NORTHERN NEVADA HOPES *your partner in health.*

Surviving and learning from a ransomware event.

Northern Nevada HOPES

- HOPES is a FQHC located in Northern Nevada
- Over 200 employees
- 10,000+ patients annually
- Patent Center Medical Home recognized by the National Council for Quality Assurance
- URAC Pharmacy recognition

Ransomware:

- Ransomware is a malware designed to **deny a user or organization access to files on their computer**. By encrypting these files and demanding a ransom payment for the decryption key, the attacker place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files.

Cyber Liability Insurance

- In the event of a ransomware attack, Cyber liability insurance carriers may be utilized to pay the ransom.
- The insurance also pays for lost revenue during a cyber attack.
- Included services consist of, Cyber forensic teams, System administration support, Cyber liability attorney, software license reimbursement(Lost licenses/ re-establishing connection or activation)

Before the “IT apocalypse…..”

- Daily backups would be performed to both on site and off site Servers.
- Cold storage backups were performed weekly to allow for an offline solution.
- All data is encrypted both at rest and while in transit.
- IT day to day was to repair and improve existing systems.

Question #1

- If your organization was unable to perform business for 24 hours, what would be the total loss in revenue?

- The U.S. was the target of 46 percent of cyberattacks in 2020, more than double any other country.

Microsoft 10-25-21

https://www.microsoft.com/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/

The Attack

- The intrusion happened in the early hours of the morning two weeks before Christmas.
- The attacker deployed the ransomware through a modified GPO allowing them to deploy it to all computers on the network.
- The group then performed a backup of the file system.

The day of….

The EMR application was not loading for all employees.

Staff are unable to receive emails.

Phone calls from staff at 7 am stating they are unable to access the system.

The IT director had scheduled PTO for two week starting the next day, The system administrator had a scheduled surgery later in the afternoon with two weeks of recovery scheduled.

System Impact

- Electronic Medical Record System
- IP phone system
- Backup systems
- Desktops and Laptops
- System Servers
- Pharmacy RX system

- The average downtime a company experiences after a ransomware attack is 22 days.

Statista

https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/#:~:text=Length%20of%20impact%20after%20a%20ransomware%20attack%20Q1%202020%2D%20Q3%202021&text=As%20of%20the%20third%20quarter,United%20States%20was%2022%20days. 2021

What happened next

System admin logged in to discover a ransomware note on the Domain controller.

Phone calls from staff regarding ransom notes on their laptops and desktops.

All systems slowly went offline.

All of the backups were deleted or encrypted.

Emergency Preparedness

- CEO was immediately notified of the issue.
- IT gathered to discuss how to best recover from the situation
- Department and Executive Directors notified of incident and asked to have all work from home staff to bring their assets into the workplace.

Question #2

- How many organizations in your area have been impacted by ransomware in the last 18 months?

The Plan

- All servers, laptops and desktops were assumed to be compromised which would require completely rebuilding.
- Identified the priority of systems to restore in order to resume business.
- Began notifying patients of the outage closing operations until further notice.
- Contact our Cyber liability insurance company to discuss our options.

Migrating the Domain

- Domain controllers control all domain access, blocking unauthorized access to domain networks while allowing users access to all authorized directory services.
- The organization scheduled to change over the domain slowly to avoid downtime and outages.
- With all systems and computers requiring a rebuild it was an opportune time to migrate the domain during this outage.
- By migrating the domain during the ransomware we were able to begin building a Hybrid architecture to allow redundancy and failover in the event of a local outage.

Cold Storage and Air Gap

- **Cold Data** storage is the storage of inactive data that is rarely used and must be retained for business or compliance purposes on a long-term basis.
- An **Air Gap** is a security countermeasure that is based on the idea of creating an impenetrable barrier between a digital asset and malicious actors

Air Gap Cold Storage….

- Cold Storage had all patient records and data systems stored in a full encrypted backup snapshot.
- The SQL services remained unencrypted on the infected machines due to separate permissions. The SQL service hosted all patient records and progress notes for all clients.
- The snapshot of the data system was two weeks old which kept most of our data and systems in tact within two weeks of the instance.

- Out of 1,086 organizations whose data had been encrypted, 96 percent got their data back.

Sophos

https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf 2021

Executing the Plan

- Assembly lines were produced to begin mass rollout of laptops and desktops for re-imaging and migrating to the new domain.
- IT staff worked around the clock rebuilding all systems and servers adding them to the domain.
- The cold storage backups were deployed to recover the impacted data.
- Cyber liability firm was utilized to do a forensic analysis of the event while also contracting a system administrator to help re-establish critical systems that were impacted.

Question #3

- Does your organization currently have cyber liability insurance?

Detection and Review

- The forensic team identified the user account compromised and responsible for the attack.
- The account was compromised through a targeted spear phishing campaign.
- All systems accessed by the attackers were encrypted and the data was unavailable to them for export

- Ransomware attacks were responsible for almost 50 percent of all healthcare data breaches in 2020.

Heath and Human Services

https://www.hhs.gov/sites/default/files/2021-hph-cybersecurity-forecast.pdf 2020

Reporting responsibility in an attack

- No patient information was compromised during the attack.
- All data potentially impacted during the event was determined to be non-critical and properly protected from any external threats
- The organization did not have to disclose the event since all records and information was protected from the threat actors.

- 95 percent of cybersecurity breaches are caused by human error.

World Economic Forum Dec-17-2020

https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education

How to react to ransomware

- 1. Isolate the Affected Systems
- 2. Report the attack
- 3. Shut down "Patient Zero"
- 4. Secure your Backups
- 5. Disable all Maintenance Tasks
- 6. Backup the Infected Systems
- 7. Identify the Strain
- 8. Decide Whether to Pay the Ransom

https://www.lepide.com/blog/how-to-react-to-ransomware-attack-in-8-steps/

Question #4

- Is your organization prepared to recover from a ransomware attack?
- Would you have to pay the ransom, and if so could you?

Prevention:

- All backup systems should not share admin privileges or domain access with the main network.
- User education is everyone's responsibility, All users should attend annual security training to reinforce best practices.
- Managed Detection and Response (MDR) services put a security team on your network monitoring unusual network and user activity. These teams specialize in locking down potential threats before they are able to deploy any specialized attacks.

Looking Back

- In total the time it took to come back online took two weeks.
- 6 months of follow up and review to identify and review both the incident and impact.
- A forensic analysis of the incident took a month.
- 8 months to receive reimbursement from the cyber liability firm.

Questions?

THANK YOU

NORTHERN NEVADA HOPES *your partner in health.*

580 W 5TH ST, RENO, NV 89503 | 775.786.4673 | NNHOPES.ORG