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

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

Disclosure Statement

- I, Corey Bishop, am employed by Newberry Hospital. 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.(HIPPA Journal; Largest Healthcare Data Breaches of 2021 (hipaajournal.com))
- The average cost to a facility for a breach is 9.23 million dollars.
- The most common entry method is phishing scams. (Up to 91%)
- The average downtime for a facility is 22 days.

CO Hospital Suffers Email Data Breach, 52K Impacted

CO Hospital Suffers Email Data Breach, 52K Impacted (healthitsecurity.com)

Michigan Medicine data breach may affect health information of nearly 3,000 patients

Updated: Mar. 03, 2022, 8:02 p.m.

Michigan Medicine data breach may affect health information of nearly 3,000 patients - mlive.com

AHA: Russia's Invasion of Ukraine Could Lead to Healthcare Cyberattacks

February 24, 2022

AHA: Russia's Invasion of Ukraine Could Lead to Healthcare Cyberattacks (healthitsecurity.com)

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

-Becker's Health IT

Updated: Feb. 10th, 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. 13th, 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)
- 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).

More Facts…

- Ryuk is generally thought to be run out of Russia by a threat actor group.
- In case you didn’t know…we aren’t exactly getting Christmas cards from Russia’s government right now…

ABC News Videos

Russia warns that a WWIII 'would involve nuclear weapons'

Sun, March 6, 2022, 5:15 AM

It Won’t Happen To Us…

- On February 21st, 2021@ 0200 , Newberry Hospital was hit with Ryuk ransomware.
- IT was onsite and 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.


I DON'T EVEN KNOW WHAT
HAPPENED...

It Won’t Happen To Us…

- Monday Feb 22nd 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.
- 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 1st. All workstations were back up also.
- All systems had been backed up on Feb. 20th at 0600.
- Moved immediately to a cloud-based vendor for HR/payroll.

Remember the Good Ol’ Days?

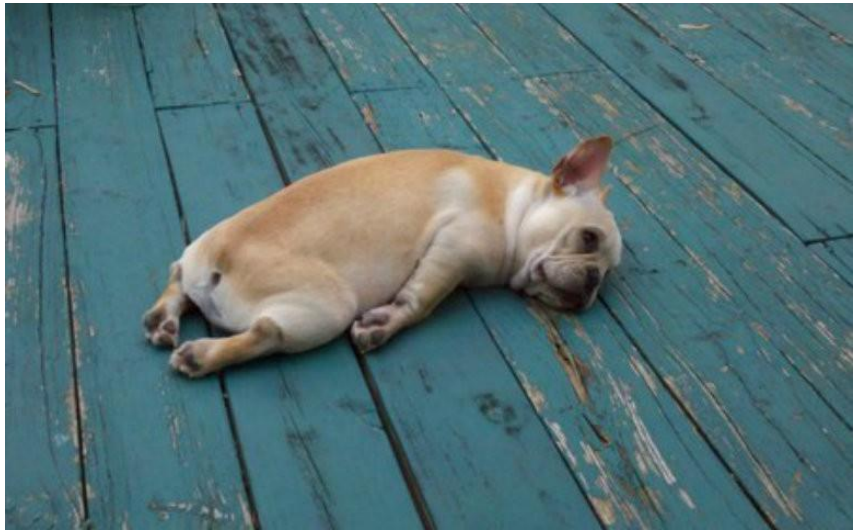
Gotcha!!

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

Finally!!!

- Thursday, March 18th 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?
- Can you restrict information leaks?
    - PIO will be your facility's best friend!

Lessons Learned

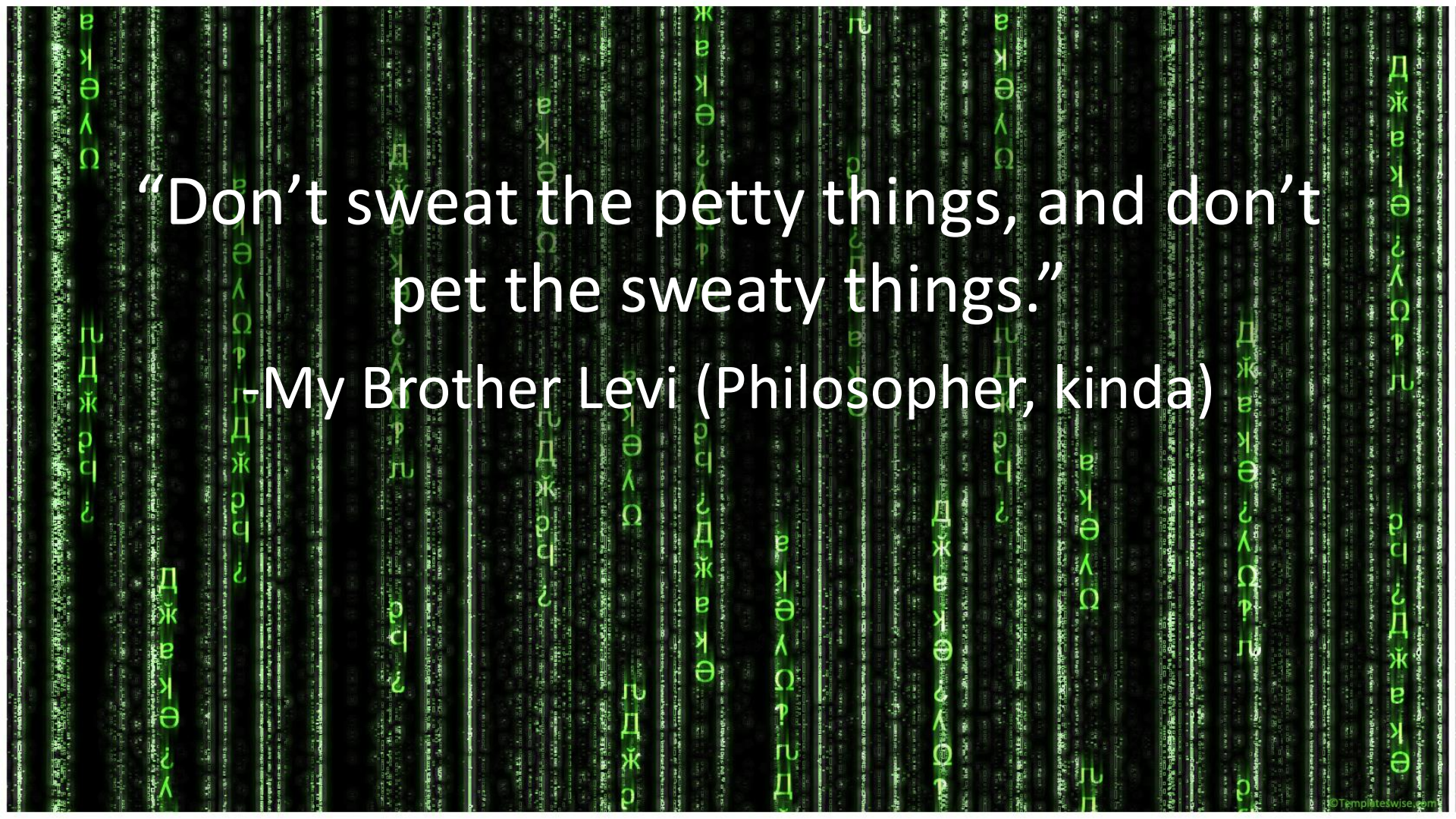
- What is your facility doing to mitigate and educate staff?
- Redundant communication systems. Do you test them? Are they accurate? Are your key players trained on them regularly?

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.


“Don’t sweat the petty things, and don’t pet the sweaty things.”
-My Brother Levi (Philosopher, kinda)

“If you fail to plan, then you are planning to fail.”

-Benjamin Franklin

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 Hospital
Corey.bishop@newberryhospital.net