Jackson County Cyber Disaster 2019

JILL SKLAR

JACKSON COUNTY JUDGE

Jackson County, Texas

Between Houston and Corpus Christi on the Texas Coast

Population 14,000+

Three incorporated cities

Largest employers

- Local Government/School System
- Agriculture
- Industry

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 Texas Military Department

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

Line of Effort 3: Recommendations for Comprehensive Network Architecture, Network Defense Plan, and Updated Policies and Procedures

- Improved Infrastructure
- Improved Firewall
- 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

Phase II Joint Cyber Response Team

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

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

Final Outcome Continued

Developing a Cyber Incident Response Plan

Member of MS-ISAC

Completed 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!