Clearwater

Healthcare – Secure, Compliant, Resilient

Monthly Cyber Briefing

November 2023

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Cyber Briefings are eligible for HIMSS & CHIME CE credit
- Recording and final slides shared within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Clearwater

Agenda

- Cyber update
- Active Risk Response

Speakers

Steve Cagle, MBA, HCISSP
CEO, Clearwater

Ricoh Danielson
CEO, 1stResponder

David Bailey, EMBA, CISSP
VP, Consulting Services, Security

Brian McManamon, MBA
GM, Managed Security Services / President, Redspin Division

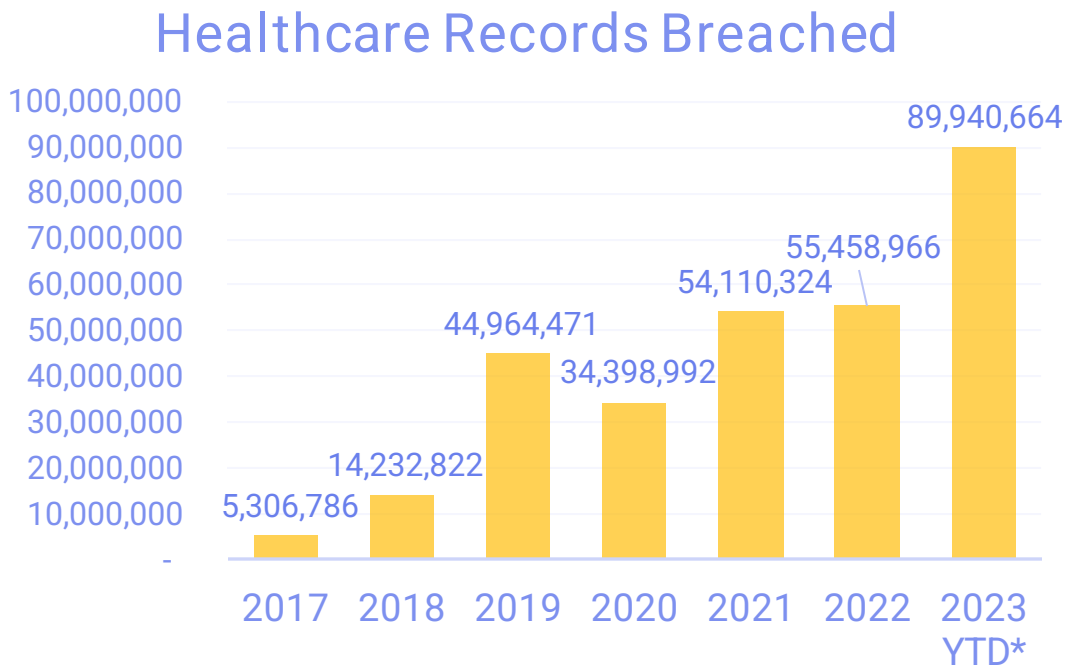
Clearwater

Cyber Update

Steve Cagle

Healthcare Breaches Increasing in Total Due to Size

- 98.7M records reported breached over the last 12 months ending October 2023[1]
- 555 YTD breaches of ~90M records is 62% increase over entire year 2022



Source: HHS Breach Portal

- Since October briefing 4M more records added to September breach figures since October Cyber Briefing (total is now 7.3M)
- As of 10/28/23 only 726K records reported breached in October, however, there is typically a delay in posting to portal, and this figure will likely increase

Most Notable Breach

Arietis Health Notifies 54 Entities About Exposure of Patient Data

- Approximately 2M records from 5/31/23 CIOP / MoveIT ransomware attack
- Affected 54 entities of its customer NorthStar Anesthesia
- Notified NorthStar on 8/23/23 ~ 3 months after breach
- Notified OCR on 9/29/23, 4 months after the breach

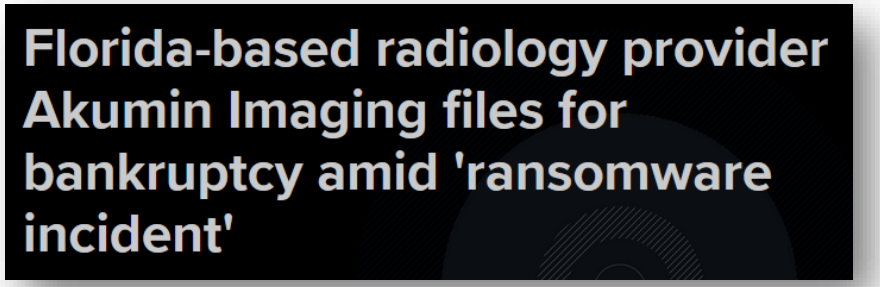
Clearwater

* Preliminary data available through 10/28/23

Notable Ransomware Attacks in Last Few Weeks

- Health Network of Hudson Valley – (HealthAlliance Hospital & Margaretville Hospital
- Became aware of incident 10/14
- 10/16 announced there was an issue
- 10/19 diverted medical patients and moved inpatients to other facilities
- 10/20 shut down all systems for 24 hours
- Hospitals receiving diversions were "overwhelmed" by additional volume
- Backlash from local residents

- 5 Ontario area hospitals affected by cyberattack
- First detected 10/23/23
- As of 10/25/23 still operating under "code grey" and not restored
- IT Service provider, Transform was attacked, affecting all 5 hospitals
- Slow to recover back-ups



- Publicly traded Akumin provides radiology services in 48 states
- Shut down systems on 10/11
- As of October 24th still not able to provide most services
- Filed for Bankruptcy on 10/22, canceling $470m in debt
- Will be taken over by debt holders

https://hudsonvalleyone.com/2023/10/17/hahvs-kingston-hospital-diverts-patients-for-two-days-without-an-announcement/
https://www.dailyfreeman.com/2023/10/19/healthalliance-hospical-in-kingston-transferring-patients-after-confirming-cyberattack-system-expected-to-shut-down-through-weekend/
https://www.firstcoastnews.com/article/news/local/akumin-imaging-files-for-bankruptcy-ransomware-incident/77-4b8966ce-e67c-4bcc-be64-d7a35e7baef4
https://radiologybusiness.com/topics/health-it/enterprise-imaging/imaging-informatics/radiology-provider-akumin-postpones-most-clinical-and-diagnostic-operations-amid-ransomware-attack
https://www.cbc.ca/news/canada/windsor/cyber-attack-wednesday-update-1.7008355
https://yaledailynews.com/blog/2023/10/13/following-cyberattack-yale-new-haven-health-asks-for-state-aid-lowered-price-to-aquire-connecticut-hospitals/

Clearwater

Financial Cost of Ransomware

Since 2016 ransomware attacks have **cost healthcare providers $77B.**

-Comparitech Report Oct 23

54% of all healthcare organizations experienced ransomware attacks in past 2 years.

-Ponemon / Proofpoint

- 539 ransomware attacks on healthcare since 2016[1]
  - Average ransomware demand was $2m
  - Down time usually weeks, but recovery takes months
- 66 disruptive ransomware attacks in 2023 on hospital systems – does not include vendors / BAs

- Business disruption is the largest cost in a ransomware attack with $1.3M average in healthcare (+30% from 2022)
- Time taken to ensure patient care was corrected averaged $1M (+51% from 2022)
- Loss of productivity averages $1.1M

Also consider:

- The cost of long-term reputational damage
- Legal fees
- Management and executive opportunity costs/time.

Clearwater

[1]*https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/*

Organizations Publicly Reporting Costs From CyberAttack

- CommonSpirit, October 2022 = a reported loss of **$160 million**
- Scripps Health, May 2021 = a reported loss of **$112.7 million**
- Harvard Pilgrim Health Care (Point32Health), March 2023 = a reported loss of **$102.7 million**
- Universal Health Services, September 2020 = a reported loss **of $67 million**
- Bio-Rad Laboratories, Inc., December 2019 = a reported loss of **$20 million**
- SmileDirectClub, April 2021 = a reported loss of **$15 million**
- Erie County Medical Center, April 2017 = a reported loss of **$10 million**

https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

Threats to Mitigate in the Current Environment

- Business email compromise is increasing and becoming more convincing and elaborate
- Credential stealing has become more sophisticated, using vishing, shmishing and social engineering tactics that evade traditional security
- Zero-day vulnerabilities are being announced frequently
- Threat actors are specifically targeting the weak points – smaller organization, financially weak organizations, and vendors/third parties that have fewer regulations (or less likely to follow standards)
- Insider threats are still an important concern and large source of breaches
- Cloud compromises are becoming more frequent, more impactful, and security is specialized and can be difficult to manage
- The **speed of a ransomware attack is now less than one day** vs average 4.5 days last year, leaving less time to detect and respond once a threat actor is in your environment

Additional Recommendations Based on Current Threat Environment

- Identify where all your ePHI is and ensure that you have thoroughly assessed individual risk scenarios and differences in controls that may exist between different applications or components based on their unique profiles
- Engage C-Suite and Board with current threat information and provide executive level overview of key risks based on your organization's specific situation
- Perform a risk assessment of your cloud environments, and get assistance as needed with remediating and optimizing security controls.
- Consider risk with your MSP or IT Services provider.
  - Determine whether you have too much concentration risk
  - Perform a detailed risk assessment, and perform technical testing of the environment
  - Use a dedicated, expert managed security services provider for Monitoring, Detection and Response
- Develop and test incident response plans, including involving stakeholders at the executive level

New Threat Resource – HSCCC

New guide on Incident response planning and exercising is available from Healthcare Sector Cybersecurity Coordinating Center. Highlights are the sections on key elements of an IR plan, lifecycle, preparation, planning, testing, detection, strategies, and creating effective IR Teams.

- National Institute of Standards and Technology (NIST)
- NIST Incident Response Framework
- NIST Special Publication 800-61
- What Is an Incident Response Plan?
- The Incident Response Lifecycle
- Incident Response Teams
- Scenario Walkthrough
- Why You Should have an IR

https://www.hhs.gov/sites/default/files/cybersecurity-incident-response-plans.pdf

Clearwater

Active Incident Response Lessons

Ricoh Danielson, 1st Responder
Brian McManamon, Clearwater
Dave Bailey, Clearwater

Active Incident Response Case Study

- Organization: 2nd Largest Medical Provider in a Large Midwest Region

Situation

- Hit with Ransomware
- Network downed and spun back up in 84 hours.
- Secret Service and L.E. Engagement

Important Elements to Consider

- Timing is everything
- Your response is your responsibility
- What you do or don't, will echo in the history of Cyber Security- Good or bad, your choice.

Forward Action

- Apply the three Fs "Find it, Fix and Forward with it"
- Apply the 6P's
- Know when to make the critical business decisions
- Always forward

1STRESPONDER
CYBERSECURITY & DIGITAL FORENSICS

The Contributing Factors

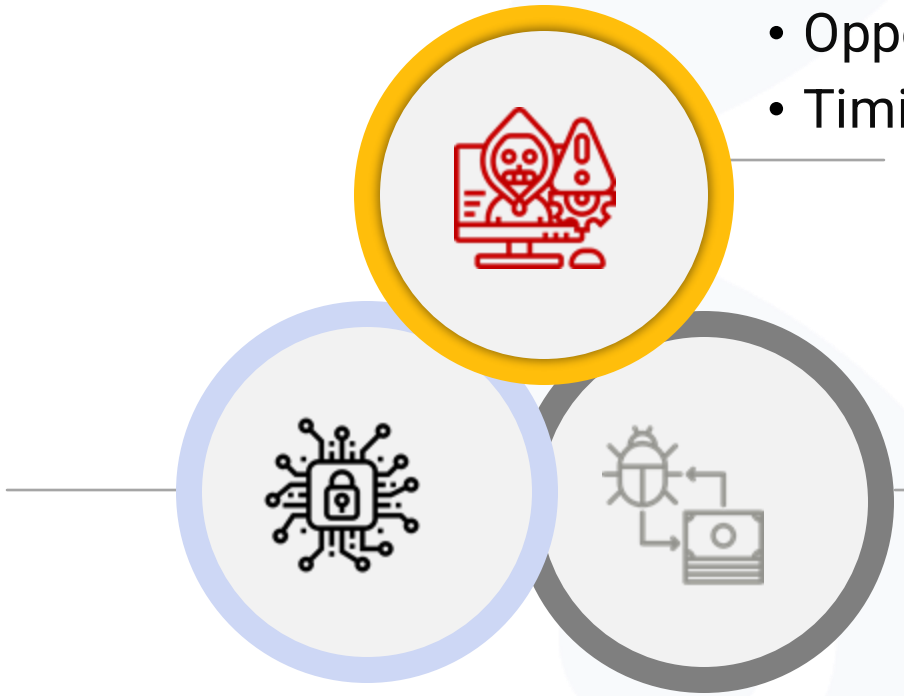
What were the contributing factors that lead to the attack?

Threat Actor Activity

- Reconning
- Opportunity
- Timing

Business Budget Control

- Budget was allocated to IT and not Cyber Security.
- Proper positioning of personnel, time, money and resources



Exposure

- Out of cycle patching
- Watch the watchers/ Watching paint dry
- Relying too much on an MSP that didn't react
- Unmanaged areas and gaps

1STRESPONDER
CYBERSECURITY & DIGITAL FORENSICS

The Threat Actor

- BianLian Ransomware Gang
- Target Healthcare, Medical and Clinics
- Leverages Living off the Land TTPs and custom malware written in Golang

1STRESPONDER
CYBERSECURITY & DIGITAL FORENSICS

Main Data Points and Key Players

Consider these…

01

Respond

Speedy response. “Eyes ups, eye on and engage the threat”
Key players: MSP, MSSP, Legal, IR firm, SOC and the village

02

Active Defence

Ensure you have the correct tools, processes and resources to have an “Active Defense”

03

Preserve

Some attorney in attorney land in a far far way place is going to ask you, “why didn’t you do XYX”? Be able to go back

04

Report

It is okay to be selfish. Ask yourself, what is the best for you?

1STRESPONDER
CYBERSECURITY & DIGITAL FORENSICS

Timeline: Key dates, times and Events

Initial Cyber Attack

Bian Lian activity noticed by MDR

April 01

1st Responder Engagement

April 30th

Incident Command now Onsite

Voluntarily Downed Network

April 30th

Out of an abundance of precaution of client Downed Network

Triage and Deployment of agents

April 30th

- Identified 236 infected devices
- No Encryption found
- Ransomware letter found

Rebuild of environment

May 1st

Client rebuilds network from the ground up

IOC and TTP

May 2-5th

- Provided security measure to implement with IOCs and TTPS
- 64base PW Script found- Unable to decrypt

Recovery

May5th

Client has moved to re-establishing of network and partial business functions

Alert/Onion site

May 5th

Threat Actor posted unknown data set on Onion site.

More Recovery

May 6th

Cautiously evaluates bringing more business functions back online

Cont'd Dark Web and Threat Actor Monitoring

May 9th

1st Responder is activity monitoring for dark web

1STRESPONDER
CYBERSECURITY & DIGITAL FORENSICS

The Path Forward

What does your path forward look like?

- Readiness
  - Have an authentic conversation and determine if the organization is ready. If not, how can we get there.
- Invest
  - Invest into the organization cyber security: readiness, security program, business risk, and cyber education
- Be Your Own 1st Responder
  - Have a Plan
  - Be Ready
  - Know When to Ask for Assistance

Clearwater

1STRESPONDER
CYBERSECURITY & DIGITAL FORENSICS

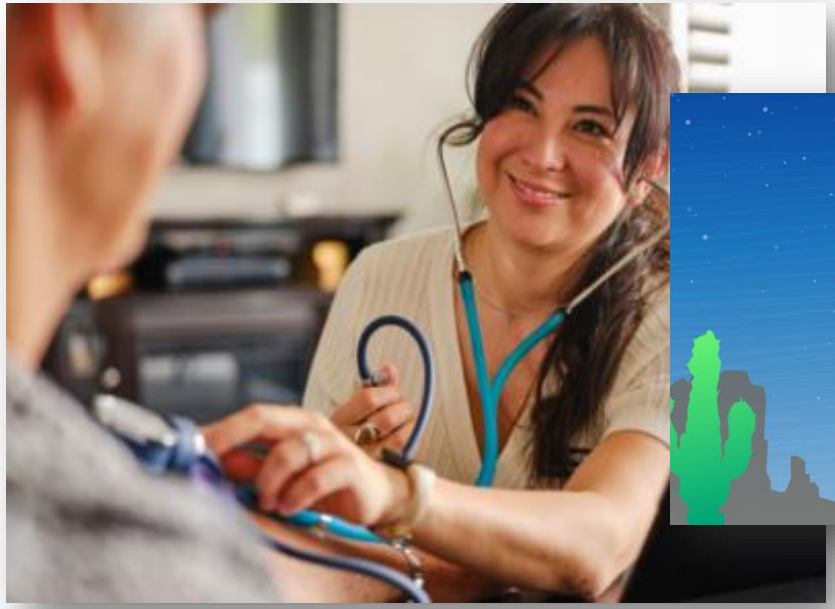
Q&A

Ricoh Danielson, 1st Responder
Brian McManamon, Clearwater
Dave Bailey, Clearwater

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Upcoming Events



Empowering Healthcare Defenders: Cybersecurity Tactics for Community & Regional Hospitals – CHIME webinar

November 29th

CHIME Fall Forum

November 9-12

Holland & Knight, Nashville Digital Health Forum

November 14th

Future Cyber Briefings

- December Cyber Briefing | 12/7
  - **Healthcare Threat Intelligence Deep Dive:**
    - Clearwater's December Cyber Briefing will feature an in-depth Threat Intelligence presentation focused on the latest threats and trends in the healthcare cybersecurity landscape.

- 2024: Cyber Briefing Series will continue!

Clearwater

Healthcare – Secure, Compliant, Resilient

Contact us

info@clearwatersecurity.com

www.clearwatersecurity.com

1.800.704.3394

1STRESPONDER
CYBERSECURITY & DIGITAL FORENSICS

ricohd@1stresponder.us

1stresponder.us

1-888-575-7895

Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.