

The information provided here is for informational and educational purposes and current as of the date of publication. The information is not a substitute for legal advice and does not necessarily reflect the opinion or policy position of the Municipal Association of South Carolina. Consult your attorney for advice concerning specific situations.



Cybersecurity in  
Today's Healthcare:  
A Review From  
Newberry Health

Presented by:  
Corey J. Bishop, RN, BSN, AEMT, CHEP-II

---

---


---

---

---

---

---



Disclosure Statement

- I, Corey Bishop, am employed by Newberry Health. I have no financial or contractual conflicts of interests with any entity discussed in this presentation.

---

---


---

---

---

---

---



Why Does This Matter?

- In 2021, 686 2021 healthcare data breaches, 44,993,618 healthcare records have been exposed or stolen. That increased to 707 in 2022 and 725 in 2023. The number of records exposed in 2023: 115,705,443.  
(HIPAA Journal: Largest Healthcare Data Breaches of 2021 (hipaajournal.com))
- The average cost to a facility for a breach is 10.1 million dollars. (Healthcare is the costliest section of the market)
- The most common entry method is phishing scams. (Up to 91%)
- The average downtime for a facility in 2021 was 7 days. In 2022, 16 days, in 2023, 18.7 days and for 2024, 27.8 days.

---

---

---

---

---

---

---



Cyber Fast Facts

- There were 2,365 cyberattacks in 2023, with 343,338,964 victims.<sup>1</sup>
- 2023 saw a 72% increase in data breaches since 2021, which held the previous all-time record.<sup>4</sup>
- Ninety-four percent of organizations have reported email security incidents.<sup>4</sup>
- Business email compromises accounted for over \$2.9 billion in losses in 2023.<sup>2</sup>
- [Cybersecurity Stats: Facts And Figures You Should Know – Forbes Advisor](#)

---

---

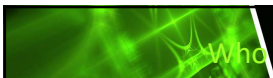
---

---

---

---

---



Who Are You People Anyways?

- Some of the most prominent threat actors include:
- RansomHub
- Black Cat
- Dark Angels
- LockBit
- Qilin Ransomware

---

---

---

---

---

---

---

**CO Hospital Suffers Email Data Breach, 52K Impacted**  
[CO Hospital Suffers Email Data Breach, 52K Impacted \(healthitsecurity.com\)](#)

**Healthcare Cyber Attacks – 276 Million Patient Records were Compromised In 2024**  
[Healthcare Cyber Attacks - 276 Million Patient Records were Compromised In 2024](#)

**Emergency services a likely target for cyberattacks, warns DHS**  
[Emergency services a likely target for cyberattacks, warns DHS - ABC News](#)

---

---

---

---

---

---

---

• **Ransomware attack affects 3.3 million patients in California**

-Becker's Health IT

Updated: Feb. 10<sup>th</sup>, 2023

- "...breach included names, SSN, diagnoses, treatments, lab results, and prescriptions."

• **Devicemakers look to secure their products amid wave of attacks**

-Becker's Health IT

Updated: Feb. 13<sup>th</sup>, 2023

- "A survey of 500 healthcare executives...found 56% experienced a cyberattack targeting an internet-connected device over the past 24 months."

---

---

---

---

---

---

---

Let's Drop Some Knowledge...

- Ryuk accounted for 3 of the 10 largest ransom payouts in 2020. (\$5.3 mil, \$9.9 mil, \$12.2mil) They accounted for 1/3<sup>rd</sup> of all ransomware attacks that year.
- Ryuk, meaning "Gift from God" in Japanese, is downloaded remotely as DaaS (Download as a Service) and can be used as a RaaS (Ransomware as a Service). Began it's use through the group WIZARD SPIDER.

How do they get their money?

---

---

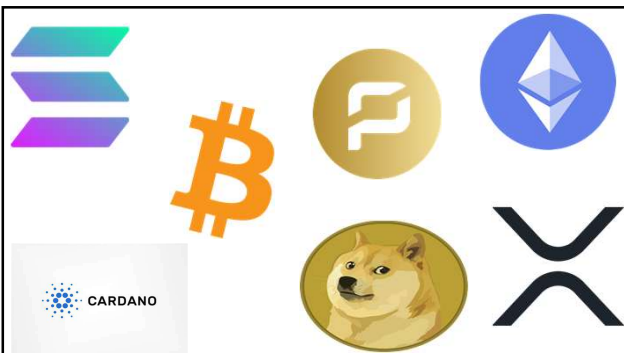
---

---

---

---

---




---

---

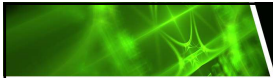
---

---

---

---

---



More Facts...

- Ryuk is generally thought to be run out of Russia by a threat actor group.

**“A year of bitter and bloody war in Ukraine has devastated the country, further isolated Russia from the West and fueled economic insecurity around the world.”**

[Russia-Ukraine War - The New York Times \(nytimes.com\)](#) March 21<sup>st</sup>, 2023

---

---

---

---

---


---

---

---

**UnitedHealth Pays Ransom After Cyberattack on Change Healthcare, Confirms Patient Data Breach**

MSN.com Updated 4/25/2024



Change Healthcare, specializing in payment and revenue cycle management tools, processes over **15 billion transactions** yearly, with one in every three patient records flowing through its systems.

---

---

---

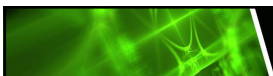
---

---

---

---

---



Change Healthcare

- Details about the Change Healthcare attack:
  - ALPHV (Black Cat)
  - 4TB of patient data
  - Entered through Citrix tool remotely using a username/password that was compromised. (No MFA in use during time of incident).
  - \$22,000,000 ransom. At first...

---

---

---

---

---

---

---

---



---

---


---

---

---

---

---



### It Won't Happen To Us...

- On February 21<sup>st</sup>, 2021@ 0200 , Newberry Hospital was hit with Ryuk ransomware.
- IT locked down all systems by 0315.
- 0900-All admin was notified and in house as well as EM and briefed on situation. (First time told possible ransom)
- 1205-All systems encrypted. AON, AIG, Stroz, FBI, and local police all aware and techs enroute from AON and Stroz.

---

---

---

---

---

---

---



---

---

---

---

---

---

---

## It Won't Happen To Us...

- Monday Feb 22<sup>nd</sup> Briefing:  
All computers, phones, EMR, and systems are down or compromised. This also includes ANYTHING tied to the network ie: payroll, billing, forms, credit card machines, tube systems, ALL radiology, scheduling, Medical Records, MAR's, HUGS system, and more.

---

---

---

---

---

---

---

## More Bad News...

- The facility was placed on TOTAL diversion. We are the only hospital in Newberry County. Next closest facility is 30 minutes away.
- EMS was bolstered due to imaging patients being taken to other facilities.

---

---

---

---

---

---

---

## I Didn't Think About That...

- -For insurance and reimbursement, ALL costs must be reported. This includes employee labor, fuel, contracted services, lost revenue, etc.

---

---

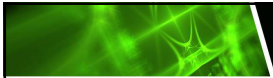
---

---

---

---

---



### Let's Think Positive

- Our EMR was restored on March 1<sup>st</sup>. All workstations were back up also. (8 ½ days)
- All systems had been backed up on Feb. 20<sup>th</sup> at 0600.
- Moved immediately to a cloud-based vendor for HR/payroll.

---

---

---

---

---

---

---

Remember the Good Ol' Days?



---

---

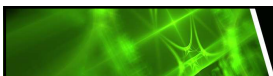
---

---

---

---

---



### Gotcha!!

- On March 3<sup>rd</sup>, through the efforts of SLED, our IT, and the FBI, we were finally able to determine the access was made through a 3<sup>rd</sup> party vendor access that still used **Windows 7** for their system.

---

---

---

---

---

---

---



## Finally!!!

- Thursday, March 18<sup>th</sup> at 1154.

Memo sent to providers and staff to lift diversion and resume normal operations!



---

---


---

---

---

---

---



## That's What Insurance Is For

- Our facility cyber premium increased 6x and our deductible increased over 10x!
- Also of note, when put out for bid, only one company even offered to insure us.

---

---


---

---

---

---

---



## What Did We Learn?

- Lots of lessons learned the hard way.
- We weren't as prepared as we thought but we were lucky.

---

---


---

---

---

---

---



### Lessons Learned

- Downtime forms...better check them! Are they current?
- Is your COOP ready? Have you drilled it/executed it?
- Where is Cyber on your HVA? What about Polycrisis?
- Can you restrict information leaks?
  - PIO will be your facility's best friend!

---

---


---

---

---

---

---



### Polycrisis

Wait...you mean there's more!?

At the same time we were dealing with this event, there was another little event going on called:

**COVID 19**

---

---


---

---

---

---

---



### Lessons Learned

- What is your facility doing to mitigate and educate staff?
- Redundant communication systems. Do you test them? Are they accurate? Are your key players trained on them regularly?

---

---


---

---

---

---

---



### Lessons Learned

- Network Security
  - Changed vendors, eliminated 3/4ths of our remote access use. Multi-factor authentication in ALL areas.
- Outside Partner Relationships
- Business Recovery

---

---


---

---

---

---

---



### Lessons Learned

- Vendor security reviews upon beginning business and then annually.
- Vastly increased server capacity both to the regular network and offline.

---

---


---

---

---

---

---



### Where Do We Go From Here?

Education and AI

**AI will be our best defense, and our worst enemy in the war against cyberterrorism.**

---

---

---

---

---

---

---

•We don't fear the monster we can't see.

• How do you request urgent support when no one outside your walls can SEE the emergency??

---

---

---

---

---

---

---

“Don't sweat the petty things, and don't pet the sweaty things.”

-My Brother Levi (Philosopher, kinda)

---

---

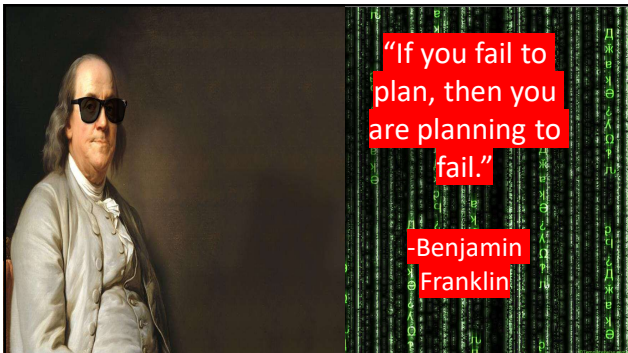
---

---

---

---

---



---

---

---

---

---

---

---



The Most Important Thing

- AT NO POINT WAS A SINGLE PATIENT'S CONFIDENTIAL INFORMATION COMPROMISED!!!

---

---

---

---

---

---

---



Thank you!!!!

Questions??

Corey J. Bishop  
Director of Surgery,  
Emergency Management  
Newberry Health  
(803) 405-7150 Office  
(803) 944-0827 Cell  
[Corey.bishop@newberryhospital.net](mailto:Corey.bishop@newberryhospital.net)

---

---

---

---

---

---

---