Journal of the American Medical Informatics Association, 00(0), 2021, 1–8
doi: 10.1093/jamia/ocab142
Research and Applications

Research and Applications

The relationship between cybersecurity ratings and the risk of hospital data breaches

Sung J. Choi [1] **and M. Eric Johnson** [2]

[1]School of Global Health Management and Informatics, College of Community Innovation and Education, University of Central Florida, Orlando, Florida, USA, and [2]Owen Graduate School of Management, Vanderbilt University, Nashville, Tennessee, USA

Corresponding Author: Sung J. Choi, PhD, Department of Health Management and Informatics, University of Central Florida, 528 West Livingston St, Orlando, FL 32801 USA; sung.choi@ucf.edu

Received 27 November 2020; Revised 1 June 2021; Editorial Decision 23 June 2021; Accepted 24 June 2021

ABSTRACT

Objective: We investigated the progression of healthcare cybersecurity over 2014–2019 as measured by external risk ratings. We further examined the relationship between hospital data breaches and cybersecurity ratings.
Materials and Methods: Using Fortune 1000 firms as a benchmark, time trends in hospital cybersecurity ratings were compared using linear regression. Further, the relationship between hospital data breaches and cybersecurity ratings was modeled using logistic regression. Hospital breach data were collected from US HHS, and cybersecurity ratings were provided by BitSight. The resulting study sample yielded 3528 hospital-year observations.
Results: In aggregate, we found that hospitals had significantly lower cybersecurity ratings than Fortune 1000 firms, however, hospitals have closed the gap in recent years. We also found that hospitals with the low security ratings were associated with significant risk of a data breach, with the probability of a breach in a given year ranging from 14% to 33%.
Discussion: Recent cyber-attacks in healthcare continue to illustrate the need to better secure information systems. While hospitals have reduced cyber risk over the past decade, they remain statistically more vulnerable than the Fortune 1000 firms against botnets, spam, and malware.
Conclusion: Policy makers should continue encouraging acute-care hospitals to proactively invest in security controls that reduce cyber risk. Best practices from other sectors like the financial services sector could provide useful guides and benchmarks for improvement.

Key words: cybersecurity, health information technology, hospital data breach, risk rating

INTRODUCTION

Over the past decade, data breaches have grown to become a significant threat for hospitals and health systems.[1–3] Recently, ransom ware attacks on hospitals have disrupted critical operations and cost millions in ransom payments.[4–6] This growth in breaches has coincided with significant investment in health information technology (IT). As part of the 2009 HITECH Act, the US government allocated nearly $40 billion in support of the adoption of electronic health records (EHRs).[7,8] By 2016, healthcare was estimated to be the fastest-growing industry in IT expenditure with a compound annual growth rate of 5.5%.[9] Virtually all nonfederal acute care hospitals (96%) possessed some stage of certified EHR technology in 2015.[10]

The federal funding of health IT adoption was accompanied by increased regulation designed to protect patient data. Hospitals receiving federal funding were required to formally attest to meaningful-use requirements, including provisions to implement policies and procedures to prevent, detect, and correct security violations based on HIPAA (Health Insurance Portability and Accountability Act) security rules.[11] Conducting an analysis of potential risks and existing vulnerabilities is the first step in identifying safeguards. This is followed by risk management, which entails implementing proper security safeguards for the assessed risks and vulnerabilities.[12] Quantifying and measuring risk are key elements of these 2 steps (analysis and management).

The HITECH Act also mandated public notification of health information breaches.[13] Since 2009, healthcare providers and entities have been required to notify patients impacted by breaches of protected health information and make a public notice to the US Department of Health and Human Services (HHS) and media organizations in cases affecting more than 500 individuals.[9,13] HHS maintains a public database called the *Breach Portal* that publishes the reported health data breaches submitted since October 2009.[14]

Despite regulatory efforts to protect patient data, health data breaches have been rising. Health data breaches reported to HHS grew from 270 in 2015 to 510 in 2019.[2] The largest breaches during that time included the Anthem breach in 2015 that exposed over 70 million individual records and the UCLA Health System breach (also in 2015) that exposed over 4 million records.[15,16] In 2019, more than 80% of Healthcare Information and Management Systems Society (HIMSS) hospitals reported that they had experienced a significant security incident in the past 12 months.[1]

Data breaches are a financial burden to hospitals on 2 fronts. First, spending on cybersecurity is needed to prevent breaches. In 2015, healthcare organizations spent on average 4%–6% of their overall IT budgets on security, spending $1M–$10M (financial services spent 7%–9%, government spent 4%–6%).[17] Healthcare organizations' spending on security as a percentage of IT budget remained constant from 2014 to 2016.[17] Second, spending on remediation is needed to recover after breaches. The Ponemon Institute estimated that the average total cost of a US data breach in 2019 was $8.19 million.[18] That translated to an average cost per breached patient record of $429.[18] While EHRs are a lucrative target for attackers,[19] the healthcare sector has historically lagged in cybersecurity compared to many other sectors including finance and retail.[20,21] For example, in 2014, only about half of the hospitals supported 2-factor authentication, which is a strategy that would greatly strengthen security.[22]

OBJECTIVE

Hospital administrators and researchers recognize that hospitals must improve cybersecurity.[1,21] As with other management initiatives, measurement is important and improved security starts with measuring risks. Quantifying cybersecurity risk is an important step in developing an effective security program that prevents data breaches. Objective measures of risk help decision-makers to make informed choices. Hospital managers and policy makers need to quantify cybersecurity risks before they can make informed decisions on where to allocate resources. In this article, we investigate the state of healthcare security and the relationship between hospital data breaches and cybersecurity preparedness using a commercially available cybersecurity risk rating system.

MATERIALS AND METHODS

Study design

We employed a retrospective longitudinal study design to examine the cybersecurity risk ratings for hospitals. First, we explored time trends in cybersecurity risks for hospitals to test the hypothesis that hospitals have lower cybersecurity risk ratings than some other industries. Then, using our novel panel data, we estimated the relationship between cybersecurity ratings and data breaches using logistic regression to test the hypothesis that cybersecurity ratings are associated with breaches.

Commercially available cybersecurity risk rating systems

Several commercial risk ratings have become available including those provided by BitSight, SecurityScorecard, and Upguard. We chose BitSight, as it is well established as one of the first external ratings organizations. We note that such externally developed ratings are not prescriptive security frameworks like NIST or ISO, but rather external ratings that monitor security performance. To our knowledge, this study is the first to examine commercial cybersecurity risk ratings for hospitals. Based on our findings, we discuss implications for hospitals and decision-makers aiming to improve preparedness against data breaches.

Firm cybersecurity rating measures

Longitudinal cybersecurity risk rating data from September 2014 to August 2019 were provided by BitSight. We gathered cybersecurity ratings at the hospital-year-month level as reported on the first day of each month. The monthly ratings were collapsed to the year level by taking the hospital-year average.

This article focuses on 2 measures of firm cybersecurity: *security rating* and *compromised system score*. A security rating is a summary measurement of an organization's cybersecurity performance in the dimensions of compromised systems, diligence, user behavior, and data breaches.[23] The compromised system score measures vulnerability against botnets, spam, and malware.[23] Both measures range from 250 to 900, with higher ratings corresponding to better security. They are analogous to credit ratings in the financial industry. Besides ratings for hospitals, we also collected rating data for the same time period for Fortune 1000 firms (5826 firm-years). The healthcare industry has been perceived to lag other sectors in security, and this large set of publicly traded firms provided a good benchmark of comparison. Of the total universe of Fortune 1000, we were able to collect rating data from 971 firms that were consistently in the Fortune list over the measurement period.

Hospital breach data

We started from a universe of hospitals that were defined as short-term, general acute-care Medicare-certified hospitals in the Medicare Hospital Cost Reports,[24] which includes about 4800 hospitals (nonfederal). Breach data were extracted from the HHS breach portal. We identified 257 hospital data breaches (unit of observation was hospital-year) from the years 2014 to 2019. If a hospital was breached multiple times in a given year, the earliest breach was recorded. To construct a sample including both breached and nonbreached hospitals, we used propensity score matching to select nonbreached hospitals that were comparable to the breached hospitals. Propensity score matching adjusted for observable differences between the breached and nonbreached hospitals.[25–28] The propensity score for assignment into the breached group was predicted using a logit model. In the logit model, we selected hospital characteristics on the right-hand side by inspecting the balance of the matched sample with standardized mean differences.[29] The logit model for breach assignment was a function of ownership, teaching status, number of beds, operating revenue, operating expenses, total revenue, total expenses, and year. Hospitals were matched using the nearest neighbor matching approach allowing for ties, with replacement, with a caliper distance of 0.2 SD. If a breached hospital matched multiple control hospitals (n) resulting in a tie, the multiple matched control hospitals were weighted by 1/n. Matching was performed using the *matching* package 4.9-3 in R.[30]

The final data set of breached and nonbreached hospitals were queried in the BitSight database, returning ratings for matched hospitals. The finalized dataset yielded 3528 hospital-year observations for years 2014–2019. The breached group included 257 unique hospitals (1542 hospital-years) and the nonbreached group included 331 unique hospitals (1986 hospital-years).

Statistical analysis

To benchmark the risk posture of the hospital segment over time, we compared their security ratings to that of large publicly traded firms in the Fortune 1000. These large publicly traded firms face scrutiny from investors and must provide risk disclosures as part of their public reporting process (Sarbanes-Oxley Act[31] reporting). First, the descriptive time trends in security risk between Fortune 1000 firms and hospitals were compared using a linear regression with a year and firm type interaction. Second, focusing on hospitals, the relationship between data breaches and security risk was modeled using a conditional logistic regression. For the logistic regression, we processed the monthly data before collapsing it to the year to ensure that the collapsed yearly ratings only included ratings from months before a breach. Specifically, (1) the monthly rating was replaced with a 1-month lag to create separation, (2) ratings from the month of breach to 12 months after a breach were replaced with the rating from the month before breach. The conditional logistic model controlled for hospital fixed-effects. This implicitly controls for confounders that do not vary over time. Standard errors were heteroskedasticity robust and allowed for within hospital correlation. Statistical analysis was performed using Stata version 15.[27,32]

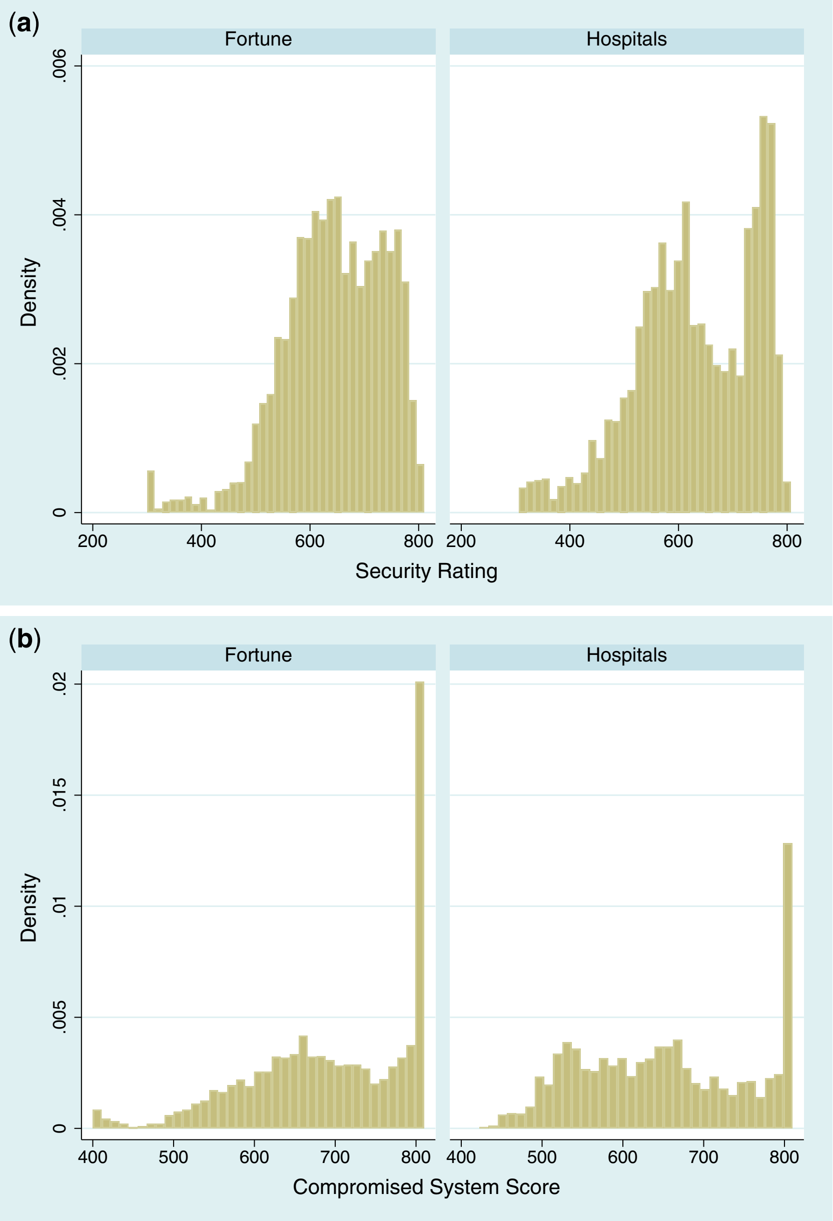

Figure 1. Histogram of security risk by firm type.

RESULTS

The distributions of the security rating for the 2 groups were skewed to the left, with most of the mass concentrated between 600 and 780 points (Figure 1a). The distribution of the compromised system score for the 2 groups had a sharp peak at 800 points (Figure 1b). Table 1 summarizes the descriptive characteristics among Fortune 1000 firms, control hospitals, and breached hospitals. For the full sample pooling all years, the average security rating for Fortune firms was 644 points while hospitals had an average of 630 points. To account for the non-normal distributions security rating and compromised system score, we used a Wilcoxon rank-sum test to compare the distributions between hospitals and Fortune firms.[33] We found that security ratings were significantly different between the 2 groups ($P < .001$). The average compromised system score for Fortune firms was 693 points while the average for hospitals was 677 points. Moreover, the distributions of compromised system score between the 2 groups were significantly different ($P < .001$).

Year trends by firm type

Figure 2 shows the count of hospital data breaches by year. The count of breaches fluctuated between 23 and 48 breaches from 2014 to 2018 (breaches in 2019 were excluded because our data did not cover the full year). Figure 3a summarizes the linear regression results for security rating time trends by Fortune 1000 firms and hospitals. Looking at the trend lines, hospitals had significantly lower security ratings than Fortune firms during 2014–2016. In 2014, the average security rating for Fortune firms was 613 points (95% CI 607, 618), the hospital average was 592 points (95% CI 583, 602), and the 21-point (95% CI −31, −10) difference between the 2 groups was statistically significant ($P < .001$) (Figure 3c). The confidence intervals for the 2 groups' scores overlap from 2017 to 2019. In 2019, the average security rating for Fortune firms was 647 points (95% CI 641, 654), the hospital average was 637 points (95% CI 628, 646) (however, the 10-point difference (95% CI −21, 0.8) between the 2 groups in 2019 was not statistically significant (Figure 3c)).

Table 1. Summary of BitSight scores by Fortune 1000 firms vs hospitals 2014–2019

	All Years		
	Fortune (N = 5826)	Hospitals (N = 3528)	*P* value
Security rating	644.13 (94.56)	629.58 (111.66)	<.001
Compromised system score	693.32 (99.05)	677.89 (110.77)	<.001
	2014		
	(N = 971)	(N = 588)	
Security rating	613.00 (92.98)	592.28 (115.72)	<.001
Compromised system score	660.04 (98.13)	637.28 (122.34)	<.001
	2019		
	(N = 971)	(N = 588)	
Security rating	647.35 (100.75)	636.95 (114.12)	.061
Compromised system score	720.26 (93.17)	708.65 (95.62)	.018

Data are presented as average (SD) for continuous measures, and n (%) for categorical measures. Continuous variables were tested across groups using Wilcoxon rank-sum.

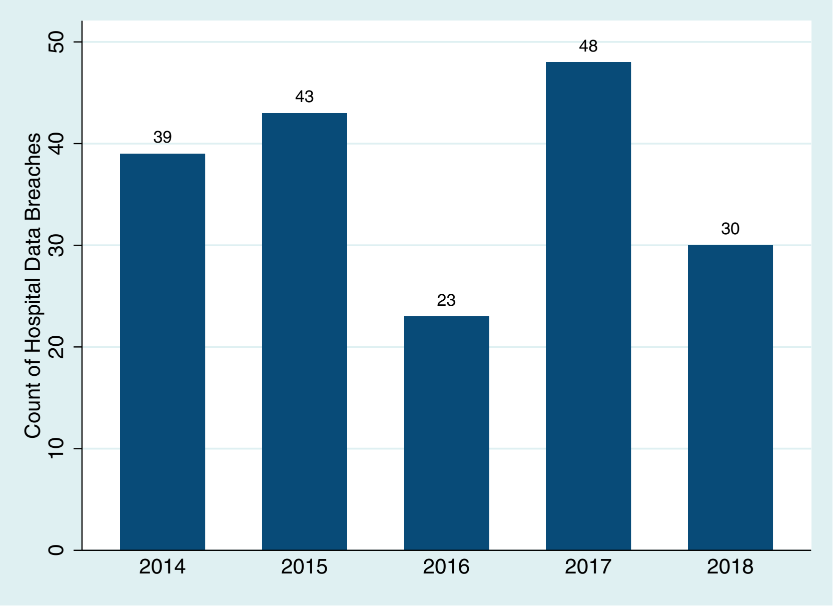

Figure 2. Count of hospital data breaches for 2014–2018.

For compromised system score time trends (Figure 3b), hospitals had significantly lower security ratings than Fortune firms during all years 2014–2019. In 2014, the average compromised system score for Fortune firms was 660 points (95% CI 654, 666) and for hospitals was 603 points (95% CI 594, 613). In 2019, the average compromised system score for Fortune firms was 720 points (95% CI 714, 726) and for hospitals was 689 points (95% CI 681, 698). However, the gap between the Fortune firms and hospitals closed over the years. In 2014, there was about a 60-point gap between the 2, but by 2019 the gap closed to about 30 points (remaining statistically significant).

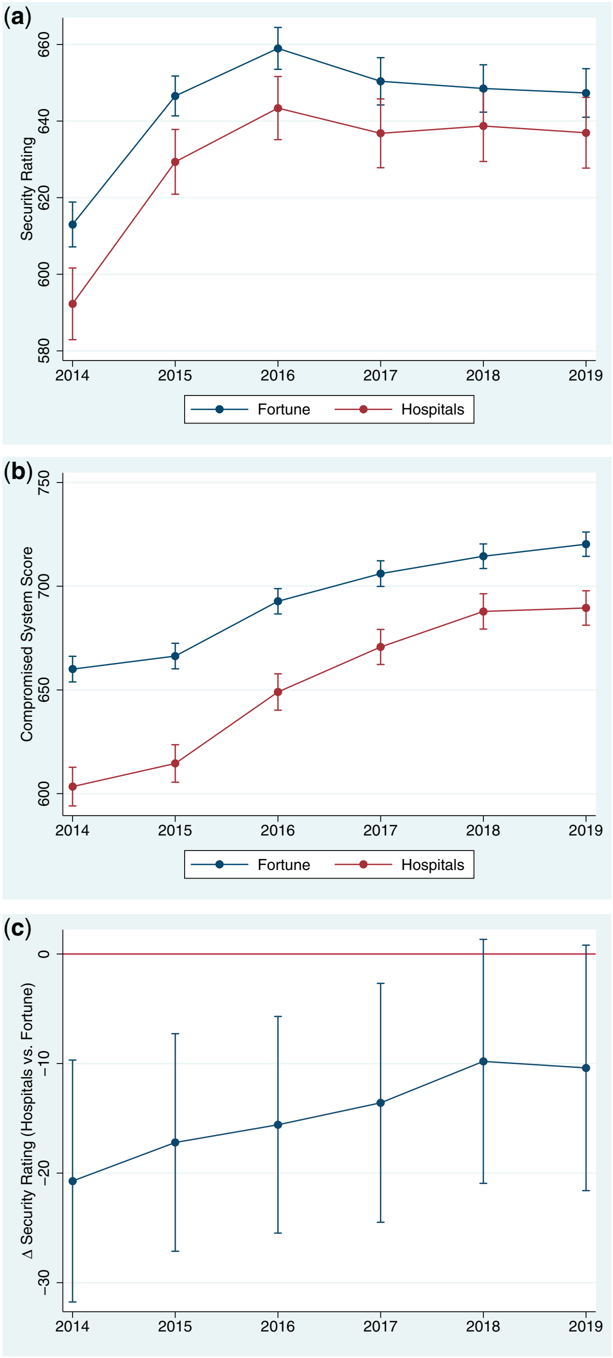

Figure 3. Summary of security risk by firm type and year with 95% confidence intervals.

Association between security rating and odds of data breach

Logistic regression estimated that a unit increase in security rating was associated with a 0.6% decrease in the odds of breach ($P = .015$), controlling for hospital effects and year effects. The estimated odds ratio coefficient is presented as predicted probabilities of having a breach in a year over a range of security rating scores in Figure 4. The prediction was made over the observed security rating range of 300–800. Security rating of 300 was associated with a 49.4% (95% CI 21.5%, 77.2%) probability of breach; security rating of 350 was associated with a 43.9% (95% CI 11.7%, 76.0%) probability of breach; and security rating of 400 was associated with a 38.3% (95% CI 2.5%, 74.1%) probability of breach. Security rating of 450 or higher was associated with a probability of breach of less than 32.9% with a 95% confidence interval including zero.

Logistic regression estimated that a unit increase in compromised system score was associated with a 0.4% decrease in the odds of breach ($P = .043$), controlling for hospital effects and year effects. The estimated odds ratio coefficient is presented as predicted probabilities of having a breach over a range of compromised system scores in Figure 5. The prediction was made over the observed compromised system score range of 400–800. Compromised system score of 400 was associated with a 44.9% (95% CI 11.5%, 78.4%) probability of breach; and compromised system score of 450 was associated with a 40.8% (95% CI 3.8%, 77.7%) probability of breach. Compromised system score of 500 or higher was associated with a probability of breach of less than 36.6% with a 95% confidence interval including zero.

DISCUSSION

Many security researchers have highlighted the rising number of healthcare data breaches and noted that healthcare providers have lagged other industries in terms of cybersecurity preparedness.[1,18,21] We indeed found that, in aggregate, hospitals had significantly lower security ratings than Fortune 1000 firms from 2014 to 2016, but the gap dropped over time and was no longer statistically significant in 2017–2019. The reduction in the gap in security rating suggests that healthcare providers are catching up to the general cybersecurity performance of large, publicly traded firms. Focusing on measures of vulnerability against botnets, spam, and malware (a subset of the overall rating referred to as the compromised system score), we found that while hospitals have improved, they remain statistically more vulnerable than the Fortune 1000. Finally, we found that hospitals with low security ratings (hospitals with scores 400 or lower) were associated with significant risk of a data breach, with the probability of a breach in a given year ranging from 38.3% to 49.4% (Figure 4); hospitals with low compromised system scores (hospitals with scores of 450 or lower) were associated with significant risk of a data breach, with the probability of a breach in a given year ranging from 40.8% to 44.9% (Figure 5).

We observe that many reported hospital data breaches have been attributed to human error (loss, theft, unauthorized access/disclosure) rather than hacking or IT incidents.[34] The large number of hospital data breaches related to human error may explain the stronger correlation with the overall security rating in the logistic regression. The security rating accounts for both technical and human elements, whereas the compromised system score focuses on a subset of technical security measures. Our results for both measures indicate that hospital executives should work to reduce risks related to both technical security controls such as updated software and security applications along with human vulnerabilities that can be

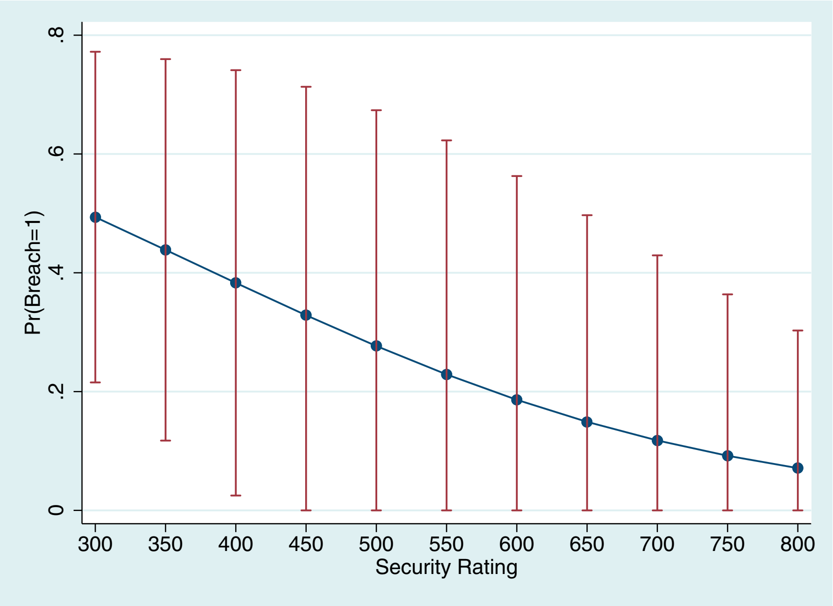

Figure 4. Predicted probabilities of breach risk by security rating among hospitals with 95% confidence intervals.

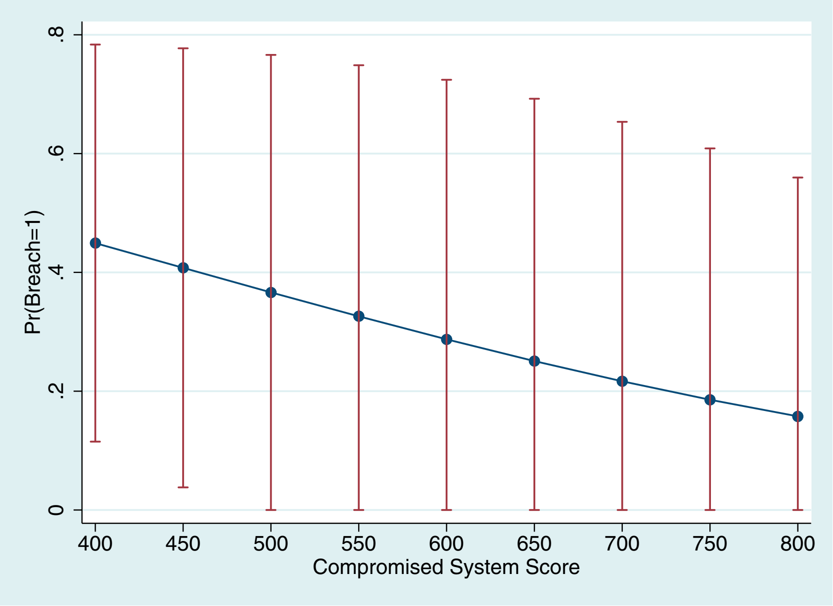

Figure 5. Predicted probabilities of breach risk by compromised system score among hospitals with 95% confidence intervals.

addressed through enhanced training and overall security culture. We note also that recent hacking and ransom ware attacks may be shifting the security landscape for hospitals, with much larger potential hospital and patient consequences. Ongoing risk assessment is needed to keep up with these threats and will likely require even further security investment. Policy makers should monitor the risk to the healthcare sector and provide incentives for hospitals to invest in risk management and overall information security.

Limitations

We included a hospital fixed effect, which controls for hospital characteristics that are time-invarying. For example, hospital ownership, size, and teaching status are unlikely to change in the short run. We also included year fixed effects that would capture other time varying effects like the state of health IT and aggregate changes in hospital security practices. However, our models did not control for other time-varying hospital characteristics that are potential confounders, such as major changes to specific hospital technology. Since most hospitals (96%) had implemented EHR by 2015,[10] this is a low concern for the study period 2015–2019. Nevertheless, additional control variables may be added in future research if data becomes accessible to researchers. Our analysis included reported health data breaches that affected more than 500 individuals. Smaller data breaches affecting fewer than 500 individuals are not published by HHS, thus were omitted from our study. There may be a significant number of undisclosed, small data breaches.[35] Finally, the methodology for the BitSight security rating is proprietary and subject to change.

CONCLUSION

We found empirical evidence that acute-care (nonfederal) hospitals have lagged larger publicly traded firms in other industries in cybersecurity but are closing the gap. We also found that poor cybersecurity ratings were associated with higher risk of a data breach. Policy makers should consider providing incentives for hospitals to proactively invest in security controls that reduce cyber risk. Best practices from other sectors can provide useful guides and benchmarks for improvement.

FUNDING

BitSight provided no financial support for this research. SJC has no connection to Bitsight, nor does he have any financial relationship with MEJ.

AUTHOR CONTRIBUTIONS

SJC performed the statistical analysis reported in this manuscript, wrote, edited, reviewed the manuscript. MEJ wrote, edited, reviewed the manuscript. Both authors are accountable for article accuracy.

DATA AVAILABILITY STATEMENT

Hospital breach data was derived from a source in the public domain: US Department of Health and Human Services Breach Portal available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Medicare Hospital Cost Reports data was derived from a source in the public domain: Centers for Medicare and Medicaid Services Hospital Cost Reports available at https://www.cms.gov/Research-Statistics-Data-and-Systems/Downloadable-Public-Use-Files/Cost-Reports/Hospital-2010-form

Cybersecurity ratings were provided by BitSight (https://www.bitsight.com) by permission. Data will be shared upon request to the corresponding author with permission of BitSight.

CONFLICT OF INTEREST STATEMENT

MEJ served as an early-stage advisor to BitSight and holds unexpired options for his involvement with the firm in 2012–2013. SJC has none to declare.

REFERENCES

1. Healthcare Information and Management Systems Society. HIMSS Healthcare Cybersecurity Survey. 2019. https://www.himss.org/himss-cybersecurity-survey Accessed July 13, 2020.
2. HIPAA Journal. Healthcare Data Breach Statistics. https://www.hipaajournal.com/healthcare-data-breach-statistics/ Accessed October 26, 2020.
3. Becker's Health IT. 50 biggest data breaches in healthcare. https://www.beckershospitalreview.com/healthcare-information-technology/50-biggest-data-breaches-in-healthcare.html Accessed October 26, 2020.
4. Drees J. UCSF pays $1M+ ransom to unlock medical school's computer systems. Becker's Hospital Review. 2020. https://www.beckershospitalreview.com/cybersecurity/ucsf-pays-1m-ransom-to-unlock-medical-school-s-computer-systems.html Accessed September 15, 2020.
5. Becker's Health IT. Hospitals are hit with 88% of all ransom ware attacks. 2016. https://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html Accessed September 15, 2020.
6. Jickling K. 300 workers reassigned or furloughed at UVM Medical Center due to cyberattack. VTDigger. 2020. https://vtdigger.org/2020/11/09/300-workers-reassigned-or-furloughed-at-uvm-medical-center-due-to-cyberattack/ Accessed November 16, 2020.
7. Centers for Medicare and Medicaid Services (CMS). Promoting interoperability programs. Centers for Medicare and Medicaid Services. 2020. https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/ Accessed October 26, 2020.
8. Park, A. Defective EHRs suffer little in fraud probes: "They're almost too big to fail." https://www.beckershospitalreview.com/ehrs/despite-fraud-busts-many-defective-ehrs-still-on-the-market-they-re-almost-too-big-to-fail.html Accessed November 26, 2020.
9. International Data Corporation (IDC). Worldwide ICT spending guide: industry and company size. 2020. https://www.idc.com/getdoc.jsp?containerId=IDC_P33207 Accessed October 26, 2020.
10. Henry J, Pylypchuk Y, Searcy T, Patel V. ONC. Adoption of electronic health record systems among U.S. non-federal acute care hospitals: 2008–2015. 2016. https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php Accessed July 13, 2020.
11. Office for Civil Rights (OCR). Security rule guidance material. HHS.gov. 2009. https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html Accessed November 23, 2020.
12. Healthcare Sector Cybersecurity Coordination Center. Quantitative risk management for healthcare cybersecurity. 2020. https://www.aha.org/system/files/media/file/2020/05/hhs-cyber-program-quantitative-risk-management-for-healthcare-cybersecurity-5-7-2020.pdf Accessed May 1, 2021.
13. Office for Civil Rights (OCR). Breach notification rule. HHS.gov. 2009. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html Accessed September 15, 2020.
14. Department of Health and Human Services. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. 2020. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf Accessed September 15, 2020.
15. Teichert E. Anthem to pay $16M in record data breach settlement. Modern Healthcare. 2018. https://www.modernhealthcare.com/article/20181016/NEWS/181019927/anthem-to-pay-16m-in-record-data-breach-settlement Accessed October 26, 2020.
16. Terhune C. UCLA Health System data breach affects 4.5 million patients. *Los Angeles Times*. 2015. https://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html Accessed October 26, 2020.
17. Filkins B. IT security spending trends. SANS Institute. 2020. https://www.sans.org/reading-room/whitepapers/leadership/security-spending-trends-36697 Accessed October 26, 2020.
18. Cost of a Data Breach Report 2019. 2019. https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/ Accessed July 13, 2020.
19. Kwon J, Johnson ME. Protecting patient data: the economic perspective of healthcare security. *IEEE Secur Privacy* 2015; 13 (5): 90–5. doi:10.1109/MSP.2015.113.
20. Finkle J. Exclusive: FBI warns healthcare sector vulnerable to cyber attacks. Reuters. 2014. https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-exclusiv- idUSBREA3M1Q920140423 Accessed October 26, 2020.
21. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. *J Med Internet Res* 2018; 20 (5): e10059.
22. Gabriel M, Charles D, Henry J, Wilkins TL. State and National Trends of Two-Factor Authentication for Non-Federal Acute Care Hospitals. https://dashboard.healthit.gov/evaluations/data-briefs/hospital-two-factor-authentication.php Accessed October 26, 2020.
23. BitSight. Security Ratings. https://www.bitsight.com/security-ratings Accessed October 26, 2020.
24. Centers for Medicare and Medicaid Services. Hospital Cost Reports. https://www.cms.gov/Research-Statistics-Data-and-Systems/Downloadable-Public-Use-Files/Cost-Reports/Hospital-2010-form Accessed October 26, 2020.

25. Rosenbaum PR, Rubin DB. The central role of the propensity score in observational studies for causal effects. *Biometrika* 1983; 70 (1): 41–55.
26. Rosenbaum PR, Rubin DB. Constructing a control group using multivariate matched sampling methods that incorporate the propensity score. *Am Stat* 1985; 39 (1): 33–8.
27. Heckman JJ, Ichimura H, Todd PE. Matching as an econometric evaluation estimator: evidence from evaluating a job training programme. *Rev Econ Stud* 1997; 64 (4): 605–54.
28. Dehejia RH, Wahba S. Causal effects in nonexperimental studies: reevaluating the evaluation of training programs. *J Am Stat Assoc* 1999; 94 (448): 1053–62.
29. Austin PC. An introduction to propensity score methods for reducing the effects of confounding in observational studies. *Multivariate Behav Res* 2011; 46 (3): 399–424.
30. Sekhon JS. Multivariate and propensity score matching software with automated balance optimization: the matching package for R. *J Stat Soft* 2011; 42 (7): 1–52.
31. Sarbanes-Oxley Act. 2002. Pub.L. 107–204, 116 Stat. 745, enacted July 30, 2002.
32. StataCorp. Stata: Software for Statistics and Data Science. 2017. https://www.stata.com/ Accessed September 15, 2020.
33. Wilcoxon F. Individual comparisons by ranking methods. *Biometr Bull* 1945; 1 (6): 80–3.
34. Choi SJ, Johnson ME, Lehmann CU. Data breach remediation efforts and their implications for hospital quality. *Health Serv Res* 2019; 54 (5): 971–80.
35. Heubusch K. Little breaches: OCR releases first “small breach” data. *J AHIMA* 2011; 82 (10): 56–7.