JACKSON COUNTY TEXAS

• Between Houston and Corpus Christi on the Texas Coast
• Population 14,000+
• Three incorporated cities
• Contract with third party IT provider
CHAIN OF EVENTS

• May 28, 2019
• Dispatcher has trouble logging into computer
• Computers are encrypted with RYUK Ransomware
• Servers disconnected from network
CHAIN OF EVENTS

- Poison pill initiated to back-up when administrator logs in
- Within minutes back-up appears to be destroyed
- All systems are shut down
- Hackers demanded $362k in bitcoins
CHAIN OF EVENTS

- May 29, 2019
  - FBI arrives for forensic memory dump
  - Agent’s device wiped clean when inserted into server
  - Buffalo Back-up Server sent to California for recovery but was not successful
- May 31, 2019
  - Jackson County Declares a State of Disaster
- June 3, 2019
  - STAR Request submitted for Texas Military Department Cyber Incident Response Support
CHAIN OF EVENTS

• June 5, 2019
  • STAR request approved, members identified for TMD Cyber Incident Response Team

• June 7, 2019
  • Site Visit by TMD and DIR
  • Forensics sent to MS-ISAC for additional support

• June 9, 2019
  • Final Memorandum Of Understanding signed by Jackson County and TMD
PHASE I JOINT CYBER RESPONSE TEAM

• June 10, 2019
  • Joint Cyber Response Team Phase I arrives in Jackson County
  • 8 Member Team from TMD
• Line of Effort 1
  • Secure restoration of critical services (interim)
    • WatchGuard – Sheriff patrol car video
    • NetData – Financial application for court system
    • Tyler – Land and Title Application for County Clerk
PHASE I JOINT CYBER RESPONSE TEAM

• Line of Effort 2
  • Triage Forensics, Cyber-Attack Point of Origin determination, and Network Mapping
    • Dispatch computer compromised through phishing email
    • Signs of Trickbot and Emotet
PHASE I JOINT CYBER RESPONSE TEAM

  - Improved Infrastructure
  - Improved Back-Up System with Air Gap
  - Centralized Managed Environment
  - User and Network Management Policies
JOINT CYBER RESPONSE TEAM

- June 14, 2019
  - TMD departed with LOE 1 & 2 complete
  - Operating at around 50% and inefficient
  - Revisited MOU with Texas Military Department and contracted for additional support

- June 24, 2019 - Joint Cyber Response Team Phase II
  - 8 Member Team from TMD
  - Goal to complete LOE 3 from Phase I
PHASE II JOINT CYBER RESPONSE TEAM

• LOE 1: Design and Establish the Long-Term Network Architecture
  • New centralized network and domain established
    • Moved from a flat network with abundant local admin rights
    • Developed a segmented network with only IT providers having admin rights
    • Firewall configuration competed and setup infrastructure for 3rd party vendor for basic intrusion detection and monitoring
PHASE II JOINT CYBER RESPONSE TEAM

• LOE 2: Re-Establish and Enable Services and Servers
  • Combined and repurposed multiple servers for more efficient use of county resources
    • County Clerk/Finance Records Management Server
      • Web-based services
    • Sheriff’s Office Records moved from interim to permanent server
PHASE II JOINT CYBER RESPONSE TEAM

• LOE 3: Image and Develop Baselines for User (Host) Systems
  • Back-up of any system not encrypted
  • Reimaged 70% of systems
  • Set up the other 30% on new devices
  • Updated all units to Windows 10
  • Final placement of all systems on the new domain
• LOE 4: Recommendations for Policies, Procedures and IT Processes
  • Draft of Acceptable Use Policy and other key policies provided to county leadership
  • Network map
  • System rebuild process
  • Future backup plan
FINAL OUTCOME

- TMD & IT provider completed six months of work in 15 days
- Since May 28, 2019 – Over 2000 work hours between TMD and IT contractors
- Cleaned and reimaged 85 old machines and purchased 31 new machines
- Moved from a flat network to a network with offices segmented
- Users are in their own organizational units and each unit has their own group policies
FINAL OUTCOME

• New Firewall with Threat Detection features
• Restored back-up from August 2018 & Sheriff’s Office from March 2019
• Additional back-up with airgap
  • Exploring other options, but limitations in rural Texas present challenges
• Continued cloud based application service for records management
FINAL OUTCOME CONTINUED

- Improved email filter through communications provider to scan for malicious emails
- New computer usage policies with much tighter security measures
  - Complex password policy
  - Automatic lock-out after non use
  - No installation or removal of software by employees
  - Use of outside devices (usbs, cds, etc.) by permission only
  - Cyber Security Training
• Developing a Cyber Incident Response Plan
• Member of MS-ISAC
• Proceeding with DIR/Secretary of State Security Assessment
• Proceeding with Department of Homeland Security CSIS Security Assessment
LESSONS LEARNED FOR SMALL ENTITIES

• Cyber attacks can be a disaster - ask for help
• Be responsive
  • Be forward thinking
  • Be prepared to share information about your system and office needs
  • Be prepared to make decisions regarding the response and recovery
  • Be prepared to find the resources that will be needed to recover and rebuild

• Collaborate with partners to be more PROACTIVE
  • Prevention, Preparedness, and Response