STUDY SESSION

TO: Mayor and Council
FROM: Margaret Brocklander
DEPARTMENT: IT
DATE: March 5, 2018
SUBJECT: After Action Report and Emergency Management

DESCRIPTION:
After Action Report and Emergency Management

RECOMMENDATION:
Margaret Brocklander will be present to discuss the after action report to the ransomware attack that occurred in October of 2017. Emergency Management concepts will also be discussed along with the report that is attached for the Council's review.

ATTACHMENTS:
After Action Report October 2017 Ransomware Attack
After Action Report
October 2017
Ransomware Attack
Purpose

The purpose of this After Action Report (AAR) is to learn from the actions taken in response to the October 2017 ransomware attack. The AAR should be used as a knowledge-sharing tool that will help staff and our community partners better understand and plan for recovery from cyber events.

This report provides an analysis of the preparedness, response, and recovery efforts of the information technology systems following the ransomware attack. The AAR is a compilation of chronology-based notes, internal and external communications and staff input. Staff input was obtained through an after action review exercise. The exercise was informal, flexible and focused on learning with two simple questions. What went well? What could have gone better?

Incident Overview

As technological innovation and advances bring us greater convenience, efficiency, and productivity, they are also generating new vulnerabilities. The Internet has created a new frontier for criminal activity in the form of cybercrime, such as ransomware.

The term “ransomware” is a type of malware that blocks access by encrypting files unless a ransom is paid. Criminals are using a technique called cryptoviral extortion, in which it encrypts the files, making them inaccessible, and demands a ransom payment in digital currency to decrypt them. In a ransomware attack, recovering the files without the decryption key is an obdurate problem – and difficult to trace digital currencies such as Bitcoin are used for the ransoms.

The IT Department responded to a call from end users reporting encrypted files on their business applications server. The IT team investigated the report, determined it to be ransomware and immediately began network shutdown. After network shutdown, the team reviewed the logs more in depth and found evidence of an extended brute force attack on the server that ended at 5:05pm and the malware file installed at 5:15pm.

The end users delayed reporting the encrypted files to the IT Department until 5:44 pm and during those precious minutes, the ransomware virus spread throughout the city’s computer systems. In less and an hour, the ransomware virus infected 85% of the city’s computer systems. The ransomware attack was carried out using the "SAMSAM worm" that traveled automatically between computers without user interaction.

Due to the severity of the ransomware attack, departments were required to modify their operations to accommodate computer absence until full recovery was completed. The City does not run on redundant servers which would minimize potential business disruption in the event of a disaster, nor does the city possess a redundant “warm-site” or “hotsite” for quick recovery of the Data Center. The process for recovery was labor intensive and required rebuilding all business application servers and approximately 300 end user computers.
Timeline

Tuesday, October 3

- A problem with a computer was reported to the helpdesk at 5:44 pm.
- Following investigation and determining it was ransomware, systems shutdown and end user computers were disconnected from the network.
- The City Manager was notified of the ransomware attack and systems shutdown.
- MS-ISAC was called in to assist with malware analysis.
- Request for assistance to metro area cities was made to assist with restoring business applications and end user computers.

Wednesday, October 4

- Notification of the ransomware attack & instructions was sent to all employees.
- City of Brighton responded to the call for assistance and began restoring servers. All critical servers were restored by late evening.
- Operations departments reported on their ability to continue operations without computers i.e. WWTP reported the plant's safety equipment and systems are all operational, and there is no foreseeable risk of violating permit or internal standards.
- A media release was issued to the local media.

Thursday, October 5

- City & County of Denver cyber security specialists assist with identifying source of the ransomware.
- Priority order by Department for restoring end user computers compiled.
- City & County of Denver desktop specialists arrive to assist with rebuilding end user computers.
- Network at Civic Center was made available for cleared end user computers.

Friday, October 6

- Rebuilding & patching test & dev servers.
- End user computer restore continues w/Denver’s assistance.
- Golf was cleared to resume operations.
- Police critical business applications restored.

Sunday, October 8

- End user computer restore at Civic Center 95% complete.
- All Police business applications were restored.
- Restoration of end user computers at Police Department continues – patrol cars were not affected.

Monday, October 9

- Additional improvements were made to business systems.
- IT Team was deployed to Service Center to restore the remaining end user computers.
- IT Team was deployed to PD to restore the remaining end user computers.
- IT Team was deployed to WWTP to restore the remaining servers and end user computers.
- Englewood WIFI enabled.

**Monday, October 9 – Friday, October 13**

- Application installs and end user computer rebuilds continued throughout the week until all users were restored to pre-ransomware condition.

---

**After Action Analysis**

The after action analysis of core capabilities was conducted by the Information Technology team. The purpose of the after action analysis was to assess the recovery process and identify areas for improvement. Table 1 depicts the core capability, objective and how well the task was performed.

**Table 1, Analysis of Core Capabilities**

<table>
<thead>
<tr>
<th>Core Capability</th>
<th>Objective</th>
<th>Performed without Challenges (P)</th>
<th>Performed with Some Challenges (S)</th>
<th>Performed with Major Challenges (M)</th>
<th>Unable to Perform (U)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess the Situation</td>
<td>• Virus entry point and identification</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Utilize MS-ISAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Initial damage assessment data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Declare Emergency</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution</td>
<td>• Emergency Management Plan Execution</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Recovery Operations</td>
<td>• Additional Resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Coordination</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Agency Outreach</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Accessibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td>• Coordinate, manage, and facilitate press release</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Coordinate, manage, and disseminate information to employees</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Conduct situational awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Assess the Situation

Strengths

**Entry Point and Identification:** The virus entry point and identification was confirmed within hours; however, in order to contain and eliminate the threat, the team needed time to research all of the threats that were present on the server, what the threats were designed to do, and the method used to propagate throughout the network.

**Network Shutdown:** Network shut down commenced immediately following notification and confirmation of the virus to prevent virus spread.

**Declare Emergency:** City leadership was notified immediately following confirmation of the virus and network shutdown.

**MS-ISAC Membership:** Multi-State Information Sharing & Analysis Center (MS-ISAC) membership provided the opportunity to engage their Computer Emergency Response Team. MS-ISAC is comprised of highly trained staff who were able to assist with malware and forensics analysis.

Areas for Improvement

**Entry Point and Identification:** City of Englewood employees rely heavily on the Information Technology infrastructure and business applications to accomplish their jobs, and it is an integral part of providing city services. Because of this reliance, IT services are considered a critical component in the daily operations, requiring these services be re-established quickly and completely. For nearly 24 hours following confirmation of the threat all available IT resources were focused on researching the threat before executing a process to begin recovery. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. The Emergency Response Plan will assist the city in establishing computer security incident response capabilities to handle incidents efficiently and effectively.
Initial Damage Assessment: A sustainable process for diagnosing and labeling end user computers was not established at the start of the incident and caused rework. In addition, the desktop inventory was not completely accurate and slowed the recovery process. A more robust inventory solution will need to be put into practice as soon as possible.

Emergency Management Plan Execution

Strengths

Local Government Experience: The restoration of business functions and allocation of available resources were prioritized based on the impact to operations and sequenced to ensure that dependent functions were restored in the right order. The prioritization and sequencing of business application restoration was achieved through IT staff’s years of local government experience and knowledge of the most critical systems.

Areas for Improvement

Cyber Disruption Plan: An Emergency Response Plan that addresses Cyber disruption to best protect the City of Englewood’s critical technology infrastructure is essential. The Plan should include a business impact analysis (BIA) and all departments should have contingency plans for their operations, which include operating without IT systems for an extended period. The BIA will determine the most critical business functions and systems, the staff and technology resources needed for operations to run optimally, and the time frame within which the functions need to be recovered for the organization to restore operations as close as possible to a normal working state.

Recovery Operations

Strengths

Agency Outreach: Fast-tracking recovery was possible thanks to strong relationships with technology leaders in the Denver metro area. Technology experts with similar technology environments responded to a request for assistance and we were able to accelerate the recovery process. The City of Brighton and the City and County of Denver were invaluable to fast tracking the recovery process.

IT staff collaboration and dedication to the City: Throughout the event, IT staff coordinated with each other to address the situation. Some of the integration was spurred by ad hoc injects of leadership, but much of the integration occurred organically among IT staff themselves.

IT Infrastructure: The new IT administration identified a multitude of issues with the infrastructure, network performance, and network security. With the support of city leadership the team implemented numerous improvements to the infrastructure, security and business systems over the last year. If those improvements were not implemented recovery would have been near impossible.

Cloud Computing: The diversity of on premise and cloud based business applications expedited the recovery of some critical systems.
Areas for Improvement

**Long-Term Staffing Sustainability:** Restoring operations as close as possible to a normal working state required long days and several weeks. Englewood IT staff were fatigued and needed relief. While staff from the City of Brighton and City and County of Denver responded to a request for assistance, formalizing resource options for recovery will need to be examined and included in the Emergency Response Plan.

**IT Infrastructure:** The IT staff has implemented a multitude of improvements highly focused on the infrastructure and security of network. Stabilizing and securing the network were the highest priority; however, the ransomware event did highlight that there is much more to do. As the network stability and security improvement projects are nearing completion attention will need to be focused on asset management, automation, cross training and process improvement.

**Patching policy:** Many vulnerabilities can be fixed by applying vendor-provided security patches. It is the city’s policy to apply the most recently released patch within one month of release. The practice of applying patches was not consistently applied across the organization. If end users were adversarial to applying the patch the IT staff accommodated their request to postpone. Strict adherence to the patching policy will be followed without exceptions.

**Roaming Profiles:** A roaming profile is a user profile that is stored on a server so users can access their information and settings regardless of what computer they are using. Roaming profiles would have increased the efficiency of restoring the end user computer. A project to implement roaming profiles is on the IT projects roadmap.

**Network Monitoring Tools:** Network security monitoring tools would have alerted IT earlier. With the implementation of IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) both increase the security level of the network, monitor traffic and inspect and packets for suspicious data.

**RDP Server:** The RDP server (source of ransomware) was identified as a risk earlier in the year; however, end users were adversarial to removing the server so IT staff accommodated their request to postpone. Striking a balance between operations productivity and maintaining secure IT systems will be addressed in ongoing emergency management planning sessions.

**Business Application Automation:** Use SCCM to push business applications - business application automation. Need a Windows Image by location and/or specific position.

**Domain Structure:** The domain structure complicated recovery

**Accessibility:** The city has two badge systems that presented access limitation for IT staff and the need to send IT staff to the same location more than once.

**Legacy Systems:** Business applications on older operating systems that cannot be patched present a security risk and will need to be addressed in the IT strategic plan to upgrade the systems or retire the systems.

**Police Business Applications:** Public Safety systems are critical systems and restoration to a normal working state needs to be immediate. Regrettably, IT staff were dependent on calling the vendor to...
install the dispatch software on workstations, which presented an unacceptable delay. In addition, business application cross training for all public safety applications was discussed but not completed. Therefore, the restoration of public safety systems was dependent on one staff person. Because IT staff is reliant on vendors and lacks cross training on critical systems the restoration suffered an unacceptable restoration timeframe. A priority for IT staff will be a cross-training program for all public safety systems to be completed within a very short timeframe.

Communications

Strengths

Public Communications: The Communications Department served as the dissemination point for all media releases, media inquiries and calls to the city.

Internal Communications: The Communications Department and IT Department jointly served as the dissemination point for all internal communications. The city used a variety of communication vehicles, including email, Everbridge, posting notices, and utilizing the leadership team to transmit information throughout their departments.

Conduct situational awareness: The recovery team was brought together several times throughout each day to review progress toward the City’s return to continuity. During the meeting, the Director reviewed progress, timelines, resources and equipment necessary to accelerate recovery.

Areas for Improvement

Communications: Develop communications means and methodologies to enable intra and extra communications for cyber events in the Emergency Management Plan.

Conclusion

Every public and private organization’s computer systems are vulnerable to cyber-criminals and hackers and the challenges are even greater when department resources are limited. The team has limited resources but it is comforting to know that many of the municipalities in the Denver metro area willingly offered to fast track recovery.

Overall, the response to the October 2017 Ransomware attack was remarkable, given the circumstances. Information Technology staff as well as resources from other municipalities, the City of Brighton and City and County of Denver worked to restore and rebuild city services.

Lessons learned from the experience will help the City of Englewood better prepare for potential cyber events. Implementing the recommendations (Areas for Improvement) coming out of the after action analysis provides the city with a greater degree of support and protection required to keep systems and services operational.

The City of Englewood is exceedingly grateful to all of the municipalities that responded to calls for assistance during the ransomware attack recovery.