Original Research

DIGITAL HEALTH

Digital Health
Volume 7: 1–15

DOI: 10.1177/20552076211059366
journals.sagepub.com/home/dhj
SAGE

# Assessing resilience of hospitals to cyberattack

**Hadi Ghayoomi[1], Kathryn Laskey[2], Elise Miller-Hooks[1], Charles Hooks[3] and Mersedeh Tariverdi[4]**

## Abstract

**Objective:** This paper investigates the impact on emergency hospital services from initiation through recovery of a ransomware attack affecting the emergency department, intensive care unit and supporting laboratory services. Recovery strategies of paying ransom to the attackers with follow-on restoration and in-house full system restoration from backup are compared.

**Methods:** A multi-unit, patient-based and resource-constrained discrete-event simulation model of a typical U.S. urban tertiary hospital is adapted to model the attack, its impacts, and tested recovery strategies. The model is used to quantify the hospital's resilience to cyberattack. Insights were gleaned from systematically designed numerical experiments.

**Results:** While paying the ransom was found to result in some short-term gains assuming the perpetrators actually provide the decryption key as promised, in the longer term, the results of this study suggest that paying the ransom does not pay off. Rather, paying the ransom, when considered at the end of the event when services are fully restored, precluded significantly more patients from receiving critically needed care. Also noted was a lag in recovery for the intensive care unit as compared with the emergency department. Such a lag must be considered in preparedness plans.

**Conclusion:** Vulnerability to cyberattacks is a major challenge to the healthcare system. This paper provides a methodology for assessing the resilience of a hospital to cyberattacks and analyzing the effects of different response strategies. The model showed that paying the ransom resulted in short-term gains but did not pay off in the longer term.

## Keywords

Cyberattack, hospital emergency services, discrete event simulation, resilience, ransomware, digital health solutions, numerical experiments, healthcare management

Submission date: 22 August 2021; Acceptance date: 25 October 2021

## Introduction

In recent years, hospitals and other health care facilities have become increasingly reliant on information technologies. From electronic health records (EHRs) to radiology, nearly all critical functions exploit communications technologies, rendering almost every aspect of daily operations vulnerable to cyberattack. Even as early as 2017, 94% of hospitals relied on EHR data for patient-related processing.[1] Moreover, in 2015, there were an estimated 4.5 billion Internet of Medical Things (IoMT) devices across the world, accounting for 30.3% of all IoT devices worldwide.[2] By 2020, this was expected to rise to 20–30 billion IoMT devices.[2] In fact, it is estimated that 83% of all medical devices are now connected and vulnerable to some form of cyberattack.[3] In medical settings, compromised records and or devices can create slowdowns or termination of procedures, preventing care for patients with critical needs and

[1]Department of Civil, Environmental and Infrastructure Engineering, George Mason University, Fairfax, VA, USA
[2]Department of Systems Engineering and Operations Research, George Mason University, Fairfax, VA, USA
[3]Writing as an individual, Senior Director, Information Technology at Suburban Hospital
[4]The World Bank Group

**Corresponding author:**
Kathryn Laskey, Department of Systems Engineering and Operations Research, George Mason University, Fairfax, VA, USA.
Email: klaskey@gmu.edu

**Table 1.** Vulnerable areas of hospital, potential malicious activities and effects.[12]

| Vulnerable Hospital Area | Malicious Activity and Effects | Possible Effect |
|---|---|---|
| **Magnetic Resonance Imaging (MRI)** | Increase MRI strength | Damage to patient and machine |
| | Mute hazardous condition alarms | Technician is unaware of hazards |
| **CT scan or X-ray** | Increase recommended radiation | Radiation sickness |
| | Encrypt internal files | Turn off, ransom demand for unlock |
| **Medical Ventilator** | Change pressure, volume, or flow alarm | Patient in danger |
| **Medical Device Data Systems (MDDS)** | Lock transfer of data | Delay in the processes |
| **Medical laboratory** | Change or remove lab results | Retaking the tests and delays |
| **Building control system (BCS)** | Turn off building utilities (e.g. electric, water) | Delays and danger for patients |
| | Change operating parameters (e.g. temp, oxygen level) | Danger for patients |
| | Crash system and changing access information | Locking all processes |
| | Shut down air handling units | Releasing hazardous materials |
| **Inter/Cloud IT networks** | Hack routers, records, websites | Delay in patient treatment |

with potential for fatalities. Such medjacking events may also include modification of the dosages of sensitive medicines or the shutting down of devices while in use in a procedure.

Estimates of the cost to the U.S. from cyberattack on primary, secondary and tertiary healthcare facilities will cost over $6 billion annually.[4] Despite their vulnerability to cybercrime and the criticality of their impacts on patient care, as of 2019 only 13% of hospitals in the U.S. conducted annual incident response drills for cyberattack scenarios.[5]

In 2017, a major cyberattack called WannaCry infected 25 acute trusts (organizational/managerial units for hospitals) in the United Kingdom, locking devices and disrupting patient care. In follow-on analysis, it was determined that all or almost all units of the National Health Service failed cybersecurity assessments.[6–8] In the U.S., the Food and Drug Administration (FDA) identified 11 types of vulnerabilities[9] wherein an external force could remotely control medical devices. With approximately 200 million medical devices at risk in 2019,[10] health care was declared a major cyber-crime target.[11]

There are several mechanisms of vulnerability that are specific to hospitals as discovered through a literature review and interviews of hospital cybersecurity experts (S. Larsen, interview, April 2020, unreferenced; M. Wilkes, interview, August 2020, unreferenced; B. Woods, interview, August 2020, unreferenced). These are well described by Ayala[12] and are synthesized in Table 1. Of special concern are attacks that can disable systems and encrypt data precluding their use as caused by, for example, ransomware, distributed denial of service (DDoS) and theft of sensitive data. Also concerning, during the most critical stages of the COVID-19 pandemic, within 2020, a time when hospitals worldwide were overwhelmed, cyberattacks against them doubled.[13] Some varieties of cyberattacks, such as Business Email Compromise (BEC), have less effect on performance of the hospitals or the patients they serve, but can still come at a cost In fact, the overall cost of BEC in the U.S. in 2018 was US$3.6 billion. In 2018, the healthcare sector was the sixth largest target for this type of attack, accounting for 5% of the total targeted victims.[14]

Table 2 compiles information about recent attacks on hospitals, their types, and impacts. Whether the focus of the attack or as a secondary outcome, many of the listed cyberattacks involve data breaches. These breaches may aim for monetary gain or to harm the reputation of a person, facility, company or government. They also compromise patient privacy and safety. Table 2 highlights the prevalence of recent ransomware attacks. Because of their prevalence and impacts, hospitals often carry insurance for such attacks.

Table 3 summarizes potential impacts of cyberattacks on hospital operations derived from reports in the literature and interviews with experts in hospital cybersecurity. The metrics include common performance measures in queueing networks.[15] These measures allow hospital managers to quantify the impact of cyberattacks.

**Table 2.** Significant cyberattacks that affected hospital performance.

| | Case | Type | Year | Reported Effects | Financial Cost | Duration (days) |
|---|---|---|---|---|---|---|
| **Pre-2020 samples** | WannaCry, half of Britain's NHS Including 16 major health centers[6,29] | Ransomware | 2017 | 200,000 PCs and 1200 equipment | $125M | 14 |
| | | | | Cancellation of 20,000 appointments | | |
| | Boston Children's Hospital[30–32] | DDoS attack | 2014 | Websites, internal and external network | $300,000 | 14 |
| | Montpellier University hospital[30,33] | Phishing | 2019 | 649 -6000 Pc and equipment | Not reported, | 5–7 |
| | Hollywood Presbyterian Medical Center[26,34] | Ransomware | 2016 | Full shutdown in PC, Email, Equipment, Networks | Demanded 9000 bitcoins | 10 |
| **2020 and later** | Champaign-Urbana Public Health District's[27,35] | Ransomware | 2020 | Internal and external network access | Not reported | <14 |
| | Vermont Hospital[36,37] | Ransomware | 2020 | Hacking HER, delays in various departments | $1.5 M per day | <7 |
| | UVM Health cyberattack[27,38] | Ransomware | 2020 | 5000 PC, network. Shutdown IT and Med Centers | $63 M | 40 |
| | | | | Postponed services during the incident | | |
| | Maryland hospital[39] | Ransomware | 2020 | Network shutdown, continue operations | Not reported | 2 |
| | | | | Postponed scheduled appointment | | |
| | Six U.S. hospitals[27,40] | Ransomware | 2020 | Networks. using Paper record | 2000 new PC | 7–14 |
| | | | | demanded $1M | | |
| | | | | Diverted ambulances during the downtime | | |
| | | | | Postponed elective procedures and services. | | |

Like in other industries, companies often find that paying the ransom could be less impactful on operations and profit margins than attempting a recovery of the compromised IT systems without the decryption key needed to remove the malware. The Vermont Hospital estimates that the cost due to delays in hospital operations from an attack in 2020 was on the order of $1.5 million per day.[16] If the difficult choice is made to pay the ransom, there is no guarantee that the attackers will hold up their end of the deal. In fact, approximately 80% of small to medium size companies globally that have chosen to pay the ransom do not receive the promised decryption key after payment[17] and sometimes a second ransom is demanded even if a first is paid. Moreover, even if the decryption key is quickly provided and all data is recovered, the system remains compromised and untrustworthy. A full recovery of the system remains necessary.

While there is a solid understanding of how an attack can impact various aspects of hospital service provision, there is less understanding of how these impacts affect hospital capacity to serve patients. The most closely related works are primarily qualitative, and quantitative works are generally focused on the vulnerability of specific equipment types. The authors were unable to find any comparable quantitative

**Table 3.** Goal and impact of a cyberattack and their measurement.

| Impacts Performance | Effect | Reason | Measure |
|---|---|---|---|
| **No** | Data breach[41] | Malicious access to databases | Patient record |
| | Business email compromise[42] | Misusing information from hacked databases | Dollars |
| | Telehealth fraud[43] | Hacking web/apps/databases, scams | Number of cases |
| **Yes** | Slowing down processes[44] | Paper work, Int/Ext net hack, web/email/app access hack | Processing times |
| | Increasing mortality[45] | Changing critical equipment functions | Mortality rate |
| | Hospital/Unit lockdown and transfer out[46] | Risk of poor treatment, equipment shutdown | Number of transfers out |
| | Cancelling scheduled surgeries[47] | Rescheduling after full recovery | Number of cancelations |
| | Increasing patients' waiting times and queue lengths | Processes time increase | Waiting time |
| | Causing patients to leave without being seen | Waiting time increase | Ave queue length |
| | Decreasing staff utilization | Decreasing number of patients due to cancellations/ closures/bottlenecks[48] | Staff/ stuff utilization |
| | Increasing staff/stuff utilization | higher workload due to slower processes/paperwork etc. | Unit performance (utilization) |
| | Increasing recovery period after attack | Improper backups, not using cloud based DBs, unsophisticated IT Expert | Recovery period |
| | Decreasing daily treated patients in the hospital[49] | Increasing processing times, hospital closure | hospital daily treated patients |

analyses in the archived literature that similarly seeks to quantify the impacts of a cyberattack on unit-level or whole-hospital performance. At a whole-hospital level, an alternative in the literature to the type of analysis described here is the tabletop exercise.[18] The approach taken in this paper is to perform computational experiments using a computer simulation of the effects of a cyberattack on hospital performance. Advantages of this approach include the ability to perform multiple runs to obtain precise statistical estimates of key performance metrics, and the ability to design and conduct computational experiments to assess the effects of different response policies.

This paper introduces resilience measures for assessing a hospital's ability to cope with and recover from a cyberattack accompanied by a demand for a ransom (a ransomware attack). Specifically, this paper studies the potential impacts of these attacks on the ability of a hospital to sustain patient care under a cyberattack that targets critical care, including

**Table 4.** Critical and Non-critical units.

| Criticality | Major Unit | Subunits |
|---|---|---|
| Critical Units | Emergency Entry | Triage, Fast-track, Trauma, ED & ED services |
| | ICU | ICU |
| | Labs & Equipment | Labs, Radiology, MRI, CT scan |
| Non-Critical Units | Operating Theaters, Pre-op, Post-op | Pre-op, OR, SICU, PACU |
| | Admitted & Discharged | Stepdown, IGW |

processes within the emergency department (ED), including trauma, the intensive care unit (ICU), laboratories, and interventional radiology. The resilience of the hospital to an attack under two potential recovery actions is assessed. These actions include: (a) undertaking a full recovery using the hospital's onsite backup or recovery solution assuming it remains uncompromised and, thus, available and (b) paying the ransom and completing a full recovery once access is restored. Resilience is considered over a 16-day period covering the period from event inception through full recovery conclusion.

Full recovery from a cyberattack typically requires extensive, system-by-system restoration, including software installation and recovery of data from backups, to ensure all remnants of malware have been removed and the systems are restored to pre-attack status. If the hospital has a strong cybersecurity preparedness framework that includes regular and real-time scans and backups, drills (including active disaster recovery drills that engage the disaster recovery sites) by the response team, and a highly skilled response team, then rapid in-house recovery may be feasible. If the cybersecurity preparedness plan is weak or nonexistent, then full recovery will necessitate bringing in outside experts, and is likely to be extremely costly both in time and money.

A whole-hospital, patient-based, and resource-constrained discrete-event simulation (DES) model of a typical urban tertiary hospital was adapted to model a cyberattack, its impacts, and recovery strategies as described in the following section. The model replicates a typical 200-bed urban tertiary (trauma level I or II) hospital. The hospital model was created in prior work[19] and extended for hazard events that affect demand, accessibility and/or functionality of the hospital.[20] Shahverdi et al.[21] modeled hazard events including flood, earthquake, large-scale mass casualty incident and a pandemic. In Shahverdi et al.[22] the hospital model was expanded to incorporate COVID-19 patient care.[22] While the impact of a wide variety of hazard event types on hospital capability and capacity were studied, cyberattack was not previously considered in these models. Modifications needed to model the effects of the cyberattack on hospital operations and the effectiveness of recovery efforts taken to mitigate its impacts are presented herein.

Results of systematically designed numerical experiments using this expanded model were analyzed (Results Section). The results indicate that substantially more emergency patients can be served within the first week of the attack by paying the ransom (assuming the attacker provides the decryption key immediately upon payment) to reduce ED closure by one day. Moreover, hospital resilience, measured in terms of the total 7-day hospital throughput as a percentage of the expected total during ordinary conditions, increases 7 percentage points when it is presumed that the ransom will be immediately paid and the resulting ED closure will be shortened by one day. Generally, the benefits of a reduction in ED entrance closure by one day are significant and warrant consideration of other plans for subverting the attack, such as cloud-based backups with restoration guarantees.

In the short term, it may appear that paying the ransom is an appropriate or necessary action. The experimental results show, however, that when looking further out, the benefits dissipate. By the end of 11 days from the attack, the benefits in terms of total patients treated of paying the ransom reduce to zero compared with using only internal resources to overcome the effects of the attack without paying the ransom. Beyond day 11, the benefits of using internal resources equal or outweigh that obtained from the approach that begins with paying the ransom. At the point when pre-attack service rates are restored under both responses (day 16), 45 additional patients will have been served by the response action that does not involve paying the ransom. Thus, while paying the ransom yields some short-term gains, if the perpetrators actually provide the decryption key as promised after payment, the results of this study suggest that in the longer term, paying the ransom does not pay off. That is, this finding suggests that paying the ransom, when considered over the full recovery period, precludes significantly more patients from receiving critically needed care.

These results provide insights for hospital administrators that can aid in determining an effective and cost-efficient plan for coping with a cyberattack. Insights from this study and implications for policy are discussed further in Discussion Section.

## Methods

### Discrete-event hospital simulation model

*Hospital Simulation*. The hospital model includes 10 key units supporting patient care for those entering the hospital through the ED (including through trauma). These units include: the ED, including triage, intensive care unit (ICU), trauma, operating rooms (OR), pre-op and post-op units (surgical intensive care unit (SICU), post-anesthesia care unit (PACU), stepdown), laboratories, and the internal general ward (IGW). Patients flow through the units as a function of their care paths, which are determined by the illness or injury they incurred prior to arrival and level of severity indexed following the Emergency Severity Index (ESI) system. Care paths originate with entry to the hospital and end upon discharge. A schematic of the units that support the care paths is provided in Figure 1(a).

The hospital model captures key elements of the layout and processes through conceptualization in terms of staff (doctors, nurses and technicians), stuff (equipment, including magnetic resonance imaging (MRI) equipment, X-ray and ultrasound machines) and space (units and beds). Each unit

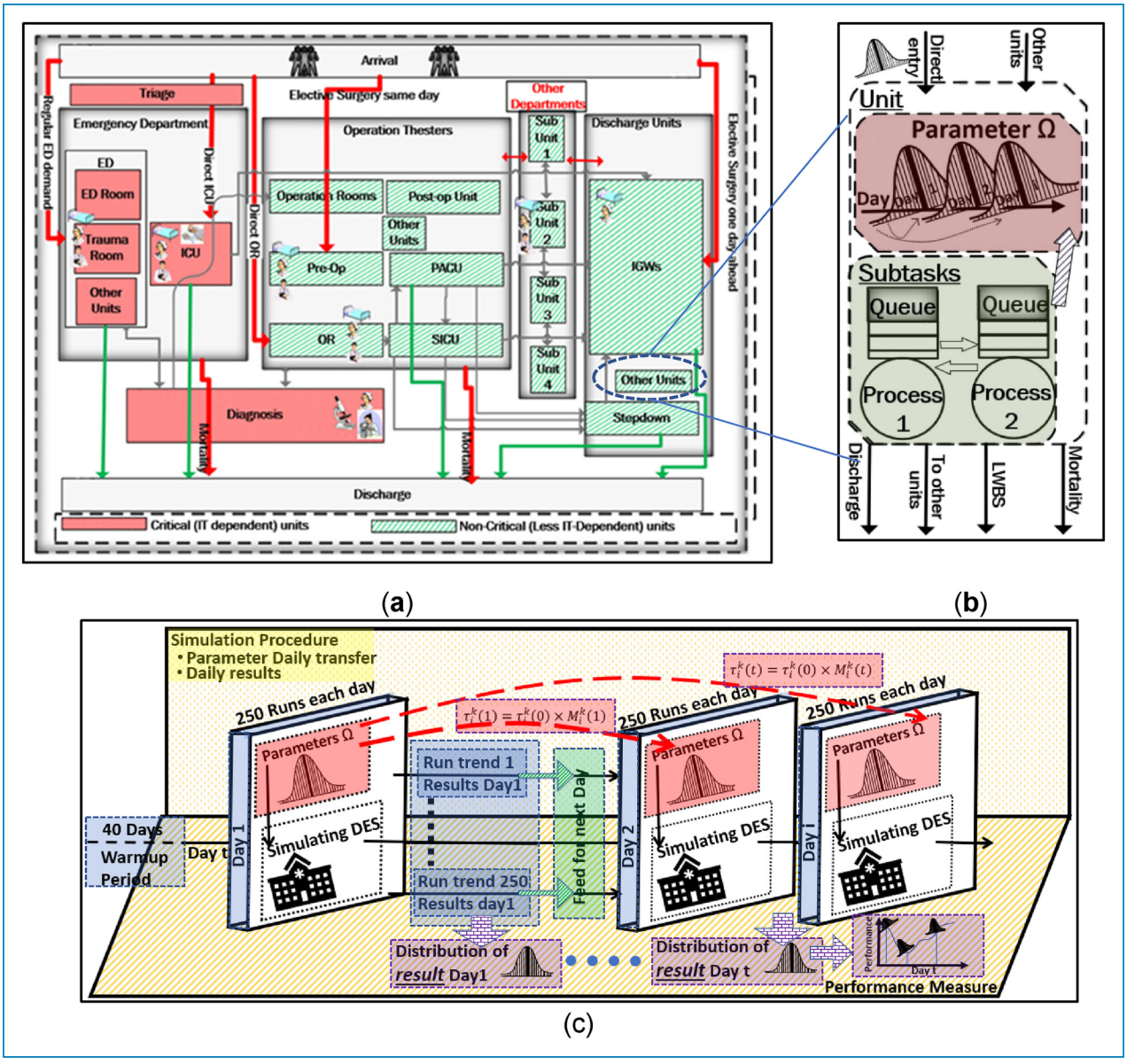


**Figure 1.** (a) schema of the hospital; (b) schema of a unit with subprocesses; (c) simulation process.

has associated processes (e.g. visit by doctor, testing, and treatments). Mathematically, the hospital model can be viewed as a queueing network, where each unit is modeled as a queue that is served by one or more servers. Upon arrival, patients (customers) enter the queue and wait for service. After completing service, the patient moves to the next queue along her care path.

Figure 1(b) is a high-level schematic of the flow of patients through a unit with its associated processes. Patients enter each unit either directly (e.g. through the ED entrance or a scheduled surgery) or from other units.

Figure 1(c) illustrates how the simulation operates. The model is stochastic: patient arrivals and their processing follow characteristic probability distributions. Assumptions, parameters, and inputs for the base model (e.g. probability distributions with their parameters and available resources) are documented in the original reference.[19] Assumptions and parameters developed for the original hospital model were developed from findings from the literature (e.g. national averages) and discussions with hospital managers within the Johns Hopkins Hospital System (JHHS), Suburban Hospital and Johns Hopkins Office of Critical Event Preparedness and Response (CEPAR). The model was verified with the help of expert collaboration and review. Additional details of the verification process are given by Tariverdi et al.[19]

As in the real world, the exact events (e.g. number of patients to arrive with their specific needs and need levels) and their timing occur differently from day to day. The

stochastic DES replicates this random setting. To evaluate the performance of the hospital, thus, a measure, such as expectation, over the various ways random events can be realized must be used. To this end, the expected performance given in terms of various performance metrics (e.g. hospital or ED throughput) is approximated by computing the average metric value over multiple replications, each with a different realization of events and their timing. Each run of the simulation follows a set of patients as they arrive at the hospital, progress through treatment, and experience outcomes (e.g. discharge or leave without being seen).

*Modeling Cyberattack Events and Recovery Strategies within the Simulation*. The hospital model was modified to incorporate the occurrence of a ransomware attack. A significant effect of a cyberattack on the provision of hospital services is the slowing down of processes that depend on information technology. This slowing of processes was represented in the simulation by adjusting the parameters of the probability distributions on the time each affected process takes. For purposes of this analysis and because it was assumed that the attack was directed against the most critical units (ED, ICU, and labs), the processing times for only these units are increased in replicating the cyberattack.

The slowdown may be significant enough that the ED can no longer accept new patients, resuming services only after its IT systems can be repaired to an acceptable level of functionality. Within the simulation model, this was achieved by adding a queue with zero processing time just prior to the ED entrance. Scheduled surgical patients enter through a separate entry point and, aside from delays in the labs, were unimpacted by the cyberattack. Like other queues, the ED pre-entry queue requires a server to process patients. To prevent patient entry, no personnel resources are assigned to this entry queue during the ED entry closure. This results in all patients who seek services through the ED to depart without entering during its closure. Once the ED entry is reopened, resources for processing patients at this queue are set to infinity.

Two response plans to the cyberattack were considered: (a) paying the ransom (*Pay*.) and then completing a full recovery and (b) undertaking a full recovery using the hospital's onsite backup or recovery solution (*NoPay*). Two additional cases were also run for comparison: a base case in which no attack occurs (*Base*) and a worst-case response plan in which the hospital does nothing to recover from the attack (*DoN*). The latter is unrealistic, but serves as a point of comparison. The ED entry is presumed to remain open under the *DoN* case. Understanding how the hospital fares when taking no response action provides insights into the hospital's inherent capacity to cope with the cyberattack.

The slowdown due to the cyberattack was represented in the simulation through the application of multipliers on pertinent model parameters. The multipliers reflect how much longer the affected processes take due to the impacts of the cyberattack and the effectiveness of response actions. Additionally, the multipliers are time-dependent. Changes in the multipliers replicate achievements from the recovery actions as they are gained over time. Additionally, the duration of the ED entry closure was set in each tested scenario according to whether the ransom is paid.

## Numerical experimental design of scenarios

The simulation was implemented in the Extendsim™ discrete event simulation software. U.S. urban hospitals often operate near capacity. Consistent with this, the emergency patient arrival rate in the model was set to 200 patients/day. Each run of the simulation begins with a 40-day "warmup" period followed by a 20-day period scenario during which various performance metrics were collected. The model was run 250 times for each of the four cases (*Pay*, *NoPay*, *DoN*, *Base*). 250 was chosen based on systematically designed experiments of between 10 and 5000 runs. This number provided a sufficient sample size for accurate estimates of performance metrics given the needed run times for completing the batch runs. A batch run of 5000 runs requires more than a day to complete. The result of making 250 runs is, thus, a statistical sample of each performance measure across the set of runs for each response plan.

The expected time $\tau_i^k(t)$ taken by process $i$ on day $t$ for response plan $k$ is calculated as in equation (1):

$$\tau_i^k(t) = M_i^k(t) \times \tau_i^{Base}(0) \quad (1)$$

Here, the multiplier $M_i^k(t) \geq 1$ represents the slowdown over the base case due to the cyberattack. Processing times spike to their highest values on the first day of the attack: $\tau_i^k(1) = \tau_i^k(0) \times M_i^k(1) = \tau_i^k(1) \geq \tau_i^k(t)$ for $t \geq 1$. If no action is taken to respond to the cyberattack, the longer processing times continue for the duration of the simulation: $\tau_i^{DoN}(t) = \tau_i^{DoN}(1)$ for $t \geq 1$.

Values for the multipliers are shown in Figure 2. Figure 2 also shows the period, for each scenario, during which the hospital stops accepting new patients into the ED, diverting emergency cases to other hospitals. The multiplier values and closure periods are based on judgments of one of the co-authors who is an expert in hospital information technology and cybersecurity. The original parameters for the no-attack base case were taken from Tariverdi et al.[19]

As shown in Figure 2, paying the ransom (the *Pay* strategy) is presumed to incur a shorter closure period (2 days), allowing a faster start to recovery. In contrast, the no-payment (*NoPay*) strategy is expected to incur a longer closure period (3 days) and a slower start to recovery, but a faster time to complete rovery. The slower time to full recovery for the payment strategy is due to the additional effort required to remove intrusion software as is needed to ensure future security from attack after full access has been restored.

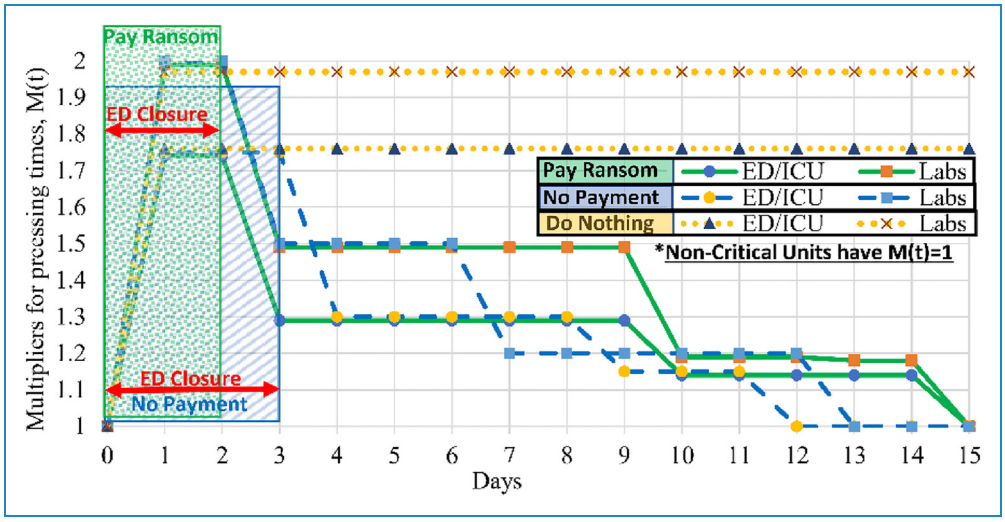


**Figure 2.** Day-dependent service time multipliers and closure periods by recovery plan.

### *Performance measures*

Performance measures were computed, exported from the simulation, and averaged over the 250 runs for the base case and each of the response plans. The metrics fall into four broad categories: (a) patients served, reported as hospital and ED throughput given in terms of total 7-day throughput and daily throughput over the event impact duration; (b) daily ED and ICU bed utilization rates, computed as the portion of total beds within the unit in use on a given day on average; (c) unmet demand (sum of patients who are turned away before triage due to ED closure or capacity limitations at triage and patients who pass through the ED triage but do not receive treatment due to prolonged waiting time); and (d) resilience.

Resilience is measured from two perspectives. First, it is taken as a ratio of experienced performance to performance under pre-attack conditions (using the base case of no attack). Here, the ratio is computed over hospital throughput by day 7, one week from the inception of the attack and day 14, two weeks after inception of the attack. This approach ensures a resilience value that is between 0 and 1. Values closer to 1 indicate less impact of the attack on overall performance. Lower impact occurs if the system is able to cope with the event via excess capacity or redundancy and/or very quick response action. This approach to resilience measurement was proposed by Chen and Miller-Hooks[23] for intermodal freight transport applications and is termed period resilience in the context of general infrastructure systems by Faturechi and Miller-Hooks.[24] These concepts were adapted here for the context of a single hospital.

Second, resilience is measured in terms of the time it takes for the system to reach a target level of functionality. This approach was recommended in the San Francisco Planning and Urban Research Association resilience standards in relation to seismic mitigation planning for San Francisco.[25] This work, they consider the time to resume services supported by utilities, transportation and buildings. Here, functionality is considered in terms of hospital throughput.

## Results

### *Hospital discharge and ED throughput performance*

Results for hospital and ED throughput are presented graphically in Figure 3. Each line shows daily performance for one of the strategies averaged over the 250 simulation runs. Error bars indicate uncertainty in the estimate due to the stochastic nature of the simulation. Additional runs beyond 250 could reduce the size of the confidence interval around each estimate.

Figure 3(a) shows the hospital profile of performance for treated patient discharge. In the *Base* case, an average of 191 treated patients are discharged each day. For both the *Pay* and the *NoPay* strategies, the number of discharged patients drops rapidly to 25 patients the day after ED closure, and begins to pick up after the ED reopens to 117 patients per day, or about 60% of normal capacity, by the 5th day after the attack. Over the following week, performance recovers more slowly under the *Pay* strategy than under the *NoPay* strategy, reflecting the longer recovery time, to ensure that no remnants of the attack remain.

A similar pattern is seen in Figure 3(b), which shows a drop to zero in ED throughput the day after the ED entry closes, followed by a recovery after reopening that is initially faster under the *NoPay* than the *Pay* strategy, but is ultimately beaten by the *NoPay* strategy.

The graphs of Figure 3, thus, show a short-term gain from paying the ransom in that the ED is able to reopen

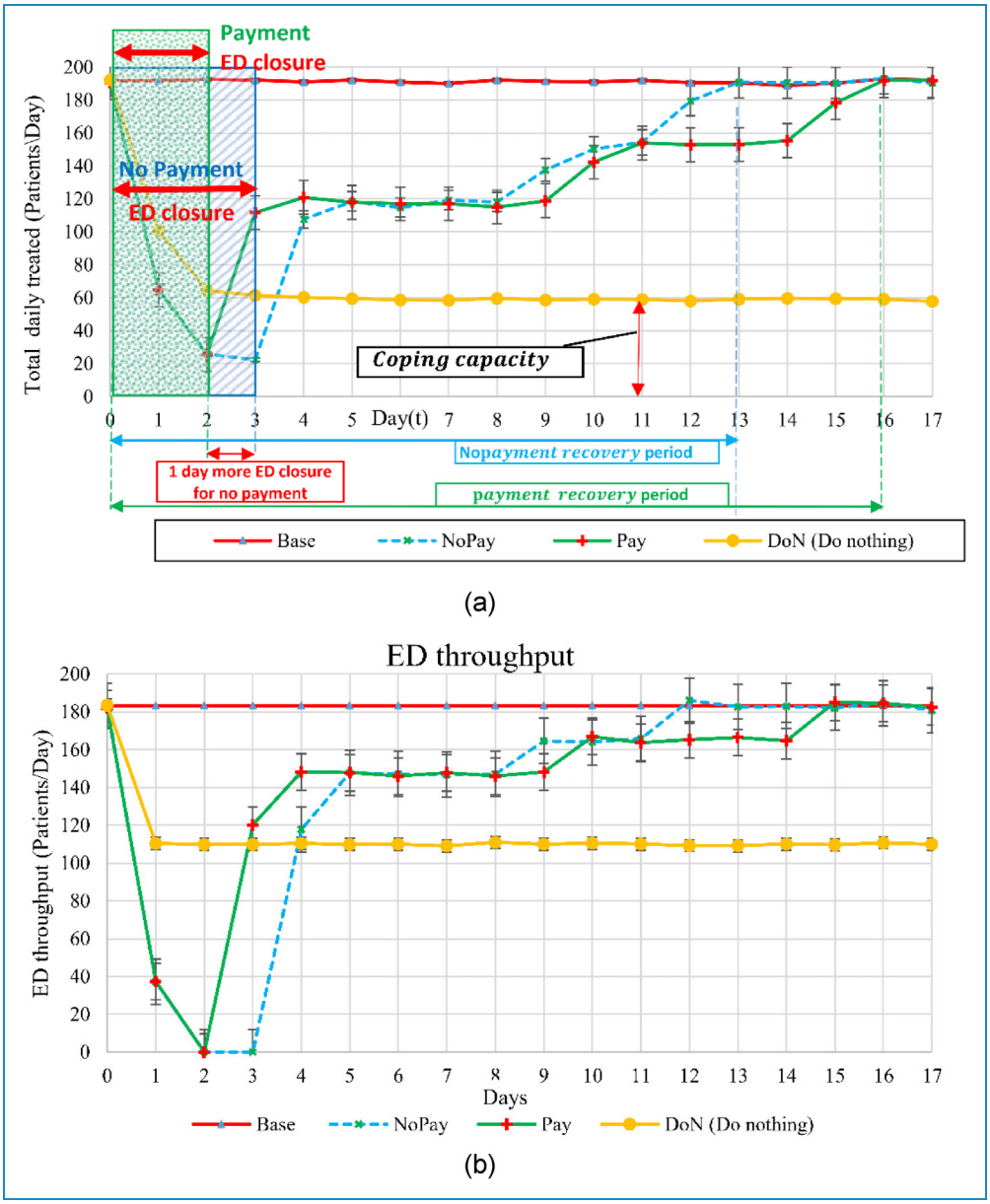


**Figure 3.** (a)total daily hospital discharge for base case and response plans (b)ED throughput.

sooner; however, this is balanced by a longer recovery to full capacity.

The inherent coping capacity of the hospital can also be seen by examining performance under the *DoN* response. If no action is taken to respond to the attack, hospital throughput drops and converges by day 3 to an average value of 60 patients/day, less than a third of the 191 patients treated under the *Base* case of no attack. For ED throughput, the throughput is less than ¼ of the normal base case, showing a diminished coping capacity to an attack of this magnitude and the necessity for developing a recovery strategy in advance.

Another view on hospital resilience is given in Table 5, which shows the day at which a given target performance level is reached. For total discharged patients, the *Pay* strategy reaches a 50% target performance level one day faster than the *NoPay* strategy, reflecting the one day shorter ED entry closure. Average discharge under both strategies reaches 80% on day 11. The *NoPay* strategy rebounds to 90% of the target levels three days faster than the *Pay* strategy.

To evaluate the resilience of the hospital under the *Pay* versus the *NoPay* strategy, Table 6 shows, for each strategy, treated patient discharge over a one-week and a two-week period, shown as a percentage of the base case and as a total number of patients. The attack has a major impact: over two weeks, both ED throughput and total patient throughput are roughly 1000 patients fewer than under

**Table 5.** First day after attack on which performance reaches various levels.

| | | | ≥ 50% | | ≥ 80% | | ≥ 90% | |
|---|---|---|---|---|---|---|---|---|
| Performance Measure | Base case | Response | Patients | Day | Patients | Day | Patients | Day |
| **Total discharged patients** | **191 (patient/day)** | *Pay* | 112 | 3 | 154 | 11 | 178 | 15 |
| | | *NoPay* | 108 | 4 | 154 | 11 | 180 | 12 |
| **ED throughput** | **175 (patient/day)** | *Pay* | 110 | 3 | 140 | 11 | 168 | 15 |
| | | *NoPay* | 107 | 4 | 139 | 11 | 170 | 12 |

**Table 6.** Resilience values.

| | | Week 1 | | Week 2 | |
|---|---|---|---|---|---|
| Performance Measure | Response | Patients | percent | Patients | percent |
| **Total discharged patients** | *Base* | 1341 | 100 | 2677 | 100 |
| | *Pay* | 675 | 50 | 1667 | 62 |
| | *NoPay* | 573 | 43 | 1695 | 63 |
| **ED throughput** | *Base* | 1224 | 100 | 2449 | 100 |
| | *Pay* | 532 | 43 | 1414 | 58 |
| | *NoPay* | 427 | 35 | 1449 | 59 |

the base case. The importance of mounting an effective response is seen by comparing these values with the *DoN* strategy, not shown in the table. For *DoN*, the loss is even greater, at over 2000 patients.

At day 7, the *Pay* strategy performs 7 percentage points higher than the *NoPay* strategy (50% vs. 43% of the pre-attack throughput, or 102 total patients). That is, paying the ransom and reopening the ED entry a day sooner allows a total of 102 more patients to be treated and discharged over the first week. However, by day 14, the *NoPay* strategy passes the *Pay* strategy (63% vs. 62% of the average pre-attack throughput, or 28 total patients).

A similar pattern occurs for ED throughput. The resilience measure at day 7 is higher for the *Pay* than for the *NoPay* strategy (43% vs. 35% of the pre-attack throughput, or 105 total patients); at day 14, *NoPay* pulls ahead by one percentage point (59% vs. 58% of the average pre-attack throughput, or 35 more patients treated under *NoPay*). That is, although the *Pay* strategy requires a shorter period of ED closure, thus allowing more patients to be treated over the first week post-attack, the faster recovery to full performance under the *NoPay* strategy means that this short-term gain is surpassed over the next week. By two weeks after the attack, the *NoPay* strategy is slightly better than the *Pay* strategy both in terms of the total number of patients treated in the ED and the total number of patients discharged from the hospital since inception of the attack. By the time the hospital reaches full recovery under both strategies, after day 16, on average 42 more patients are discharged from the hospital and 41 more patients treated in the ED in total under the *NoPay* strategy than under the *Pay* strategy.

## Unit utilizations

Figure 4(a) and (b) show utilization for the ICU and ED, respectively. Comparing these two graphs, the ICU shows a longer lag in returning to routine levels than the ED. This is in part due to the slowdown and in part to demand. That is, there is a lag in patients reaching the ICU from other units. In the base case, the ICU and ED operate with average utilization of about 70% and 40%,

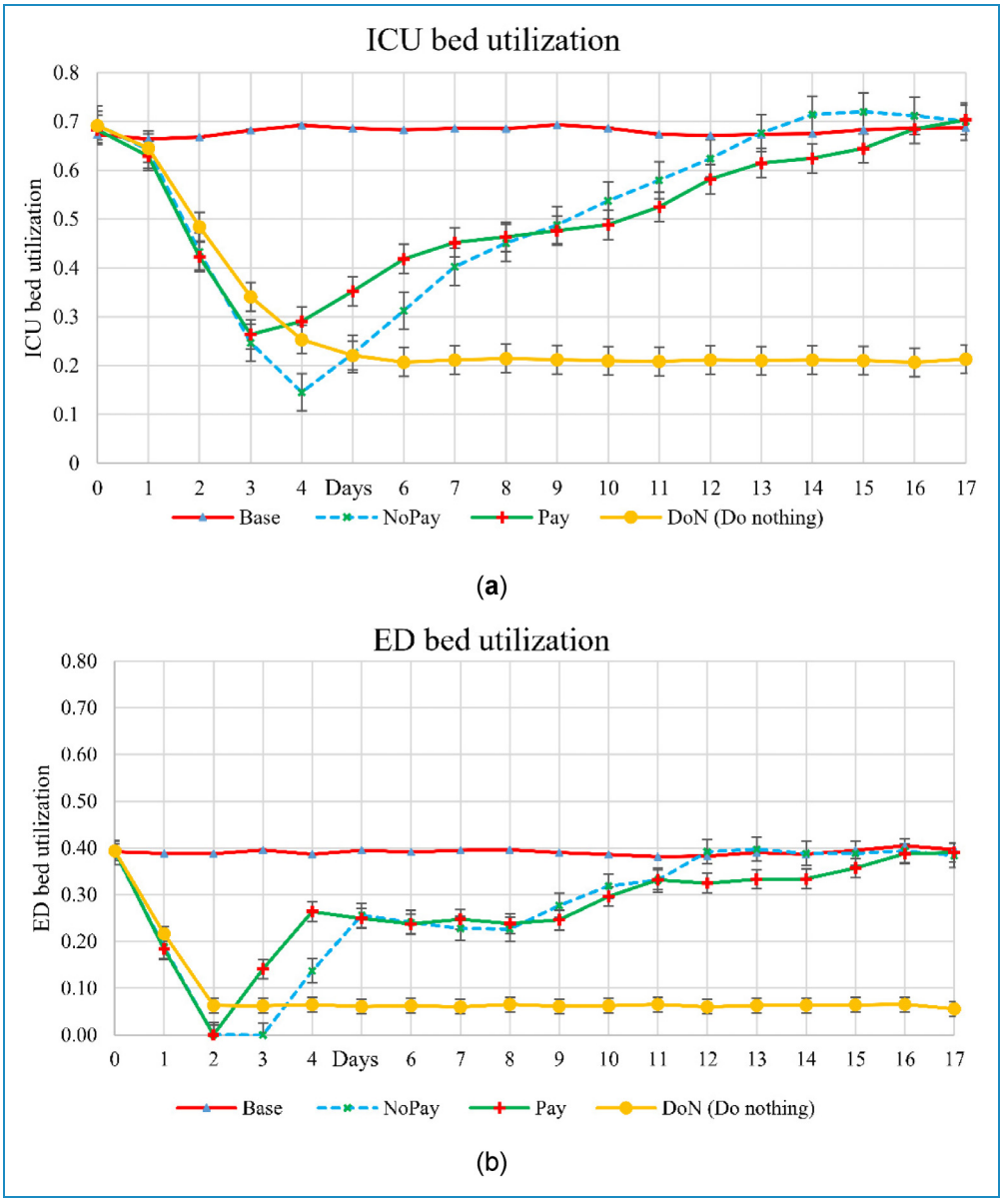


**Figure 4.** Unit utilization rates in: (a) ICU and (b) ED.

respectively. The extra capacity can be used to compensate for surge demand and output slowdown. Note that utilization can exceed that of the *Base* case when the processing time is higher because of the cyberattack, leading to patients remaining longer in the unit. These considerations should be recognized when planning for the capacity needed to achieve resilience to cyberattacks and other disruptions.

## Unmet demand

Figure 5(a) shows unmet demand. In the worst case of the *DoN* strategy, unmet demand averages 160 patients/day. This is over six times the base case, wherein an average of 26 patients/day are unserved. The *Pay* strategy shows a longer period of elevated unmet demand than the *NoPay* strategy due to the longer period of elevated multipliers (see Figure 2) consistent with the extended duration needed to complete the system recovery.

The total unmet demand from day 3 (ED reopening for the *Pay* strategy) through day 5 (day after reopening for the *NoPay* strategy) is 102 patients fewer for the *Pay* strategy than for the *NoPay* strategy. This is the cost in unmet demand for the additional day of ED closure. The total unmet demand from day 6 through day 16 (when the hospital is fully recovered under both *Pay* and *NoPay* strategies) is 147 patients more under the *Pay* strategy than for the *NoPay* strategy. This is the cost in unmet demand for the longer recovery time of the *Pay* strategy. Thus, after full

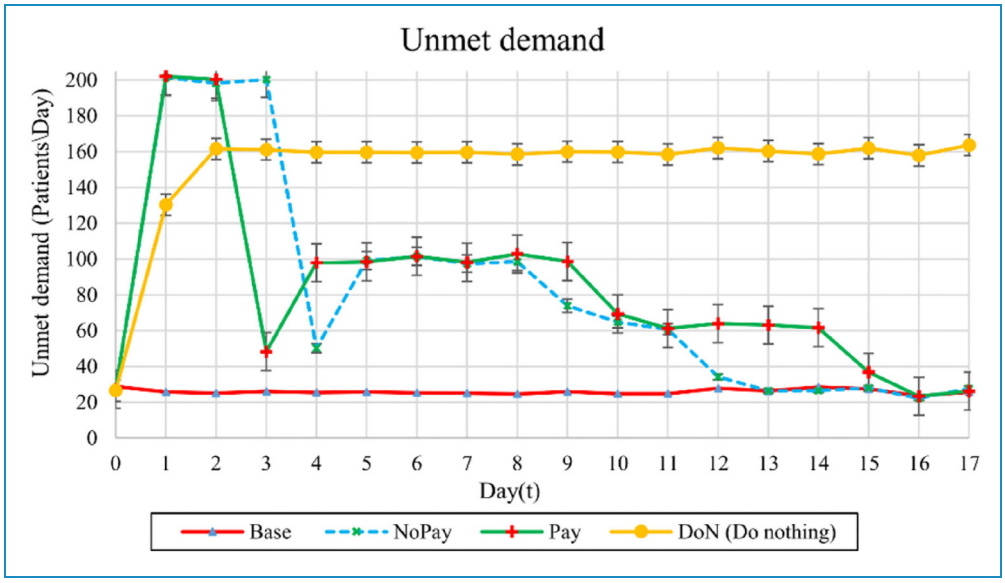


**Figure 5.** Unmet demand, including those patients who are turned away before triage and patients who cannot receive treatment in reasonable time due to prolonged waits.

recovery, on average, 45 fewer patients (or between 30 and 60 with 95% confidence) were served in runs when the ransom was paid than in runs when onsite recovery was undertaken.

## Discussion

As concerns grow about cyberattacks against hospitals, this paper provides a methodology for quantitatively assessing the effect of cyberattacks on hospital performance metrics, outputs, and different response scenarios. A discrete event simulation model of a trauma III hospital was adapted to model a cyberattack involving ransom and to analyze the effects of different response strategies.

Results of the model runs showed that the envisioned cyberattack scenario had a major impact on the performance of the test hospital. Under recovery strategies that do and do not pay a ransom, total patient throughput drops by approximately 1000 patients out of about 2700 total patients over a two-week period. In both cases, the ICU showed a longer lag in returning to routine capacity than the ED. This is due both to the slowdown from the attack and the lag in patients reaching the ICU from other units once they are admitted again through the ED. ICU utilization sometimes exceeded routine levels after the attack, indicating that excess capacity may contribute to the hospital's resilience.

There was a short-term gain from paying the ransom in that roughly 100 more total patients were served in the first week post-attack due to a shorter ED closure when the ransom was paid. However, paying the ransom resulted in a slower time to full recovery due to the additional effort needed to ensure all remnants of the attack were removed. Over the approximately two weeks until the hospital returned to normal functionality, the short-term gain from paying the ransom was more than offset by the faster return to normal functioning under the nonpayment option. By the time full recovery was achieved, approximately 45 fewer patients were served when the ransom was paid than when onsite recovery was undertaken.

Analysis conducted here uses hospital-wide and unit-based patient throughputs, unmet demand, and unit-based utilization as key performance indicators. These metrics are important determinants of the hospital's ability to provide emergency care to patients, but are not the only factors that should be considered in determining a best strategy for coping with a ransomware attack. Other effects of the attack, such as delays in diagnosis, impact on quality of care, and adverse patient outcomes due to delays should also be carefully weighed.

Additional effects of a cyberattack include disruption of non-emergency services, such as scheduling and conducting elective surgeries. The attack may also impact patient length of stay in affected hospital units. Longer service times could impede the recovery, as patients who enter may need to stay longer. With data on these impacts, this study can be extended to quantify the outcomes from these factors. Moreover, further investigation of other cyberattack scenarios could provide additional insights.

Paying the ransom can have other negative consequences as well. There is no guarantee that the attackers will provide the decryption key even if the ransom is paid; there is no guarantee of full recovery;[26] attackers may even demand a second ransom;[27] and payment encourages future attacks.[28]

Although victims of a ransomware attack often pay the ransom, these considerations, along with the results of the model and the recommendations of the FBI,[28] suggest that the short-term gains from paying the ransom may not prove to be worthwhile in the longer term. Further study is required to more fully understand the ramifications for the patients across hospital units of a No Pay strategy and their magnitude as a function of the hospital's in-place recovery capabilities and capacity.

This paper focuses specifically on a ransomware attack where the main attack mode is through penetration of one or more systems and encryption of critical data, including, for example, the electronic medical records. There are numerous other forms of attack of equal concern, e.g. a DDoS or phishing attack with incursion that overcomes security barriers. The methods applied in this work may also be used to study a hospital's resilience to such attacks as they often involve similar methods of recovery with comparable delays in enabling full services.

Offsite disaster recovery solutions, such as duplicative data centers, may allow for real- or near real-time recovery, obviating the need to pay a ransom to attackers. Hospitals also have the option to purchase cloud-based recovery solutions, the cost of which depends on the contracted time-guarantee on restoration. The specific value of such cloud-based alternatives to a hospital in terms of patients served and greater hospital resilience could be considered in future simulation studies.

**Acknowledgements:** We sincerely appreciate Scott Larsen, Matthew Wilkes, and Beau Woods for lending their time in interviews that provided valuable subject-matter expertise in hospital cybersecurity.

**Author Contributions:** HG implemented the cyberattack model in the simulation, designed and ran the experiments, prepared the results, and contributed to the writing. KBL and EM-H. developed the concept, supervised the study, advised on the experiments and interpretation of the results, and wrote portions of the paper. CH as a hospital IT expert advised on how to model effects of and responses to a cyberattack, guided the design of the cyberattack scenario, provided feedback on the model and results, and reviewed the paper. MT advised on the experiments and interpretation of the results.

**Declaration of Conflicting Interests:** The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding:** The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Virginia Research Investment Fund through the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation and workforce development (grant number 223587) and by the World Bank Group and National Science Foundation (grant number 2027624).

**Ethical approval:** This research did not make use of human subjects. The George Mason University Office of Research Integrity and Assurance confirmed that no IRB approval was necessary for the interviews that were conducted with hospital information technology experts.

**Guarantor:** KBL

**ORCID iD:** Hadi Ghayoomi https://orcid.org/0000-0002-8134-1784
Kathryn Laskey https://orcid.org/0000-0002-3106-140X

**Peer review**

## References

1. Parasrampuria S and Henry J. Hospitals' use of electronic health records data, 2015-2017. *Office of the National Coordinator for Health Information Technology (ONC)*; 2019. Report No.: No. 46.
2. Frost & Sullivan. Internet of Medical Things, Forecast to 2021 [Internet]. *Frost & Sullivan*; 2017 Jun [cited 2021 Jun 1]. Report No.: K1AB-01-00-00–00. Available from: https://store.frostcom/internet-of-medical-things-forecast-to-2021.html.
3. Safety Detectives Cybersecurity Team. Healthcare Cybersecurity: The Biggest Stats & Trends in 2021 [Internet]. *The SafetyDetectives research lab*; 2021 [cited 2021 Jun 3]. Available from: https://www.safetydetectives.com/blog/healthcare-cybersecurity-statistics/.
4. Fuentes Rosario M. Cybercrime and Other Threats Faced by the Healthcare Industry [Internet]. *Trend Micro Incorporated*; [cited 2021 Aug 2]. Available from: https://documents.trendmicro.com/assets/wp/wp-cybercrime-and-other-threats-faced-by-the-healthcare-industry.pdf.
5. Black Book Market Research LLC. Healthcare Data Breaches Costs Industry $4 Billion by Year's End, 2020 Will Be Worse Reports New Black Book Survey [Internet]. *Cision distribution by PR Newswire*. 2019 [cited 2021 Jul 20]. Available from: https://www.prnewswire.com/news-releases/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-will-be-worse-reports-new-black-book-survey-300950388.html.
6. Morse A. Investigation: WannaCry cyber attack and the NHS [Internet]. National Audit Office (NAO); 2017 May [cited 2021 Aug 5]. Report No.: 9781786041470. Available from: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.
7. Davis J. Nearly a year since WannaCry and all 200 National Health Service trusts failed cybersecurity assessments [Internet]. *Healthcare IT News*. 2018 [cited 2021 Mar 13]. Available from: https://www.healthcareitnews.com/news/nearly-year-wannacry-and-all-200-national-health-service-trusts-failed-cybersecurity.
8. Chappell B and Penman M. Ransomware Attacks Ravage Computer Networks In Dozens Of Countries. *NPR* [Internet]. 2017 May 12 [cited 2021 Aug 4]; Available

from: https://www.npr.org/sections/thetwo-way/2017/05/12/528119808/large-cyber-attack-hits-englands-nhs-hospital-system-ransoms-demanded.
9. Food and Drug Administration (FDA). URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication [Internet]. Food and Drug Administration; 2019 Oct [cited 2021 Mar 13]. Available from: https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce.
10. Franklin C. Series of Zero-Day Vulnerabilities Could Endanger 200 Million Devices [Internet]. *Dark Reading*. 2019 [cited 2021 Mar 13]. Available from: https://www.darkreading.com/endpoint/series-of-zero-day-vulnerabilities-could-endanger-200-million-devices/d/d-id/1335379.
11. Dyrda L. "It's not a good week for healthcare": Health system IT execs react to recent ransomware attacks [Internet]. *Becker's healthcare*. 2020 [cited 2021 Mar 13]. Available from: https://www.beckershospitalreview.com/cybersecurity/it-s-not-a-good-week-for-healthcare-health-system-it-execs-react-to-recent-ransomware-attacks.html.
12. Ayala L. Cybersecurity for Hospitals and Healthcare Facilities - A Guide to Detection and Prevention. 1st ed. Berkeley, CA: Apress; 2016, 15–65.
13. Davis J. RamaOnHealthcare - Healthcare Cyberattacks Doubled in 2020, with 28% Tied to Ransomware [Internet]. *RamaOnHealthcare*. 2021 [cited 2021 Jun 2]. Available from: https://ramaonhealthcare.com/healthcare-cyberattacks-doubled-in-2020-with-28-tied-to-ransomware/.
14. The Financial Crimes Enforcement Network (FinCEN). Financial Trend Analysis: Manufacturing and Construction Top Targets for Business Email Compromise [Internet]. *Financial Crimes Enforcement Network*; 2019 Jul [cited 2021 Jul 30]. Available from: https://www.fincen.gov/news/news-releases/financial-trend-analysis-manufacturing-and-construction-top-targets-business.
15. Shortle JF, Thompson JM, Gross D, et al. *Fundamentals of Queueing Theory*. 5th Edition. Hoboken, New Jersey: Wiley; 2018, 417–517.
16. Sams J. Vermont hospital cyber attack cost estimated at $1.5M a Day [internet]. *Insurance Journal* 2020 [cited 2021 Aug 2]; Available from: https://www.insurancejournal.com/news/east/2020/12/15/593996.htm.
17. Seals T. Exclusive Ransomware Poll: 80% of Victims Don't Pay Up [Internet]. *Threat post* 2021 [cited 2021 Jul 14]. Available from: https://threatpostcom/ransomware-victims-dont-pay-up/166989/.
18. Maggio LA, Dameff C, Kanter SL, et al. Cybersecurity challenges and the academic health center: an interactive tabletop simulation for executives. *Acad Med* 2021 Jun 1; 96: 850–853.
19. TariVerdi M, Miller-Hooks E, Kirsch T, et al. A resource-constrained, multi-unit hospital model for operational strategies evaluation under routine and surge demand scenarios. *IISE Transactions on Healthcare Systems Engineering* 2019 Apr 3; 9: 103–119.
20. TariVerdi M, Miller-Hooks E and Kirsch T. Strategies for improved hospital response to mass casualty incidents. *Disaster med Public Health Prep* 2018 Dec; 12: 778–790.
21. Shahverdi B, Tariverdi M and Miller-Hooks E. Assessing hospital system resilience to disaster events involving physical damage and demand surge. *Socioecon Plann Sci* 2020 Jun; 70: 100729.
22. Shahverdi B, Miller-Hooks E, Tariverdi M, et al. Assessing strategies for improving hospital capacity for handling patients during a pandemic. *Healthcare Management Science*, in review.
23. Chen L and Miller-Hooks E. Resilience: an indicator of recovery capability in intermodal freight transport. *Transportation Science* 2012 Feb 1; 46: 109–123.
24. Faturechi R and Miller-Hooks E. A mathematical framework for quantifying and optimizing protective actions for civil infrastructure systems. *Computer-Aided Civil and Infrastructure Engineering* 2014; 29: 572–589.
25. Poland C. The Resilient City: Defining What San Francisco Needs from its Seismic Mitigation Policies [Internet]. Earthquake Engineering Research Institute; 2008 Jan [cited 2021 Jun 19]. Available from: https://mitigation.eeri.org/resource-library/policy-and-community-planners/the-resilient-city-defining-what-san-francisco-needs-from-its-seismic-mitigation-policies.
26. Sienko C. Ransomware Case Studies: Hollywood Presbyterian and The Ottawa Hospital [Internet]. *Infosec Resources*. [cited 2020 Jun 19]. Available from: https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/ransomware-case-studies-hollywood-presbyterian-and-the-ottawa-hospital/.
27. Dyrda L. The 5 most significant cyberattacks in healthcare for 2020 [Internet]. *Becker's IT health*. 2020 [cited 2021 Mar 14]. Available from: https://www.beckershospitalreview.com/cybersecurity/the-5-most-significant-cyberattacks-in-healthcare-for-2020.html.
28. Federal Bureau of Investigation (FBI). Ransomware Prevention and Response for CEOs [Internet]. Federal Bureau of Investigation FBI; 2016 Jul [cited 2021 May 30]. Available from: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-ceos.pdf/view.
29. Ghafur S, Kristensen S, Honeyford K, et al. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digital Medicine* 2019 Oct 2; 2: 1–7.
30. Genovese M. Top 5 cyberattacks against the health care industry [Internet]. *Stormshield*. 2019 [cited 2021 Mar 13]. Available from: https://www.stormshield.com/news/top-5-cyberattacks-against-the-health-care-industry.
31. Kolbasuk McGee M. Boston Children's Hospital DDoS Attacker Convicted [Internet]. *bank info security*. 2018 [cited 2021 Mar 13]. Available from: https://www.bankinfosecurity.com/boston-childrens-hospital-ddos-attacker-convicted-a-11279.
32. Athena M. DDoS Attacks | How DDoS affected Boston Children Hospital? [Internet]. *The Threat Report (TTR)*. 2019 [cited 2021 Mar 14]. Available from: https://thethreatreport.com/story-behind-the-ddos-attack-vs-boston-children-hospital/.
33. Living L. Hackers Are Coming For Medical Devices, Here's How to Defend [Internet]. *Cyware Hacker News*. 2019 [cited 2021 Mar 13]. Available from: https://cyware.com/news/hackers-are-coming-for-medical-devices-heres-how-to-defend-293d45cc.

34. Storm D. Hollywood hospital hit with ransomware: Hackers demand $3.6 million as ransom [Internet]. *Computerworld*. 2016 [cited 2021 Mar 13]. Available from: https://www.computerworld.com/article/3032310/hollywood-hospital-hit-with-ransomware-hackers-demand-3-6-million-as-ransom.html.
35. Pressey D. C-U Public Health District's website held hostage by ransomware attack [Internet]. *The News-Gazette*. [cited 2021 Mar 14]. Available from: https://www.news-gazette.com/news/local/health-care/c-u-public-health-districts-website-held-hostage-by-ransomware-attack/article_2dadedcd-aadb-5cb1-8740-8bd9e8800e27.html.
36. Barry E and Perlroth N. Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack. *The New York Times* [Internet]. 2020 Nov 26 [cited 2020 Dec 1]; Available from: https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.
37. Coble S. Ransomware Attack Costs Health Network $1.5m a Day [Internet]. *Infosecurity Magazine*. 2021 [cited 2021 May 31]. Available from: https://www.infosecurity-magazine.com:443/news/ransomware-attack-costs-health/.
38. Laura D. UVM Health cyberattack losses to exceed $63M: 5 details [Internet]. *Becker's IT health*. 2020 [cited 2021 Mar 13]. Available from: https://www.beckershospitalreview.com/cybersecurity/uvm-health-cyberattack-losses-at-63m-and-counting-5-details.html.
39. Davis J. Ransomware Attack on Maryland's GBMC Health Spurs EHR Downtime [Internet]. *HealthITSecurity*. 2020 [cited 2021 Mar 14]. Available from: https://healthitsecurity.com/news/ransomware-attack-on-marylands-gbmc-health-spurs-ehr-downtime.
40. Dyrda L. 6 hospital ransomware attacks in 24 h prompts US advisory: 8 things to know [Internet]. *Becker's IT health.* 2020 [cited 2021 Mar 14]. Available from: https://www.beckershospitalreview.com/cybersecurity/6-hospital-ransomware-attacks-in-24-hours-prompts-us-advisory-8-things-to-know.html.
41. Seh AH, Zarour M, Alenezi M, et al. Healthcare data breaches: insights and implications. *Healthcare (Basel) [Internet* 2020 May 13 [cited 2021 Mar 25]; 8(2): 133. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/.
42. ProCircular. Business Email Compromise Incident: Large Health Care Organization [Internet]. *ProCircular*. [cited 2021 Jul 9]. Available from: https://www.procircular.com/case/business-email-compromise-incident-with-large-health-care-organization/.
43. HHS Office of Inspector General. National Health Care Fraud Takedown [Internet]. *Office of Inspector General | Government Oversight | U.S. Department of Health and Human Services*. 2020 [cited 2021 Jul 9]. Available from: https://oig.hhs.gov/newsroom/media-materials/2020takedown/. 2020.
44. Collier K. Cyberattack hits major hospital system, possibly one of the largest in U.S. history [Internet]. *NBC News*. 2020 [cited 2021 Jul 23]. Available from: https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254.
45. cynerio.com [Internet]. Rise in Cyber Attacks on Healthcare Institutions Increases Patient Mortality [Internet]. *cynerio*. 2020 [cited 2021 Jul 23]. Available from: https://www.cynerio.com/blog/rise-in-cyber-attacks-on-healthcare-institutions-increases-patient-mortality.
46. Alder S. Methodist Hospital in Lockdown After Ransomware Attack. *HIPAA Journal [Internet]* 2016 Mar 21 [cited 2021 Jul 23]; Available from: https://www.hipaajournal.com/methodist-hospital-in-lockdown-after-ransomware-attack-3363/.
47. Evans M. Cyberattack Causes Surgeons to Cancel Some Operations. *Wall Street Journal [Internet]* 2017 Jun 28 [cited 2021 Jul 23]; Available from: https://www.wsj.com/articles/cyberattack-causes-surgeons-to-cancel-some-operations-1498686899.
48. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin M-V, Calcavecchia F, Anderson D, et al. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making* 2020 Jul 3; 20: 146.
49. Akpan N. Ransomware and data breaches linked to uptick in fatal heart attacks [Internet]. PBS NewsHour. 2019. Available from: https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.