2018 Cyber Security Incident

Matanuska Susitna Borough

July-September 2018

July 23, 2018

- Emergency Management staff computer starts acting up
  - Laptop with computer docking station
- DES Director computer starts acting up
  - Desktop CPU
  - IT responds to assess
  - Computers are backed up and exchanged
- All other computers are functioning as normal

July 24, 2018

- Computers are offline
  - No internet
  - No emails
  - Institute liberal leave policy

July 26, 2018

- First Public Information disseminated
- The Mat-Su Borough has been the victim of a multi-pronged, multi-vector cybersecurity incident resulting from a series of viruses, malware, and ransomware used by third-party hackers to disable our systems. Because of the nature of the attack, the Mat-Su Borough has had to entirely rebuild its systems. We have had teams of borough employees and outside IT specialists working overtime to bring systems back online in the most secure way possible and to restore borough operations. This is a time consuming process, but the Mat-Su Borough has worked as quickly as possible to restore services and investigate this incident.

July 31, 2018

- Disaster Declaration
  - "... the Borough's computer infrastructure, including computers/laptops, most Borough servers, networked telephones, and the email exchange have been compromised; and
  - WHEREAS, the cyber-attack has caused major disruption in Borough services and loss of productivity, which may continue for a prolonged time; and
  - WHEREAS, the Borough's IT department staff are working a great deal of overtime, and IT service providers have been engaged at significant expense, and, ...".

Assembly Briefing

- …and so the group that we are facing that has unleashed this particular attack is a very well organized group and they're using the most sophisticated tools and have done a lot of damage across the country to include us." Our victim number is 210 for this virus, Wyatt said, meaning that 209 others are victims before us. In Alaska, so far Valdez also has the virus.
- **'Lying dormant'-** That elaborate setup gave the cyberattack a long lead time, and that the malware was "lying dormant" on a borough server since as early as May 3. It wasn't until July 17, after IT installed the latest update of its McAfee anti-virus software, that it started detecting activity from the Trojan component.
- **On July 23, the IT staff developed a script to remove the bits McAfee missed, but it now appears that triggered the worst part of the cyberattack: "This action, of attacking back, seemed to trigger the virus to launch the Crypto Locker component…"**

Assembly Briefing, cont.

- “The incident response has been incredible. The FBI commented several times during design sessions with me how rapid and how efficient you guys have been in containing and dealing with the effort. I think your IT teams have done a wonderful job. Everybody's very exhausted. I'm mumbling because I'm beyond exhaustion for the last six days. I think everybody needs a pat on the back and some encouragement and this is going to be a long journey to recover. ... This is cyber crime and this is the future that we are dealing with.“- MSB Contractor

Public Information, z. Hollander

- The borough is still recovering from the "insidious" attack that clobbered phones, email and online systems and decommissioned some 650 desktop and server computers, officials there said Monday. Many of the disabled computers and multiple outlying offices remained offline.
- Employees dragged out typewriters. Departments working without computers shifted to pen and paper.

Response

- The Borough first disconnected servers from each other, then disconnected the Borough itself from the Internet, phones, and email, as it recognized it was under cyber attack. Since then, infrastructure is steadily being rebuilt, computers cleaned and returned, and email, phones, and Internet connection becoming restored.
- The "zero-day" attack, which means the anti-virus software makers do not yet have the definitions of the virus in their software to catch and remove the threat. The Borough gave them theirs so they can write new protections from this virus. The Borough awaits the new software.

What it affected…

- This new threat doesn't stop at your primary systems. It gets in to corrupt your back up servers and disaster recovery systems. Primary international venders such as Dell and Cisco have not seen this before, until now.
- “It’s a new world,”.
- Some 20 different agencies and vendors, including former employees, have supported the Borough’s response, offering brainpower and resources to untangle the forensics of the attack. The FBI cyber crimes unit has been working with the Borough since last week on gathering such evidence.

Emergency Management thoughts…

- Emergency Management is ALL HAZARDS
  - Should be involved early and at the forefront
- COOP Planning to include cyber systems being down
  - Vital Staff/Leave Policy
  - Paychecks
    - Taxes
    - Medicare
    - Grants/Reports
    - Ability to take credit card payments
- Rebuilding Systems-how to function in the meantime…
- Public Information
  - Reporters
  - You Tube channels with contractors detailing response
  - International Interest
  - Letting the public know how impressed the FBI is of the response-Active Investigation
  - Long press releases or bullet points for services
    - https://www.matsugov.us/news/msb-cybersecurity-incident-august-28-update

Emergency Management thoughts…cont.

- IMT Response
  - EOC vs ISM
  - IT folks become the Operations Section
  - How do you run your operation with out computers?
  - Do you need to be a computer expert to lead the response?
  - Interacting with IT contractors-protocols, finances, etc…
  - Policy Changes
    - Local, State, Tribal and Federal
- When rebuilding the IT system
  - Work arounds
  - Tighter security-hardware, software, personnel
  - Expectation Management
- Mitigation for future events
  - Stockpile off the system
  - Off server emails
    - Records Retention
    - Legal Requirements
  - EM Software off the system or cloud based
  - Prepping and updating information schedule

Questions???

- What is your communications plan for a breach and the incident response that follows?
- How much of your incident response are you willing to share? How much is your boss willing to share?
  - What about to vendors, clients, patients?
  - Long term affects
    - Financial
    - Programmatic
    - Public Trust
- Do you pay the ransom?
- Does your cyber insurance cover data losses? Do you have cyber insurance? What is the deductible?
- Does the State consider this a disaster? Does FEMA?
  - Why or why not?