Lessons Learned From a Cyber Attack

Sharon Blount-Baker – Crawford Co., AR

Carrie Kilgore, Crawford Co., AR

Brandon Krause - Bay Co., MI

March 24, 2022

3 Most Common Types of Cyber Attacks

- Ransomware - A type of Malware that uses malicious software designed to block access to a computer system until a sum of money is paid.
- Malware - Is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants.
- Phishing - The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Ransomware In Crawford County, AR

- What Happened?
  - How it affected County wide Services.
  - How it affected the County Recorder's Office.
  - How it affected the Public.
- Data loss or Compromised Data.
  - Backup Systems
- Getting the County services restored to 100%.

Protective Measures

- **Protective Measures:**
  - LRMS is on a separate server.
  - Encrypted e-mail on the county server.
  - Backup Hardware (Laptops, VPN's, Hot Spots).
  - Cloud back-up.
    - Daily
    - Annually

Corrective Measures

- **Corrective Measures:**
  - Purchased enough iPads for entire staff.
  - All Recorder employee's drives were moved to the LRMS server.
  - Retrain LRMS staff, IT staff and other vendors to updated system procedures.

Phishing In Bay County, MI

- What Happened?
  - Microsoft Exchange Vulnerabilities
    - Old e-mail platform, Microsoft Outlook 2010
  - Phishing attack
    - Phishing training.....Is it enough?

The First 24 Hours

- The steps the County IT Department took:
  - Shut down e-mail server
  - Contacted the county's risk management company, Michigan Municipal Risk Management Authority (MMRMA) https://mmrma.org/
  - Shut down Network
  - Disconnected all Hardware from the network

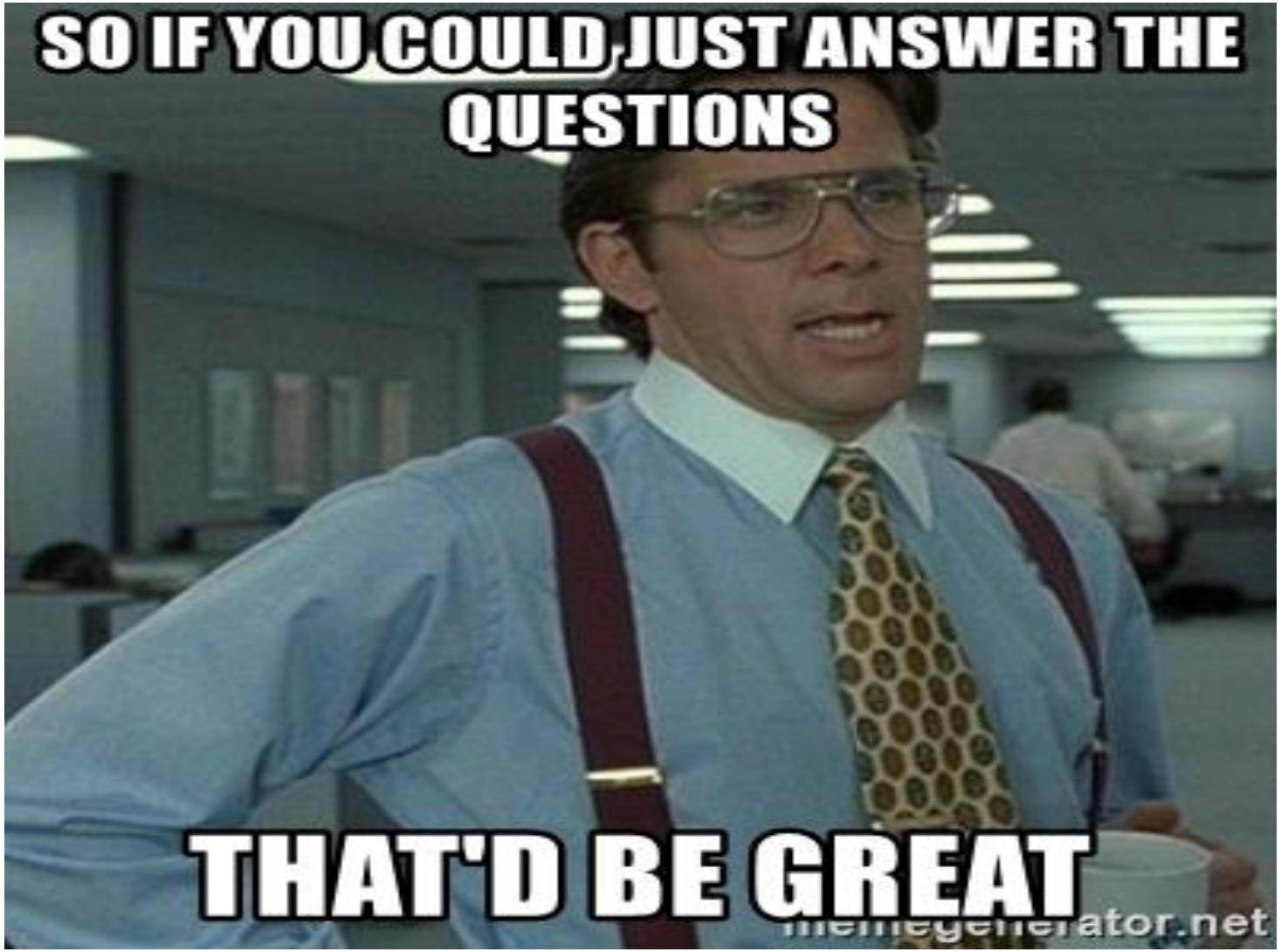
Chaos In The Office

- What to expect after a Cyber Security Attack:
  - Loss of Server access.
  - Loss of email capabilities.
    - Loss of contacts and all saved emails.
    - Cannot contact any outside Vendors, Constituents or Clients.
  - Loss of Network access.
  - Loss of network telephone system.
  - No access to all hardware and software.
    - Software and hardware restoration but no IT, network, or server support for several days.
    - Recording comes to a halt.

Corrective Measures

- Installed Carbon Black Software system
  - Continuously scans all servers and hardware
  - Eliminates the threats from adware, malware and phishing
  - Endpoint Threat detection
    - Endpoint detection and response, also known as endpoint threat detection, is a cybersecurity technology that continually monitors an "endpoint" to mitigate malicious cyber threats.

Questions/Comments



Contact Info

Sharon Blount–Baker

Sblountbaker@crawfordcircuitcourt.org

Office: 1-479-474-1821

Carrie Kilgore

Cjkilgore@crawfordcircuitcourt.org

Office: 1-479-474-1821

Brandon Krause, CPM

Krauseb@baycounty.net

Office: 1-989-895-4228