

# Centro Cyber Security Event and Response



- In 2020, Centro was cyber attacked
- The event happened late at night
- The attacker gained access through a server
- Some files were extracted
- Some files were encrypted (locked)
- A ransom was requested

- A Cyber Security firm was engaged
- They became our negotiators
- We assessed the content of the extracted files
- Fortunately, we had high quality back-ups
- We decided to restore the back-ups
- This took approximately 1 week

## **Poor judgment and Policies**

- No policies regarding server firewalls
- IT associates lacked understanding
- Passwords needed elevated

## **Lack of Tools and Protection**

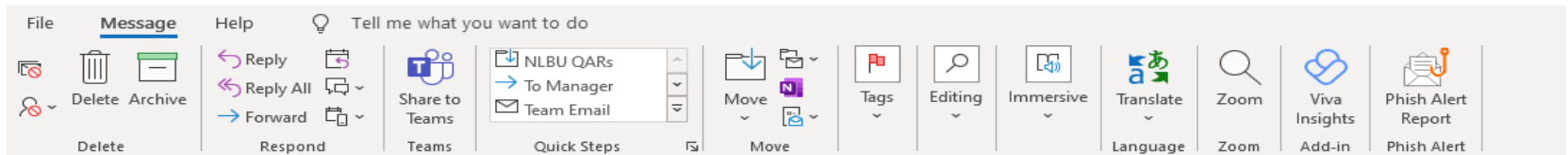
- Software updates lacking
- Inadequate network monitoring
- Inadequate Server protection
- Inadequate/dated hardware

- Updated end-of-life hardware/software
- Nightly backup strategy enhanced:
  - 1<sup>st</sup> back-up stored locally
  - 2<sup>nd</sup> back-up stored at offsite data center
  - 3<sup>rd</sup> back-up at undisclosed location (air gapped)
- Sophos Antivirus installed
- 3<sup>rd</sup> Party regular patching
- Upgraded to Microsoft 365







- Centro partnered with Involta (company) and Alertlogic (software) to monitor network:
  - 24/7/365 Monitoring
  - Local Network Operation Center
  - 400+ Agents available
  - System consistently scans the network
- Bi-Weekly meetings with the Security Center



- Caution with external e-mails:



## Cyber Security Panel

 Anna Evans <anna@webbandevans.com>  
To  Spence, Alvin;  Patrick Long;  Adam Covington  
Cc  Adam Webb  
 You replied to this message on 3/9/2023 1:27 PM.

 Reply  Reply All  Forward  

Thu 3/9/2023 11:21 AM

**[Think BEFORE you click! This email was generated from outside of the Centro Inc. organization.]**

Hello all,

Thank you again for volunteering to share about your cyber security experience at the Executive Forum. Our plan is for each of you to speak for approx. 5 minutes about your companies' challenges and successes. Then we will open up for discussion. We have this session scheduled on Tuesday, March 20 from 10am-10:30am local time. If you have any questions or concerns, please let me know.

Thank you,  
Anna

- Controlled testing (phishing)

- Training:

KnowBe4 Security Tips - Social Engineering Study Guide



Security Hints & Tips <SecurityTips@KnowBe4.com>  
To ● Spence, Alvin

 Reply  Reply All  Forward  

Fri 3/3/2023 10:43 AM

## SECURITY HINTS & TIPS:

### Social Engineering Study Guide

Social engineering is when someone tries to manipulate you into performing an action or sharing confidential information. Unfortunately, cybercriminals use social engineering to access computer systems, gather information, or make money. Most successful social engineering attacks are caused by human error. If you familiarize yourself with common social engineering methods, you may be able to recognize and stay safe from an attempted social engineering attack. In this study guide, you can learn about social engineering and ways you can protect yourself from social engineering attacks.

#### Social Engineering Tricks

Cybercriminals can use several different methods to trick you with a social engineering attack. Let's go over three common social engineering methods that you may encounter and examples of each method:

- Foster a culture of feedback & empowerment