Cybersecurity for CMIOs

AMDIS 2024

Eric M. Liederman, MD, MPH, FACP, FHIMSS

CEO, CyberSolutionsMD, LLC
Former National Leader of Privacy, Security & IT Infrastructure
Kaiser Permanente

Christian Dameff, MD, MS

Medical Director for Cybersecurity
C0-Director UCSD Center for Healthcare Cybersecurity
UC San Diego

“There are two types of companies:
those that have been hacked,
and those who don't know they have been hacked.”

John T. Chambers

Cybersecurity in Healthcare

The realities of healthcare IT's complexities, "not to mention the extremely time-poor staff that need both maximum convenience and security from IT operations," make it hard for the industry to protect itself

Devon Ackerman, Global head of incident response and cyber risk, Kroll
The State of Cyber Defense: Diagnosing Cyber Threats in Healthcare April 2024

Healthcare's Digital Transformation

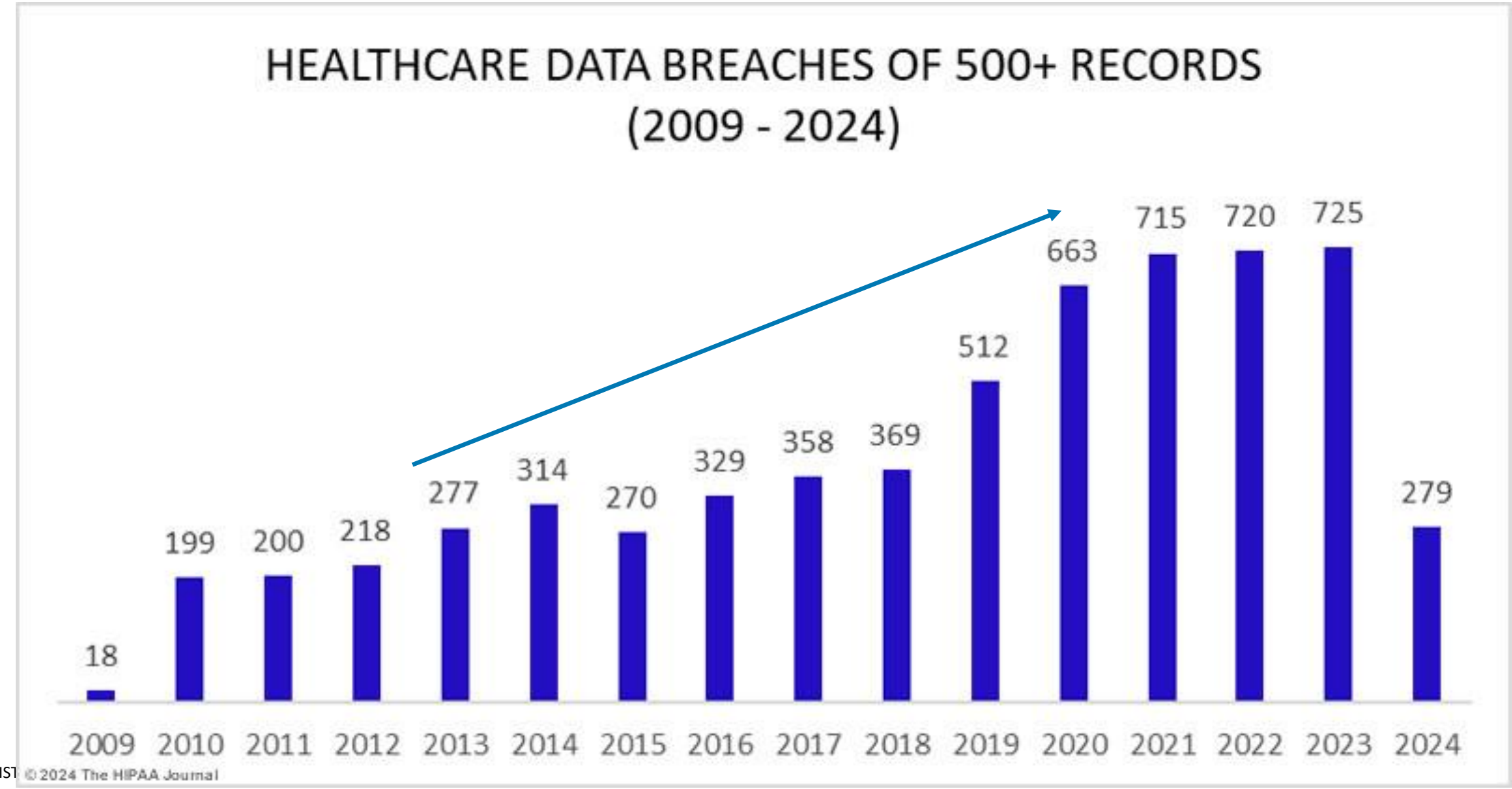
Rapid advancement in telemedicine, wearables, secure electronic messaging, and cloud/internet-hosted services.
With new digital tools, comes increasing reliance on cybersecurity.

The Threat is Increasing

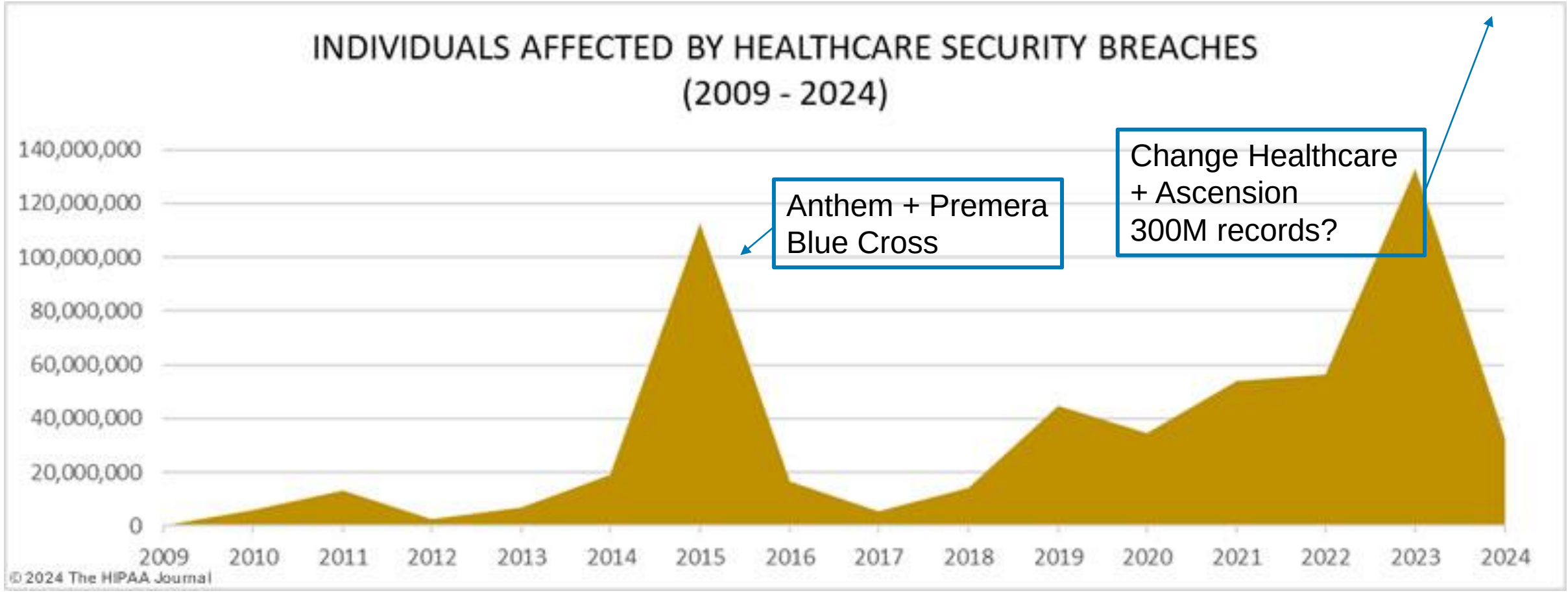
With the emergence of ransomware, denial of service and extortion schemes, the threat of business disruption and the loss of patient privacy is at an all-time high.

Healthcare **remains** a top target for cybercriminals

Healthcare Hacking Over Time



Healthcare Breaches Over Time



Healthcare Breach Impacts

From the Ponemon Institute: Cyber Insecurity in Healthcare 2023

88% of organizations had 1 or more cyber attacks in the past 12 months

37% experienced ransomware attacks that disrupted care

37% experienced BEC attacks that disrupted care

49% experienced supply chain attacks that disrupted care

Cybersecurity Threat Actors

	CYBER CRIME AS A SERVICE	ORGANIZED CRIME
Motive	Financially motivated, paid % of profit	Financially motivated
Characteristics	**Allows others to rent infrastructure** for attacks: botnets, phishing tools, and vulnerability scanning of targets	Aim to **collect ransom, personal data, including medical records, credit cards and social security numbers** Typically have an **industry focus** Efficient, **profit-focused quick attacks** with **high return on investment** Increasing sophistication using denial of service **ransomware**

Cybersecurity Threat Actors

	STATE-SPONSORED	HACKTIVISTS
Motive	Research, espionage and **sensitive proprietary information**	Motivated by social justice causes to seek confidential information to **defame or damage an enterprise**
Characteristics	**Highly-skilled** and **highly-persistent** groups with **unlimited resources** Employ **sophisticated and previously unknown methods** (e.g., custom malware, wipeware) Pursue and achieve **specific objectives** Maintain a **low profile** to cover their tracks and remain in the network for months, if not years	**Unstructured** coalitions of individuals that come together based on **common cause** Rely on **social engineering** techniques Employ **less sophisticated** attack methods due to resource limitations Engage **armies of infected computers** available in the dark web

Threat Vectors

Social Engineering	Exploiting human nature	Email phishing, spear phishing and whaling; telephone and in person fraudulent representations
Internet Surfing	Malware-laced Internet pages, links & downloads	“Drive-by” and hidden malware
Credential Theft	Exploiting stolen user IDs & passwords	Elevated access accounts (system and database administrators, report writers) present greatest risk

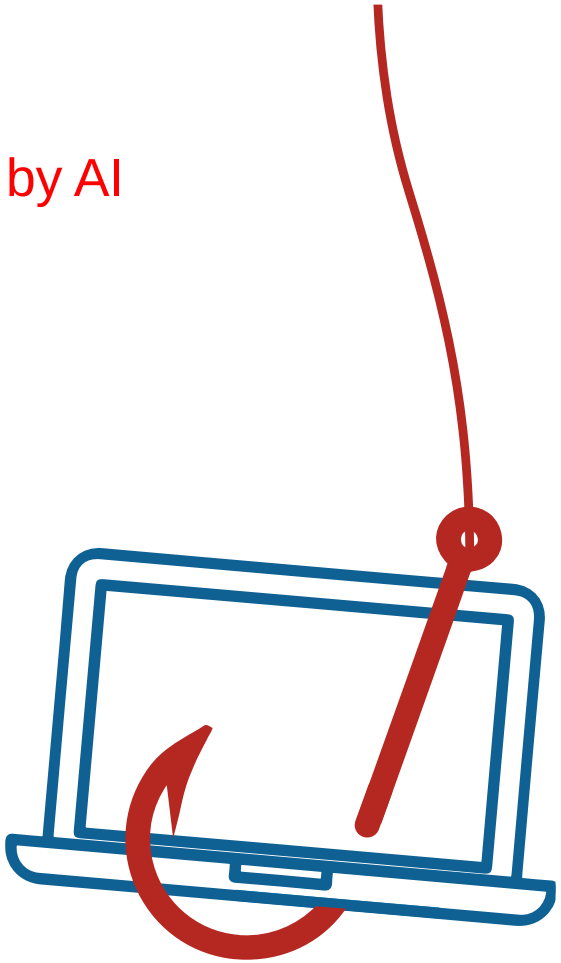
Threat Vectors

Network	Disrupt network traffic, or breach network	Movement to the cloud expands paths attackers can take, and Denial of Service attacks are challenging to prevent
Software bugs	Software bugs, and unpatched systems	Provide breach entry points. Requires ongoing work to keep versions up to date and to apply patches across complex enterprises
Configuration errors	Systems with configuration errors	Requires constant testing and assessment of applications and infrastructure. Biomedical devices are a special challenge

Social Engineering Threats

- **Phishing campaigns**
  - Mass emails from “your bank”
  - Targeted emails from “your boss” (spear phishing)
  - Senior executive targeting – a “subpoena” (whaling)
  - “Angler phishing” is a new tactic where criminals register fake social media accounts that masquerade as customer support accounts
    - They monitor real support accounts for irate customer messages and then quickly jump in to send messages back to those users, loaded with malicious links

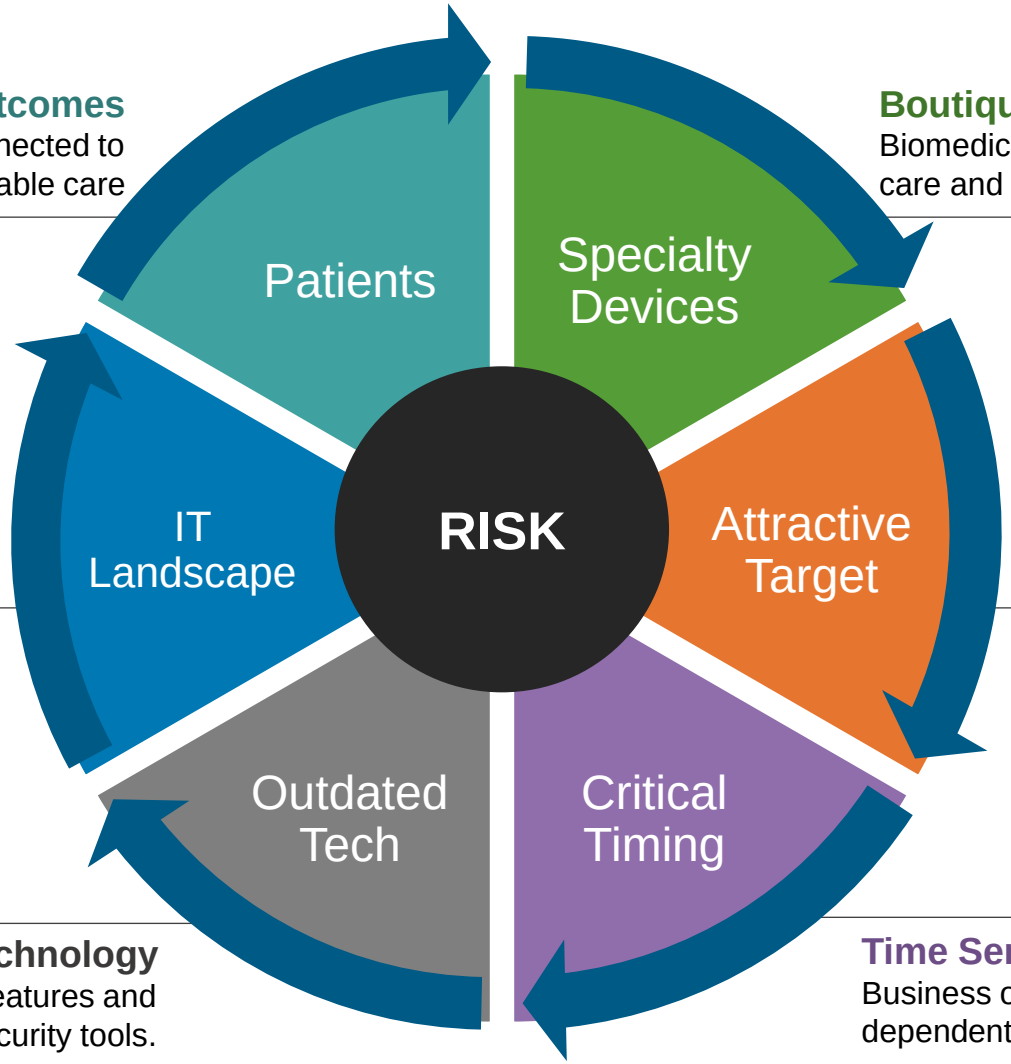
Supercharged by AI



- **Imposter domains**
  - Appear to be legitimate websites

- **Phone calls**
  - From “the Help Desk” or “Microsoft” telling you your computer has been infected and they need to remote in to fix it.

The Complicating Factors for Healthcare Cybersecurity



Patient Outcomes
Technology intimately connected to patients for sustainable care

Boutique Clinical Technology
Biomedical devices for accessibility, home care and telehealth functions.

Complex IT Ecosystem
Combination of on-site and virtual applications, platforms and devices.

High Attacker Interest
Provides high pay out opportunities for cybercriminals.

Legacy Technology
Medical devices which may lack modern features and compatibility with traditional cybersecurity tools.

Time Sensitive Operations
Business operations and speed requirements vary dependent on the healthcare delivery focus

Clinical and Operational Impacts of Cyber Attacks

Direct Impacts

- Back to 1996
  - Pen and paper (except no charts or chart rooms)
  - No patient data, including appointments
  - No communications except cell phones (and no on call directories)
  - No results routing (except by runners and vacuum tubes)
  - Impaired lab and radiology throughput

- Financial hits
  - Paper (or no) billing
  - Impaired payroll processing
  - Diverted patients

- Typically 4-6 weeks to EHR restoration, 3-6 months to full restoration

Cyber Blast Radius

JAMA Network | Open™

Original Investigation | Emergency Medicine

Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US

Christian Dameff, MD, MS; Jeffrey Tully, MD; Theodore C. Chan, MD; Edward M. Castillo, PhD, MPH; Stefan Savage, PhD; Patricia Maysent, MHA, MBA; Thomas M. Hemmen, MD, PhD; Brian J. Clay, MD; Christopher A. Longhurst, MD, MS

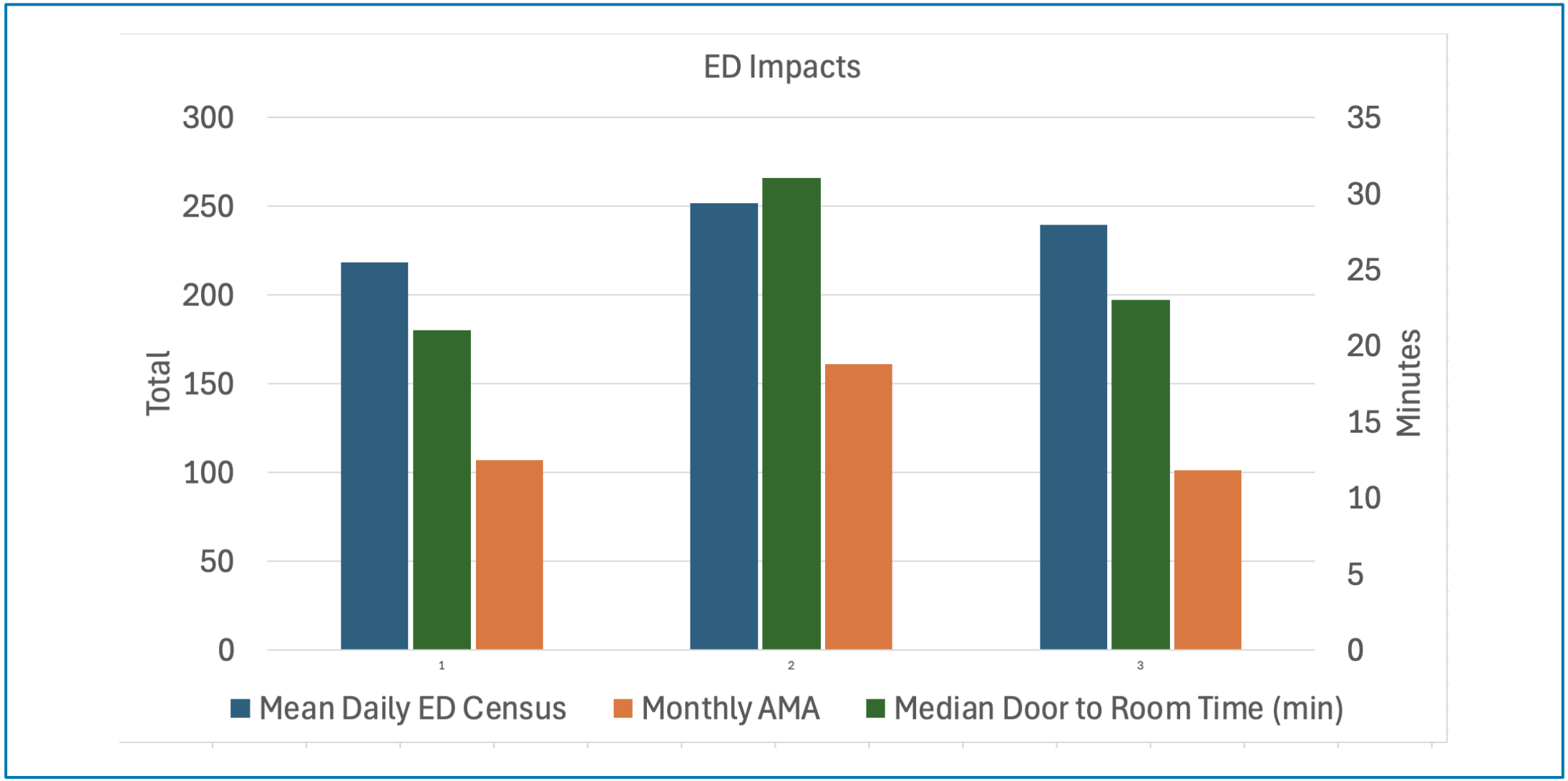
Abstract

IMPORTANCE Cyberattacks on health care delivery organizations are increasing in frequency and sophistication. Ransomware infections have been associated with significant operational disruption, but data describing regional associations of these cyberattacks with neighboring hospitals have not been previously reported, to our knowledge.

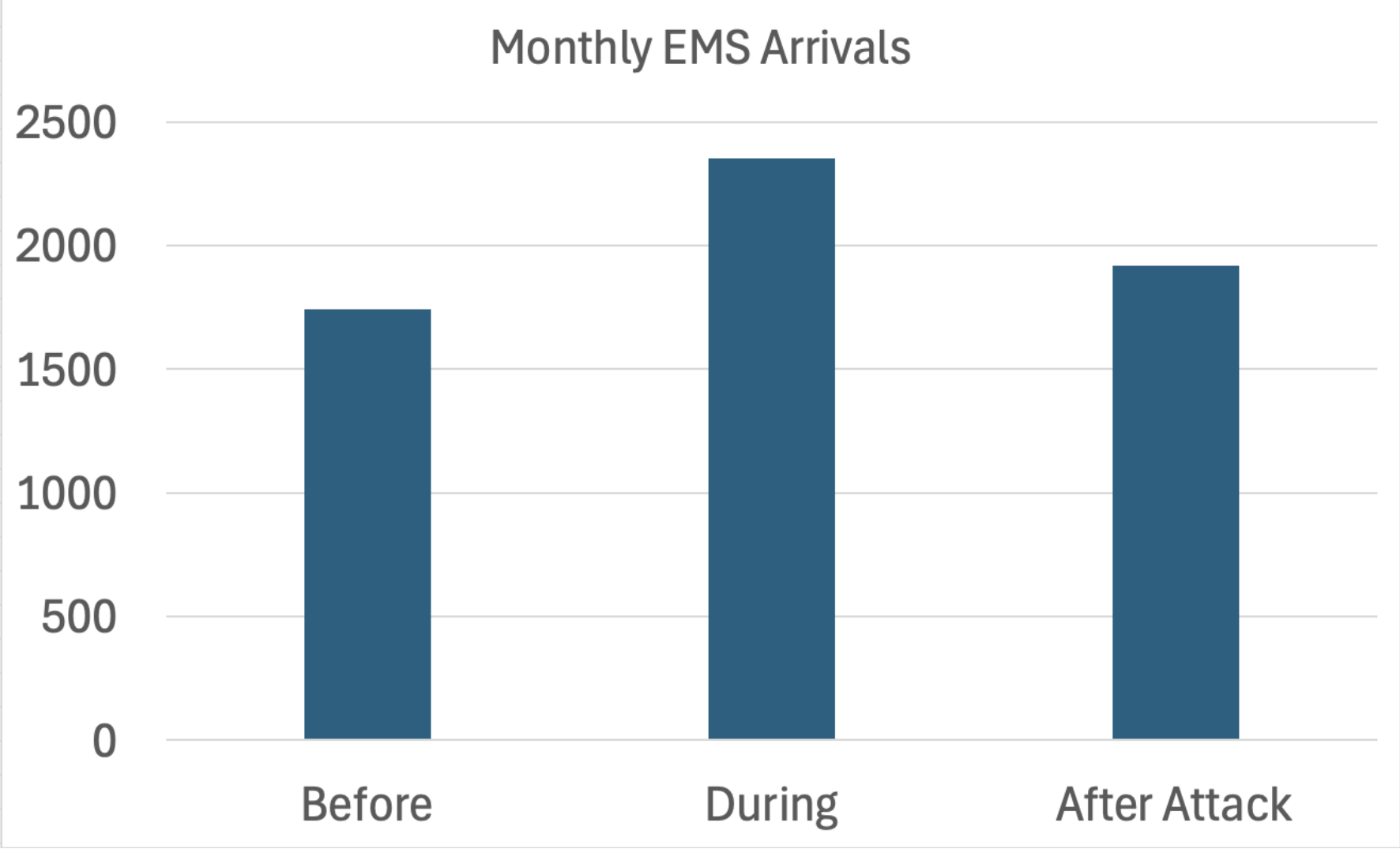
Key Points

Question What are the associated regional health care disruptions in hospitals adjacent to health care systems under ransomware cyberattack?

Finding: Emergency Care Was Significantly Impacted

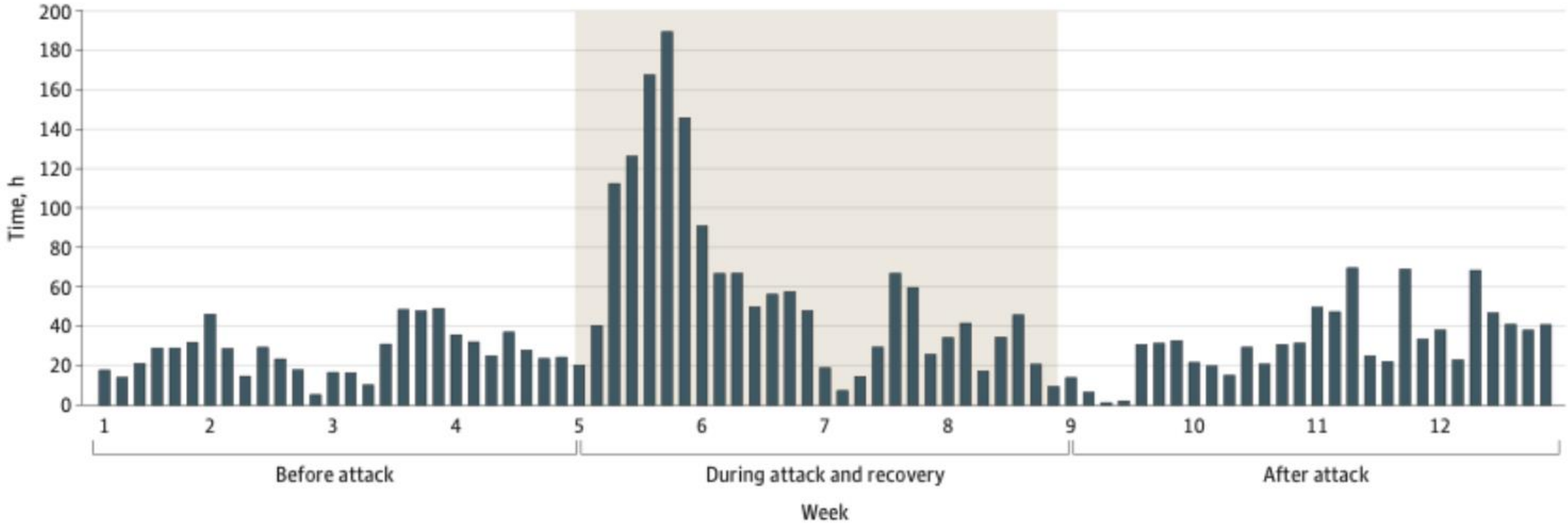


Finding: Prehospital Care Was Significantly Disrupted

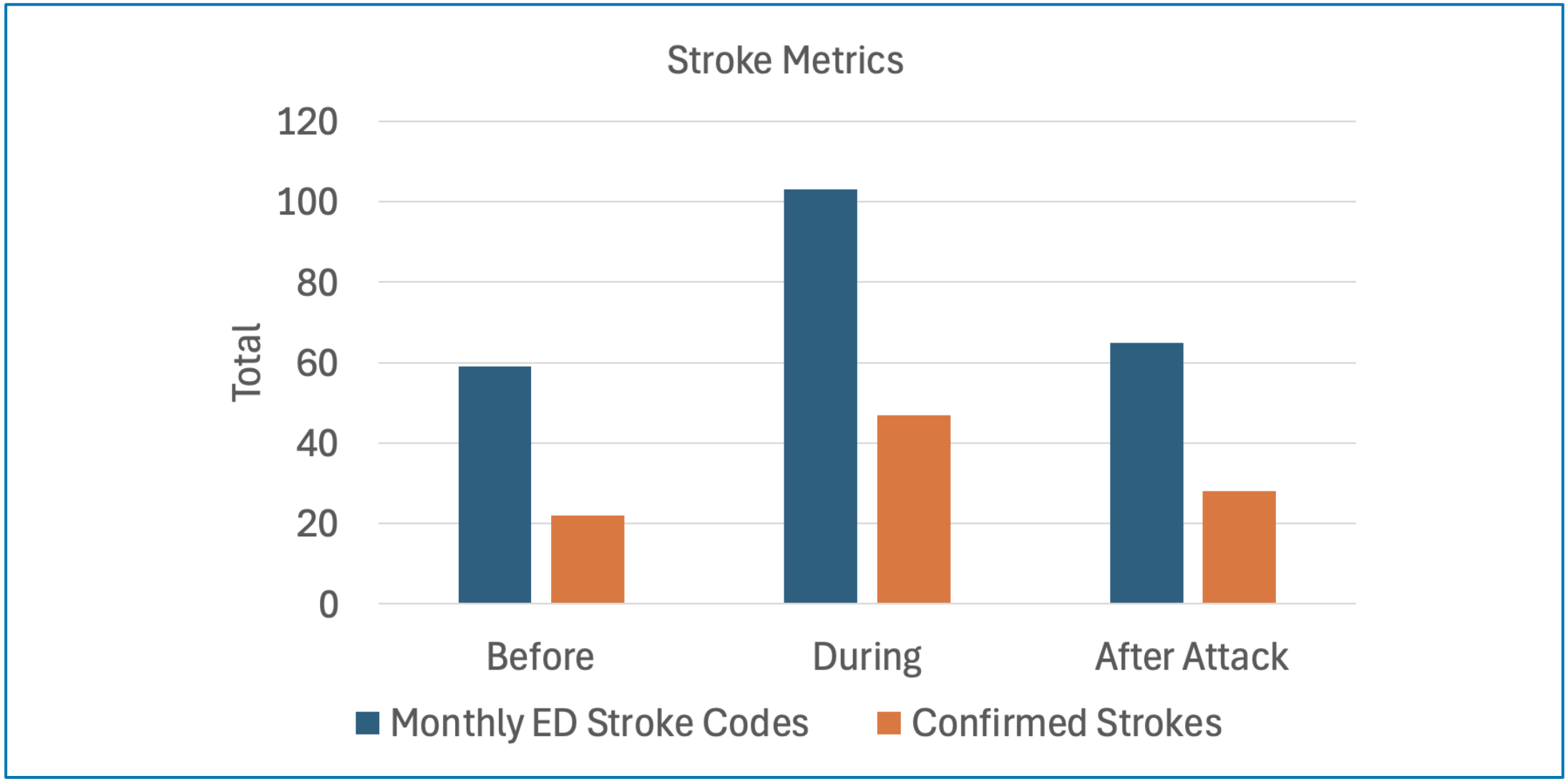


Finding: Prehospital Care Was Significantly Disrupted

Figure 2. Cumulative San Diego County Emergency Medical Services Diversion Hours Per Day



Finding: Very Sick Stroke Patients Flooded Neighboring Hospitals



Patient Outcomes

Critical Care Explorations

Society of Critical Care Medicine
The Intensive Care Professionals

Crit Care Explor. 2024 Apr; 6(4): e1079.
Published online 2024 Apr 10. doi: 10.1097/CCE.0000000000001079

PMCID: PMC11008621
PMID: 38605720

Ransomware Cyberattack Associated With Cardiac Arrest Incidence and Outcomes at Untargeted, Adjacent Hospitals

Thaidan T. Pham, MD,[1] Theoren M. Loo, MS,[2] Atul Malhotra, MD,[3] Christopher A. Longhurst, MD, MS,[4,5] Diana Hylton, MD,[6] Christian Dameff, MD, MS,[4,7,8] Jeffrey Tully, MD,[6] Gabriel Wardi, MD, MPH,[3,7] Rebecca E. Sell, MD,[9] and Alex K. Pearce, MD[3]

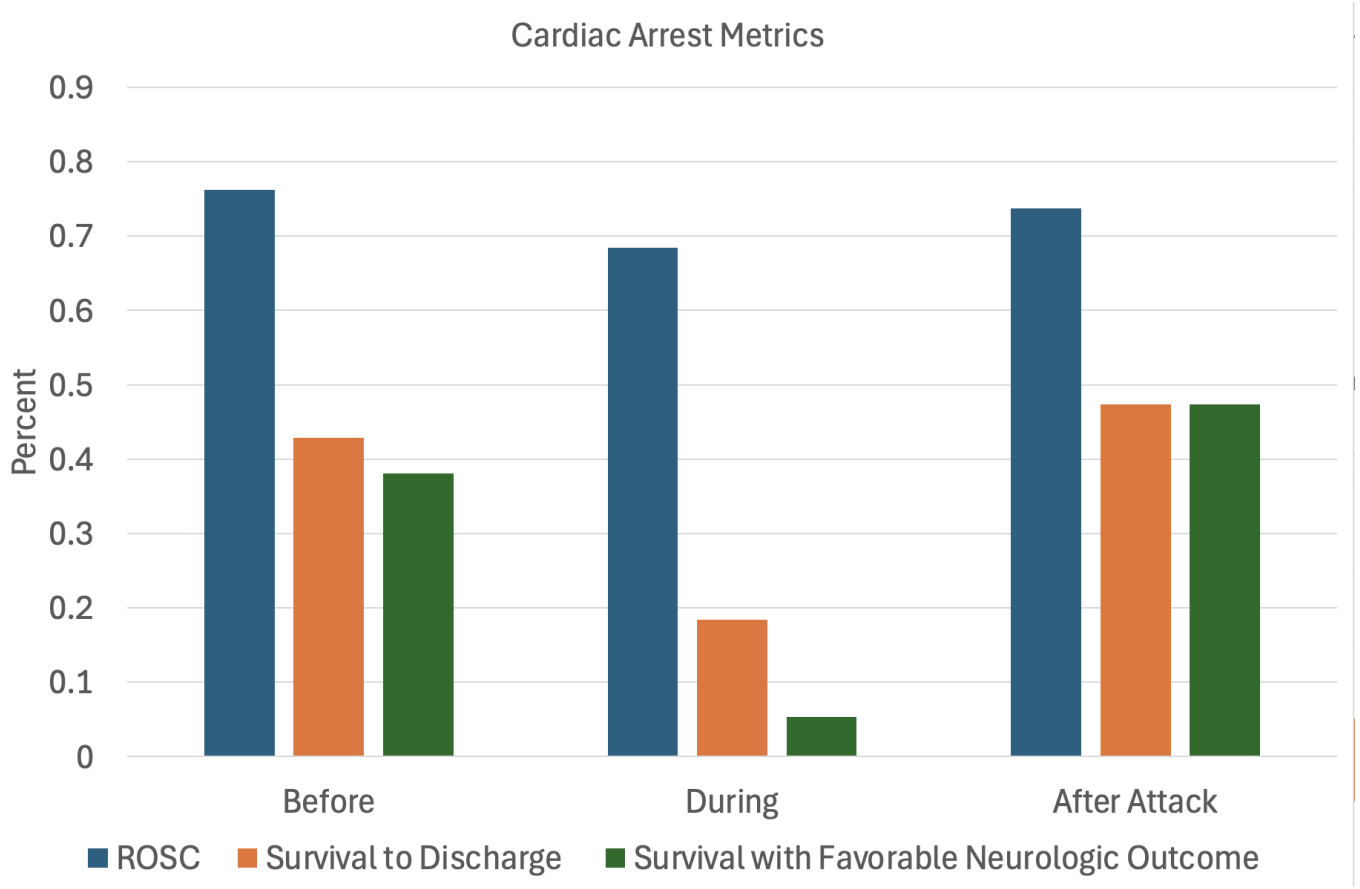
Cardiac Arrest Outcomes Next to Ransomware

KEY POINTS

Question: Are ransomware cyberattacks on healthcare delivery organizations (HDOs) associated with increased cardiac arrest (CA) incidence and adverse outcomes at adjacent untargeted hospitals?

Findings: This cohort study of two untargeted academic hospitals adjacent to an HDO under a month-long ransomware cyberattack evaluated 78 CAs: 21 during pre-attack, 38 during attack, and 19 during post-attack phases. During the attack phase, decreases in survival with favorable neurologic outcome were observed.

Meaning: This study suggests cyberattacks are associated with worse outcomes for patients suffering from out-of-hospital CA at untargeted, adjacent hospitals, highlighting the critical need for cybersecurity disaster planning and regional healthcare systems resiliency.



Examples of Risk Flashpoints

Password Length	Password Rotation	Multifactor Authentication	Account Lockout Thresholds	Application and Website Blocks
Geofencing	Filetype Blocks	Website Isolation	Use of Personal Devices	Security “UI” Experience
Resiliency & Restoration Prioritization	Data Loss Prevention (DLP)	Incident Response Coordination	Cyber Training Requirements	Phishing Campaigns

Contrasting Perspectives

CISO Extreme

Threat Focused

Technology Driven

Incentivized to drive cyber risk as low as is possible – even at the expense of usability, and therefore patient risk

+

Care Delivery Extreme

Patient Focused

Concerned about stability, user experience

Incentivized to keep availability and usability high – even at the expense of security

Where are you?

Controls are implemented which impede care delivery, increasing healthcare risk

Needed controls are held back from implementation for fear of impeding care delivery, which increases organizational cyber risk

How to  the Gap

- Develop organizational Cybersecurity governance
- Foster relationships between clinical, operational and Cyber leaders
- Jointly assess Cybersecurity maturity and gaps
- Develop holistic plans to close gaps systematically
- Jointly develop decision pathways for Cybersecurity events and crises
- Plan and schedule regular Cyber exercises
- Assess and improve “right of bang” Cyber resilience and recovery capabilities

Sample Governance Model

Executive Sponsors

CEO, Chief Legal Officer, CISO, CIO, Head of Human Resources,
Chief Compliance Officer, Physician Leader, Government Relations

Steering Committee

CISO, IT Operations Executive, Chief Digital Officer, Human Resources, Physician leads for Privacy, Security, and Informatics, IT Finance, Care Delivery IT, Operations leader(s)

Specialty Governance Forums For:

Countermeasures
Privacy Monitoring (Insider Threat)
Biomedical Technology Devices
Cloud Technologies
Data Governance
HIPAA, PCI, and Third-Party Assurance
Red Team and Penetration Testing

Examples of Risk Resolution

Password Length Data driven	Password Rotation None*	Multifactor Authentication Everywhere*	Account Lockout Data Driven	Application/ and Website Blocks Joint decisions
Geofencing Joint decisions	Filetype Blocks Joint decisions	Website Isolation Allows personal mail	Use of Personal Devices Yes*	Security “UI” Experience Customer feedback
Resiliency & Restoration Prioritization Led by operations	Data Loss Prevention (DLP) Joint effort	Incident Response Coordination Playbooks	Cyber Training Requirements Joint decisions	Phishing Campaigns Suportive, not punitive

Benefits of Joint Governance Approach

Approach

- Joint business-cyber sponsorship
- Co-development of risk strategy
- Partnership and trust-building
- Diversity of thought
- Cross-functional networking

Benefits

- ☑ Increased dialogue and reduced friction between business and cyber
- ☑ Better outcomes with more workable solutions
- ☑ Reducing cyber risk without increasing patient care risk
- ☑ Improved crisis-response
- ☑ Faster implementation of controls & patches
- ☑ Reduced career risk

Eric Liederman, MD, MPH
CyberSolutionsMD
CyberSolutionsMD@gmail.com

Christian Dameff, MD, MS
UC San Diego
CENTER FOR HEALTHCARE CYBERSECURITY
cdameff@health.ucsd.edu