces a philosophy of data flexibility. In the event of an MSA, the data in use in the production environment can be thrown away and replaced with a backup copy of data with minimal data loss. This avoids payment for encrypted data by allowing compromised data to be wiped and replaced with clean copies taken from backups done no more than every 24 hours. These backup copies are monitored on a daily basis as well as checked with Cyclic Redundancy Checks (CRC) to avoid corruption of data.

The framework below provides an overview of the City of Ripon's response to a Malicious Software Attack:

1. Isolation
    a. In the event of a Malicious Software Attack (MSA) detection and isolation are crucial in limiting the amount of data lost and damage done to the network. The City of Ripon employs endpoint protection on all devices on the network to detect any intrusions. If an intrusion is detected, the IT Team will attempt to isolate the infected devices as much as possible. The City of Ripon is divided into three main networks, limiting the reach of any MSA that breaches the network.
2. Clean and Restore
    a. After the threat of an MSA has been isolated and can no longer spread, the cleaning phase will begin. All infected devices will be wiped to factory defaults and scrubbed of data as much as possible before being subjected to a second round of testing. Once all infected data has been removed from the devices, they can be rebuilt from backups and placed back into circulation.
3. Monitoring
    a. After an MSA has been addressed, the IT Team will continue to monitor the network affected for any changes or signs of reinfection.
4. Training
    a. One of the most important aspects of preventing an MSA is the continuous training of end users. Many malicious software requires user action to infect a network. The most common forms come from phishing emails that deliver infected attachments, or through drive-by downloads acquired by visiting infected sites. The City of Ripon utilizes continuous training to educate end users on methods to identify and avoid phishing attempts or malicious code sent through attachments.