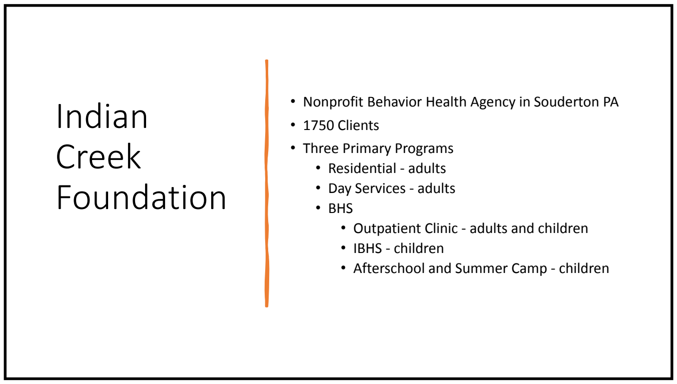
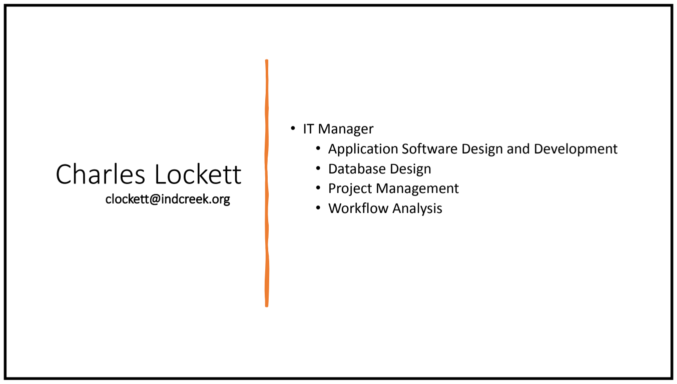
Indian Creek Foundation

Ransomware Attack



Indian Creek Foundation

- Nonprofit Behavior Health Agency in Souderton PA
- 1750 Clients
- Three Primary Programs
  - Residential - adults
  - Day Services - adults
  - BHS
    - Outpatient Clinic - adults and children
    - IBHS - children
    - Afterschool and Summer Camp - children



Charles Lockett

clockett@indcreek.org

- IT Manager
  - Application Software Design and Development
  - Database Design
  - Project Management
  - Workflow Analysis

Infrastructure and Application Landscape

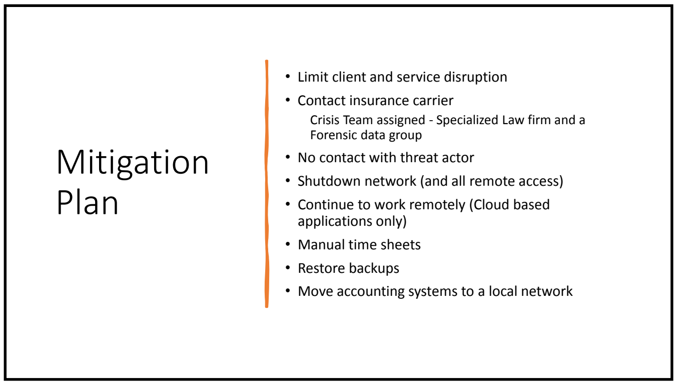
- 300 Users
- 5 Internal Servers, 150 desktop PCs, 30 laptops
- 8 Highspeed Printer/copier/scanners
- Facility Security – cameras, door access
- Time and Attendance system – Self Hosted
- GL and AP Accounting systems – Self Hosted
- Residential Staff Scheduling system – Self Hosted
- EHR system – Cloud Based
- Microsoft Office 365 – Cloud Based
- Payroll - Cloud Based

The Attack

- Discovered February 6th by IT Support Staff
- Appeared to be a network failure
- Unable to sign on to the primary network console
- Unable to sign on to any PC attached to the network
- Ransomware message, with instructions, was displayed on an alternate network console
- Was later learned that the hackers gained access through a dated remote access utility and spent 6 hours roaming through the network

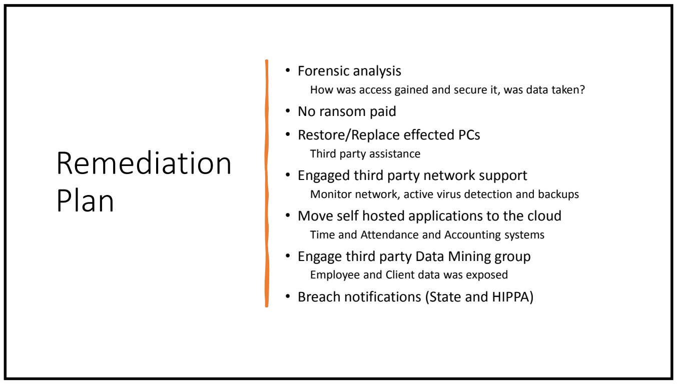
The Damage

- All files on the network servers were encrypted
- All files on the network connected PCs were encrypted
- All file extensions were changed to “LOCKBIT”
- Time and Attendance system was disabled
- Accounting systems were disabled
- User PCs were disabled
- Shared drives were not accessible
- Printers/copiers were disabled
- Time clocks were disabled
- Building security systems were disabled



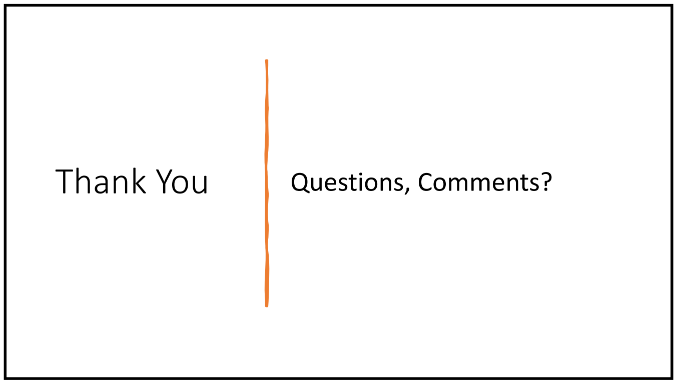
Mitigation Plan

- Limit client and service disruption
- Contact insurance carrier
  - Crisis Team assigned - Specialized Law firm and a Forensic data group
- No contact with threat actor
- Shutdown network (and all remote access)
- Continue to work remotely (Cloud based applications only)
- Manual time sheets
- Restore backups
- Move accounting systems to a local network



Remediation Plan

- Forensic analysis
  - How was access gained and secure it, was data taken?
- No ransom paid
- Restore/Replace effected PCs
  - Third party assistance
- Engaged third party network support
  - Monitor network, active virus detection and backups
- Move self hosted applications to the cloud
  - Time and Attendance and Accounting systems
- Engage third party Data Mining group
  - Employee and Client data was exposed
- Breach notifications (State and HIPPA)



Thank You

Questions, Comments?