Cybersecurity: Recovery After a Ransomware Attack

Bill James, MHA, COE
Talley Eye Institute
Evansville, Indiana

Financial Disclosures:
* None

First Things First:
Huge thank you to Jeff Brockette and Michael Sullivan
April 2019

What happened:

- Our practice was hacked with Gandcrab V5.2 ransomware by Russian hackers
  - All servers and several workstations were involved
  - All affected files were encrypted with the extension .WNMYGNJIV
  - EHR, Email, and other files affected; all backups failed
- Each affected folder had a .txt file, describing what needed to be done to recover our data

April 2019

What we did, Day 1:

- Contacted our health law attorney
- Contacted the FBI
  - Their recommendation was that we not pay the hackers, but
  - They understood if we made the decision to pay the ransom
- Searched for companies who have experience with decryption of files
- Determined that we felt more comfortable paying a reputable company that could decrypt instead of paying the hackers
April 2019
What we did, Day 1:
 Continued to see patients through this mess
   Our retina staff pulled previous injections through the medication inventory system
   Our anterior segment physicians are referral-based, and most patients were new patients
 Follow up patients and post-ops:
   Utilized prior OCTs, Optos images, visual fields, and other diagnostic testing for historical data
   Contacted the ASCs to get op reports for post-op patients

April 2019
What we did, Day 2:
 Informed staff of what has happened and what we were doing to recover data
 Informed staff to tell the patients (for now) that our servers had crashed
 Begin decryption process of data
   All servers
     Which affected PCs needed to be decrypted vs. wiped and rebuilt

Two Weeks Later...
Terabytes of Data Finally Encrypted
 Day-to-day operations back to "normal"
   Entered data from paper charts into the EHR into the system
 Determine if PHI had been compromised
   Difficult to determine
   Companies can do a "deep dive" of your data to determine:
     How information was exfiltrated
     If PHI had been exposed
Six Weeks Later – What We Learned

- An old account that was no longer used had been compromised
- A brute force attack was launched on this account to gain access
- Malware was uploaded to our RDP server
  - 16 executables were launched in a span of 20 minutes
- The executables allowed hacking of the Administrator account
- Ransomware installed on devices, but
- PHI had not been compromised

Six Weeks Later – Disclosure

- Report information to:
  - HHS
  - State Attorneys General (in our case, Indiana, Illinois, and Kentucky)
  - Media
  - Referring Doctors
  - Patients
  - Send a Letter Detailing Events of the Attack
    - What information was involved
    - Steps Patients could take to protect themselves
    - Contact information for the practice if they have questions

Six Weeks Later – Disclosure

- HHS and AG reports
  - Work with your attorney to provide this information, which should include:
    - HIPAA policies and procedures
    - Password management policies
    - Notice of Privacy Practices
    - Previous Risk Assessments and Penetration Test Reports
    - How your practice has responded to the results of these
    - A description of the incident
    - What security steps have been taken since the attack
Expenses Incurred

- Our IT company acknowledged a portion of the blame for the backup failure
  - Did not charge us for their work
- Payment for data recovery: $167,000
  - This included stronger antivirus protection from the recovery company
  - Also included email protection tools
- "Deep Dive" to confirm no exfiltration of data: $20,000
- Legal fees: $35,000
- All covered and repaid through our cybersecurity insurance policy

New Policy and Procedure Changes

- Backups done every hour
  - Loaded to a local appliance and moved offsite
  - Backup data is tested and encrypted
  - Air-gapped (no connection between the backup and our network)
- Continue to obtain appropriate penetration tests, vulnerability tests, and risk assessments
  - Discuss the results of these in board meetings
  - Document the observations and recommendations in the board meeting minutes
  - Designate these items as fixed, working on, or known and acceptable risks

- All staff undergo annual HIPAA training, cybersecurity awareness testing
  - Use phishing emails to see if staff are paying attention
  - Discuss cybersecurity regularly in staff meetings
  - Document this in the staff meeting minutes
- Check all accounts (Windows, EHR, SonicWall, etc.) to ensure all former employees are deactivated
  - Ensure password complexity and enforce changing at least every 90 days
New Policy and Procedure Changes

- Use multifactor authentication whenever possible
- Administrator password restricted
  - IT company and CIO have this password
  - Minimum 25 characters (ex., gaFDz5Myx7mvEHWHBSYDF)
  - Changed regularly
- Make sure that your cybersecurity insurance policy is up to date
- Include cybersecurity in your disaster recovery plan and incident response plan
- Cybersecurity policy coverage is $1MM

Ongoing expenses

- Annual vulnerability testing, penetration testing, etc. for MACRA and MIPS compliance: $18,000
- Cybersecurity insurance premium: $17,000
- Estimated IT support for cybersecurity: $13,000
  - Includes offsite backup management, cybersecurity awareness training, etc.

Four Years Later...

- The HHS / OCR can contact your practice or your attorney
  
  My name is [redacted], and I'm an investigator with the U.S. Department of Health and Human Services / OCR, Office for Civil Rights [redacted] the message is regarding OCR's investigation into [redacted], which has recently requested for me to follow up and discuss this matter with you further. Please let me know your availability for a small call at your earliest convenience. Thank you.

- The OCR wants to know if:
  - You have continued your risk assessments, penetration tests, etc.
  - You have continued to respond to these accordingly
  - You have continued to provide training to staff all appropriate training
Four Years Later...

- Document, document, document
- More information is better
- Demonstrate ongoing efforts to keep your systems and data secure

Finally, a happy ending

- The OCR determined that we were maintaining compliance
  - Recommended ongoing monitoring and updating
  - No further action needed
  - The OCR may check in periodically

Questions?

Bill James
812.437.7620
bjames@talleyeyeinstitute.com