Salud Family Health

AFTERMATH OF A SECURITY BREACH

THE UNANTICIPATED JOURNEY

2023 Best Practices Forum

LABOR DAY WEEKEND 2022

While John was fishing…

The threat actors were also phishing…

LABOR DAY WEEKEND 2022

- On Monday Sept. 5th, Salud's 3rd party vendor CrowdStrike notified Salud that something was wrong
  - Irregularities were detected in our system; we had been breached
- John was immediately notified, and remained completely calm

LABOR DAY WEEKEND 2022

- John started contacting our Executive Team
  - Initially, Salud's CMO Dr. Pradeep Dhar thought John was joking…
- Quickly reverted back to Incident Command structure that we used during the early pandemic
- Salud's IT Department was all hands-on deck
- Contacted our cyber insurance company

THE EARLY RESPONSE

- Salud Incident Command Team met early the next day at 7:00AM
- During this meeting, the threat actors (Lorenzo Gang) started emailing our staff stating that Salud had been breached
  - The email said that Salud needed to pay ransom if we didn’t want information to be posted on the dark web
  - They spammed these emails, using Salud email accounts that had access to all-employee email group

THE DARK WEB

WHAT ARE YOU DOING ON THE DARK WEB??
I FORGOT MY PASSWORD, SO I'M LOOKING IT UP.
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

- Dark Web definition = the part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable
  - ➢ Represents about 5% of total content on the web

SHUTTING IT ALL DOWN

- Decided to lock down Microsoft Outlook
- Learned the Microsoft Teams was also compromised and locked it down
- Turned off access to electronic health records
- Just to let us know that they were in our entire system, they starting continuously printing at all clinics and printers needed to be shut down

ASSEMBLING THE TEAM

- Completed putting the response team together
  - Salud Incident Command Team
  - Salud IT department
  - Forensic IT team
  - PR Firm
  - Salud Lawyers
  - Law firm that specializes in clients experiencing cyber attacks

INITIAL PRIORITIES

- Initial priorities for the team
  - Step 1= Figure out how they got in
  - Step 2 = Figure out how we get them out
  - Step 3 = Figure out how we keep them out moving forward
  - Step 4 = Determine what information they accessed

FORENSIC IT PROCESS

- Salud's IT Department had to work closely with the forensic IT team in order to provide them appropriate access and the information they needed
- The entire Salud Incident Command Team met with the forensic IT team twice daily so that we were always up to date with the progress of restoring systems

HOW THEY GOT INTO OUR SYSTEM

- It was determined that the threat actors got into our system through an open admin account on an unused phone server
- Upon investigation, it was learned that our brand of phone system is commonly targeted as it has known security vulnerabilities
- Once in the system, they gained lateral access as many of the admin passwords were the same throughout the system

HOW WE GOT THEM OUT OF OUR SYSTEM

- Salud’s IT team, in cooperation with our partners, began segregating the infected servers
- Immediately removed the unused phone server that was the entry point
- All malware was deleted
- All servers were rebuilt from scratch
- Quickly improved the firewall configurations
- As a precaution, Salud reset over one thousand credentials and logins to try and prevent the threat actors from accessing equipment

Administrator

The password is incorrect. Try again.

BRINGING THE SYSTEM BACK ONLINE

- After rebuilding the servers and getting clearance from the 3rd party forensic IT team, the servers were individually cleared to bring back online
  - ➢ It took1.5 weeks to bring our electronic health record back online
  - ➢ It took 3 weeks to bring our phones and Contact Center back online
- This delay in access to our computer systems obviously had a dramatic impact on clinical services

IMPACT ON CLINICAL SERVICES

- Medical
  - ➢ Could not access the electronic health record, referrals, labs, or diagnostic images
  - ➢ Could not use the phone system for telehealth visits or calling patients
  - ➢ Could provide only an extremely limited scope of services for patients if they showed up at the clinic
    - o Continued high priority care such as OB care
  - ➢ Communicated with local hospitals that our system was down, and we could not transmit Salud patient information to them

IMPACT ON CLINICAL SERVICES

- Medical continued
  - Created a text message group chat to communicate with site Medical Directors
  - Immediately sent Luma (not impacted by breach) text messages to patients stating that their appointments were cancelled
    - Also used Luma to send updates to the personal cell phones of Salud employees
  - After a few days, developed a paper documentation process to start seeing patients again
    - Patients were asked to bring their medication bottles with them to appointments so we could recreate the medication list
    - All telehealth visits were converted to in clinic visits since the phones still weren’t working

IMPACT ON CLINICAL SERVICES

- Dental
  - Could not access medical record, dental record, or dental radiographs
  - Dental is procedure based and without radiographs, dental is very limited in what they can do
  - Dental provided denture adjustments, fluoride treatments, hygiene, etc.

BEHAVIORAL HEALTH

- Behavioral Health
  - Visits were cancelled for the first few days until the paper documentation process was implemented
  - No telehealth could be done until the phones and Contact Center were back up
  - Behavioral Health providers came into clinics to see patients

PHARMACY

- Pharmacy
  - Pharmacy's server was not compromised
  - Severely impacted by not being able to receive phone calls
  - Fewer patients being seen in the clinic resulted in less scripts being written

MOST DEVASTATING IMPACT OF BREACH

- Ultimately, the most devastating impact of the breach was clearly that our live Salud Executive Team fantasy football draft at Buffalo Wild Wings had to be cancelled the day after the breach
  - Our fantasy football season never recovered from the computer selecting our teams for us this year….

THE TEAM CAME TOGETHER TO HELP

- Since our computer systems were down, all remote employees were brought into the clinics and administrative building to help with other tasks
  - For many staff members, this was the first time they had seen each other in person since before the pandemic
- Facilities Department recruited staff to help paint clinics where needed
- Some staff were yoga trainers, and they provided sessions for staff wellness
- Performed maintenance on equipment
- Performed a deep clean of our buildings
- Staff had a positive attitude and wanted to help

FORENSIC IT WORK

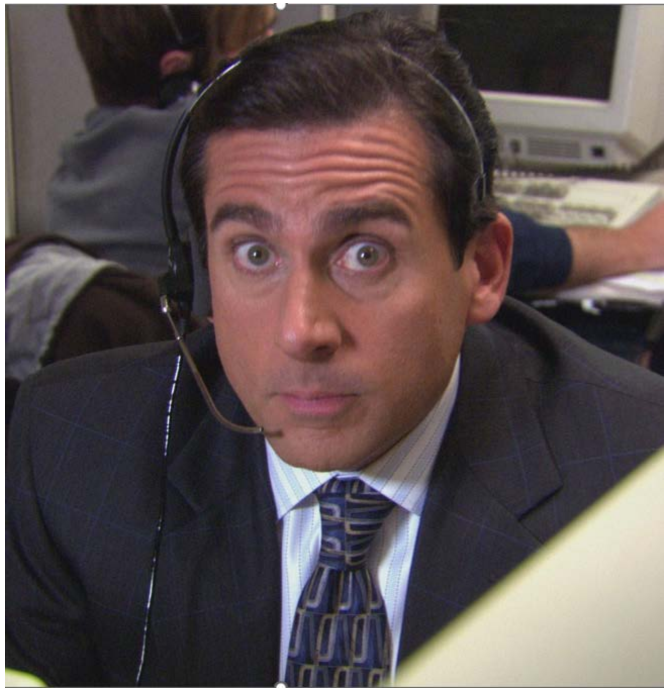
- The forensic IT team got to work to learn what information was accessed
  - Discovered that the threat actors accessed the personal drives of multiple employees as well as the shared drive for all Salud employees
  - Learned that they weren't able to access our electronic health record (which is internally hosted), accounting system, payroll, human resources, credentialing software, website, or social media accounts
  - Also discovered that they tried to encrypt our data, but weren't able to do so as CrowdStrike prevented this from happening

FORENSIC IT WORK

- Confirmed that they were able to download Personal Health Information
  - They downloaded over 200 gigabytes of data
- Discussed at length whether we could be certain which files were accessed
  - Did we want to open every file to identify every person with exposed PHI?
- After weeks of discussion, we determined that it wasn't feasible to scrub the data to that level

NOTIFICATIONS ABOUT THE BREACH

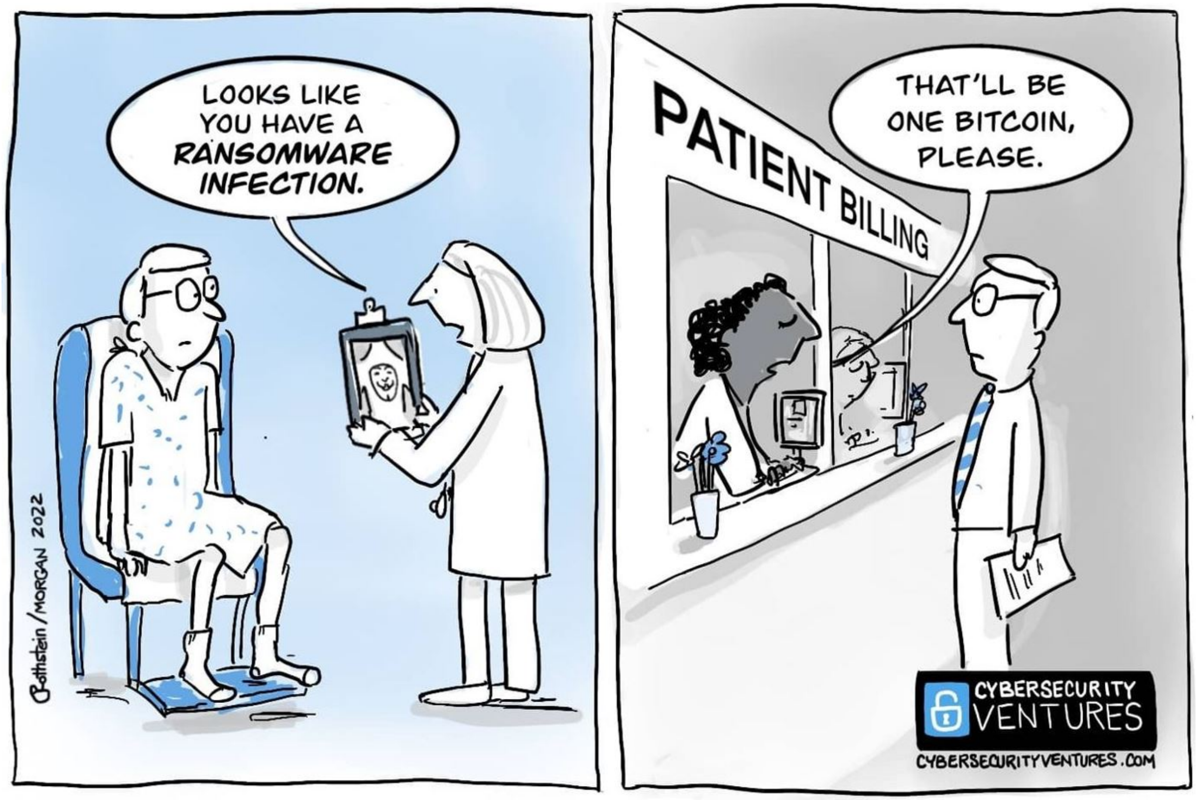
- Since we couldn't scrub down to the level each affected person with certainty, we decided to notify every patient that was in our eCW database
  - This was over 400,000 patients
- Salud offered one year of credit monitoring
  - Our lawyers recommended this as a best practice
- Salud hired a company to run a call center to answer patient and employee questions
- Posted notice about the breach on our website and in newspapers
  - We had to demonstrate that we covered our service area



NOTIFYING OUTSIDE ENTITIES

- We also notified outside entities:
  - HRSA
  - Colorado state attorneys
  - Other State Attorney offices
  - Regional Accountable Entities
  - Colorado Medicaid Office
  - HHS
  - Internet Crime Complaint Center
  - CMS Security and Privacy Incident Report

NEGOTIATING WITH THE THREAT ACTORS

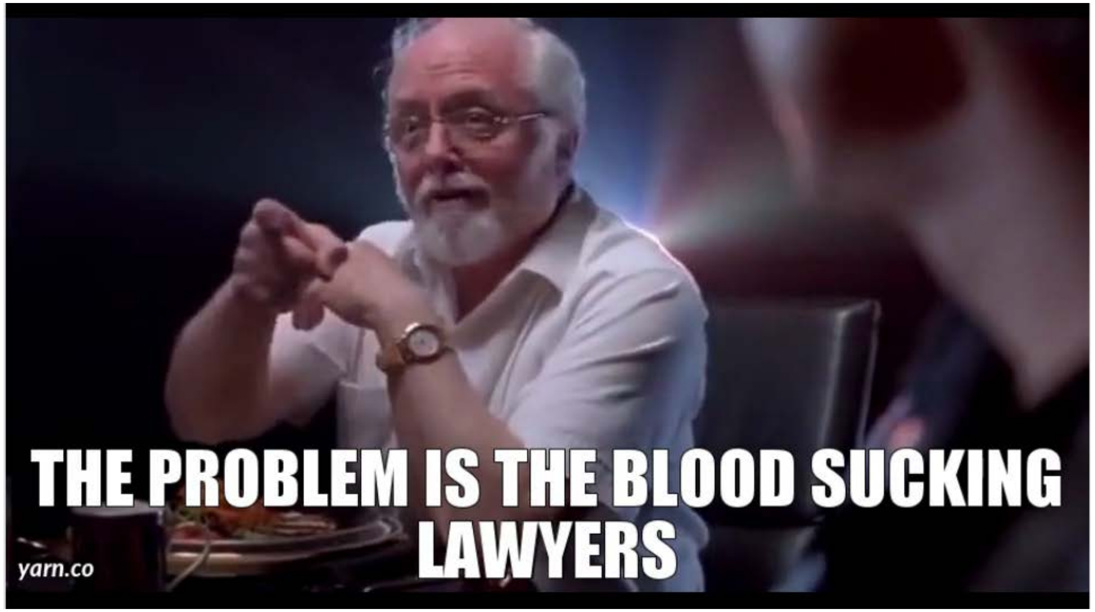

LOOKS LIKE YOU HAVE A RANSOMWARE INFECTION.
THAT'LL BE ONE BITCOIN, PLEASE.
PATIENT BILLING
Rothstein/MORGAN 2022
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

- There was a ransom demand in order to prevent the information on the dark web
- Salud's 3rd party law firm did the negotiating
- Threat actors try to keep their reputation of doing what they say they will
- Salud decided not to pay the ransom since there was no guarantee that they wouldn't publish on the dark web even if we paid

NEGOTIATING WITH THE THREAT ACTORS

- The threat actors did publish the information on the dark web and were upset that we did not pay
- We know they are still trying to get into our systems because we didn't pay them
  - They will be back!
  - They actually caused phone disruptions to our system about 2 months after the initial breach

BLOOD SUCKING LAWYERS



- After the information was published on the dark web, our 3rd party lawyers who specialize in data breaches wanted Salud to cross check the posted files to see if we missed notifying any impacted patients
  - The lawyers of course wanted to charge for this service and earn more money
  - However, Salud had already notified all past/present patients and staff

CLASS ACTION LAWSUIT

- Following this breach, Salud has been served with Class Action Lawsuits
  - ➢More lawyers seem to get involved
  - ➢This process is still ongoing

MOVING FORWARD

- This IT breach brought our entire organization to a halt
- It was devastating for our capacity to provide important health services to our patients
- It was like a tornado, and we had to pick up the pieces afterwards
- We must do everything we can to prevent this from happening again in the future!

MOVING FORWARD

- Steps we have taken to improve our security since the breach
  - We are evaluating our entire phone system's security
  - Hired multiple companies to evaluate our IT security
  - Plan to purge our EHR of charts that are over 10 years old
  - Evaluating whether we move more servers to the cloud rather than host internally
  - Managing our user ID and passwords more efficiently
  - Implementing industry best practices for onboarding and offboarding of user IDs
  - Updating Admin passwords so they are different, making it more difficult to travel within the system

LESSONS LEARNED

- Everyone needs to have cyber insurance
  - Salud was fortunate to have a good cyber insurance policy when this breach occurred
  - Two months prior to this breach, Salud had increased our cyber policy to 3 million dollars
    - Prior to this increase, Salud had only a minimal tack-on to our general insurance policy
  - It is likely that Salud will have a more difficult time getting cyber insurance in the future
  - Health Centers should evaluate whether their electronic health records allow them to purge old patient charts
    - Salud's EHR currently does not have a process to accomplish this, but they are aware of the need and they are working on it
- Make sure that obsolete equipment and software are no longer connected to the network

QUESTIONS

THANK YOU!

John Santistevan
President and CEO
Salud Family Health, CO
JSantistevan@saludclinic.org

Pradeep Dhar
Chief Medical Officer
Salud Family Health, CO
PDhar@saludclinic.org

Salud Family Health