Best Practices for Overcoming Ransomware: One District’s True Story
Chris Langford
Director of Network, Infrastructure, and Cyber Security
Lewisville ISD

Tell about yourself and the district.
Wasn’t with LISD at the time which means I can tell the story without bias.
120 sq. miles, 70 campuses, 6,500 staff, and 53,000 students

Does anyone not know what Ransomware is?
Session Outline

• Incident Timeline
• Step through incident
• Best practices that were used during incident
• Best practices that have been implemented since incident
• Best practices that still need to be implemented
• Importance of end-user training
• Importance of backups
• Q&A

End bullet: I’m not going to promote specific products or solutions. There is an entire room filled with those in this building. I’m going to focus on best practices and techniques. The products and solutions that support those are yours to choose. Each environment is different and what works in LISD, might not be right for your district.
Incident Timeline - May 10, 2016

- Incident reported to the Helpdesk and ransomware discovered by a Network Engineer
- Infected machines re-imaged to remove ransomware
- Network shares restored from backups
- Network shares and machines tested to confirm full functionality
- Incident investigated and documented
Incident Timeline - May 10, 2016

Incident reported to the Helpdesk and ransomware discovered by a Network Engineer
Incident report/discovery

• The Helpdesk received calls first from users in Central Admin about not being able to access files on their hard drives and network shares.
• This quickly spread to users in the Special Education building and office staff at many of the schools.
• At the same time, the Network Engineer primarily responsible for the SAN started receiving thousands of alerts from the SAN anti-malware software.
• In total, there were over 200,000 alerts during the day of the incident.
Incident Timeline - May 10, 2016

Incident reported to the Helpdesk and ransomware discovered by a Network Engineer.
Incident Timeline - May 10, 2016

- Incident reported to the Helpdesk and ransomware discovered by a Network Engineer
- Initial steps taken to remove ransomware
Initial Steps Taken to Remove

• The specific ransomware was determined to be a variant of CryptoLocker.

• Re-imaging the end-user machines was not done immediately, because many users had files saved on their hard drives that they needed.

• Desktop support contacted our then anti-malware vendor to see if they could remove the malware. They could not.

• Desktop support then researched other products that might be able to remove the malware. They tried multiple solutions, but none worked.

Bullet 2 tip: Educate users not to store files on local machines. Use OneDrive, Google Drive, or network shares.
Incident Timeline - May 10, 2016

- Incident reported to the Helpdesk and ransomware discovered by a Network Engineer
- Initial steps taken to remove ransomware
Incident Timeline - May 10, 2016

- Incident reported to the Helpdesk and ransomware discovered by a Network Engineer
- Infected machines re-imaged to remove ransomware
- Initial steps taken to remove ransomware
Machines re-imaged

- All infected end-user machines were re-imaged to remove the ransomware.
- Desktop Services coordinated with the Datacenter Team to re-image the infected machines shortly before the network shares were restored from backup.

Bullet 2 tip: Need good coordination between your teams in this type of situation.
Incident Timeline - May 10, 2016

- Incident reported to the Helpdesk and ransomware discovered by a Network Engineer
- Initial steps taken to remove ransomware
- Infected machines re-imaged to remove ransomware
Incident Timeline - May 10, 2016

- Incident reported to the Helpdesk and ransomware discovered by a Network Engineer
- Initial steps taken to remove ransomware
- Infected machines re-imaged to remove ransomware
- Network shares restored from backups
Network shares restored from backup

• Shortly after the infected machines were re-imaged, the network shares were restored from backup.
• The backup provider’s support had to be contacted to complete the restore process.
• The restore process had to be completed through the command line, not through the standard method.

Bullet 3 tip: Make sure your hardware and software providers have great support.
Incident Timeline - May 10, 2016

- Incident reported to the Helpdesk and ransomware discovered by a Network Engineer.
- Infected machines re-imaged to remove ransomware.
- Initial steps taken to remove ransomware.
- Network shares restored from backups.
Incident Timeline - May 10, 2016

- Incident reported to the Helpdesk and ransomware discovered by a Network Engineer
- Initial steps taken to remove ransomware
- Infected machines re-imaged to remove ransomware
- Network shares restored from backups
- Network shares and machines tested to confirm full functionality
Machines and shares tested to confirm functionality

- All systems and shares were inspected to confirm full functionality.
- There was no evidence of any malware being present.

Bullet 2 tip: Why test machines after a re-image? Some malware can survive a re-image. Certain rootkits and BIOS-infecting malware can still be present. Important to verify after re-image.
Incident Timeline - May 10, 2016

- Incident reported to the Helpdesk and ransomware discovered by a Network Engineer
- Initial steps taken to remove ransomware
- Infected machines re-imaged to remove ransomware
- Network shares and machines tested to confirm full functionality
- Network shares restored from backups
Incident Timeline - May 10, 2016

- Incident reported to the Helpdesk and ransomware discovered by a Network Engineer
- Initial steps taken to remove ransomware
- Infected machines re-imaged to remove ransomware
- Network shares and machines tested to confirm full functionality
- Network shares restored from backups
- Incident investigated and documented

Incident investigated and documented
Investigation and documentation

- The time spent resolving this incident from the time it was reported to when it was resolved was about 6 hours.
- During the incident, it was determined that the ransomware was delivered through a macro in a Word document that was emailed to dozens of LISD staff members.
- Also during the incident, an email alert was sent to all staff detailing the ransomware email and directing staff to delete it, if received.
- As more staff members opened the document, more machines and shares were infected.
- The alerts from the SAN anti-malware program were notifying the engineers that a file had been changed on a per file basis, which is why there were over 200,000 alerts.
- All of the details and the procedure for resolving the incident were then documented and saved.

Bullet 3 tip: Communication with end-users during this type of incident is key. They need to be aware of what is happening and how they should respond.
Incident Timeline - May 10, 2016

- Incident reported to the Helpdesk and ransomware discovered by a Network Engineer
- Initial steps taken to remove ransomware
- Infected machines re-imaged to remove ransomware
- Network shares restored from backups
- Network shares and machines tested to confirm full functionality
- Incident investigated and documented
Best practices used during incident

• A system to monitor the SAN and notify appropriate personnel of the changes that were occurring.

• End-users knew to report issues to the Helpdesk.

• A knowledgeable Helpdesk and Datacenter staff that quickly began working on the issue.

• Usable, secure, and tested backups of all data on the network shares.
Best practices implemented since incident

- Active Directory Audit to remove unneeded permissions from user accounts.
- Disabled macros in Office and Office 365 for all users that don’t need them.
- Migrated to new, cloud-based anti-malware program that is much more effective at blocking this type of attack.
- Implemented Technology Security Advisory emails that are sent to all staff whenever there is a need.
- Taken steps to ensure timely OS patch install rollouts.

**Bullet 1:** Share permission and user permissions, i.e. execute and admin permissions.
**Bullet 2:** Very important. According to PhishMe, 93% of all phishing emails contain ransomware. Also, need to block Javascript files and .zip files, if possible in your environment.
Best practices that still need to be implemented

• Expand user training over email and network security and social engineering.
• Upgrade backup solution to newer, more secure solution.
• Implement cloud-based email security in Office 365.
• Implement threat intelligence client on all endpoints.
• Implement holistic network security solutions that communicate with each other.
Importance of end-user training

• End-users are your first line of defense.
• End-users are your last line of defense.
• End-users may be your only line of defense.
• End-user training is very important.
Types of end-user training

• Email alerts regarding specific threats.
• Email alerts describing how to recognize malware and how to respond.
• Email alerts describing how to recognize social engineering and how to respond.
• Send out your own phishing emails and see who gives out their personal information.
• Formal, required training either developed in-house or purchased through a partner.

Bullet 1: Ensure your security personnel are subscribed to security email lists, reading security blogs, following security-related Twitter feeds, and are member of security-related Linkedin groups.
Importance of backups

• In many cases, secure backups are your only hope against a ransomware outbreak.

• Without backups, you either pay the ransom or lose your data.

• Having backups is not enough. The integrity of the backups should be tested on a regular basis.

• A ransomware outbreak is not the time to be testing your backups.

Q&A
In conclusion...

- It’s not a matter of if, but a matter of when you will be hit with a ransomware attack or outbreak.
- The most important best practices to have in place are trained, competent end-users and tested, secure backups.
- If you can only have one of those, go with backups, as they are less likely to fail than end-users.
- Also, blocking macros through policy and Javascript files and .zip files in email is very important.
Thank you!