The Governance Institute presents

Managing Cybersecurity Risk in America's Hospitals: A Leadership Imperative

June 15, 2023 | 2:00–3:00 p.m. Eastern

presented by

Steve Cagle, M.B.A., HCISSP, CEO, Clearwater

and

Jim Brady, Ph.D., CHCIO, CDH-E, CISM, CRISC, CISSP, QTE, FHIMSS, FCHIME
Vice President, Cybersecurity & Risk Management and CISO,
M Health/Fairview

Today's Presenters

Steve Cagle, M.B.A., HCISSP
CEO, Clearwater

- Leader of firm recognized as healthcare's top security advisors & consultants and top compliance & risk management solution
- Former CEO, Moberg Pharma North America
- Former CEO, Alterna LLC
- Former Executive & Principal, Sparta Systems, Inc.
- 20+ years B2B software & professional services, pharmaceuticals
- B.S., Finance, Rutgers Business School
- M.B.A., NYU Stern School of Business

Today's Presenters

Jim Brady, Ph.D., CHCIO, CDH-E, CISM, CRISC, CISSP, QTE, FHIMSS, FCHIME
Vice President, Cybersecurity & Risk Management and CISO, M Health/Fairview

- Leads M Health/Fairview's Cybersecurity, Governance, Risk, and Compliance, Service Delivery, Network, Unified Communications, End User Services, and Computer, Cloud, Storage, and Database teams
- Independent Corporate Boardroom Certified Qualified Technology Expert
- Former CIO, Los Angeles County Department of Health Services
- Former CIO, Kaiser Permanente Orange County
- Former CISO, Hawaii Health Systems Corporation
- Former Enterprise Information Systems Services Manager, Cedars-Sinai Health System

Learning Objectives

After viewing this Webinar, participants will be able to:

Identify the connection between cyberattacks and patient safety in hospitals

Define reasons why cybersecurity has become a critical business risk.

Describe actions senior leaders and boards can take to manage cybersecurity risk at the enterprise level

Continuing Education

Continuing education credits available

IPCE CREDIT™

In support of improving patient care, The Governance Institute, a service of National Research Corporation, is jointly accredited by the Accreditation Council for Continuing Medical Education (ACCME), the Accreditation Council for Pharmacy Education (ACPE), and the American Nurses Credentialing Center (ANCC) to provide continuing education for the healthcare team. This activity was planned by and for the healthcare team, and learners will receive 1 Interprofessional Continuing Education (IPCE) credit for learning and change.

AMA: The Governance Institute designates this live activity for a maximum of ***1 AMA PRA Category 1 Credit(s)™***. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

ACHE: By attending this Webinar offered by The Governance Institute, a service of National Research Corporation, participants may earn up to **1 ACHE Qualified Education Hour** toward initial certification or recertification of the Fellow of the American College of Healthcare Executives (FACHE) designation.

Criteria for successful completion: Webinar attendees must remain logged in for the entire duration of the program. They must answer at least three polling questions. They must complete the evaluation survey in order to receive education credit. Evaluation survey link will be sent to all registrants in a follow-up email after airing of the Webinar.

CPE: The Governance Institute is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its Web site: www.nasbaregistry.org.

NATIONAL REGISTRY OF CPE SPONSORS

In accordance with the standards of the National Registry of CEP Sponsors, CPE credits will be granted based on a 50-minute hour.
Field of study: Business Management & Organization
Program level: Overview
Prerequisites: None
Advanced preparation: None
Delivery method: Group Internet based
Maximum potential CPE credits: 1

Disclosure Policy

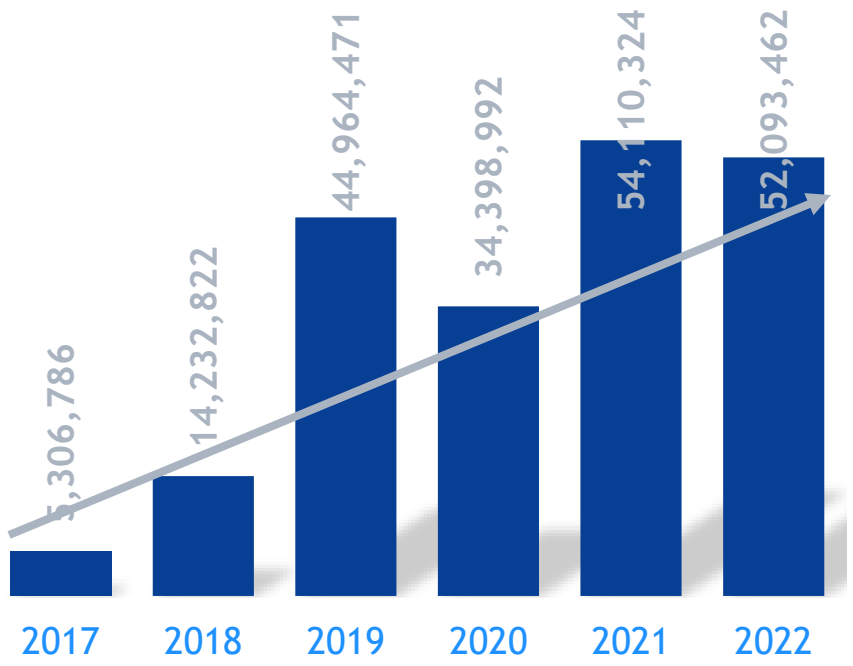
- As a Jointly Accredited Provider, The Governance Institute's policy is to ensure balance, independence, objectivity, and scientific rigor in all of its educational activities. Presentations must give a balanced view of options. General names should be used to contribute to partiality. If trade name are used, several companies should be used rather than only that of a single company. All speakers, faculty, moderators, panelists, and staff participating in The Governance Institute conferences and Webinars are asked and expected to disclose to the activity audience any financial relationships within the prior 24 months with a company ineligible for accreditation as defined by the Joint Accreditation Interprofessional Continuing Education Standards for Integrity and Independence in Accredited Continuing Education and any real or apparent conflict(s) of interest that may have a direct bearing on the subject matter of the continuing education activity. The potential for conflicts of interest exists when an individual has the ability to control or influence the content of an educational activity **and** has a financial relationship with an *ineligible company*. Ineligible companies are organizations that are not eligible for accreditation whose primary business is producing, marketing, selling, re-selling, or distributing healthcare products used by or on patients. Significant financial interest or other relationships can include such thing as grants or research support, employee, consultant, major stockholder, member of the speaker's bureau, etc. the intent of this policy is not to prevent a speaker from making a presentation instead, it is The Governance Institute's intention to openly identify any potential conflict so that members of the audience may form his or her own judgements about the presentation with the full disclosure of the facts.
- It remains for the audience to determine whether the presenters outside interests may reflect a possible bias in either the exposition or the conclusion presented. In addition, speakers must make a meaningful disclosure to the audience of their discussions of off-label or investigational uses of drugs or devices.
- All faculty, moderators, panelists, staff, and all others with control over the educational content of this Webinar have signed disclosure forms. The planning committee members have no conflicts of interests or relevant financial relationships to declare relevant to this activity.
- This educational activity does not include any content that relates to the products and/or services of a commercial interest that would create a conflict of interest. There is no commercial support or sponsorship of this conference.
- None of the presenters intend to discuss off-label uses of drugs, mechanical devices, biologics, or diagnostics not approved by the FDA for use in the United States.

Discussion Flow

1. **Healthcare Cybersecurity Trends & Effect on Patient Safety**
2. Learnings from M Health Fairview's Cyber Risk Management Program
3. The Board's Role in Cybersecurity, Liabilities, and Other Considerations
4. Q&A

Healthcare Cyber Landscape: A Perfect Storm

Healthcare records breaches



Key factors

- Growing attack surface
- Highly valuable data
- Highly targeted (109 current threat actors targeting healthcare)
- Low level of maturity
- Limited resources

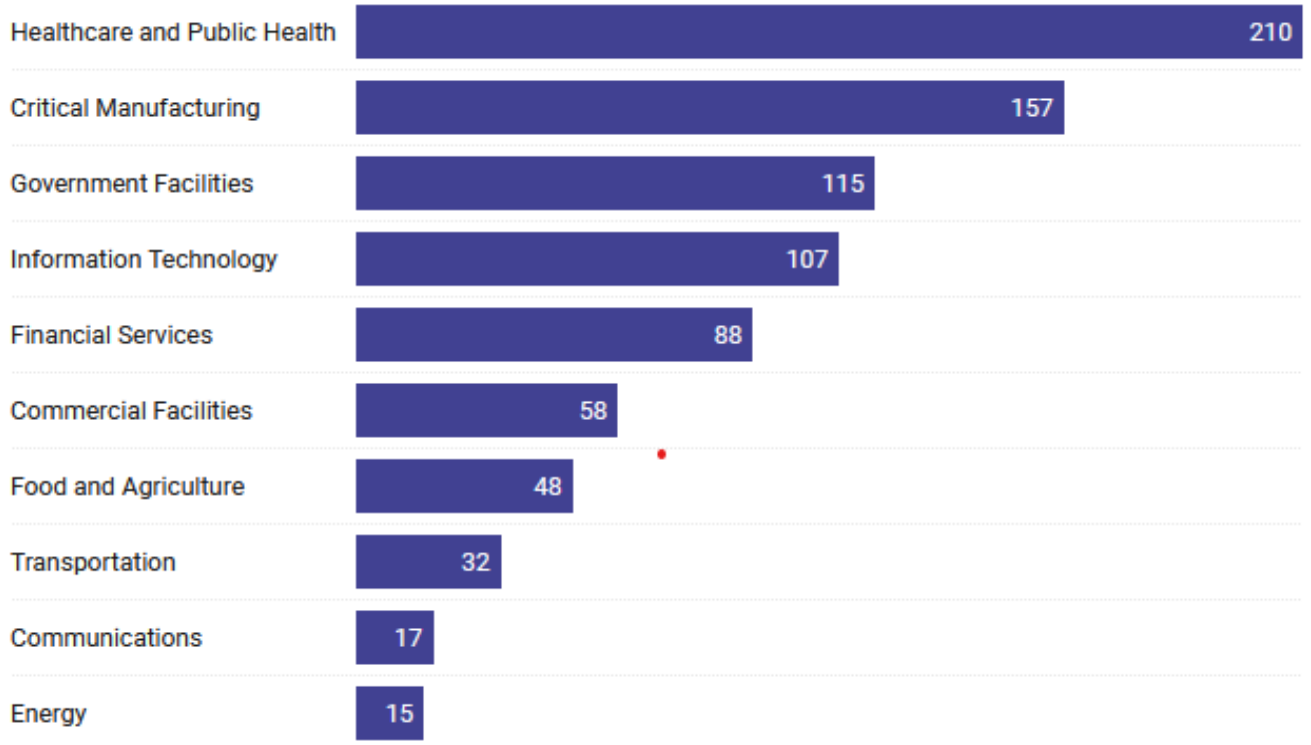
Ransomware: Increasing Risk to Healthcare Organizations

According to the FBI, **healthcare is the most targeted** industry for ransomware attacks of all critical infrastructure industries.[1]

The number of **ransomware attacks on healthcare has doubled** in the past five years.[2]

Health sector hardest hit in ransomware targeting critical infrastructure

Number of ransomware infections in 2022, by sector



1 Federal Bureau of Investigation Internet Crime Report 2022. Internet Crime Complaint Center.

2 Hannah T. Neprash, Ph.D., Claire C. McGlave, M.P.H., and Dori A. Cross, Ph.D., et al., "Trends in Ransomware Attacks on U.S. Hospitals, Clinics, and Other Health Care Delivery Oranizations, 2016-2021," *JAMA Health Forum.* 2022; 3(12):e224873. doi:10.1001/jamahealthforum.2022.4873.

Chart: Matt Kapko/Cybersecurity Dive; source: FBI. Created with Datawrapper.

Recent Ransomware Events

Reported May 4

Tennessee health system stops all operations amid cyberattack recovery

Jessica Davis May 4, 2023

Murfreesboro Medical Clinic & SurgiCenter was forced offline after a cyberattack. (Adobe Stock Images)

Reported May 12

Staten Island Hospital operating in network downtime amid ransomware attack

Jessica Davis May 12, 2023

Richmond University Medical Center's main campus in Staten Island, New York. The center is one of several healthcare facilities currently attempting to fully restore services in the wake of a cyber attack. (Credit: Richmond University Medical Center)

Reported May 23

Cyberattack on Norton Health spurs long waits, prescription and lab delays

Jessica Davis May 23, 2023

A cyberattack at Norton Healthcare in Louisville, Ky., is leading to pharmacy and lab delays. (U.S. Air Force)

[Tennessee health system stops all operations amid cyberattack recovery | SC Media (scmagazine.com)]

[Cyberattack on Norton Health spurs long waits, prescription and lab delays | SC Media (scmagazine.com)]

Cybersecurity IS Patient Safety

2021: CISA reported ransomware causes worsened health outcomes as measured in **excess deaths** due to disruption. [1]

2022: Of all providers who had a ransomware attack, **22% reported increased in mortality rates** following the attack.[2]

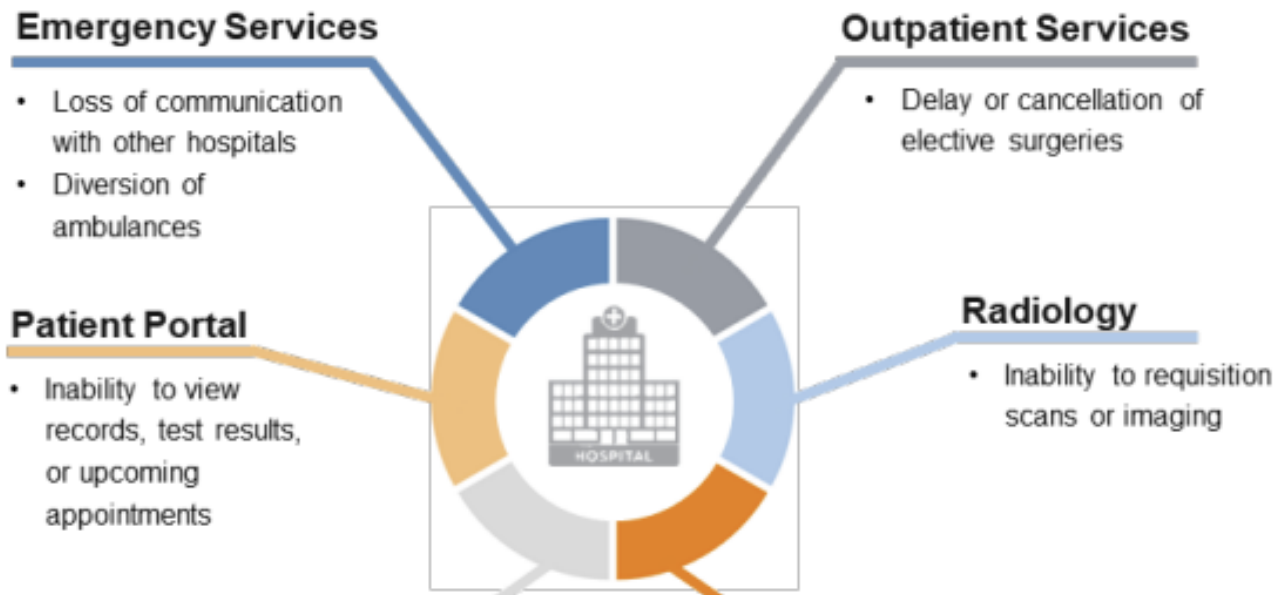
2023: A recent JAMA study found hospitals adjacent to others affected by ransomware attacks may see disruptions in patient care and **risks to increased mortality**.[3]

2023: FBI and DOJ now treating patient cyber-attacks as **"threat to life"** crimes. [4]

1 *Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm,* Cybersecurity and Infrastructure Security Agency (CISA), September 2021.
2 Kevin Collier, "Cyberattacks Against U.S. Hospitals Mean Higher Mortality Rates, Study Finds," *NBC News,* September 8, 2022.
3 Christian Dameff, M.D., M.S., et al., "Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the U.S.," *JAMA Network Open,* 2023; 6(5):e2312270.
4 *Hospital Resiliency Landscape Analysis,* Healthcare and Public Health Sector Coordinating Council, Office for Civil Rights, Centers for Medicare and Medicaid Services, and HHS 405(d) Working Group, Joint Publication, March 2023.

Cybersecurity IS Patient Safety

Hospital System Services and Departments Disrupted by Cyber Attack



Polling Question #1

A key factor in the increase in cyberattacks is:

a. Insurance companies are increasing insurance coverage with lower premiums
b. Rapid expansion of the attack surface
c. FBI recommends to pay ransom
d. None of the above

Discussion Flow

1. Healthcare Cybersecurity Trends & Effect on Patient Safety
2. **Learnings from M Health/Fairview's Cyber Risk Management Program**
3. The Board's Role in Cybersecurity, Liabilities, and Other Considerations
4. Q&A

Polling Question #2

Ransomware causes increased patient safety risk, and is associated with increased mortality rates due to:

a. Ambulance diversion to other hospitals, which delays emergency care
b. Delayed or reduced quality of treatment due to lack of patient data or ability to have tests performed
c. Reduced capacity at other adjacent medical facilities due to overflow
d. All of the above

Polling Question #3

Is your board informed of risks that exceed its threshold?

a. Yes – on an ongoing basis
b. Yes – annually
c. Yes – sporadically
d. No

Discussion Flow

1. Healthcare Cybersecurity Trends & Effect on Patient Safety
2. Learnings from M Health Fairview's Cyber Risk Management Program
3. **The Board's Role in Cybersecurity, Liabilities, and Other Considerations**
4. Q&A

Critical Tasks for the Board

- Establish a culture of cybersecurity
- Set your appetite for cyber risk
- Discuss and prioritize your unique high risks
- Ensure resources for your cybersecurity and resiliency program

Additional Liabilities and Concerns

- Healthcare is the most expensive industry to have a breach ($10.1M average cost, per the latest Ponemon Institute study).
- Cyber insurance premiums are increasing and may not cover the cost of a major incident.
- Class action lawsuits are increasing in number and size.
- Enforcement action is now more commonly occurring with State Attorney Generals and the FTC, as well as through HHS OCR.
- New cyber incident reporting requirements for critical infrastructure owners as required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).
- SEC proposed rules requiring cyber incident reporting and cybersecurity program disclosures.

Polling Question #4

Boards should engage on which of the following regarding cyber risk management:

a. Conducting assessments of the organization's cybersecurity program
b. Making decisions on which technical controls to implement
c. Determining the organization's risk appetite and authorizing the leadership team to respond to risks above the threshold
d. Reviewing and approving specific security operating procedures

Final Thoughts

- Healthcare will continue to be highly targeted by threat actors.
- Cyberattacks are a top business and patient safety risk for all healthcare organizations.
- Some organizations have responded well and, as a result, avoided devasting attacks.
- The board plays a crucial role in setting the tone for the organization's cyber risk management strategy.

Questions & Discussion

Contact Us…

Steve Cagle
CEO
Clearwater
steve.cagle@clearwatersecurity.com

Jim Brady
VP Cybersecurity & Risk Management and CISO
M Health/Fairview
jim.brady@fairview.org

The Governance Institute
1245 Q Street
Lincoln, NE 68508
(877) 712-8778
Info@GovernanceInstitute.com