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.

Monthly Cyber Briefing

January 2023

Moderator: Jenny Davis

An Industry Leader Focused on One Mission

Move organizations across the healthcare ecosystem to a more secure, compliant, and resilient state so they can successfully fulfill their missions.

How we help you become more secure, compliant, and resilient:

- Deep pool of experts across a broad range of cybersecurity, privacy, and compliance domains
- Proprietary, purpose-built technology enables efficient identification and management of cybersecurity and compliance risks
- Tech-enabled, 24x7x365 Security Operations Center with incident response capabilities
- Services and technologies can be integrated into valuable, cost-effective managed services
- All from a single, trusted partner

Healthcare's Top-Rated Security Advisors

Healthcare's Top-Rated Compliance & Risk Management Solution
Sixth Consecutive Year

Mac McMillan
Founder & Advisor
CynergisTek, a Clearwater Company

Dave Bailey
VP, Consulting Services
Clearwater

Chuck Podesta
CIO
Renown Health

Cyber Update

Mac McMillan

CYBER EVENTS IN DECEMBER – LAST MONTH/YEAR RECAP

San Gorgonio Memorial Hospital breach amplifies why Healthcare is such a **target rich** environment. The breach reported in Dec. involved patient names, addresses, DoB, medical record info, visit info, clinical info, provider names, service dept., SSN, drivers license numbers, bank accounts and health insurance info. Dec. 27 LCMHS reports ransomware attacks affecting 270,000 patients.

Social Blade that tracts users use of social media such as YouTube, Twitter, Facebook, Twitch, Instagram, DailyMotion and Mixer sites **reports breach after stolen data offered for sale** on Darkweb. What's for sale? Email addresses, password hashes, client IDs, IP Addresses, tokens for business API users, authentication tokens for connected accounts and non-personal and internal data. Still feel good about social media?

OKTA, Lastpass, Rackspace, Solarwinds, AccessPress, all tier 1 supply chain partners experience cyber attacks exposing customer data and critical internal information such as source code. Attacks on supply chain partners and ransomware attacks continued to be strong impactors in the cybersecurity story for Dec. and all of 2022. The increase in cryptocurrencies and the anonymity of payments continues to encourage attackers.

THREAT UPDATES – LOOKING AHEAD TO 2023

THREAT INSIGHT

The number of exploitable vulnerabilities has risen every three months consistently. Many vulnerabilities are **still being exploited** more than a year from discovery (Log4J). And attacks on **ubiquitous applications** like OKTA show how rapidly the attack surface can grow. **Leaked data** has become its own market place.

VULNERABILITIES

Hackers **continue to innovate** and create more dangerous exploits for vulnerabilities like Log4Shell, ProxyLogon, ZeroLogon, etc. demonstrating importance of addressing **legacy** issues. Organizations with more than 100 employees experience a **far greater percentage** of unpatched vulnerabilities.

HUMANS

More than 90% of cyber breaches are caused by **human error**. **Fatigue, apathy** towards proactive defense affects nearly half of organizations. Nearly 2/3 of companies see **daily phishing attempts**, and phishing leads to breach 40% of the breaches experienced. Lack of qualified staff, higher salaries, difficult recruitment plagues cyber workforce.

CHALLENGES

More regulation, social media, AI adoption, Quantum computing, cyber workforce shortage, more bots, more targeted ransomware, more evolving insurance requirements, Insider threats (Lap$us), 5G, APIs, Integration, active defenses, cloud, supply chain, deepfakes, ChatGPT, spyware for HR, 3,200 cyber vendors

CYBER RESILIENCE

OPERATING IN CHAOS EFFECTIVELY

- DEFINED AS: The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises of systems that use or are enabled by cyber resources.
- ACHIEVED BY: Planning, Training, Practicing, and Executing with or without direction.
- CHARACTERIZED BY: Swift action, independent decision making, decisive engagement, coordination efforts, precision, close teamwork.

IN CHAOS SWIFT ACTION ENHANCES OUR CHANCES OF SURVIVAL

"We're surrounded. They can't get away this time."
- LtGen. Chesty Puller, USMC at the Battle for Chosin Reservoir, Korea 1952

PLAN, TRAIN, PRACTICE, EXECUTE

- When ambushed, every Marine knows to turn in unison towards the fire, taking cover if possible and begin to return suppressive fire and moving toward the enemy.
- A Naval aircraft carrier with an average crew age of 19.5 years and both Marine and Naval aviators can launch an Alpha Strike, approximately 80 – 90 aircraft, in 30 minutes.
- Every Marine Commander knows that as the battle unfolds, they "will not" be in a position to tell their Marines what to do. They conceive and communicate the plan, their Marines have trained and practiced and know their role and responsibilities, and when the fighting starts "they" execute.
- **Cyber attackers are relentless and unpredictable, which means you never know exactly when or how they will strike, but you do know they will strike, so readiness is the only responsible answer.**

5 Best Practices to Increase Your Cyber Resiliency in 2023

Chuck Podesta & Dave Bailey

Presenters

Dave Bailey, CISSP

VP, Consulting Services

- Served as the Director of Technology & Security at Mary Washington Healthcare
- 12+ years of healthcare cybersecurity experience & 12+ years of experience serving in the Air Force

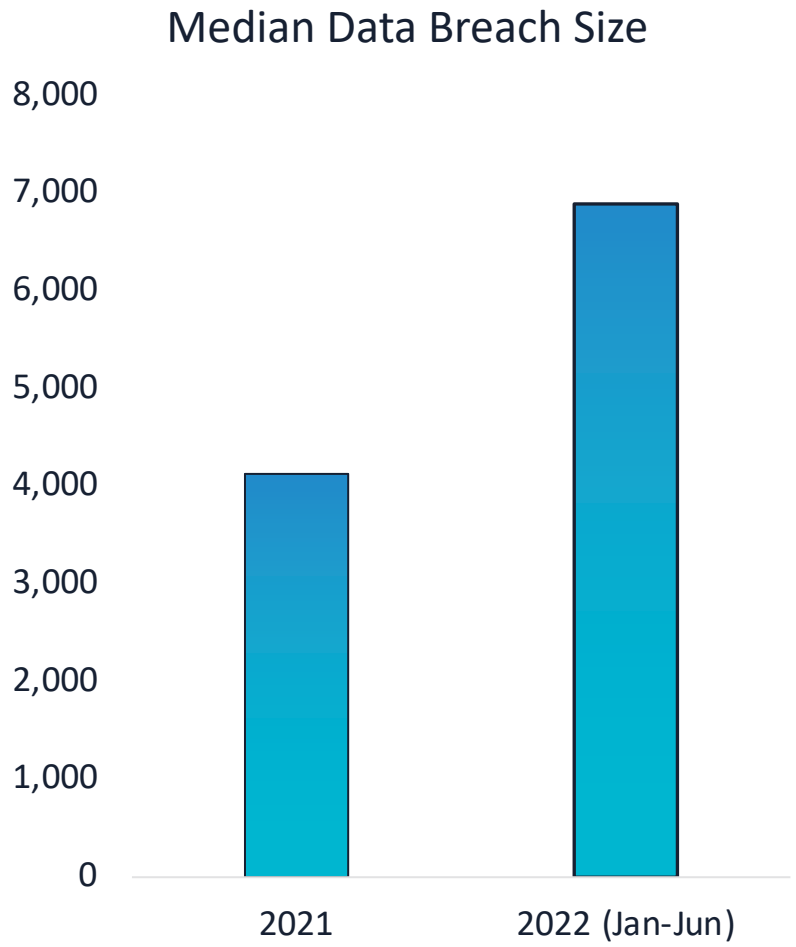
Chuck Podesta

CIO

- 38+ years of experience working in information technology (IT).
- 27 of which served as (CIO) at healthcare organizations across the country
- Joined Renown Health from the University of Connecticut Health System

Healthcare is the biggest target for cyber attacks.

- 57% of healthcare organizations report being hit by a ransomware attack in the last 3 years
    - Of those who experienced a ransomware attack, 60% revealed the attack disrupted some business processes completely
- About 22% of organizations reported an increased mortality rate post ransomware attack

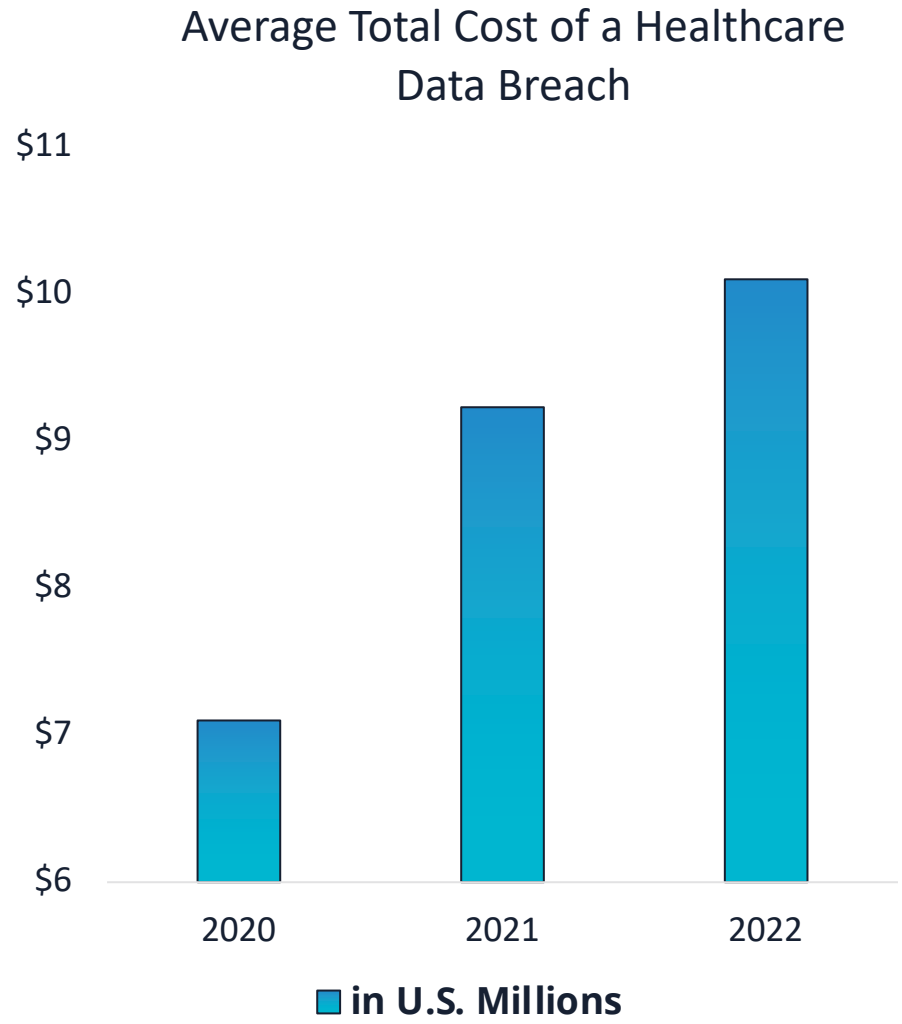


Sources: Health IT Security, Ponemon/IBM 2022 Cost of a Data Breach Report

Healthcare is the most expensive industry to suffer a breach.

- The average cost of a healthcare breach has now eclipsed $10 million, exceeding all other industries
- Cyber insurance premiums are doubling for many healthcare organizations.

Sources: Ponemon/IBM 2022 Cost of a Data Breach Report, Fierce Healthcare



#1: Ensure You're Insured

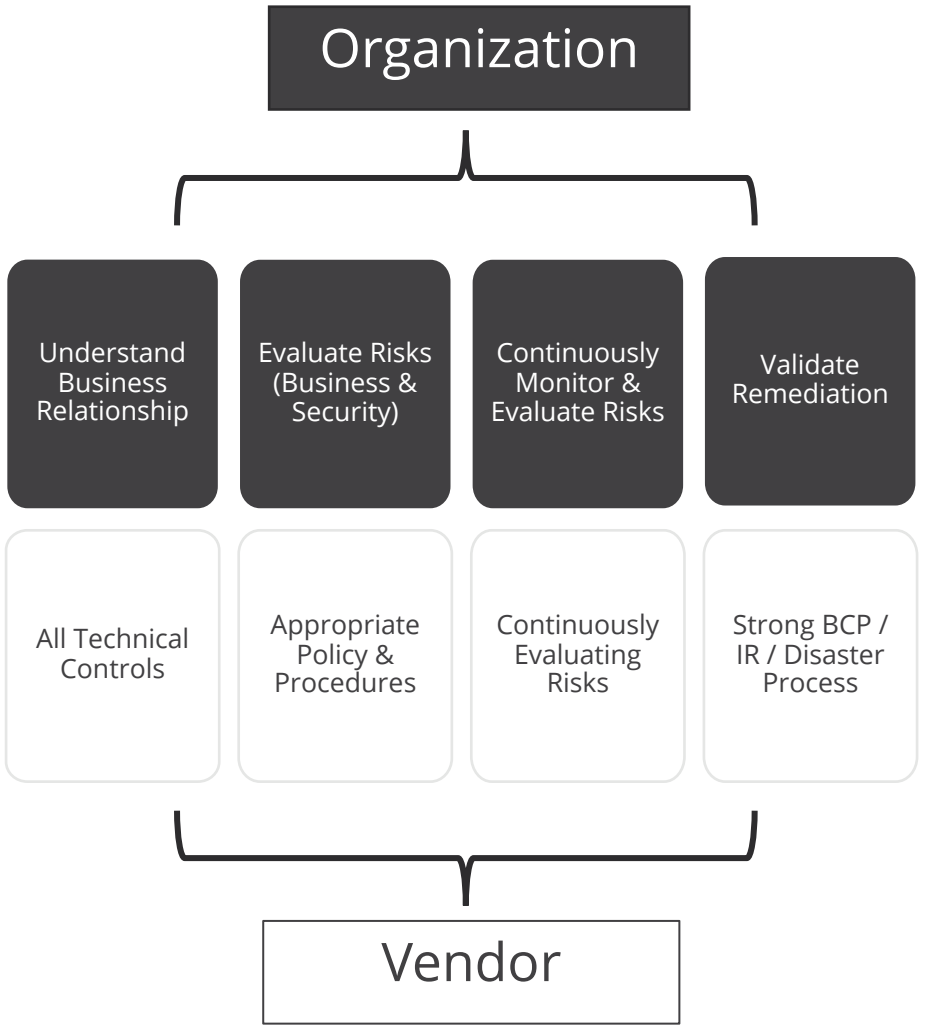
- Implement Security Continuous Monitoring
- Endpoint & Network Detection & Response
- Multi-Factor Authentication
- Privileged Access Management

- *The self-insured approach*
- *Lloyd's of London*
- *Renown's experience*

#2: Know Your Supply Chain Risk

- What vendors are you using today?
- Evaluate the business & security risks for each of these vendors
- Prioritize & Track
- Build Enforcement Mechanisms

- *Kronos*
- *+18M records exposed in 2022 by Third parties*



#3: Continually Assess Risk

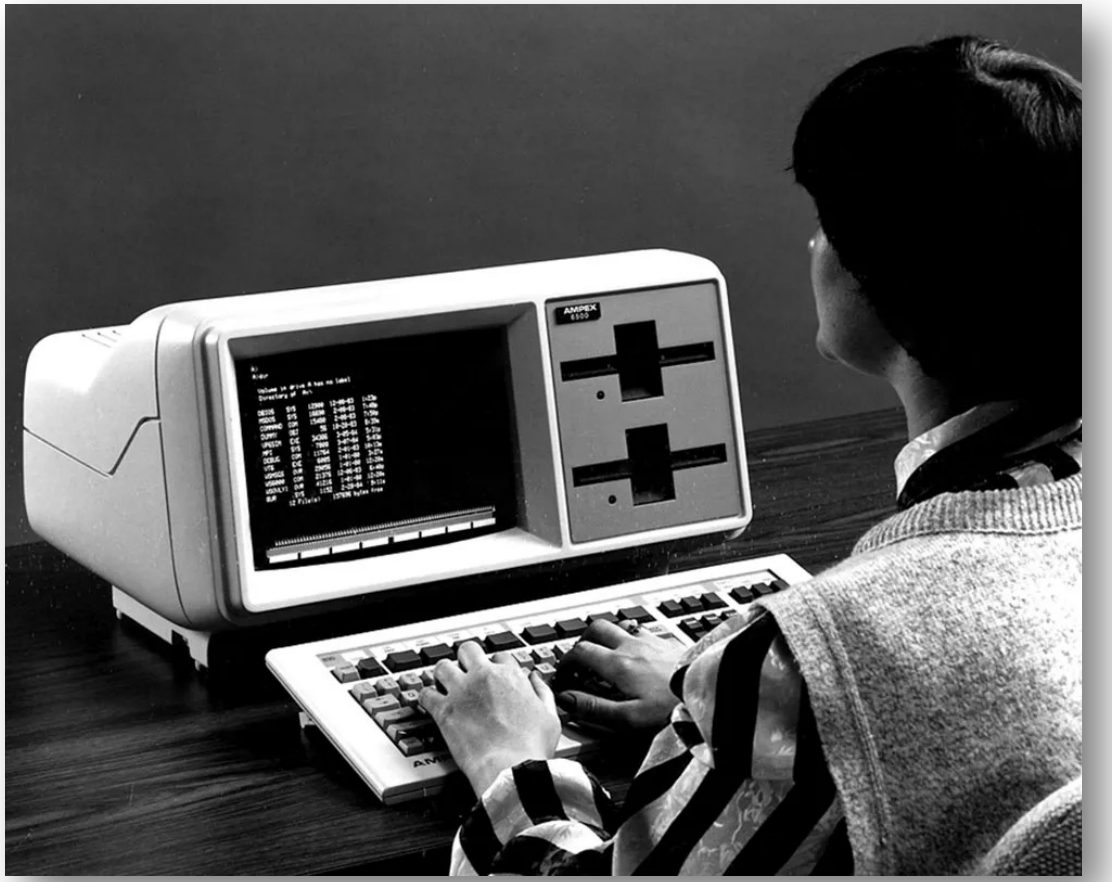
- Know your enterprise - you can’t protect what you don't know. Have identification & control over all your assets (everything data, people, etc...)
- Know/define your risk tolerance
- Have a plan & work the plan

- *Everyone is getting better over time*

#4: Eliminate Legacy & Unsupported Systems

- Assess Risk & Inform business on impacts
- Include total cost of ownership
- Implement a policy or standard for hardware/software

- *Start the conversation, you'll be surprised*
- *Elimination Round*



#5: Validate, Practice, & Rehearse Everyday

- Validate the effectiveness of your investments
- Develop runbook & practice it
- Rehearse what to do in a crisis

- *Exercise to build strength*

Close

1. Ensure You're Insured
2. Know Your Supply Chain Risk
3. Continually Assess Risk
4. Eliminate Legacy & Unsupported Systems
5. Validate, Practice, & Rehearse Everyday

- *Prevent skyrocketing cyber insurance price increases or loss of coverage*
- *Reduce general / overall risk*
- *Increase availability*

CLEARWATER CYNERGISTEK A Clearwater Company TECH LOCK A Division of Clearwater

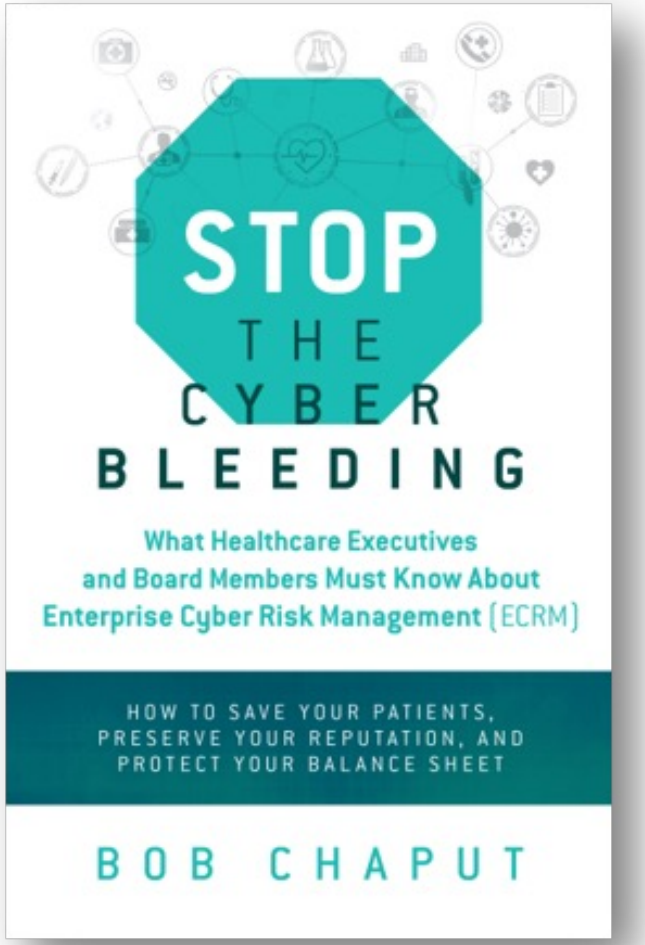
Mac McMillan

Dave Bailey

Chuck Podesta

Additional Educational Resources…

[A Must-Watch Series for Healthcare Leaders]



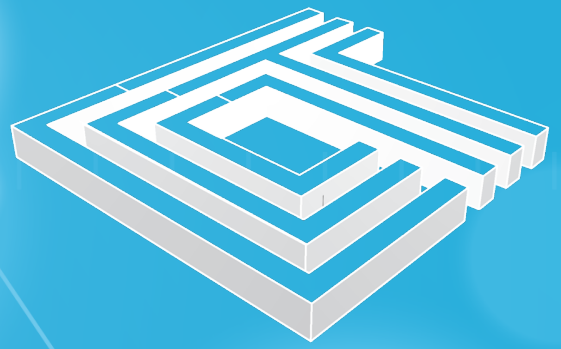
Available in digital, paperback, &, audio format.

https://amzn.to/33qr17n

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

CLEARWATER

HEALTHCARE CYBER RISK MANAGEMENT



CYNERGISTEK

A Clearwater Company

TECH LOCK®

A Division of Clearwater