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.

Clearwater

Healthcare – Secure, Compliant, Resilient

Monthly Cyber Briefing

May 2023: Healthcare Threat Intelligence

Logistics

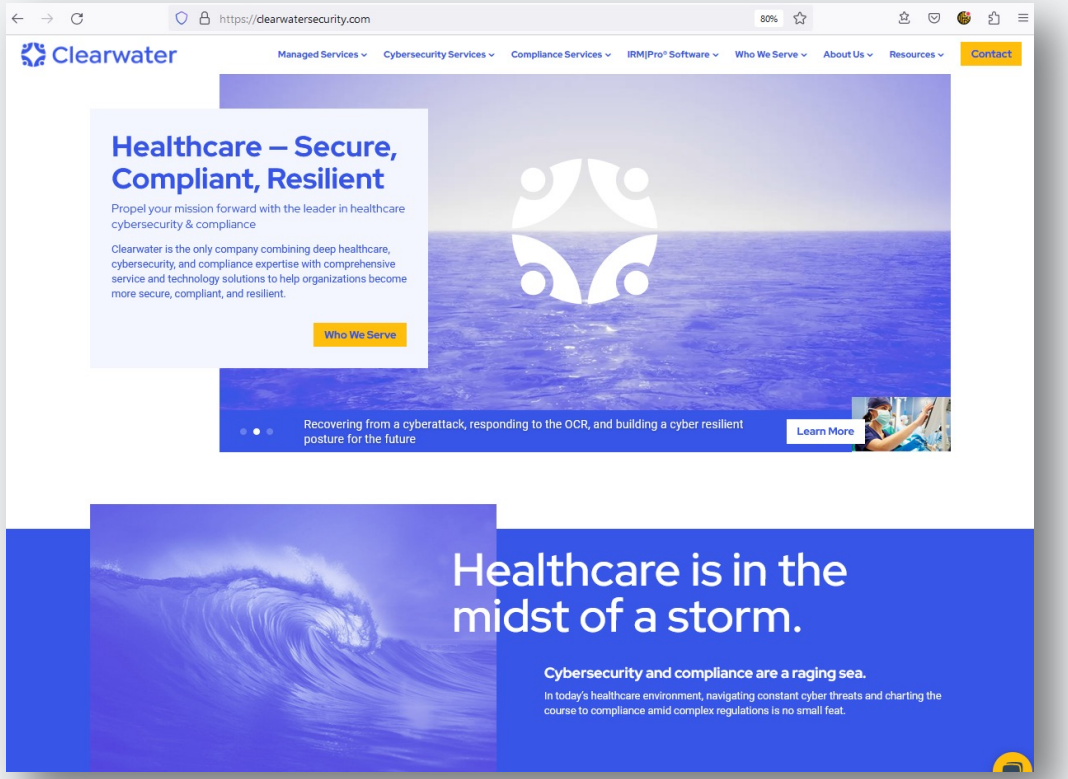
- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Cyber Briefings are eligible for HIMSS & CHIME CE credit
- Recording and final slides shared within 48 hours

Agenda

- Clearwater Update
- Updates from HHS 405(d) HICP Program
- Key Takeaways for Hospital Resiliency Landscape Analysis
- Threat Briefing

Company Announcements

- Clearwater has a new brand identity
- New corporate website: www.clearwatersecurity.com
- Email domain has changed to clearwatersecurity.com – please white list
- Company legal name is now Clearwater Security and Compliance LLC however, we will still go by “Clearwater”



New Clearwater Security & Compliance website

May’s Speakers

Steve Cagle, MBA, HCISSP

Chief Executive Officer

Dave Bailey, CISSP

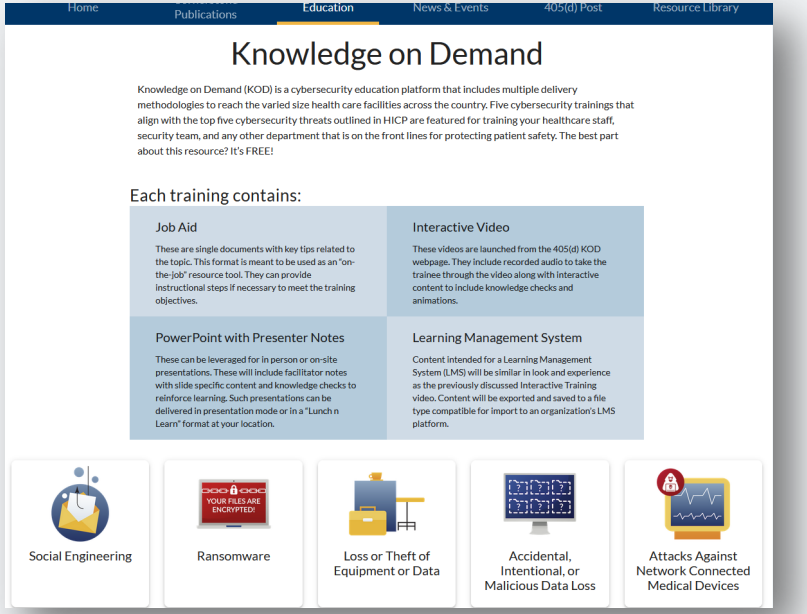
VP, Consulting Services

Cyber Update

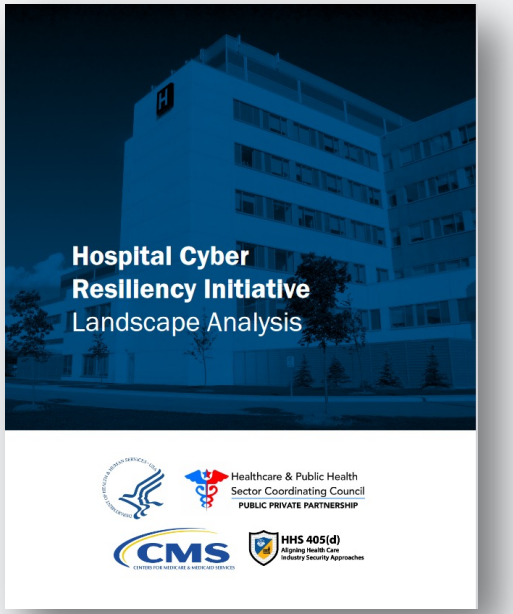
Steve Cagle

Updates from HHS 405(d) HICP Program

[The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) 2023 Edition]



[Knowledge on Demand]



[Hospital Resiliency Landscape Analysis]

Hospital Cyber Resiliency Initiative Landscape Analysis

- Objectives
  - Understanding of the current cybersecurity capabilities and preparedness across participating U.S. hospitals
  - Input into prioritized cybersecurity practices as well as other considerations the U.S. government might take in improving cybersecurity resiliency
- Data Sources
  - Threat data from U.S. government, vendors, and open source intelligence
  - CHIME's Most Wired Survey (n=377), sponsored by First Health Advisory
  - A survey (n=59) conducted in partnership with Censinet, the American Hospital Association (AHA) and KLAS
  - 20 conversations with hospitals across U.S.

Key Findings of Hospital Cyber Resiliency Landscape Analysis

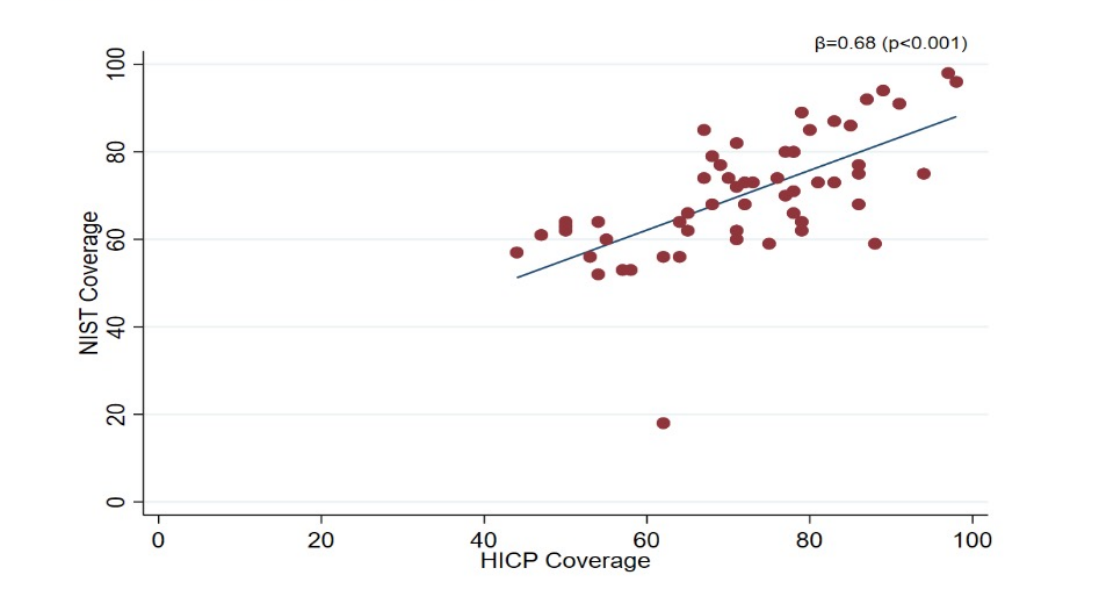
Ransomware	Directly targeted ransomware attacks aimed to disrupt clinical operations are #1 Threat to Hospitals
Inconsistent Controls	Variable adoption of security controls coupled with a changing landscape expose hospitals to more cyber attacks
Email Protection	Hospitals measure success in implementing email protections which is key to success
Supply Chain	Supply chain risk is pervasive for hospitals: half don't assess risk for patient safety concerns
Medical Devices	Minority don't have their third parties all covered and half don't assess risk for patient safety concerns

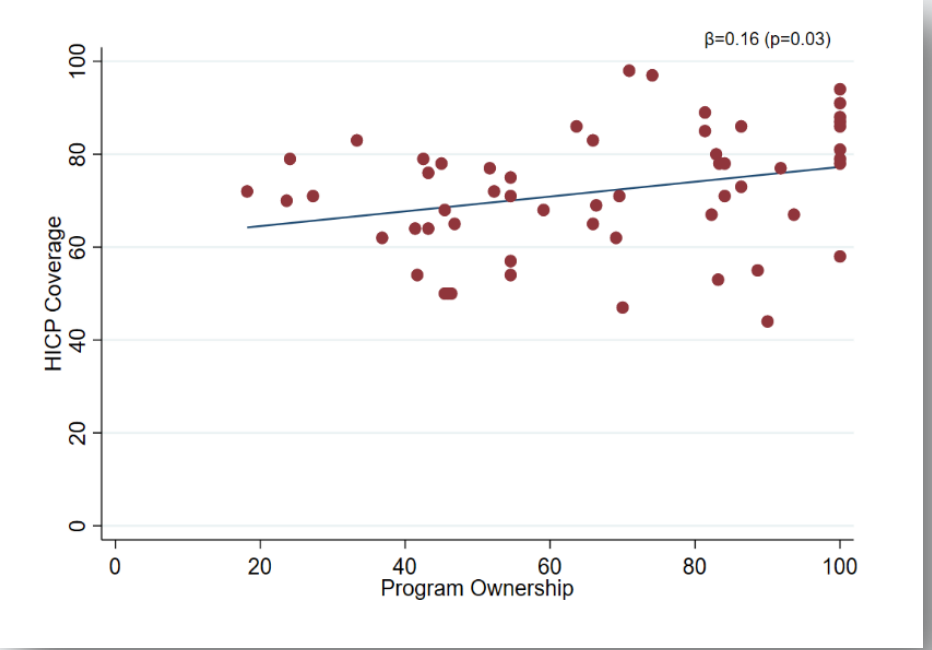
Key Findings of Hospital Cyber Resiliency Landscape Analysis (continued)

Resiliency	There is significant variation in cybersecurity resiliency among hospitals – investment levels in cybersecurity vary between 0.07% and 0.75%
Legacy hardware & Software	The use of antiquated hardware, systems, and software by hospitals is concerning
Cyber Insurance	Cybersecurity insurance premiums continue to rise, as do retention, while coverage limits fall, and cost of a breach is higher than ever before
Talent	Securing cyber talent with requisite skills and experience is challenging, especially for smaller hospitals
HICP Adoption	Adopting HICP improves cyber resiliency – 0.6 correlation with the NIST Cybersecurity Framework

Correlation Between HICP & NIST CSF & Program Ownership

Strong correlation between program HICP and NIST CSF, and CISO program ownership and adoption of HICP





Clearwater Recommendations

- Perform on-going risk analysis of all information systems at the asset level to identify where gaps exist and create risk response plan based on risk level
- Consider following SP 800-37 when implementing new systems – categorize system, select and implement controls, perform risk analysis, and determine authorization to operate/use
- Move from quarterly scans to vulnerability management – ongoing scanning and remediation
- Conduct more sophisticated penetration testing such as red teaming
- Conduct a security controls validation assessment to test your defenses against specific attack scenarios
- Review network segmentation of unpatched unsupported devices
- Employ more advanced security awareness training and phishing / social engineering testing
- Architect your third-party risk management program such that it creates a tiered approach to assessing vendors based on risk to patient safety

Healthcare Threat Intelligence

Dave Bailey

"The essence of risk management lies in maximizing the areas where we have some control over the outcome while minimizing the areas where we have absolutely no control over the outcome."

-Peter L. Bernstein

Purpose

Provide an overview of today’s adversarial threat

Present a healthcare industry assessment of the adversary

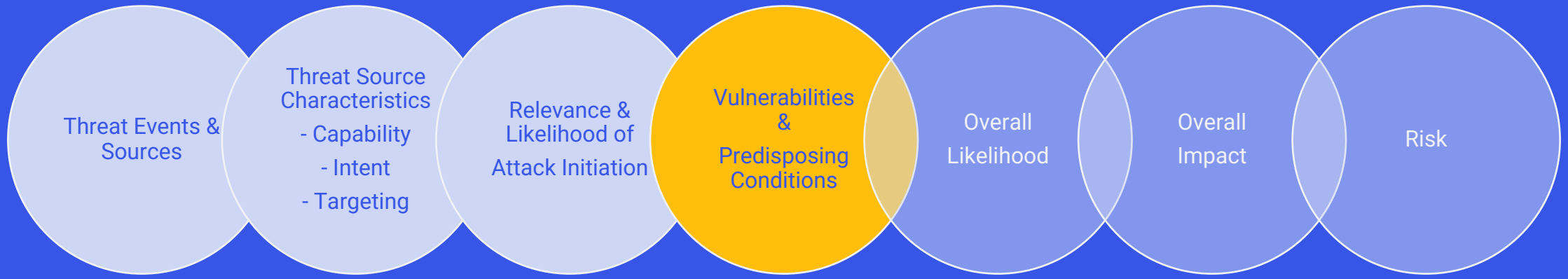
Provide top drivers of risk

Changing Risk Priorities in Healthcare

- Past
  - Risk was managed with clinical focus
  - Cyber risk management was focused on regulatory compliance
  - Data breaches were most feared
  - Audits and fines from the Office for Civil Rights were likely
  - Data protection and compliance were primary goals
- Present
  - Risk is managed as a business issue
  - Cyber risk management is focused more on availability and patient safety
  - Major incidents (ransomware) most feared: Business shut down or failure
  - Patient safety risk with clinical technology, Internet of Things
  - Business resilience is now the primary goal

Defining Risk

Risk defined by NIST 800-30



Know your Adversary | Know your Security Program | Know your Risk

Healthcare Threat Assessment

Focus: Adversarial Threat

Relevant Current Events And Indicators

Joint Cybersecurity Advisory: #StopRansomware: LockBit 3.0

The LockBit 3.0 ransomware operations function as a Ransomware-as-a-Service (RaaS) model and is a continuation of previous versions of the ransomware, LockBit 2.0, and LockBit. Since January 2020, LockBit has functioned as an affiliate-based ransomware variant; affiliates deploying the LockBit RaaS use many varying TTPs and attack a wide range of businesses and critical infrastructure organizations, which can make effective computer network defense and mitigation challenging.

HC3: New Data Breaches from CLOp and Lockbit Ransomware Groups

On April 28, 2023, Ransomware-as-a-service (RaaS) groups Cl0p and Lockbit recently conducted several distinct attacks, exploiting three known vulnerabilities (CVE-2023-27351, CVE-2023-27350, and CVE-2023-0669).

The Cl0p ransomware used was traced to the threat actor known as Lace Tempest, and overlapped with FIN11 and TA505

HC3: Threat Briefing: EMRs A Top Target for Cyber Threat Actors

On April 07, 2023, the Health Sector Cybersecurity Coordination Center (HC3) shared a report "April 6 Threat Briefing: EMRs A Top Target for Cyber Threat Actors."

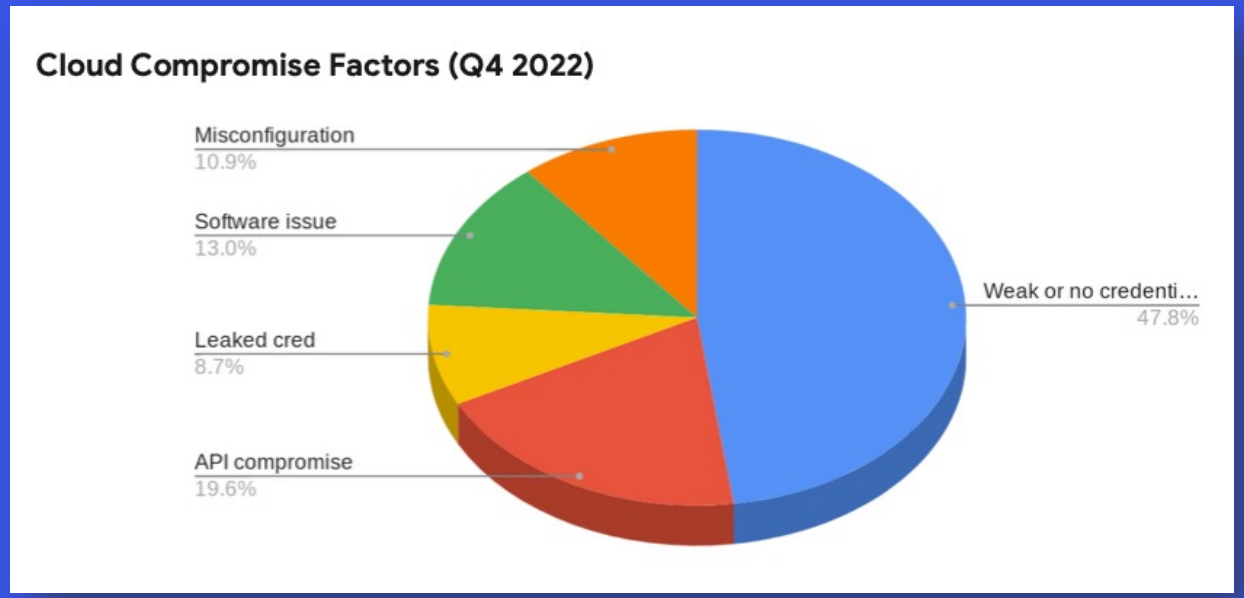
Relevant Industry Threat Briefings:

- Top threats against electronic medical and health records:
  - Phishing attacks
  - Fraud
  - Data Breaches and vulnerabilities
  - Malware and ransomware attacks
  - Encryption blind spots
  - Cloud threats/Third-party risks
  - Employees/Insider threats

HHS Briefing

Relevant Industry Threat Briefings:

Credentials & API issues continue to lead compromise factors…



Relevant Industry Threat Briefings:

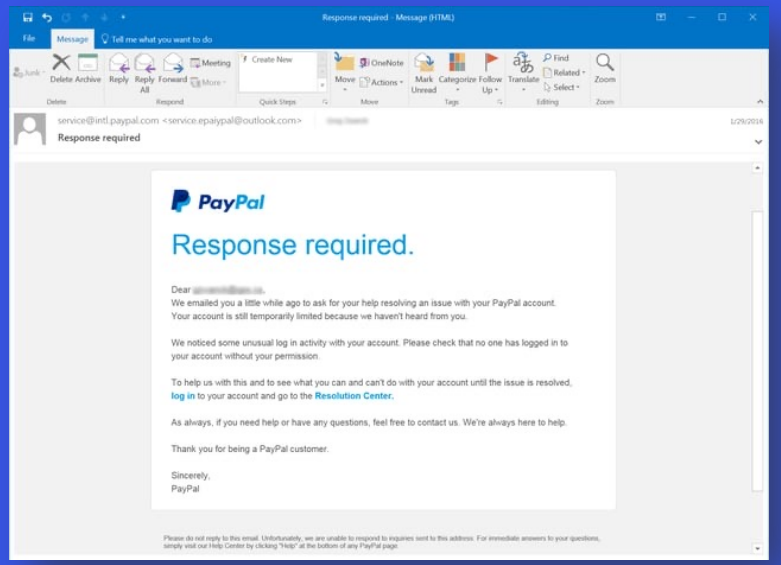
Hospital Cyber Resiliency Initiative Landscape Analysis: Threats

- Ransomware and Ransomware-as-a-Service (RaaS) attacks
- Cloud exploitations by threat actors
- Phishing/Spear-Phishing Attacks; specifically, those attacks that overcome MFA through social engineering
- Software and zero-day vulnerabilities
- Distributed Denial of Service attacks (DDoS)

Healthcare Industry: Accidental and Insider Threat

- Unintentional Insider Threat: Erroneous actions taken by individuals
- Intentional Insider Threat: Actions taken by individuals to knowingly harm the organization or violate policy or the law

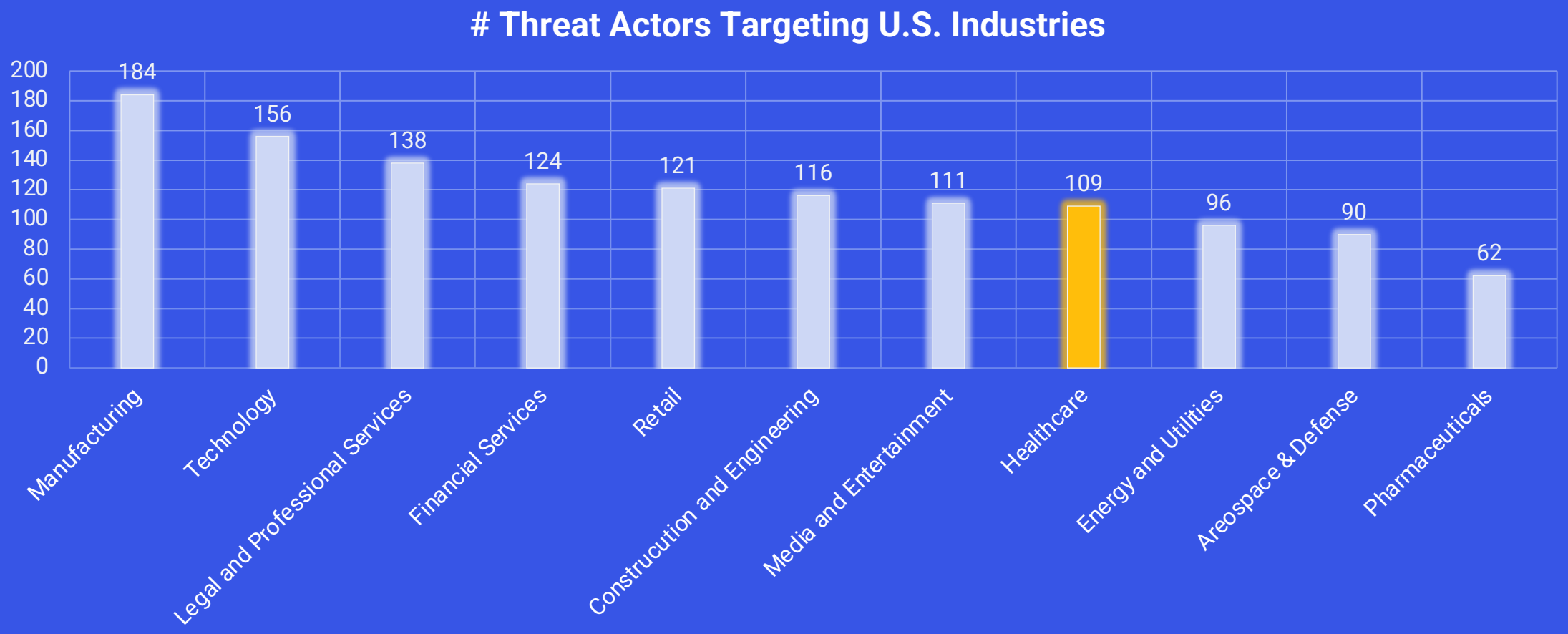
- Primary Threat Vector of the Adversary: The user continues to be the primary threat vector as the source for malware and initiation of attack



- Medium size (250 – 999 employees) Healthcare & Pharmaceuticals ranked #2 (of 19 industries) with a 36.6% Phish-Prone Percentage
- In 2022, across all industries and all sizes, the average Phish-prone Percentage was 32.4%, up 1 point from 2021. That means one out of three employees was likely to click on a suspicious link or email or comply with a fraudulent request.

Threat Actor Overview

As of April 2023, 109 threat actors target the US healthcare industry



Source: Mandiant Threat Intelligence

Threat Intelligence Report – As of April 2023

- 235 Actors targeting US Industries
- 109 Actors targeting US Healthcare Industry
- Europe and Asia are primary known target source regions

Source Region	# Actors
Europe	20
Asia	48
Unknown	41
Total Targeting US Healthcare	**109**

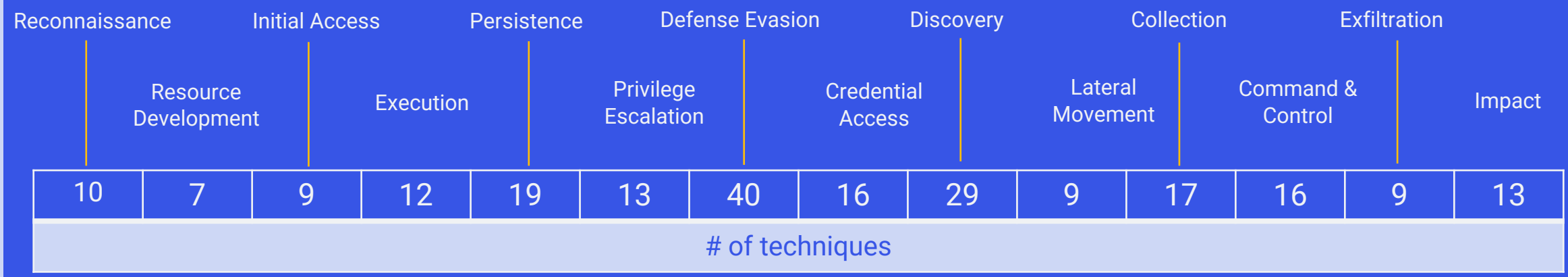
Source: Mandiant Threat Intelligence

Dwell Time Investigation by Type 2022

Median 10 Days	Median 5 Days	Median 12 Days
All Investigations	Ransomware Investigations	Non-Ransomware Investigations

"Although the percentage of intrusions involving ransomware has decreased globally, Mandiant observed a consistent percentage of investigations (22%) in the Americas involving ransomware compared to last year"

Typical Ransomware: How They Attack



MITRE ATT&CK Enterprise Tactics

Assumptions and Takeaways From an Attack

A threat actor was present on your network

Data may be exfiltrated; assume it was and prove otherwise

At least one account was compromised; most likely many

Network may still be compromised; assume it was and prove otherwise

Healthcare Threat Assessment: Characteristics of the Adversary

CAPABILITY	Very Low · Low · Moderate · High · **Very High**	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
INTENT	Very Low · Low · Moderate · **High** · Very High	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
TARGETING	Very Low · Low · Moderate · **High** · Very High	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
RELEVANCE	Possible · Predicted · Anticipated · **Expected** · Confirmed	The threat event or TTP has been seen by the organization's peers or partners.
LIKELIHOOD	Very Low · Low · Moderate · **High** · Very High	Adversary is almost certain to initiate the threat event.

Top Drivers of Risk

An Analysis from Clearwater Assessments and Security Operations Center

Top 5 Drivers of Risk: Clearwater Risk Analysis

Clearwater's data says…

Inadequate safeguards to protect user identities	Lack of User Activity Review	Inadequate log aggregation & monitoring	Weak password controls	Lack of user account protections
Systems that process store or transmit ePHI are not multi-factored enabled or integrated securely into a single sign-on capability	User activity and user permissions are not formally reviewed or integrated into continuous monitoring	System logging is not formally aggregated or integrated into continuous monitoring	Systems are not enforcing strong password requirements on users	Systems are not preventing simultaneous user logins or have adequately address failed login attempts

Top 5 Drivers of Risk: Clearwater SOC

Clearwater's data says…

MFA Fatigue

As organizations expand MFA, they are trying to make easier on the end user, and inadvertently making it easier for the user to "approve" access that is not theirs

Native Cloud Logging

Organizations are trusting that default logging in cloud services is adequate, not realizing they may be limited in scope, duration, and content to better understand what occurred

Unpatched, Legacy, or Unsupported Systems

Ineffective vulnerability management programs and lack of system development lifecycle

Inconsistent Controls Implemented

Organizations are applying different security controls for production, corporate, and development environment creating gaps in visibility and protection

Incomplete or Outdated Awareness Programs

Modern threats and tactics are changing, and many organizations have a relatively static awareness program that does not reflect this

Top 5 Drivers of Risk: Clearwater NIST CSF Assessments

Clearwater's data says…

Unpatched, Legacy, or Unsupported Systems	Lack of system hardening and configuration management	Lack of Network Segmentation	Inadequate safeguards to protect user identities	Missing Business Impact Analysis of Critical Functions
Ineffective vulnerability management programs and lack of system development lifecycle	Ineffective practices to protect network connected devices; especially medical devices	Incomplete strategies to minimize the attack surface and segment critical assets and functions	Poor user management practices for domain, local admin, & business applications	Missing or incomplete Business Impact Analysis that supports the response and recovery from cyber attack

Clearwater Recommendations

- Perform on-going risk analysis of all information systems at the asset level to identify where gaps exist and create risk response plan based on risk level
- Consider following SP 800-37 when implementing new systems – categorize system, select and implement controls, perform risk analysis, and determine authorization to operate/use
- Move from quarterly scans to vulnerability management – ongoing scanning and remediation
- Conduct more sophisticated penetration testing such as red teaming
- Conduct a security controls validation assessment to test your defenses against specific attack scenarios
- Review network segmentation of unpatched unsupported devices
- Employ more advanced security awareness training and phishing / social engineering testing
- Architect your third-party risk management program such that it creates a tiered approach to assessing vendors based on risk to patient safety

Q&A

Steve Cagle

Dave Bailey

We are here to help.

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

Upcoming Events

TN HIMSS Golf Tournament | June 9th

Digital Health Forum | May 17-18, 2023

June Cyber Briefing | June 1, 2023

Clearwater

Healthcare – Secure, Compliant, Resilient

Contact us

info@clearwatersecurity.com

www.clearwatersecurity.com

1.800.704.3394