

ENSURING DATA SYSTEM REILIABILITY, RESILIENCE, AND INTEROPERABILITY

Christian Dameff, MD, MS, FACEP



**CHRISTIAN DAMEFF
"QUADDI"**

- Associate Professor of:
 - Emergency Medicine
 - Biomedical Informatics
 - Computer Science
- Co-director Center for Healthcare Cybersecurity
- Medical Director of Cybersecurity

@ University of California San Diego

Thesis:

1) Modern healthcare is critically dependent on connected technology

Thesis:

2) Modern healthcare is vulnerable to cyber threats that disrupt, delay, and degrade care

Thesis:

3) Clinicians are ill equipped to care for patients when this technology fails

Thesis:

4) Many technology failures can result in disaster level impacts

2021

The San Diego Union-Tribune

Subscribe Now
\$4/4 weeks

Scripps enters fourth week of ransomware attack



Cyber Attack Blast Radius



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.

OBJECTIVE To examine an institution's emergency department (ED) patient volume and stroke care metrics during a month-long ransomware attack on a geographically proximal but separate health care delivery organization.

DESIGN, SETTING, AND PARTICIPANTS This before and after cohort study compares adult and

Key Points

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

Findings This cohort study of 2 academic urban emergency departments (EDs) adjacent to a health care delivery organization under a month-long ransomware attack



Finding: Emergency Care Was Significantly Impacted

Table 2. Health Care Delivery Organization B ED Census, Recurrence, and Throughput Metrics

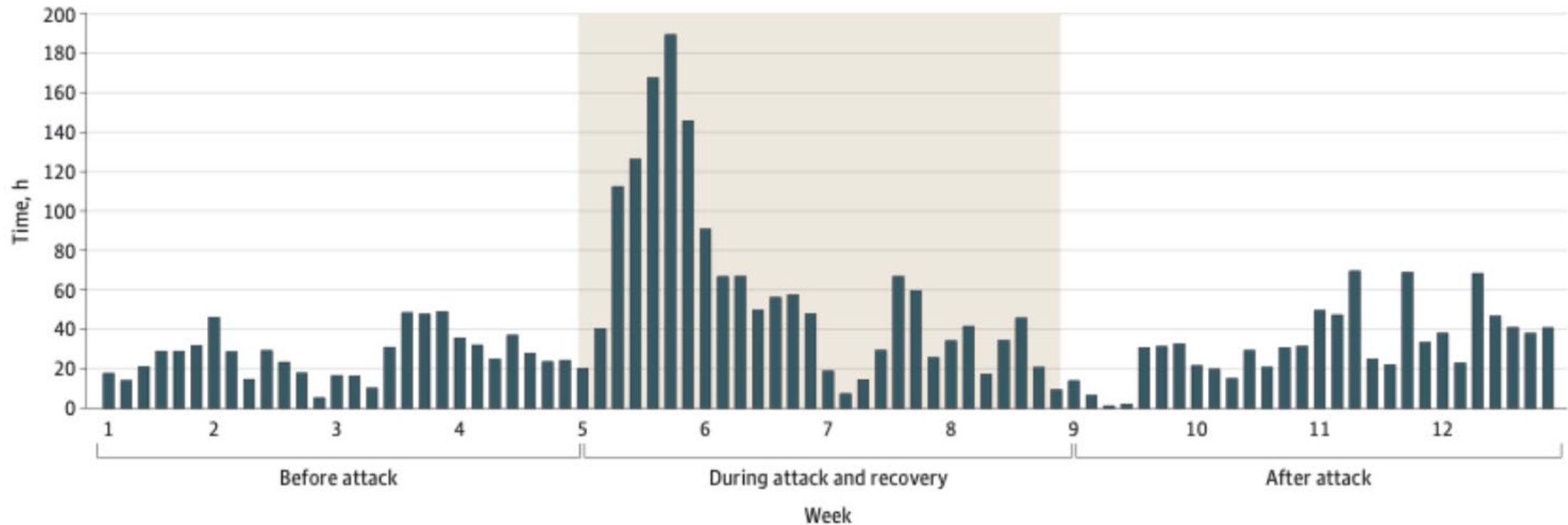
Characteristic	Before attack (n = 6114)	During attack and recovery (n = 7039)	After attack (n = 6704)	P value			
				Overall	Before attack vs attack	Attack vs after attack	Before vs after attack
ED daily census, mean (SD)	218.4 (18.9)	251.4 (35.2)	239.4 (21.3)	<.001	<.001	.13	<.001
EMS arrivals, mean (SD)	1741 (28.8)	2354 (33.7)	1920 (28.9)	<.001	<.001	<.001	.90
Admissions, mean (SD)	1614 (26.4)	1722 (24.5)	1648 (24.6)	.02	.01	.87	.02
Left without being seen, mean (SD)	158 (2.6)	360 (5.1)	260 (3.9)	<.001	<.001	<.001	<.001
Left against medical advice, mean (SD)	107 (1.8)	161 (2.3)	101 (1.5)	.002	.03	<.001	.28
Eloped, mean (SD)	77 (1.3)	102 (1.4)	91 (1.4)	.65	No further statistical analysis performed ^a		
7-d ED revisits, mean (SD)	514 (12.6)	563 (12.2)	548 (12.1)	.79	No further statistical analysis performed ^a		
30-d Readmission, mean (SD)	237 (14.7)	241 (14.0)	234 (14.2)	.85	No further statistical analysis performed ^a		
Median door-to-room time (IQR), min	21 (7-62)	31 (9-89)	23 (8-66)	<.001	<.001	<.001	.001
Admitted median total length of stay (IQR), min	614 (424-1093)	822 (497-1524)	680 (452-1271)	<.001	<.001	<.001	<.001
Discharged median total length of stay (IQR), min	290 (198-421)	307 (203-453)	298 (201-432)	<.001	<.001	.04	.03

Abbreviations: ED, emergency department; EMS, emergency medical services.

^a Due to insignificant overall P value.

Finding: Prehospital Care Was Significantly Disrupted

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



Conclusions

This cohort study found an associated increase in ED volume (ie, census), EMS arrivals, patients who left without being seen, waiting room times, total ED LOS for admitted patients, county-wide ED diversion time, stroke code activations, and confirmed strokes at 2 hospitals near an adjacent health care organization under a month-long ransomware attack. These findings support the need for coordinated regional cyber disaster planning, further study on the potential patient care effects of cyberattacks, and continued work to build technical health care systems resilient to cyberattacks such as ransomware.

Cardiac Arrest Outcomes Adjacent to Ransomed Hospitals

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](https://doi.org/10.1097/CCE.0000000000001079)

PMCID: PMC11008621

PMID: [38605720](https://pubmed.ncbi.nlm.nih.gov/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](#), MD³



Finding: 10-fold decrease in survivability with favorable neurologic outcome



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.

Despite similar rates of ROSC for all CAs between phases, there were differences in overall survival with a favorable neurologic outcome ($p < 0.001$), driven by an increase in OHCA mortality. We observed a decrease in survival with favorable neurologic outcome for OHCAs during the attack phase compared with the pre-attack (4.5% vs. 40.0%; $p = 0.02$) and post-attack (4.5% vs. 41.2%; $p = 0.01$) phases. In the post-attack phase, we saw survival with favorable neurologic outcome return to pre-attack levels for OHCAs (41.2% vs. 40%; $p = 0.94$). While speculative, EMS diversions may have contributed to worse outcomes for OHCAs by prolonging

Thesis:

5) Lawyers, bureaucrats, and risk adverse healthcare organizations use HIPAA to stifle critical information sharing.

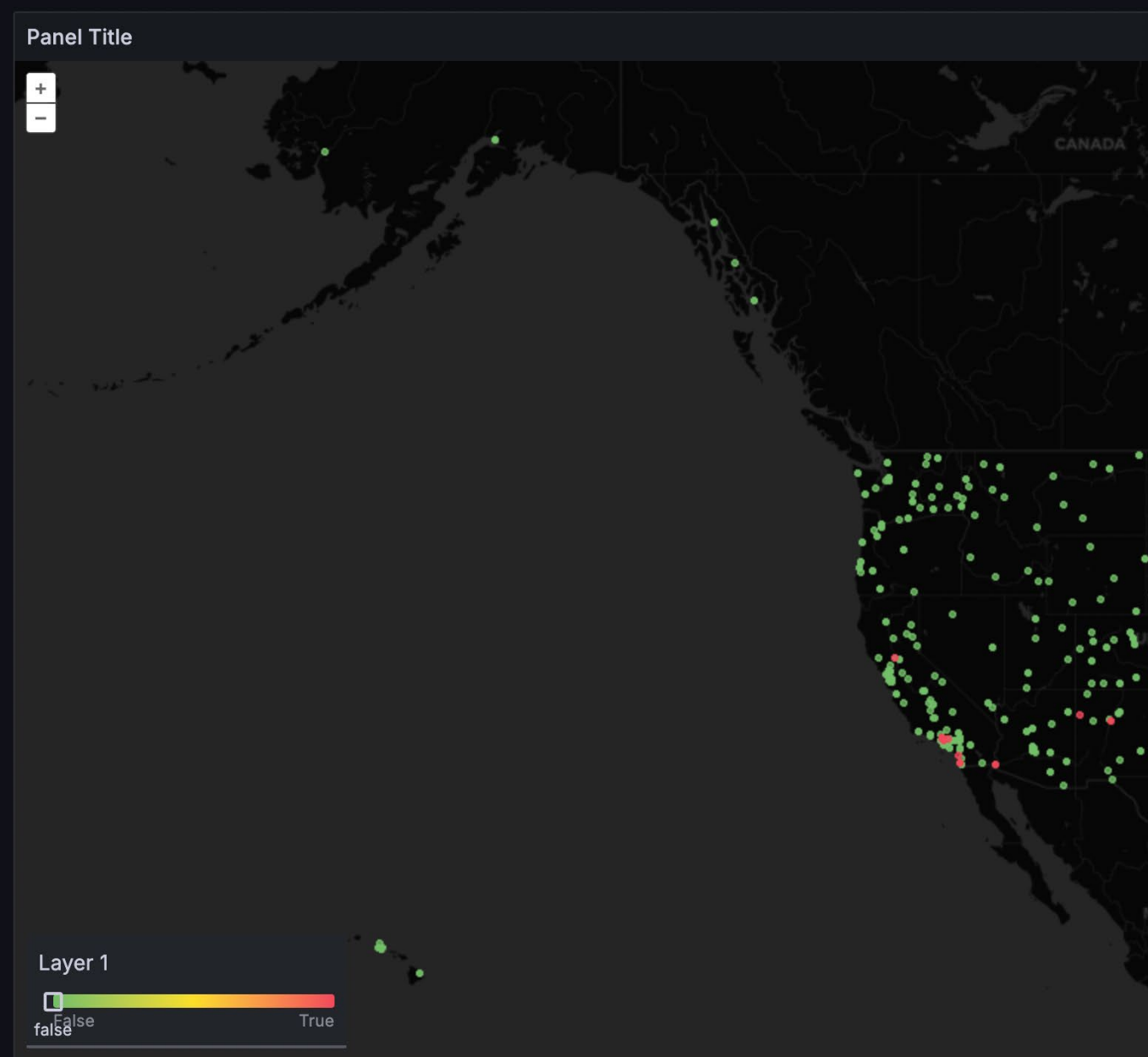
Thesis:

6) Many people have fought in the data wars.
Few lived. Many died.

Assertion: Use technical systems to gather data, infer connections, and ultimately better prepare for disasters. Think outside the box.



Example: internet measurement tools



Layer 1 4

▼ hospital: Monument Health

Time	2025-01-14 11:23:33
hospital	Monument Health
fhir_id	https://ehrmobile.regionalhealth.org/interconnect-prd-fhir/api/FHIR/DSTU2/
is_ransomware	false
Latitude	43.8
Longitude	-104

> hospital: Monument Health

> hospital: Monument Health

> hospital: Monument Health



Original Investigation | Health Informatics



Patient Care Technology Disruptions Associated With the CrowdStrike Outage

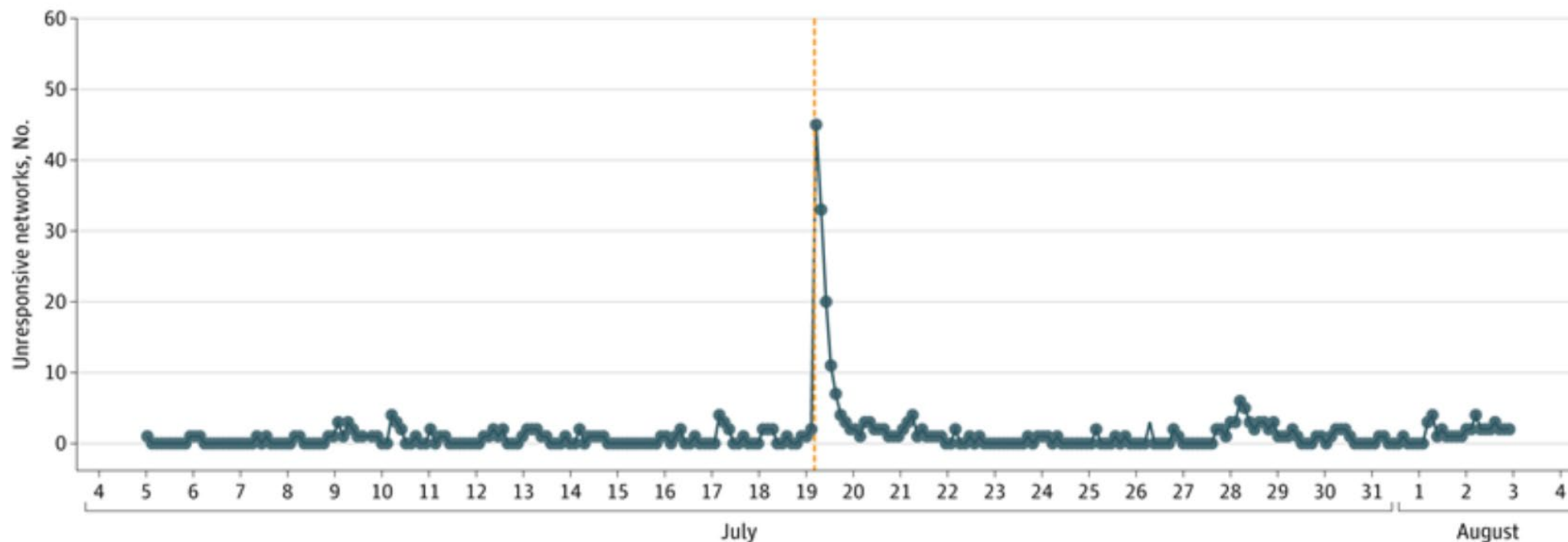
Jeffrey L. Tully, MD^{1,2}; Sumanth Rao, MS³; Isabel Straw, BMBS, PhD¹ ;
Rodney A. Gabriel, MD, MAS^{1,2,5}; Christopher A. Longhurst, MD, MS^{1,5}; Stefan Savage, PhD^{1,3}; Geoffrey
M. Voelker, PhD^{1,3}; Christian J. Dameff, MD, MS^{1,3,4,5}

» [Author Affiliations](#) | [Article Information](#)

 [RELATED ARTICLES](#)  [FIGURES](#)  [SUPPLEMENTAL CONTENT](#)



Figure 2. Unresponsive Health Care Delivery Organization (HDO) Fast Healthcare Interoperability Resource End Points Prior, During, and After the CrowdStrike Outage



[Go to Figure in Article](#)

The vertical orange line marks the time point at which the CrowdStrike outage occurred, July 19, 2024.

Figure 1. Geospatial Map of the Identified Health Care Delivery Organizations Inferred to Have Service Disruptions Using Address Space Scans

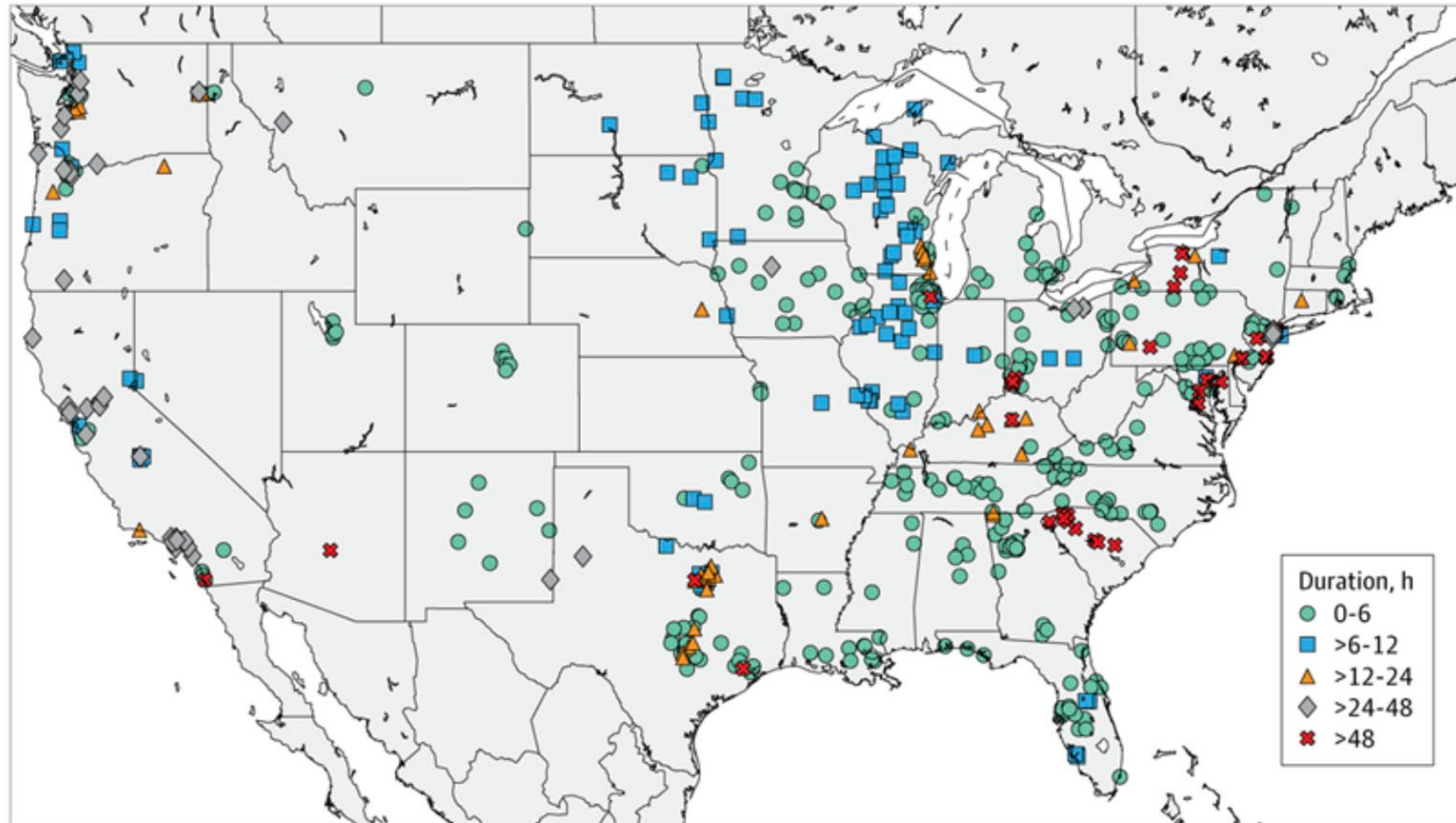


Table. Evaluation of Services With Outages and Their Relevant Clinical Utility

Table. Evaluation of Services With Outages and Their Relevant Clinical Utility

	Category of service			
	Patient facing	Operationally relevant	Research relevant	Not relevant / Unknown
Proportion of total affected services, No. (%) (n = 1098)	239 (21.8)	169 (15.4)	58 (5.3)	631 (57.5)
Examples of identified services and relevance to patient care	Staff portals for viewing patient health records, access to platforms for viewing prehospital clinical information, fetal monitoring systems and device management for telemonitoring, secure document transfer for inter-hospital transfers, access to imaging systems for viewing patient scans	Staff scheduling systems for regular and on call shifts, bill payment systems for health care insurers, clinical workforce management and optimization systems, portal for ordering facilities services, networked printers in the clinical environment, digital systems for establishing patient wait times and patient flow in the hospital environment	Access to databases for clinical trial operations, information websites for research laboratories, patient enrollment systems for rare disease research programs, staff login for clinical research management systems, REDCap research environment for academic centers, login portal for researchers at academic health centers	Testing and staging environments (preproduction), webpage for medical school alumni programs, donation websites for academic centers, medical education websites for students

This approach required 0 billable lawyer hours.

**Are we missing the forest for the trees?
What detail of data do we actually need?**

Think like a hacker. Obey the law. Move faster.

Q&A