

## Brief Report

**Cite this article:** Sullivan N, Tully J, Dameff C, Opara C, Snead M, Selzer J. A national survey of hospital cyber attack emergency operation preparedness. *Disaster Med Public Health Prep.* 17(e363), 1–4. doi: <https://doi.org/10.1017/dmp.2022.283>.


### Keywords:

cyber attack; healthcare cybersecurity; ransomware; emergency management; cyber disaster

### Corresponding author:

Jordan Selzer,  
Email: [jselzer@gwu.edu](mailto:jselzer@gwu.edu).

# A National Survey of Hospital Cyber Attack Emergency Operation Preparedness

Natalie Sullivan MD<sup>1</sup> , Jeffery Tully MD<sup>2</sup>, Christian Dameff MD<sup>3,4</sup>, Chibuzo Opara MD<sup>5</sup>, Mackenzie Snead MD<sup>5</sup> and Jordan Selzer MD, MPH<sup>1</sup>

<sup>1</sup>Department of Emergency Medicine, George Washington University, School of Medicine, Washington, DC, USA; <sup>2</sup>Department of Anesthesiology, Division of Perioperative Informatics, University of California San Diego, School of Medicine, La Jolla, California, USA; <sup>3</sup>Department of Emergency Medicine, University of California San Diego, School of Medicine, La Jolla, California, USA; <sup>4</sup>Department of Biomedical Informatics, University of California San Diego, School of Medicine, La Jolla, California, USA and <sup>5</sup>Howard University College of Medicine, Washington, DC, USA

## Abstract

**Objective:** Cyberattacks on healthcare systems are increasing in frequency and severity. Hospitals need to integrate cybersecurity preparedness into their emergency operations planning and response to mitigate adverse outcomes during increasingly likely cyber events. No data currently exist regarding the level of preparedness of United States hospital systems for cybersecurity attacks. We surveyed hospital emergency managers to assess cybersecurity preparedness for these events.

**Methods:** Fifty-seven emergency managers representing hospitals across the United States participated in an online Qualtrics survey regarding current preparedness and response procedures for cybersecurity hazards.

**Results:** Survey responses between April 2019 and May 2021 demonstrated that a majority of hospital systems surveyed included cybersecurity disasters in their HVA (82.4%; 47/57), and most ranked it as 1 of their top 5 priorities (57.4%; 27/47). However, over half denied specifically mentioning cybersecurity in their Emergency Operations Plans (EOPs; 52.6%; 30/57). Fourteen of the 57 hospital systems (24.5%) endorsed previously activating an emergency response for a cybersecurity incident unrelated to information technology (IT) failure.

**Conclusions:** The survey results suggest that American hospitals are currently underprepared for cybersecurity disasters. We emphasize the importance of prioritizing cybersecurity in Hazard Vulnerability Analyses (HVAs) and implementing specific EOP annexes for cybersecurity emergencies.

The Hospital Incident Command System (HICS) based on the National Incident Management System (NIMS) and the Incident Command System (ICS) provides healthcare organizations and hospitals with the structure and principles necessary to conduct emergency management and contingency planning. This system takes into account the Disaster Cycle of prevention, mitigation, preparedness, response and recovery. Effective emergency management includes prevention where actions may prevent a hazard from occurring and mitigation and preparedness where efforts may lessen the impact of an anticipated hazard. Successful systems focus on preparedness actions that have the potential for maximum impact at significantly lower cost than when resources are focused on the response phase of disaster. Some hazards, however, cannot be avoided completely; therefore, an effective response plan is also an essential to emergency management.

Organizations create Emergency Operations Plans (EOP) to establish actions and organizational structures in response to a hazard event that exceeds the capacity of normal operations. EOPs provide thorough role descriptions, delineate specific responsibilities and identify assigned resources. A well-established tool, Hazard Vulnerability Analysis (HVA), informs EOPs by identifying and prioritizing projected hazards based on their likelihood and potential impact. Hospitals face many possible hazards and must allocate limited resources according to their HVA to optimize outcomes. EOP design focuses on an all-hazards approach with additional planning associated with specific events located in appendices.<sup>1</sup>

As medicine advances, technological systems allow for a standard of care that simultaneously integrates different medical devices, testing, and patient monitoring. Healthcare systems both large and small use a variety of connected medical technologies such as electronic medical records (EMR) to store sensitive patient information and to communicate across facilities and between providers. Patients receive implants of wirelessly connected medical devices, such as defibrillators and insulin pumps, that provide life-sustaining medical support.

As these technologies allow providers access to new care workflows, they may also expose medical systems and patients to novel vulnerabilities including disruptions and even potentially

© The Author(s), 2023. Published by Cambridge University Press on behalf of Society for Disaster Medicine and Public Health, Inc. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

malicious functions.<sup>2</sup> With the healthcare industry increasingly dependent on connected technologies, failures to secure critical systems have become commonplace. Healthcare cybersecurity attacks are increasing in frequency and severity.<sup>1</sup> Data loss, monetary theft, attacks on medical devices, and infrastructure attacks are among the increasing cyber threats to healthcare.<sup>3</sup> Ransomware, one of the most prevalent forms of cyberattacks, occurs when an outside actor breaks into a network, encrypts the contained information, and then restricts access until ransom is paid.<sup>4</sup> Health-care organizations represent high value targets for ransomware because they maintain protected health information which, when compromised, may result in financial risk, legal liability, and regulatory penalties.<sup>3</sup>

While all hospitals undergo intermittent downtime, these typically happen with some warning and are relatively brief with a known timeframe. However, cyberattacks occur suddenly, with unique features including multiple systems simultaneously impacted and prolonged downtimes. Between 2012 and 2018, almost half of 166 downtime events across US hospitals involved a cyberattack.<sup>5</sup> Downtime contingency workflows and planning may mitigate patient impact during these events and proper cyber preparedness may prevent them all together.

No data currently exist regarding the level of preparedness in the US Hospital systems for cybersecurity attacks. This is true internationally as well. Through a survey of emergency managers in hospitals across the country, we further investigate preparedness with regard to this hazard.

## Methods

We created and distributed a brief survey to hospital emergency management personnel across the United States. To preserve anonymity and thus improve response rate, investigators did not collect personally identifying information. The questions focused on preparedness and prior cyberattack response (Appendix 1).

The authors collected the data using the survey software program Qualtrics XM (Qualtrics, Seattle, WA). Expert opinion obtained through discussions with professionals working in hospital emergency management, cybersecurity and response as well as clinicians and individuals working at health-care facilities during cyberattacks informed the questions for the survey. The survey was then distributed throughout University of California (UC) hospital system emergency management listserv as well as ASPR TRACIE Express, a national listserv of health-care emergency preparedness personnel. The UC listserv reached 5 UC hospitals with 1 respondent each. Invitees received 2 emails requesting that only emergency managers complete the anonymous survey between April 2019 and May 2021. In this context, emergency managers were defined as individuals functioning in a role focused on reducing hazards, coping with disasters- and supporting a structure to reduce vulnerability. All respondents represented individual hospital systems within the United States. Each participant completed the electronic survey in English. Participants completed the survey online and Qualtrics XM anonymized the data.

Due to the nature of open invitation by means of listserv, a response rate is unavailable. Additionally, due to the de-identified nature of the data, geographic distribution and characterization of individual healthcare facilities was not possible. Incomplete responses were not included in the final analysis.

Researchers received de-identified results. Researchers analyzed the answers to each question separately. Authors used Microsoft

Excel (V16.49, Redmond, WA) to perform a quantitative analysis of the data which demonstrated the proportions of respondents represented by each answer.

## Results

The authors collected 57 completed survey responses between April 2019 and May 2021. These survey responses provided data for the following results.

### HVA

A majority of hospital systems surveyed included cybersecurity disasters in their HVA (82.4%; 47/57), with 4 respondents unsure as to whether there was an entry. Of those who affirmed there was a cybersecurity disaster entry in their HVA, 57.4% ranked it as 1 of their top 5 priorities (27/47).

Fourteen (29.7%) of the total 47 respondents with cybersecurity disaster in their HVAs ranked it specifically as their third priority overall.

### EOP

While most hospital systems did include cybersecurity disaster in their HVAs, more than half denied specifically mentioning cybersecurity in their EOPs (52.6%; 30/57), with an additional 10.5% (6/57) stating they were unsure as to whether cybersecurity was included (Figure 1). Of the 36.8% (21/57) of hospital systems who included cybersecurity disaster in their EOPs, only 52.4% (11/21) of respondents used external resources to create their emergency plan. Two respondents specifically referenced the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security when creating their EOP. One source listed the 2021 X-Force Threat Intelligence Index from IBM as a reference, specifically citing the "Vulnerabilities Surpass Phishing as Most Common Infection Vector" section. Other external sources referenced included "documents," "cyber threats," "HHS and vendor support," and "websites."

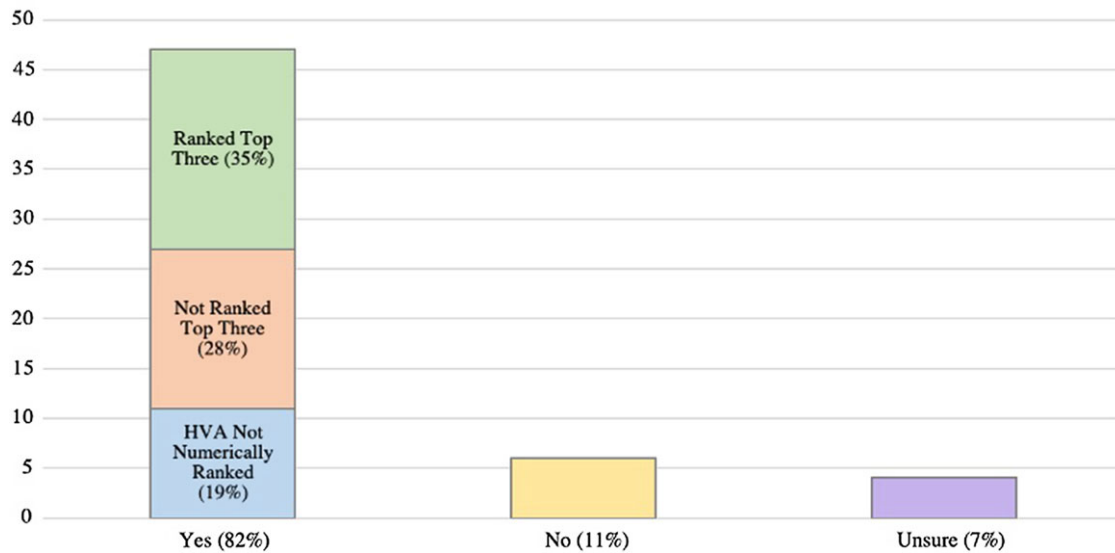
Fourteen of 30 (46.6%) of the hospital systems without cybersecurity disasters listed in their EOP plan to add an entry within the upcoming year.

### Cybersecurity Disaster Practice and Emergency Response Activation

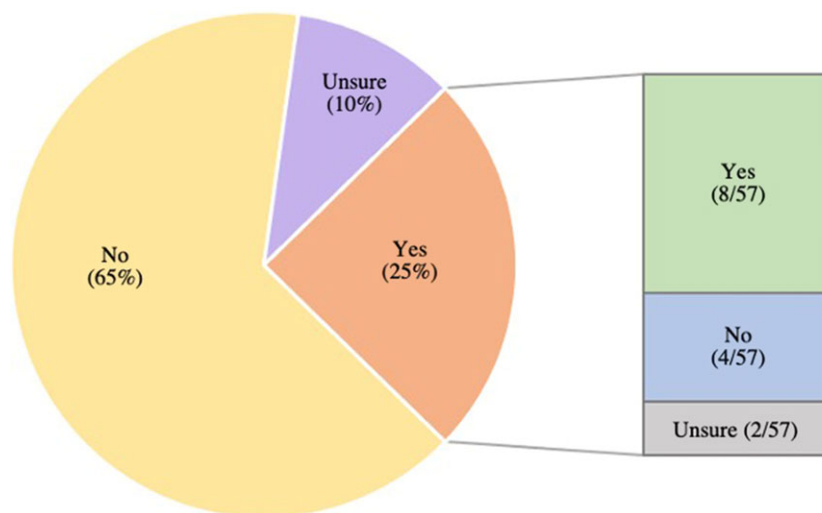
Fourteen of the 57 hospital systems (24.5%) endorsed previously activating an emergency response for a cybersecurity incident unrelated to information technology (IT) failure (Figure 2). Of those, a majority had an existing cybersecurity disaster entry in their EOPs and had previously performed a full-scale drill or tabletop exercise relating to cybersecurity (57.1%; 8/14). Most of these hospital systems (92.8%; 13/14) stated they additionally included cybersecurity disasters in their HVA (Figure 3). Of the 43 respondents who denied a prior emergency response activation (ERA) for cybersecurity disaster, only 37.2% (16/43) previously performed a full-scale drill or tabletop exercise related to cybersecurity.

## Discussion

A report published by CISA in 2021 described increases in ambulance diversion, intensive care unit bed use, and mortality consequent to hospital cyberattacks.<sup>6</sup> The frequency of cyberattacks on



**Figure 1.** Are cyber security disasters included in your Hazard Vulnerability Assessment? (n = 57).



**Figure 2.** Has a cyber security incident ever resulted in an emergency response activation at your organization? If yes, did your organization have a cyber security disaster plan in your Emergency Operation Plan prior to the incident? (n = 57).

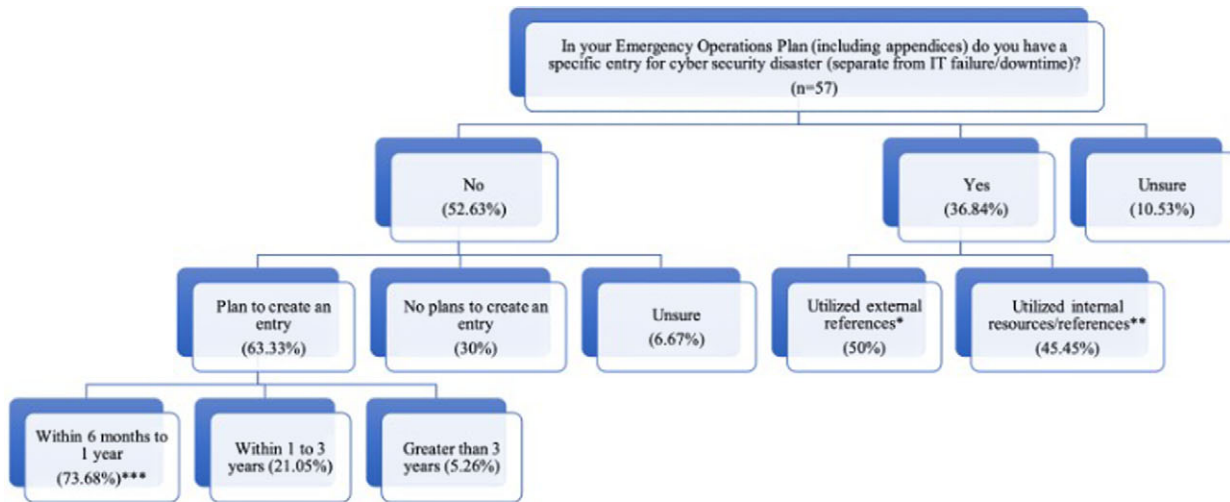
health-care organizations exceeds any other sector.<sup>7</sup> Despite the escalating risk and the potential for devastating consequences, this survey demonstrates a lack of preparedness and mitigation strategies among a large proportion of American hospitals.

Although a majority of systems surveyed included cyberattack in their HVA, only slightly over half prioritized it as one of their top hazards. This is consistent with a prior study of 27 health-care emergency managers in West Virginia where only 30% of respondents had an all-hazards plan and EOP for cybersecurity events.<sup>8</sup> The EOP is the action component of a hospital’s preparedness. It allows for organizations to delineate roles, tasks, and workflow during a threat to normal operations. Due to the unique nature of cyberattacks, an all-hazards approach that is typically used in disaster response is unlikely to suffice. Cyberattacks occur at the speed of the Internet without warning, require specialists in

information security (IS) and greatly compromise the existing clinical flow.<sup>9</sup> EOPs that take into account the cyber-specific hazard provide additional guidance to providers and managers of an emergent IT system shutdown.

Many factors contribute to the difficulty of fully addressing and even evaluating preparedness among American hospitals for cyberattack. The costs of identifying vulnerabilities and the subsequent negative media attention likely inhibit hospital systems from divulging a lack of preparation.

Furthermore, the relatively burgeoning threat of cyberattacks and their evolving nature present a unique challenge to preparedness in medicine. Often in the traditional medical environment, practitioners use more antiquated, or “legacy” computer technology which is unsupported by vendors, resulting in greater vulnerability. They often have limited training in simple cyber



\*The external references mentioned by respondents included non-specific entries including "websites," "documents," or "cyber threats." Two hospital systems reported using CISA, one hospital system reported using "HHS and vendor support," and one hospital system utilized the 2021 IBM Security Report, "Vulnerabilities Surpass Phishing as Most Common Infection Vector."

\*\*10 out of the 22 respondents who endorsed having an entry in their EOP for cyber security disaster utilized internal resources and references; 1 respondent omitted.

\*\*\*5 out of 19 respondents who endorsed having plans to create an entry reported a creation time frame within 6 months. 9 out of 19 respondents reported a creation time frame of 6 months to 1 year.

**Figure 3.** In your emergency operations plan do you have a specific entry for cyber security disaster? ( $n = 57$ ).

hygiene. Limited budgets and overburdened health-care workers also lead to the use of outdated technology and disincentivize investing in adequate preparedness measures. In systems that remain unaffected by cyberattack, IS personnel and emergency managers may lack resources to pursue preventative measures or knowledge regarding these specific threats.

Authors have dedicated entire books to hospital preparedness and response procedures for cyberattacks. Likewise, the federal government through multiple agencies offers hospital guidance on hospital cyberattack emergency operations.<sup>10</sup> This myriad of resources may inform hospital hazard analyses and EOPs. In a hospital, multiple pivotal response areas exist—emergency management administration, clinical staff, and IS and IT staff among them. Preparedness and mitigation require health-care organizations to hire and train IS/IT specialists to directly respond to cyberattacks but must also educate and drill clinical staff on downtime procedures and clinical flow.

### Limitations

More specific geographic and demographic data regarding the respondents to this survey may provide further insight into the applicability of the data. However, to protect the anonymity of these sites, we cannot provide further identifying information. The data gleaned from this survey is limited and may not fully represent the spectrum of health-care institutions. Further research may identify gaps in preparedness and highly successful methods for mitigation. Data collected during real life breaches, information sharing, and increased collaboration between hospital emergency managers may also provide further insight into successful responses.

### References

1. Paganini P. Cyberattack reports quadrupled during Coronavirus outbreak, FBI warns. Security Affairs. 2020. Cited July 12, 2020. Accessed January 10, 2023. <https://securityaffairs.co/wordpress/101879/cyber-crime/fbi-coronavirus-attacks-spike.html>
2. Tully J, Selzer J, Phillips JP, *et al.* Healthcare challenges in the era of cybersecurity. *Health Secur.* 2020;18(3):228-231.
3. Perakslis ED. Cybersecurity in health care. *N Engl J Med.* 2014;371(5):395-397.
4. Kruse CS, Frederick B, Jacobson T, *et al.* Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care.* 2017;25(1):1-10.
5. Larsen EP, Rao AH, Sasangohar F. Understanding the scope of downtime threats: a scoping review of downtime-focused literature and news media. *Health Informatics J.* 2020;26(4):2660-2672.
6. CISA. Provide medical care is in critical condition: analysis and stakeholder decision support to minimize further harm. Cybersecurity and Infrastructure Security Agency. 2021. Accessed January 10, 2023. [https://www.cisa.gov/sites/default/files/publications/CISA\\_Insight\\_Provide\\_Medical\\_Care\\_Sep2021.pdf](https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf)
7. HealthITSecurity. Healthcare Accounts for 79% of All Reported Breaches, Attacks Rise 45%. Cited January 24, 2022. Accessed January 10, 2023. <https://healthitsecurity.com/news/healthcare-accounts-for-79-of-all-reported-breaches-attacks-rise-45>
8. Branch LE, Eller WS, Bias TK, *et al.* Perceptions of hospital emergency preparedness for cyber threats: a statewide survey. *Cyber Threats and Healthcare Organizations: A Public Health Preparedness Perspective* 2018;1001:91. <https://researchrepository.wvu.edu/cgi/viewcontent.cgi?article=4749&context=etd>
9. Dameff C, Farah J, Killeen J, *et al.* Cyber disaster medicine: a new frontier for emergency medicine. *Ann Emerg Med.* 2020;75(5):642-647.
10. Office of the Chief Information Officer (OCIO). Cybersecurity. Cited January 24, 2022. Accessed January 10, 2023. <https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/index.html>