LAWRENCE, EVANS & CO., LLC

Investment Banking | Healthcare Finance | Consulting

Healthcare Cybersecurity and Compliance: Investment Update

January 2023

Table of Contents

Main Report

Appendix

Healthcare Cybersecurity / Compliance Overview

Importance of Cybersecurity in Healthcare

With the increasing amount of patient data being stored and shared electronically, healthcare cybersecurity is more important than ever to protect both patients and healthcare organizations from potential harm. Investors should consider the below implications:

Scope of Report

- Complexities of healthcare IT systems, aging infrastructure of hospitals and healthcare organizations, increasing use of telemedicine, hybrid workforce and connectivity of various IoT devices collecting and transporting data
- Growing trend in cyber attacks specifically at the lower middle market healthcare organizations that are typically under funded in IT and cyber defense
- Increasing costs of cyber insurance and complying with regulations
- Summary of PE / VC Investments

Market Opportunity

- Healthcare cyber breaches have seen a 5-year growth of 11% CAGR (estimated to be much higher due to underreported breaches) with each breach costing an average of $10.1 million
- Healthcare cybersecurity growth of 17.5% CAGR through 2030
- Supply of quality cyber professionals and ethical hackers is short by an estimated 600,000 openings and 3.5 million openings by 2025
- Growing use of out-sourced cyber services including by M&A professionals
- Fragmented, growing industry ripe for investment and consolidation
- Cybersecurity is a part of the ERC and ESG framework

Healthcare Top Data Breaches (All Time)

1) 78.8M patient files Anthem (Health Plan) *2015*
2) 26.1M patient files American Medical Collection Agency *2019*
3) 11.0M patient files Premera Blue Cross (Health Plan) *2015*

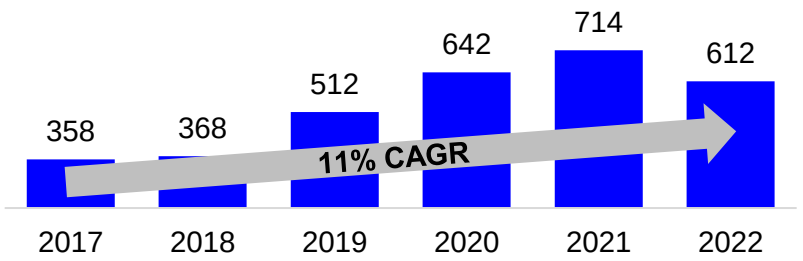
Healthcare Top Data Breaches 2022

1) 4.1M patient files OneTouchPoint (Business Associate)
2) 3.6M patient files Eye Care Leaders (Business Associate)
3) 3.0M patient files Advocate Aurora (Provider)

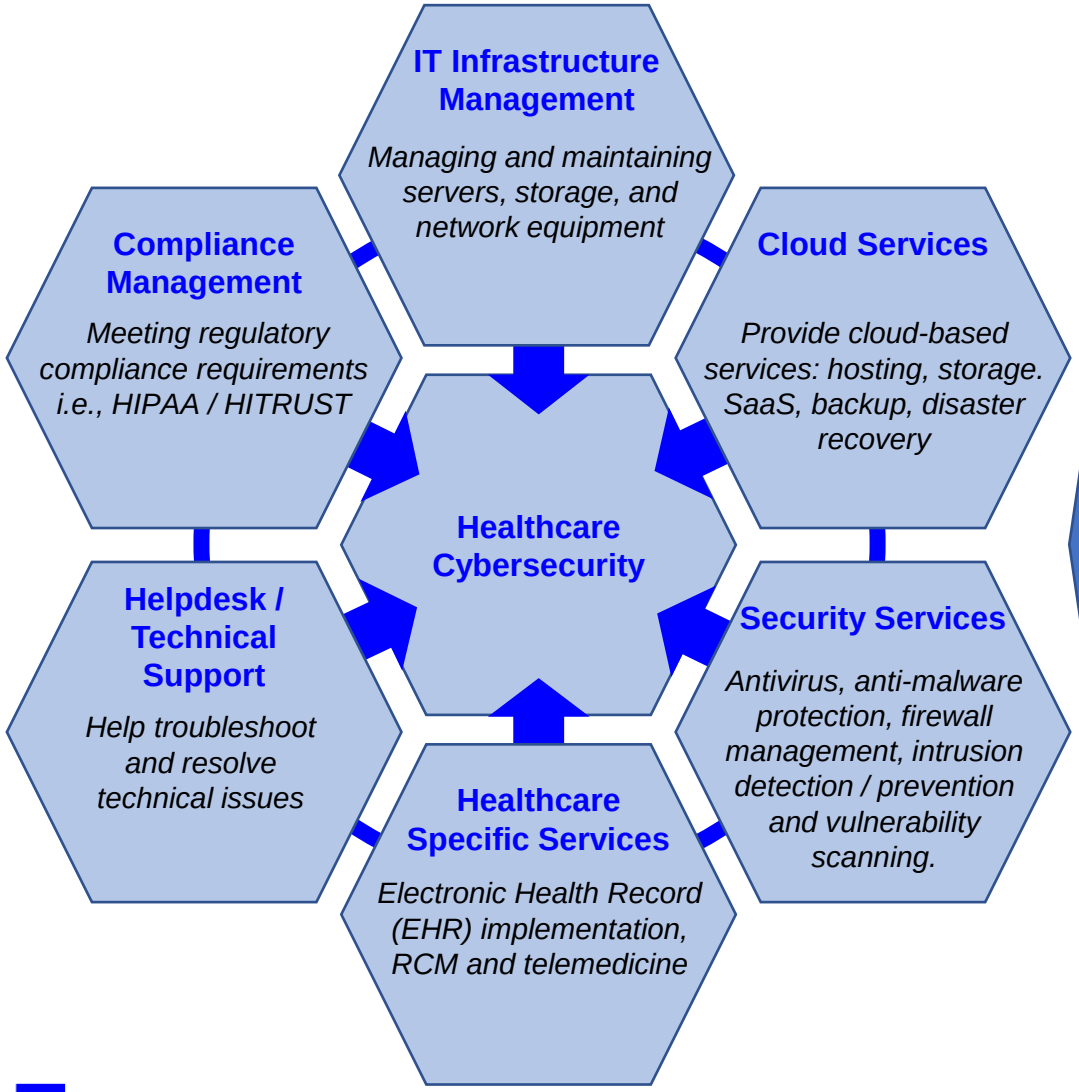
Top 5 Cyber Attacks by Industry

1) **Healthcare / Life Science**
2) Banking / Credit / Financial
3) Government / Military
4) Education
5) Critical Infrastructure including Energy / Utilities

Healthcare Data Breaches of >500 Records



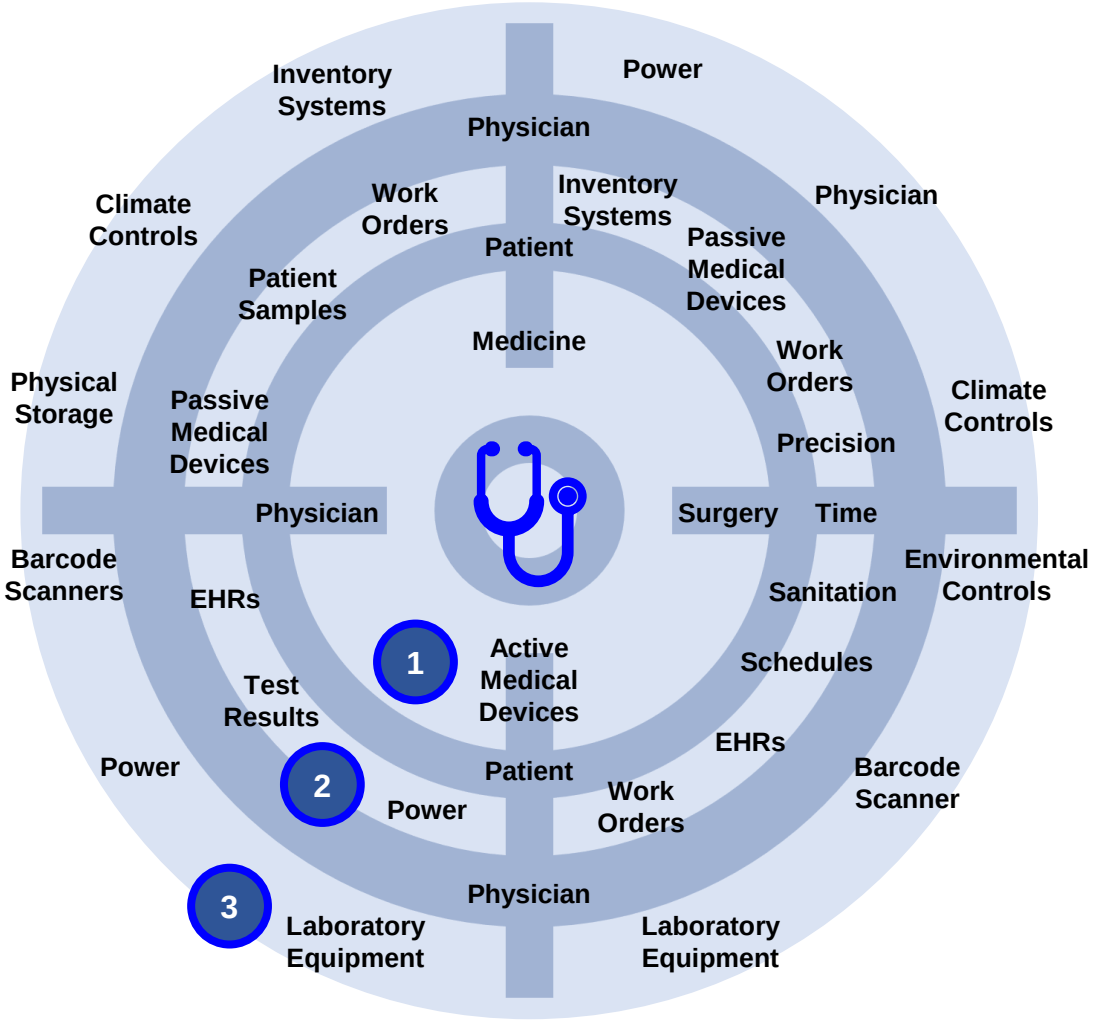
Healthcare Cybersecurity / Compliance Universe



- The healthcare space has few companies that provide “pure play” cybersecurity services and instead many overlap with one or more managed service lines.
- Many of the largest cybersecurity players do not offer tailored solutions that meet the unique challenges of securing healthcare data in accordance with HIPAA. Therefore, healthcare expertise in the space is valued at a premium.
- Healthcare organizations often require several software and security providers to provide coverage against the broad range of cybersecurity / compliance threats.
- Over 50% of SMBs have implemented AV and email / spam protection, with network and cloud security as the top areas planned for investment in the next year.
- Most states still only allocate between 2 - 10% of their budgets on cybersecurity efforts while on average, hospitals spend 5% of their IT budget on cybersecurity, leaving them vulnerable to increasingly sophisticated attacks.

*Data per Public Disclosures, Datto: 2022 State of Ransomware Report, 2022 Deloitte-NASICO Cybersecurity Study, Sophos: The State of Ransomware in Healthcare 2022

Threat Actor Targeting Within Healthcare Organizations



1 Primary Attack Surface

- Clinicians
- Medicine
- Patients
- Surgery
- Active Medical Devices *(AMD)*

2 Secondary Attack Surface

- Patient Samples
- Test Results
- Electronic Health Records *(EHR)*
- Passive Medical Devices *(PMD)*
- Work Orders
- Connected Power
- Schedules
- Inventory Systems
- Sanitary Conditions
- Procedure Precision
- Time

3 Tertiary Attack Surface

- Inventory Systems
- Climate Controls
- Environmental Controls
- Physical Storage
- Physical Transport
- Barcode Scanner / Printers

**Data per HEAL Security*

Data Threats and Defense in Healthcare Cybersecurity

Data Security Threats

Ransomware	Malware & Spyware	Distributed Denial of Service	
Phishing & Spearfishing	Insider Data Breaches	Deep Fakes	Other

Healthcare is the most targeted industry for cyberattacks with nearly 50 million patients impacted and an average cost per breach of $10.1 million in 2022

Targets *(Ranked by frequency)*

1 Clinics	2 Hospitals	3 Ambulatory Surgical Centers	4 Mental / Behavioral Health Organizations
5 Physician / Dental Practices	6 Post-Acute Care Organizations	7 Individual Physicians & Patients	Over half of all attacks affected multiple facilities.

In 2022, JAMA discovered 44% of attacks resulted in care delivery disruptions (41.7% of cases disruptions exceeded two weeks), 10.2% resulted in rescheduling care and 4.3% of attacks required ambulance diversion.

Compliance

Assessments	Gap Analysis	CMMC	FedRAMP / State RAMP
NIST	HIPAA	HISTRUST	GRC Monitoring

Healthcare Organizations are subject to mandatory compliance which can result in significant fines / lawsuits if breached, and nonmandatory compliance which can further aid in safeguarding data

Cybersecurity

Security Risk Assessments	Penetration Testing	Vulnerability Scanning	Remediation
Forensic Analysis	Incident Response	End-Point Monitoring	BDCR

Healthcare organizations face significant penalties when mandatory compliance is breached and therefore are encouraged to develop a strong cybersecurity framework which can include the above services

Employee / Personnel Training

Phishing Detection	Awareness Training	Threat Reporting	Certification Training	Cyber Defense Training

Even the strongest adherence to compliance and a strong cyber security network can still be undermined by employees that are not properly trained to avoid common threats to data security

**Data per Public Disclosures, Cerberus Sentinel Investor Deck (April 2022), JAMA: Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, (December 2022)*

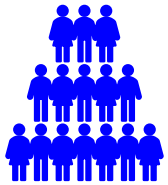
Healthcare Cybersecurity by the Numbers

#1

Industry for cyber complaints reported to the FBI in 2021

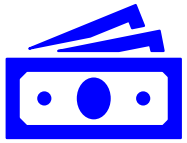
49.2M

Individuals affected by healthcare cyber security breaches in 2022



$10.1M

Average cost of a data breach vs. an average of $4.4 million across all other industries

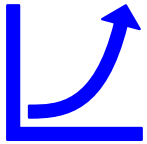


612

Healthcare breaches affecting >500 individuals reported in 2022

94%

YoY increase in ransomware attacks on healthcare organizations (2021-2022)



90%

Of ransomware attacks cause loss of business / revenue

61%

Of ransomware attacks result in data encryption

10x

Health records' value vs. stolen credit card information

5%

Hospital spending of their IT budget on cybersecurity; significantly below other industries

**Data per the U.S. Department of Health and Human Services, FBI's Internet Crime Complaint Center and Sophos' State of Ransomware in Healthcare*

Healthcare Cybersecurity Insurance

Despite their efforts, healthcare organizations with robust compliance, cybersecurity and employee training can still be the victim of a cyber attack. Healthcare cybersecurity insurance can offer an additional layer of legal and financial protection in the event an organizations' safeguards fail.

Select Healthcare Cybersecurity Insurance Coverage Offerings			
Notifying affected individuals of a data breach	Legal fees and settlements in the event of a lawsuit	Providing credit monitoring services to those affected	Public relations and crisis management
Cyber extortion and ransom payments	Business interruption and lost income	Cybercrime and fraud coverage	Data recovery and restoration

Additional Coverage: In addition to general coverage provided by cyber insurance, healthcare cybersecurity insurance can include coverage for HIPAA fines and penalties, regulatory investigations, and costs associated with forensic investigations.

Qualifying: Healthcare organizations must have robust cybersecurity measures in place, including incident response plans and regular security testing, in order to qualify for healthcare cybersecurity insurance and minimize the risk of a data breach.

Cost: Healthcare cybersecurity insurance is nearly always far more expensive than other industries as healthcare records can sell for up to 10x more than stolen credit card information.

Legislation: Cybersecurity insurance can offer protection against currently pending legislation and provide coverage as organizations adapt to the ever-changing regulatory landscape. (Full overview of *pending legislation located in Appendix)*

Key Statistics: A 2022 State of Ransomware report was released by Datto on January 17, 2023. The report surveyed nearly 3,000 IT professionals in small to medium-sized businesses (SMBs) and found the following:

- 69% of SMBs currently have cyber insurance and 34% of those without cyber insurance are highly likely to get it in the next year.
- 42% of SMBs with cyber insurance think it's extremely likely that a ransomware attack will happen in the next year, while only 16% of SMBs without cyber insurance think the same.

**Data per LECO insights, Sophos' State of Ransomware in Healthcare, Datto: 2022 State of Ransomware*

Largest Healthcare Data Breaches in History

Rank	Name of Covered Entity	Year	Covered Entity Type	# Affected	Cause of Breach
1	Anthem Inc.	2015	Health Plan	78,800,000	Hacking/IT Incident
2	American Medical Collection Agency	2019	Business Associate	26,059,725	Hacking/IT Incident
3	Premera Blue Cross	2015	Health Plan	11,000,000	Hacking/IT Incident
4	Excellus Health Plan, Inc.	2015	Health Plan	10,000,000	Hacking/IT Incident
5	Science Applications International Corporation	2011	Business Associate	4,900,000	Loss
6	University of California, Los Angeles Health	2015	Healthcare Provider	4,500,000	Hacking/IT Incident
7	Community Health Systems Professional Services	2014	Business Associate	4,500,000	Hacking/IT Incident
8	Advocate Medical Group	2013	Healthcare Provider	4,029,530	Theft
9	**OneTouchPoint**	**2022**	**Business Associate**	**4,112,892**	**Ransomware Attack**
10	Medical Informatics Engineering	2015	Business Associate	3,900,000	Hacking/IT Incident
11	**Eye Care Leaders**	**2022**	**Business Associate**	**3,649,470**	**Hacking/IT Incident**
12	Banner Health	2016	Healthcare Provider	3,620,000	Hacking/IT Incident
13	Florida Healthy Kids Corporation	2021	Health Plan	3,500,000	Hacking/IT Incident
14	Trinity Health	2020	Business Associate	3,320,726	Hacking/IT Incident
15	Newkirk Products, Inc.	2016	Business Associate	3,466,120	Hacking/IT Incident
16	20/20 Eye Care Network, Inc	2021	Business Associate	3,253,822	Hacking/IT Incident
17	**Advocate Aurora Health**	**2022**	**Healthcare Provider**	**3,000,000**	**Impermissible Disclosure (website tracking code)**
18	Dominion Dental Services, Inc.	2019	Health Plan	2,964,778	Hacking/IT Incident
19	AccuDoc Solutions, Inc.	2018	Business Associate	2,652,537	Hacking/IT Incident
20	Forefront Dermatology, S.C.	2021	Healthcare Provider	2,413,553	Hacking/IT Incident
21	**Connexin Software**	**2022**	**Business Associate**	**2,216,365**	**Hacking/IT Incident**
22	21st Century Oncology	2016	Healthcare Provider	2,213,597	Hacking/IT Incident
23	**Shields Healthcare Group**	**2022**	**Business Associate**	**2,000,000**	**Hacking/IT Incident**
24	Xerox State Healthcare, LLC	2014	Business Associate	2,000,000	Unauthorized Access/Disclosure
25	**Professional Finance Company**	**2022**	**Business Associate**	**1,918,941**	**Ransomware Attack**
26	IBM	2011	Business Associate	1,900,000	Unknown
27	Dental Care Alliance, LLC	2021	Business Associate	1,723,375	Hacking/IT Incident
28	GRM Information Management Services	2011	Business Associate	1,700,000	Theft
29	NEC Networks, LLC d/b/a CaptureRx	2021	Business Associate	1,656,569	Hacking/IT Incident
30	**Baptist Medical Center and Resolute Health Hospital**	**2022**	**Healthcare Provider**	**1,608,549**	**Hacking/IT Incident**

Indicates Breach in 2022 **Data per the U.S. Department of Health and Human Services*

2015 Anthem Data Breach

Anthem®

~78,800,000 Affected

"Largest Healthcare Data Breach in History"

The 2015 Anthem data breach was first discovered in February 2015 but was believed to have begun in December 2014. The attackers are believed to have used a sophisticated phishing campaign to gain access to sensitive personal information, including names, birthdates, Social Security numbers, addresses, phone numbers, and email addresses of customers and employees. Additionally, some customers' income data was also accessed. The FBI and other law enforcement agencies were quickly brought in to investigate the incident, but to this day the identity of the attackers remains unknown.

The fallout from the incident was significant including, but not limited to:

- Facing numerous class-action lawsuits and paying large settlements to affected customers
- $115 million settlement paid to affected customers, the largest data breach settlement in U.S. history
- $39.5 million settlement paid to a multi-state coalition made up of 44 states and Washington, D.C
- $16 million HIPAA settlement paid to the U.S. Department of Health and Human Services
- Was forced to offer affected customers 2 years of credit monitoring and identity protection services
- Faced heavy scrutiny from regulators / lawmakers over the security practices that enabled the attack Anthem was forced to take several steps to improve its security measures and strengthen its compliance with industry standards. They also revamped their IT security infrastructure and employee training to prevent similar breaches in the future.

The incident brought attention to the need for better cybersecurity practices in the healthcare industry and led to calls for increased regulatory oversight of the industry. It's considered the largest health data breaches in history as it affected nearly 80 million individuals.

**Data per Public Disclosures*

Select 2022 Healthcare Data Breaches

OneTouchPoint

April 2022

~4,100,000 Affected

OTP provides outsourcing and automation of document management and print functions for several industries including healthcare

On April 28, 2022, OTP discovered encrypted files on its computer systems and immediately launched an investigation with the assistance of third-party forensic specialists. The investigation determined that there was unauthorized access to its servers and it would be unable to determine the specific files the unauthorized actor viewed within its network.

- Compromised data included: names, addresses, birth dates, date / description of service, diagnosis codes, information provided as part of a health assessment, member IDs and social security numbers.
- OTP eventually had to mail physical letters to potentially impacted individuals on behalf of its insurance carrier partners including Anthem, Blue Cross Blue Shield, Humana and Kaiser Permanente.
- At least two other entities – Arkansas Blue Cross and Blue Shield and Blue Shield of California Promise Health Plan – also sent data breach notifications after learning that their subcontractor, Matrix Medical Network, was impacted by the OneTouchPoint ransomware attack.

OTP is now facing a class action lawsuit as a result of the breach. The lawsuit alleges that while the breach was discovered in late April, OTP waited several months, until July 27, to begin notifying impacted individuals.

CommonSpirit

October 2022

~623,000 Affected

CommonSpirit Health is the second-largest non-profit health system in the U.S., consisting of around 1,500 clinics and hospitals in 21 states

On October 3, 2022, CommonSpirit Health experienced a data security incident that forced it to take systems offline, including its electronic medical record (EMR) and other critical IT systems. These steps were taken to protect systems from damage, contain the breach, and prevent unauthorized access to sensitive data.

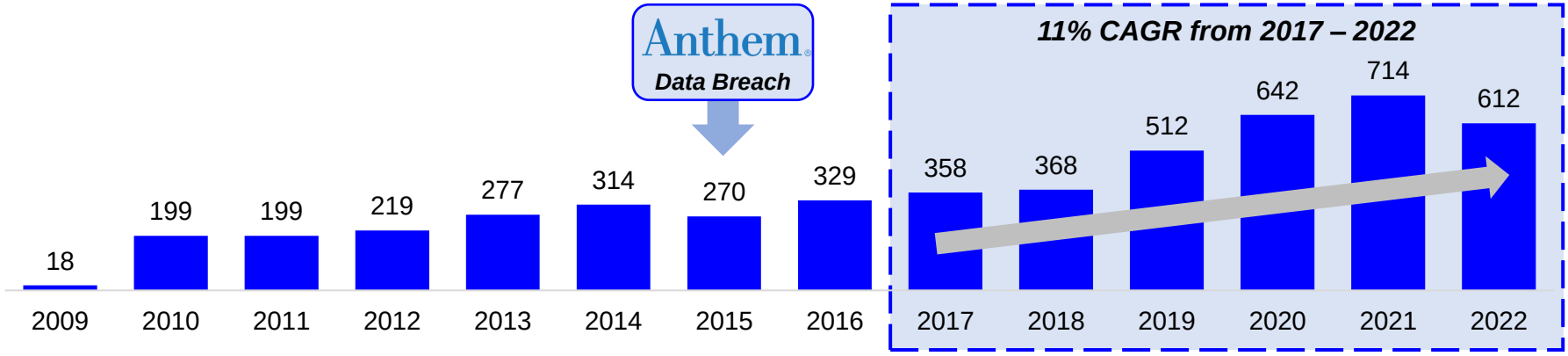
- Soon after the incident, hospitals and other care facilities across the country began to confirm they had also been compromised.
- Several facilities confirmed they had been affected and were operating under emergency procedures due to the lack of access to essential IT systems including hospitals in Iowa, Illinois, Nebraska, Tennessee, and Washington.
- The decision was taken to cancel, postpone, or reschedule some patient appointments and procedures. Access to the patient portal was temporarily suspended, and offline procedures were followed for processing prescriptions.

The breach was determined to be a ransomware attack and the investigation remains ongoing. CommonSpirit was formed 3 years ago following a megamerger between Dignity Health and Catholic Health Initiatives. Cybersecurity experts have noted that mergers can often expose systems that are poorly integrated.

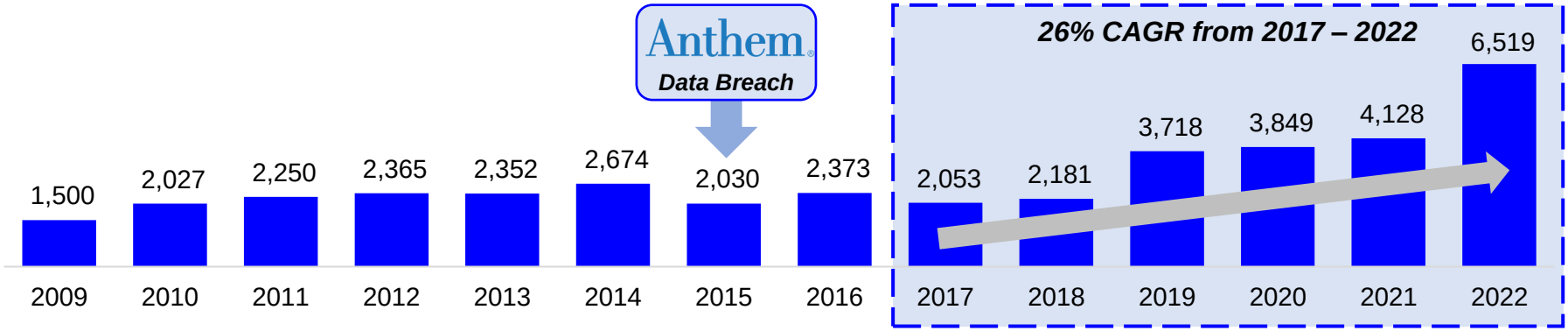
**Data per Public Disclosures*

Healthcare Data Breach Trends

Healthcare Data Breaches of >500 Records



Median Healthcare Data Breach Size



Data breaches have become more frequent and typical attacks have become more intrusive. The Ukraine War was responsible for a slight disruption in volume in 2022 but is expected to rebound higher in 2023. Additionally, prior years were likely underreported as past legislation was more relaxed in requiring disclosure.

**Data per the U.S. Department of Health and Human Services*

Healthcare Cybersecurity / Compliance: 2023 Outlook

Threats

- The pandemic accelerated U.S. healthcare companies transition from physical storage to online / cloud-based storage for medical records and patient data. This data migration will certainly continue in 2023.
- The war in Ukraine briefly disrupted cyber threat activity from Eastern Europe in 2022, causing a slight decrease in overall volume for the year. However, with an impending recession and rising geopolitical tensions, 2023 will likely continue the trend of attacks becoming more frequent and sophisticated.
- Ransomware has become the most prevalent form of healthcare data breaches and have quadrupled since the onset of the pandemic.
- Ransomware is likely to continue to be the most prevalent form of attack in 2023. Threat actors will continue to focus on shutting down systems for ransom payment and extracting data for resale.
- Data from the U.S. Department of Health & Human Services indicates attackers are shifting away from large hospital systems to focus on the types of companies PE firms invest in, like smaller and mid-sized healthcare entities and third-party vendors.
  - This is partially a result of larger healthcare players bolstering cyber security frameworks in recent years, making them more difficult targets for potential hackers.

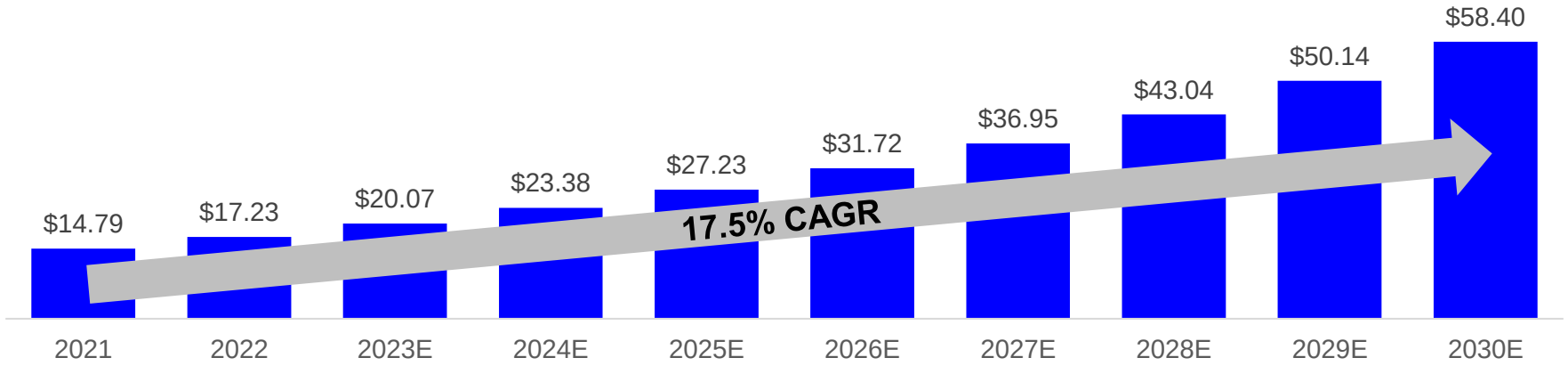
Threat Management

- In 2023, regulatory requirements and the threat of operational impacts will require a meaningful understanding of data security and quantitative security risk assessments by PE firms, with particular attention to unique risks faced by niche businesses.
  - Tailored approaches are likely to be more effective vs. catch-all solutions from cybersecurity firms lacking healthcare expertise.
- The uptick in breaches of third-party vendors highlights the need for implementing strong third-party risk management programs in 2023 and / or revisiting those already in place.
- Cyber insurance remains difficult to acquire, particularly for smaller companies serving healthcare organizations. By leveraging broader insurance relationships, PE firms can look to assist their portfolio companies in the coming year.
  - Alternatively, PE firms can assess platform opportunities within the healthcare cyber security space to capitalize on the growing threats facing the industry.
- Aggressive, financially-focused attorneys are increasingly interested in cybersecurity litigation, so we expect duplicative data breach lawsuits to increase in 2023 and insurers to focus more on coverage limits. PE firms can assist portfolio companies by maintaining a relationship with counsel familiar with their portfolios to efficiently manage these matters in a cost-effective manner.
- 53% of senior executives surveyed by MergerMarket are dedicating more resources to cybersecurity due diligence in their most recent deals compared to 12-24 months ago, including 21% who are dedicating significantly more resources. Additionally, 69% agree that a positive cybersecurity due diligence appraisal leads to a higher valuation.

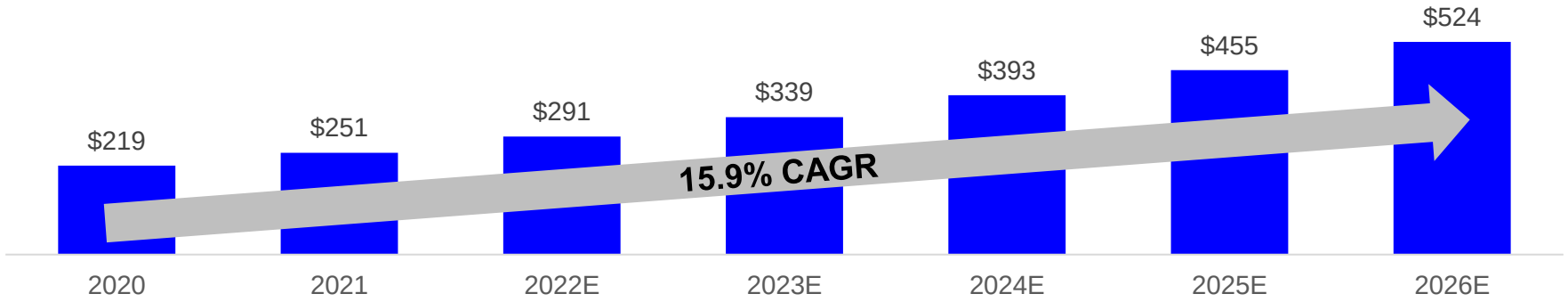
**Per Bass, Berry & Sims 2023 Healthcare Private Equity Outlook & Trends, MergerMarket: Under Attack Cyber Due-Diligence*

Healthcare Cybersecurity: 2023 Market Size Outlook

Global Healthcare Cybersecurity Market Size 2021 - 2030 *(US$ billions)*



Healthcare Penetration Testing Market Outlook *(US$ millions)*



The Global Healthcare Cybersecurity Market is expected to more than triple in size by 2030, while the Healthcare Penetration Testing Market is expected to nearly double in size by 2026

**Data per Precedence Research*

Healthcare Cybersecurity / Compliance: Deal Activity

Announced	Deal Type	Bidder (Sponsor)	Target	Size (US$mms)	Target Description	Multiples	
						Revenue	EBITDA
Dec-22	M&A (Platform)	**Silversmith Capital Partners** **Health Velocity Capital** **Nordic Consulting Group**	**Fortified Health Security** *(Subsidiary of medSR)*	n/a	Provider of cyber privacy and security software intended to protect patient data and reduce risk throughout the healthcare ecosystem	n/a	n/a
Nov-22	M&A (Add-On)	**CyberMaxx** *(Periscope Equity)*	**CipherTechs**	$33.0	Provider of a full-service cybersecurity solution portfolio across governance, risk and compliance and offensive / defensive security. Expands CyberMaxx's healthcare cyber capabilities	n/a	n/a
Nov-22	M&A (Add-On)	**CloudWave** *(ABRY Partners)*	**Sensato Cybersecurity Solutions**	n/a	Provider of cybersecurity services company focused on protecting healthcare providers from ransomware events and other cybersecurity threats	n/a	n/a
Aug-22	Growth Capital (Add-On)	**Bluff Point Associates** **Health Enterprise Partners**	**Intraprise Health**	$3.0	Provider of cyber security services, HITRUST certifications, HIPPA Compliance and Risk Management services to healthcare organizations	n/a	n/a
Jul-22	M&A (Add-On)	**Clearwater Compliance** *(Altaris Capital Partners)*	**TECH LOCK**	n/a	Provider of security management, threat detection, incident response, and compliance services	n/a	n/a
Jun-22	M&A (Add-On)	**ForeScout Technologies** *(Advent International)* *(Crosspoint Capital Partners)*	**Cysiv**	n/a	Provides threat hunting SOC with a managed security stack for hybrid cloud, network and endpoint security	n/a	n/a
May-22	M&A (Add-On)	**Clearwater Compliance** *(Altaris Capital Partners)*	**CynergisTek** *(f.k.a. Auxilio, Inc.)*	$16.2	Provider of privacy, compliance, IT audit, and cybersecurity services to healthcare organizations; Company was previously publicly traded under the ticker NYSEMKT:AUXO	1.0x	nmf
Jan-22	M&A (Add-On)	**ForeScout Technologies** *(Advent International)* *(Crosspoint Capital Partners)*	**CyberMDX Technologies**	n/a	Provider of medical cybersecurity solutions that delivers threat prevention for medical devices and clinical networks	n/a	n/a

Note: Only pure-play Healthcare Cybersecurity / Compliance transactions shown
**Data per Pitchbook, MergerMarket and public disclosures*

Healthcare Cybersecurity / Compliance: Deal Activity

Announced	Deal Type	Bidder (Sponsor)	Target	Size *(US$mms)*	Target Description	Multiples	
						Revenue	EBITDA
Jan-22	Growth Capital	**Primus Capital**	**CORL Technologies**	n/a	Provider of tech-enabled managed services for vendor risk management and compliance to the healthcare industry	n/a	n/a
Jan-22	Growth Capital	**Primus Capital**	**Meditology Services**	n/a	Provider of information risk management, cybersecurity, privacy and regulatory compliance consulting to healthcare organizations	n/a	n/a
Dec-21	M&A (Add-On)	**DAS Health** *(Sheridan Capital Partners)*	**Itentive Healthcare Solutions**	n/a	Provider of a complete suite of consulting, managed services and solutions to its physician practice customers	n/a	n/a
Aug-21	M&A (Platform)	**Periscope Equity**	**CyberMaxx**	n/a	Provider of software that utilizes institutionalized healthcare expertise to target healthcare and other highly regulated industries that require specialized security solutions	n/a	n/a
Aug-21	Growth Capital	**Warburg Pincus**	**A-LIGN Assurance** (FTV Capital)	n/a	Provider of cyber-security and compliance services serving the Healthcare industry	n/a	n/a
May-21	M&A (Add-On)	**DAS Health** *(Sheridan Capital Partners)*	**Itelegan**	n/a	Provider of healthcare management software to support physicians and medical practices	n/a	n/a
Feb-21	M&A (Platform)	**Sheridan Capital Partners**	**DAS Health**	n/a	Provider of managed IT, cloud hosting, cybersecurity, revenue cycle management and chronic care management for hospitals and healthcare companies	n/a	n/a
Jan-21	M&A (Add-On)	**Intraprise Health** *(Bluff Point Associates)* *(Health Enterprise Partners)*	**HIPAA One**	n/a	Provider of cloud-based HIPAA compliance automation software for healthcare providers, health plans and business associates	n/a	n/a

Note: Only pure-play Healthcare Cybersecurity / Compliance transactions shown
**Data per Pitchbook, MergerMarket and public disclosures*

Healthcare Cybersecurity / Compliance: PE PortCos

Investment Date	Sponsor	Portfolio Company	Company Type	Add-Ons	PortCo Website
Jan-21	abry partners	CloudWave	Cloud Hosting, Cybersecurity	**2022:** Sensato Cybersecurity Solutions (n/a)	Healthcare Data Security Experts | CloudWave (gocloudwave.com)
Aug-20	Advent International GLOBAL PRIVATE EQUITY; CROSSPOINT CAPITAL	ForeScout	Cybersecurity, Cyber Compliance	**2022:** Cysiv (n/a) **2022:** CyberMDX Technologies (n/a)	Forescout – Automated Cybersecurity Across Your Digital Terrain
Jan-19	POINT72 HYPERSCALE	AGIO	Cybersecurity, Cyber Compliance, HITRUST Assessor	**2019:** Intersection	Managed IT & Cybersecurity for Financial Services (agio.com)
Jul-18	FTV CAPITAL; WARBURG PINCUS	A-LIGN	Cybersecurity, Cyber Compliance, HITRUST Assessor	**2021**: Growth Capital from Warburg Pincus (n/a)	A-LIGN | Compliance, Cybersecurity, Cyber Risk & Privacy
Jan-18	ALTARIS	CLEARWATER COMPLIANCE	Cybersecurity, Cyber Compliance	**2022:** TECH LOCK (n/a) **2022**: CynergisTek ($16.2mm)	Cybersecurity and HIPAA Compliance Solutions | Clearwater (clearwatercompliance.com)
May-19	SUNSTONE PARTNERS	AVERTIUM	Cybersecurity, Cyber Compliance, HITRUST Assessor	**2020:** 1440 Security (n/a) **2019:** Terra Verde (n/a) **2019:** TruShield Security Solutions (n/a)	Avertium | Managed Security Services & Consulting Provider
May-18	BLUFFPOINT ASSOCIATES; HEP HEALTH ENTERPRISE PARTNERS	Intraprise HEALTH	Cybersecurity, Cyber Compliance, HITRUST Assessor	**2018:** Blueprint Healthcare (n/a) **2021:** HIPAA One (n/a)	Intraprise Health - Security Services, HITRUST, TPRM
May-17	SAGEWIND CAPITAL	BYLIGHT	Cloud Hosting, Cybersecurity, Cyber Compliance, HITRUST Assessor	**2019:** Cole Engineering Services (n/a) **2019:** Phacil (n/a) **2017:** Axom Technologies (n/a)	www.bylight.com

**Data per Pitchbook, MergerMarket and public disclosures*

Healthcare Cybersecurity / Compliance: PE PortCos

Investment Date	Sponsor	Portfolio Company	Company Type	Add-Ons	PortCo Website
Mar-12	Rezon8 Capital & Advisory Group; New Capital Partners	ControlCase	Cybersecurity, Cyber Compliance, HITRUST Assessor	**2016:** Growth Capital from New Capital Partners (n/a)	ControlCase | Global Provider of Compliance as a Service (CaaS)
Dec-16	Bluffpoint Associates	NETGAIN	Cloud Hosting, Cyber Compliance, Cyber Security	**2018**: Afinety **2018:** iManaged Solutions	Netgain Technology | Cloud Technology & Industry Experts (netgaincloud.com)
Jan-15	New Mountain Capital LLC	ACA	Cyber Compliance, HITRUST Assessor	n/a	Governance, risk, and compliance advisor in financial services | ACA Group (acaglobal.com)
Aug-21	Periscope Equity	CyberMaxx	Cybersecurity	**2022:** CipherTechs ($33mm)	CyberMaxx | Healthcare and Financial Services Cybersecurity
Jan-22	Primus	CORL technologies	Cyber Compliance	n/a	Third-Party Risk Management for Healthcare - CORL Technologies
Jan-22	Primus	Meditology Services	Cybersecurity, Cyber Compliance	n/a	Home Page - Meditology Services
Feb-21	Sheridan Capital Partners	DASHealth	Cloud Hosting, Cybersecurity RCM, Chronic Care Management	**2021:** Itelegan **2021:** Itentive Healthcare Solutions	DAS Health | Healthcare Business and IT Solutions
Dec-22	Silversmith Capital Partners; Nordic; healthvelocity Capital	Fortified Health Security	Cybersecurity, Cyber Compliance, HITRUST Assessor	n/a	Fortified Health Security | Healthcare Cybersecurity Experts

**Data per Pitchbook, MergerMarket and public disclosures*

Healthcare Cybersecurity / Compliance: Emerging Mkt.

Company	Active Investors	Description	Last Valuation Date	Last Known Valuation	Total Raised	Website
Censinet	Ballad Ventures, Cedars-Sinai, Excelerate Health Ventures, HLM Venture Partners, LRVHealth, MemorialCare Innovation Fund, Rex Health Ventures, Schooner Capital	Developer of a third-party risk management platform to manage threats that exist amongst vendors	Dec-22	$38.0	$22.3	www.censinet.com
ClearDATA	Arena Capital Partners, Excel Venture Management, Flare Capital Partners, Heritage Group, HLM Venture Partners, Humana, InnovationFund, Jeffrey Margolis, MemorialCare Innovation Fund, Merck Global Health Innovation Fund, Michael Fritz, Norwest Venture Partners, William Geary	Developer of a healthcare security and compliance platform designed to harness the untapped value of public health data	Nov-18	$216.0	$80.4	www.cleardata.com
Cynerio	Accelmed Ventures, ALIVE Israel Healthtech Fund, Consensus Business Group, Elron Ventures, IM Infinity Innonation, Menora Mivtachim, MTIP, Rafael Development Corporation, Samsung NEXT Ventures	Developer of a cybersecurity platform designed to protect clinical networks and connected medical devices	May-21	$43.0	$37.0	www.cynerio.com
HEAL Security	Health2047 Inc. UnitedHealthcare Group Venture Fund	Provider of actionable intelligence data on cyber vulnerabilities across the healthcare sector	Feb-22	n/a	$2.3	healsecurity.org
Intruno	Healthbox, Texas Medical Center	Developer of a cloud and appliance-based privacy monitoring and reporting platform built to combat cybersecurity threats	n/a	n/a	n/a	www.intruno.com

**Data per Pitchbook, MergerMarket and public disclosures*

Healthcare Cybersecurity / Compliance: Emerging Mkt.

Company	Active Investors	Description	Last Valuation Date	Last Known Valuation	Total Raised	Website
Medcrypt	Alumni Ventures, Anzu Partners, Chestnut Street Ventures, Dolby Family Ventures, Eniac Ventures, Friedman BioVentures, Grant Park Ventures, Intuitive Ventures, Johnson & Johnson Innovation - JJDC, LRVHealth, Nex Cubed, Oronoco Investments, Oslo Cancer Cluster Incubator, Safeguard Scientifics, Section 32, Sway Ventures, Wharton Alumni Angels, Y Combinator	Operator of a proactive security platform intended to protect medical devices	May-19	$19.5	$33.8	www.medcrypt.co
Medsec	Hemal Nayak	Operator of a cyber-security research company providing vulnerability research / security solutions	n/a	n/a	n/a	www.medsec.com
QIX	TEDCO	Developer of a cloud-based healthcare compliance software designed to offer comprehensive security services	n/a	n/a	n/a	www.qixsecure.com
Scope	Crossbeam Venture Partners, Free Solo Ventures, Martin Ventures, Sound Ventures, SV Angel, Thrive Capital, Vast Ventures	Developer of healthcare security platform that provides managed detection / response against cyberattacks	Mar-22	$75.0	$20.0	www.scopesecurity.com
Tausight	.406 Ventures, Flare Capital Partners, Polaris Partners	Developer of PHI security software designed to reduce healthcare cyber incidents	Feb-21	$45.0	$25.0	www.tausight.com

**Data per Pitchbook, MergerMarket and public disclosures*

Key Healthcare Cybersecurity / Compliance Takeaways

- ✓ **Targets of Threat Actors:** Cyber threats can and have targeted clinics, hospitals, ambulatory surgical centers, behavioral health organizations, dental practices and post-acute care organizations.
- ✓ **Growth Opportunities:** The industry continues to see an increase in threats and attacks which analysts estimate will lead to the industry growing from $17 billion in 2022 to $58 billion in 2030 (17.5% CAGR).
- ✓ **Top Targeted Industry:** Healthcare is now the #1 target for threat actors and is likely to continue to be an attractive target as PHI is up to 10x more valuable than financial data.
- ✓ **Highly Understaffed:** The current cyber professional shortfall of 600k is projected grow to 3.5 million by 2025.
- ✓ **Underinvestment:** Hospital and healthcare security spend is below average at 2 – 5% of IT budgets. This is particularly true of lower middle market companies that private equity is targeting. These budgets will be forced to grow in-line with threats.
- ✓ **Outsourcing:** Increasing costs and shortages of qualified staff, has made it more important than ever for healthcare organizations to outsource compliance and cybersecurity to third-party providers.
- ✓ **Diversified Service Models:** Healthcare companies are increasingly involved in several cyber and compliance service offerings to become a “one stop shop” for healthcare organizations with many types of profitable business models to pursue.
- ✓ **Variety of Cybersecurity Services:** There is a broad variety of services that cybersecurity / compliance providers can use to address each organizations needs including: GAP Analysis, Penetration Testing, Vulnerability Scanning, Phishing Detection, Forensic Analysis and Cyber Defense training amongst many others.
- ✓ **Compliance:** Organizations are required by law to adhere to HIPAA and QSR, while other compliance measures are helpful in safeguarding data but not mandatory such as HITRUST, NIST and SOC-2.
- ✓ **Increasing Regulation:** Congress, the SEC, HHS and other government agencies have identified the threat cybersecurity attacks pose to the industry and will continue to press further regulation of the industry.
- ✓ **Cybersecurity Insurance:** Is increasingly expensive and will likely continue to demand a premium vs. other industries.
- ✓ **Private Equity / Venture Capital Interest:** A growing number of investors are looking to capitalize on the attractive market trends of healthcare cybersecurity and are seeking platforms / add-ons at an unprecedented rate.

LAWRENCE, EVANS & CO., LLC

Investment Banking | Healthcare Finance | Consulting

Appendix

Mandatory Healthcare Compliance Laws

These laws and regulations are put into place to protect sensitive health information that should be safeguarded from leaks / cyberattacks. Failing to comply with the following regulations can lead to fines or criminal prosecution. Below are the most critical healthcare compliance laws.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Originally signed into effect in 1996, HIPAA aims to protect patients' sensitive health information. HIPAA compliance is mandatory for all healthcare organizations and their business associates. While HIPAA is specific to the United States, most countries have a similar equivalent. HIPAA is made up of three rules:

1) **The Privacy Rule** limits the disclosure of an individual's health data. This information gets classified as protected health information (PHI), which is protected under HIPAA. This typically includes data secured on electronic information systems, which are vulnerable to cyberthreats.
2) **The Security Rule** mandates that HIPAA-covered entities complete a risk assessment. A risk assessment is conducted by a compliance officer and is intended to find security risks within your company.
3) **The Breach Notification Rule** demands that HIPAA-covered entities notify the right channels when they've had a breach of protected health information.

QUALITY SYSTEM REGULATION (QSR)

Quality System Regulation is an FDA-led initiative to increase the cybersecurity of medical devices. **This was partially created because of ransomware attacks that shut down medical facility networks.** These attacks could cause medical devices like pacemakers, drug infusion pumps, or insulin pumps to stop functioning and harm patients.

QSR standards require medical device manufacturers to incorporate data encryption or authentication on their devices. While these standards mostly apply to medical device manufacturers, the FDA states that healthcare establishments share the responsibility. Penalties for QSR non-compliance include fines of up to $500,000 and criminal prosecution.

The risk of HIPAA violations is greatly reduced when working with a reputable assessor and bolstering patient data protection by utilizing outside cybersecurity / compliance services

**Data per Public Disclosures, Meriplex: How to Meet Healthcare Cybersecurity Regulations 2022*

Non-Mandatory Healthcare Compliance Guidelines

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBERSECURITY FRAMEWORK

The NIST framework is a voluntary set of guidelines that protects your business against cyberattacks. While NIST was originally developed as a mandatory framework for government entities, they've revised it to include non-government functions, like health and human services.

The latest NIST framework is free to adopt and has a huge variety of applications. NIST is designed to easily scale and integrate across industries, making it a great choice for any business.

HITRUST COMMON SECURITY FRAMEWORK (CSF)

The HITRUST CSF is a security framework that increases security standards in the healthcare industry. While not compulsory, it is an excellent tool that can guarantee your company passes the healthcare cybersecurity standards set by HIPAA. HITRUST is a comprehensive, globally-certifiable security program. It covers 19 different sections specific to the healthcare industry, some of which include:

Information Protection	Mobile Device Security	Network Protection
Password Management	Incident Management	Education Training and Awareness

HITRUST is the industry's compliance plan benchmark. Follow the HITRUST standards to show that your business is serious about cybersecurity. *(Refer to the following page for list of approved HITRUST assessors)*

SERVICE ORGANIZATION CONTROL 2 (SOC 2)

SOC 2 is a procedure that examines service providers (not specific to healthcare). The audit determines if a company is securely managing third-party data, like patient information, to protect information and ensure privacy. Healthcare organizations that store data on the cloud benefit from SOC 2 compliance as it reduces the threat of cyber attacks and act as a competitive differentiator. Healthcare organizations can further enhance their own cybersecurity / HIPAA compliance by also ensuring that all third-party vendors with access to patient data are SOC 2 compliant.

These healthcare regulations aren't compulsory but are effective for future-proofing an organization's cybersecurity and ongoing mandatory healthcare compliance.

**Data per Public Disclosures, Meriplex: How to Meet Healthcare Cybersecurity Regulations 2022*
Note: This list is not exhaustive of all non-mandatory guidelines, others include ISO 27001 and COBIT among many others.

Approved HITRUST Assessors

24BY7 Security	**Coalfire**	I.S. Partners LLC	PriceWaterhouse Coopers
360 Advanced	CompliancePoint	**Intraprise Health**	Protiviti
AARC-360	**ControlCase**	Jacobian Engineering	PYA, P.C.
ACA Aponix	Copeland Buhl	King & Spalding LLP	Quantum Security
Agio	Crimson Security Inc.	KirkpatrickPrice	Resiliam
A-LIGN	Crowe LLP	KPMG	Risk Analytics
Aprio, LLP	Cyberguard Compliance	KraftCPAs PLLC	Risk3 Sixty LLC
Armanino LLP	Deloitte & Touche LLP	Lark Security	RSI Security
Assure Professional, LLC	Digital Forge	Layer 8 Security	RSM US LLP
AT&T Consulting	Dixon Hughes Goodman	LBMC Security & Risk Services	Schellman & Company, LLC
Avertium	Drummond Group	Linford & Company	Secureworks
AXIA Partners	ecfirst	Lurie	Security Compliance Associates
Baker Tilly	EHNAC	The Mako Group	SecurityMetrics, Inc.
BDO	Eide Bailly LLP	Maloney + Novotny LLC	Smith & Howard
Beyond LLC	Elliot Davis	Marcum LLP	Specialized Security Services, Inc.
Blue Orange Compliance	emagine it	Meditology Services	Tanner LLC
Bonadio Group	Ernst & Young LLP	Moss Adams	TECH LOCK, Inc.
Brown Smith Wallace LLP	ESHA IT	NCC Group	Tevora
By Light Professional IT Services	Focal Point Data Risk Assurance	NTT Security	Urbane Security
The Cadence Group	Formos Consulting	Optum	Vicis Law PC
Carr, Riggs & Ingram	**Fortified Health Security**	Palindrome Technologies	Wipfli LLP
Cherry Bekaert	Frazier & Deeter	Plante Moran	Wolf & Company, PC
CliftonLarsonAllen LLP	Grant Thornton LLP	Postlethwaite & Netterville	Xpio Health

Indicates Private Equity Backing

**Data per HITRUST Alliance*

Key Pending Cybersecurity Legislation

Healthcare Cybersecurity Act of 2022

- HHS must coordinate with the Cybersecurity and Infrastructure Security Agency (CISA) must make resources, including cyber-threat indicators and appropriate defense measures, available to federal and nonfederal entities that receive information through HHS programs.
- HHS must provide training on cybersecurity risks and mitigation strategies to owners of assets in the health care and public health sector.
- HHS must update the Healthcare and Public Health Sector Specific Plan to address, among other topics, the impact of the risks on rural entities and small- and medium-sized entities, cybersecurity workforce shortages in the sector, and challenges related to COVID-19.

SEC: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

- Require registrants to disclose information about a material cybersecurity incident after it is determined that it has experienced a material cybersecurity incident.
- Require registrants to provide updated disclosure relating to previously disclosed cybersecurity incidents and to require disclosure, when previously undisclosed immaterial cybersecurity incidents has become material.
- Require organizations to determine what role is responsible for oversight of cybersecurity risk: the entire board, specific board members, or a board committee. Organizations must also disclose the processes used to communicate cybersecurity risks and the frequency of security discussions with the board.

**Data per Public Disclosures, Congress.gov, United States Securities and Exchange Commission*

Future Cybersecurity Policy Considerations

Establishing Minimum Cyber Hygiene Practices for Healthcare Organizations

- Given the risks to patient safety that result from cybersecurity intrusions, Congress may implement a requirement that all health care organizations be familiar with and apply certain minimum cybersecurity practices as standard operating procedure. This could also carry over into physical security like hospitals having emergency and standby power systems.

Addressing Insecure Legacy Systems

- The Health Care Industry Cybersecurity Task Force report recommended that government and industry develop incentive programs to phase out legacy equipment. Some have suggested that a model based on the 2009 Car Allowance Rebate System (CARS) or “cash for clunkers,” the federal program that helped take less fuel-efficient cars off the road, would be a helpful way to phase out these insecure pieces of equipment and software systems.

Safe Harbor / Immunity if Healthcare Organizations Implement Adequate Security Measures

- Congress is considering policies that encourage information sharing and encourage industry-wide learning and improvement by being encouraged to share vulnerabilities and responses. Congress may consider incentives that would provide narrowly-defined protections for health care organizations that are transparent with risks, intrusions, and their responses to both.

Cyber Insurance Measures

Cyber insurance is increasingly expensive and that the application process is extensive and sometimes burdensome. A thriving market for cyber insurance could lower overall risks by introducing minimum cyber hygiene requirements. Some proposals that have been raised include:

- Creating a federal reinsurance program that covers plans that require minimum cyber hygiene, allowing the industry to adopt a better hygiene posture without a full government mandate.
- Standardizing coverage elements and providing incentives for insurance companies to adopt them.
- Creating a cyber insurance program similar to the one created by the Terrorism Risk Insurance Act (TRIA) to create a transparent system of shared public and private compensation for certain insured losses resulting from a certified act of nation-state cyberattacks.

**Data per Senator Mark Warner: Cybersecurity is Patient Safety (November 2022)*

Health Sector Cybersecurity Coordination Center

The Health Sector Cybersecurity Coordination Center (HC3) was created by the Department of Health and Human Services to aid in the protection of vital, controlled, healthcare-related information, and to ensure that cybersecurity information sharing is coordinated across the health and public health sector.

Mission

To support the defense of the Healthcare and Public Health Sector's (HPH) information technology infrastructure by strengthening coordination and information sharing within the sector, and by cultivating cybersecurity resilience, regardless of organizations' technical capacity.

Background

HC3 was established in response to the Cybersecurity Information Sharing Act of 2015 — a federal law mandated to "improve the cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats, and for other purposes.

Sector Support

HC3's role is to work with the HPH sector to understand the threats it faces, to learn adversaries' patterns and trends, and to provide information and approaches to the sector on its defense. Additionally, HC3 facilitates access to knowledge-based resources necessary to support robust cybersecurity programs and mitigate damage in security breach situations.

Benefits

HHS partners with the HPH sector to increase awareness and foster consistency with cybersecurity practices. It allows various audiences to gain access to increased cybersecurity awareness, increases vigilance and detection for sector defense and information sharing within the HPH sector allows for an enterprise-level view of cybersecurity risk management.

Health Sector Cybersecurity Coordination Center Partnerships

Aligning Healthcare Industry Security Approaches: Develops guidelines, practices, and methodologies to strengthen the healthcare and public health (HPH) sector's cybersecurity posture against cyber threats.

Assistant Secretary for Preparedness and Response: Partners with public / private sectors to improve readiness / response capabilities.

Cybersecurity and Infrastructure Security Agency: Works to defend against threats and collaborates with industry partners to build more secure and resilient infrastructure.

Federal Bureau of Investigation: Works to protect the U.S. from cyber-attacks.

HHS Office of Inspector General: Protects the integrity of HHS programs as well as the health and welfare of program beneficiaries.

Healthcare and Public Health Sector Coordinating Council: Addresses security and resiliency challenges to the healthcare sector.

**Data per the Health Sector Cybersecurity Coordination Center*

Healthcare Compliance & Cybersecurity: Key Terms

- **APT:** Advanced Persistent Threat, a type of cyber attack in which an attacker establishes a long-term presence on a victim's network in order to steal sensitive information or disrupt operations.
- **COBIT:** Control objectives for information and related technology
- **DSS:** Data Security Standards
- **DDoS:** Distributed Denial of Service, a type of cyber attack in which a network or website is overwhelmed with traffic from multiple sources, making it unavailable to legitimate users.
- **Encryption:** The process of converting plain text into a coded format that can only be deciphered with a key. Encryption is used to protect sensitive information from unauthorized access.
- **EHR:** Electronic Health Record, which is an electronic version of a patient's medical history that is maintained by the healthcare provider.
- **Firewall:** A security system that controls access to a computer network by monitoring and filtering incoming and outgoing network traffic.
- **HIPAA:** The Health Insurance Portability and Accountability Act, which sets standards for protecting sensitive patient information.
- **HITECH:** Health Information Technology for Economic and Clinical Health Act, a federal law that provides funding and incentives to promote the adoption and meaningful use of electronic health records (EHRs) and health information exchange (HIE).
- **IAM:** Identity and Access Management, The process of managing and controlling access to computer systems and networks by ensuring that only authorized users can access sensitive information.
- **ICS:** Industrial Control Systems, which are used to control and monitor industrial processes, such as those in healthcare facilities.
- **Malware:** Malicious software (viruses, worms, and Trojans) that can damage or disrupt computer systems and steal sensitive information.
- **MCCP:** Managed Cybersecurity & Compliance Providers
- **MSPs:** Managed Service Providers
- **MSSP:** Managed Security Service Provider
- **NIST:** National Institute of Standards and Technology, which provides guidance and recommendations for cybersecurity in various industries, including healthcare.
- **Penetration Testing:** The process of simulating a cyber attack on a computer system or network in order to identify vulnerabilities and assess the effectiveness of security controls.
- **PCI:** Payment Card Industry
- **PHI:** Protected Health Information, which refers to any information about a patient's health status, treatment, or payment for healthcare services that can be used to identify the patient.
- **Phishing:** A type of social engineering attack in which bad actors pose as a trustworthy entity via phone, email, or text message in order to steal personal information from the recipient.
- **Ransomware:** Malicious software that encrypts a victim's files and demands a payment in exchange for the decryption key.
- **SOC:** Security Operations Center, a centralized location where an organization's security personnel monitor / respond to security threats.
- **Spear Phishing:** Attempts are targeted toward specific individuals or groups of individuals. They may include the recipient’s name, position, company, or other information that would set the potential victim at ease. The attacker may even claim they’re the recipient’s boss with an urgent request.
- **Two-Factor Authentication (2FA):** A security measure that requires a user to provide two forms of identification, such as a password and a fingerprint or a security token, in order to access a system or network.
- **Whaling:** Similar to spear phishing, except that it targets high-level employees, like executives or directors.
- **Smishing:** Text message version of phishing attacks. They may be targeted, like spear phishing, but they may also be more general, appearing to come from their bank or Amazon, for example

Referenced List

External Assessors Archives - HITRUST Alliance

Healthcare Data Breach Statistics (hipaajournal.com)

Healthcare Cybersecurity Market Size, Growth, Report 2022-2030 (precedenceresearch.com)

0320658680B8F1D29C9A94895044DA31.cips-report.pdf (senate.gov)

33-11038-fact-sheet.pdf (sec.gov)

2022 SMB ransomware report reveals increased cybersecurity investments | Security Magazine

soc2-ebook.pdf (hubspotusercontent20.net)

2022 Deloitte-NASCIO Cybersecurity Study

Executive Order on Improving the Nation's Cybersecurity | The White House

Censinet Report V13

https://jamanetwork.com/journals/jama-health-forum/fullarticle/2799961

https://www.precedenceresearch.com/healthcare-cybersecurity-market

Sophos: The State of Ransomware in Healthcare 2022

Bass, Berry & Sims 2023 Healthcare Private Equity Outlook & Trends

Meriplex: How to Meet Healthcare Cybersecurity Regulations 2022

Cerberus Sentinel: Cybersecurity is a Culture, Not a Product (April 2022)

MergerMarket: Under Attack Cyber Due-Dilligence

HEAL Security: Investor Presenation

Lawrence Evans & Co., LLC Overview

Lawrence, Evans & Co. LLC "LECO" is a national boutique advisory firm. LECO provides a full range of capital raising (debt & equity), mergers & acquisitions including buy-side/sell-side, as well as financial and operational restructuring services. Since 2003, we have offered advice and support for every process and structure – from short-term solutions to long-term goals. The firm caters to the **Healthcare Providers and Service Companies** (senior housing, hospital, physician services, home health, hospice, behavioral health, RCM, HCIT, CCM, RPM, SDOH, etc.), **Transportation and Logistics** (trucking, warehouse, supply-chain), **Business Services** (managed IT and cyber).

M&A Advisory *Buy-Side / Sell-Side*	**Capital Raising** *Debt / Equity*	**Turnaround & Restructuring**
▪ Private Company Sales	▪ Strategic Capital Options	▪ Turnaround Management
▪ Division / Subsidiary Divestitures	▪ Valuations & Financial Assessments	▪ Debt Restructuring / Refinancing
▪ Buy-side search for proprietary	▪ Bridge Financing, Real Estate, Bonds	▪ Orderly Liquidations
▪ Acquisition Advisory Services	▪ Private Equity, Family Office	▪ Chief Restructuring Officer (CRO)
▪ Private Market Financings	▪ Lines of Credit, Senior Debt	▪ Bankruptcy Planning / 363 Sales
▪ LBO's and Recapitalizations	▪ Debt Mezzanine, Unitranche	▪ Receivership / Trustee

Select Transactions

Contact Us

Neil Johnson
Managing Partner

Email
njohnson@lawrenceevans.com

Phone
(614) 448-1304

Address
88 E Broad St, Suite 1750
Columbus, OH 43215