INTERNATIONAL JOURNAL OF MEDICAL INFORMATICS 83 (2014) 122–130

journal homepage: www.ijmijournal.com

Characteristics of health IT outage and suggested risk management strategies: An analysis of historical incident reports in China

Jianbo Lei[a,b,*], *Pengcheng Guan*[a], *Kaihua Gao*[a], *Xueqin Lu*[a], *Yunan Chen*[c], *Yuefeng Li*[d], *Qun Meng*[d], *Jiajie Zhang*[b], *Dean F. Sittig*[b], *Kai Zheng*[e,f]

[a] *Center for Medical Informatics, Peking University, Beijing, China*
[b] *School of Biomedical Informatics, University of Texas Health Sciences Center at Houston, Houston, TX, USA*
[c] *Donald Bren School of Information and Computer Sciences, University of California, Irvine, CA, USA*
[d] *Center for Statistics and Informatics, Ministry of Health, China*
[e] *School of Public Health Department of Health Management and Policy, University of Michigan, Ann Arbor, MI, USA*
[f] *School of Information, University of Michigan, Ann Arbor, MI, USA*

ARTICLE INFO

Article history:
Received 28 January 2013
Received in revised form
12 October 2013
Accepted 14 October 2013

Keywords:
Health information system
Electronic health records
Patient safety
Accident prevention
Failure prediction
Failure recovery, maintenance and self-repair
Safety critical systems

ABSTRACT

Background: The healthcare industry has become increasingly dependent on using information technology (IT) to manage its daily operations. Unexpected downtime of health IT systems could therefore wreak havoc and result in catastrophic consequences. Little is known, however, regarding the nature of failures of health IT.

Objective: To analyze historical health IT outage incidents as a means to better understand health IT vulnerabilities and inform more effective prevention and emergency response strategies.

Methods: We studied news articles and incident reports publicly available on the internet describing health IT outage events that occurred in China. The data were qualitatively analyzed using a deductive grounded theory approach based on a synthesized IT risk model developed in the domain of information systems.

Results: A total of 116 distinct health IT incidents were identified. A majority of them (69.8%) occurred in the morning; over 50% caused disruptions to the patient registration and payment collection functions of the affected healthcare facilities. The outpatient practices in tertiary hospitals seem to be particularly vulnerable to IT failures. Software defects and overcapacity issues, followed by malfunctioning hardware, were among the principal causes.

Conclusions: Unexpected health IT downtime occurs more and more often with the widespread adoption of electronic systems in healthcare. Risk identification and risk assessments are essential steps to developing preventive measures. Equally important is institutionalization of contingency plans as our data show that not all failures of health IT can be predicted and thus effectively prevented. The results of this study also suggest significant future work is needed to systematize the reporting of health IT outage incidents in order to promote transparency and accountability.

* *Corresponding author at*: Center for Medical Informatics, Peking University, 38 Xueyuan Rd, Haidian District, Beijing 100191, China. Tel.: +86 10 8280 5901; fax: +86 10 8280 5900.
E-mail address: jblei@hsc.pku.edu.cn (J. Lei).
1386-5056/$ – see front matter © 2013 Elsevier Ireland Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijmedinf.2013.10.006

1. Introduction

The widespread adoption of health information technology (IT) has been taking place in most industrialized countries as well as some developing countries such as China [1–3]. As a result, healthcare provider institutions around the world have become increasingly dependent on using IT to manage their patient care delivery and hospital/clinic operation processes. These include time-sensitive and mission-critical processes in settings such as emergency rooms and surgical and intensive-care units.

Health IT that provides computerized decision-support functionalities has also become an indispensable tool aiding clinicians in their medical practice. For example, clinicians are more and more reliant on using order-sets stored in computerized prescriber order entry (CPOE) systems for complex medication prescriptions or procedure orders [4,5]. They may not necessarily know, or remember, what constitutes an order-set. Such overdependence on technology could over time 'deskill' healthcare workers, and create chaos when health IT systems become unexpectedly unavailable [4–6].

Although the reliability of computing hardware has significantly improved over the past several decades, the complexity of software has escalated. This is especially true in healthcare [7,8]. At the same time, many provider institutions must adopt tens, if not hundreds, of different IT applications supplied by different vendors. These systems are often interdependent on one another in order to provide a full spectrum of services. In such highly complex environments, system failures are inevitable. It is therefore believed that the occurrence of health IT outage at any given healthcare institution is no longer a matter of whether, but when [7,8]. Many factors may be responsible for health IT failures such as capacity overrun, hardware malfunction, software defects, human errors, computer virus/hacker attack, and natural disasters [9].

Analyzing historical outage incidents can be a valuable means to better understand health IT vulnerabilities and subsequently inform more effective prevention and emergency response strategies. It has been shown that most existing IT risk analysis techniques are grounded in the classical probability theory, which postulates that the past is an indication of the future [10,11]. No prior systematic research has been conducted to examine the health IT outage events reported in public mainstream news outlets, however. We performed a careful PubMed search using many keywords and combinations of keywords in an attempt to identify relevant studies. We also searched in Wanfang (wanfangdata.com.cn), China National Knowledge Infrastructure (cnki.net), and VIP Journal Integration Platform (cqvip.com), the three most popularly used scientific literature databases indexing research papers published in Chinese journals. The searches either yielded no results, or the articles retrieved were related but not closely relevant [e.g., 12,13]. The list of keywords we used is provided in Appendix 1.

In this study, we conducted a qualitative analysis to summarize, thematize, and make inferences of health IT outage events that occurred in China. The analysis was based on news articles and incident reports publicly available on the internet. Even though less developed compared to many western countries, nearly 50% of hospitals and ambulatory care practices in China have by now adopted the basic forms of electronic health records (EHR) systems, practice management systems (often referred to as Hospital Information System in China, or HIS), picture archiving and communication system (PACS), and CPOE [3,14]. While not all results from this China study are generalizable to other countries, we believe certain insights may have broad implications because the fundamental architecture of health IT, thus its vulnerabilities, is more or less the same. These include vulnerable hardware components, capacity constraints, complex messaging and interoperability mechanisms, human errors, threats from the internet, and natural disasters.

2. Methods

2.1. Data collection

To obtain news articles and publicly available incident reports describing health IT outage events in China, we performed a comprehensive internet search using two popularly used web search engines: Baidu (baidu.com) and Google (google.com). Baidu is the dominant search engine in the Chinese web controlling approximately 78.3% of the market share [15]. Worldwide, it is among the top five most frequently visited websites according to Alexa Internet [16].

To facilitate the search, we compiled a list of keywords and combinations of the keywords and their varied forms of spellings, which we believe is reasonably inclusive. The list is provided in Appendix 2. Two graduate students specialized in health informatics (KG and XL) conducted the search and independently evaluated the records returned by the two search engines. Another graduate student research assistant, also trained in health informatics (PG), audited a random set of the results. Discrepancies and disagreements were resolved through group discussions among the investigator team.

2.2. Data analysis

To analyze the content of the articles and reports retrieved, we applied a deductive grounded theory approach [17] leveraging a synthesized IT risk conceptual framework proposed by Sherer and Alter [18]. Based on a systematic review of 46 research papers published in the area of information systems, Sherer and Alter found that most prior conceptualizations of IT risk focus on negative outcomes and their constructs generally fall into the following three categories: risk components, risk factors, and probability of negative outcomes [18].

We first coded the data based on this conceptual framework, referred to as the Synthesized IT Risk Model in the remaining parts of this paper. Then, we examined the recurring themes that emerged from the data to understand common causes of health IT outage and common risk management strategies used to prevent or minimize the adverse impact of the failures. We also recorded and analyzed metadata associated with the reported health IT outage events whenever available, such as date and time when an event occurred, general characteristics of the healthcare setting (e.g., location and hospital type), and scope of the impact.

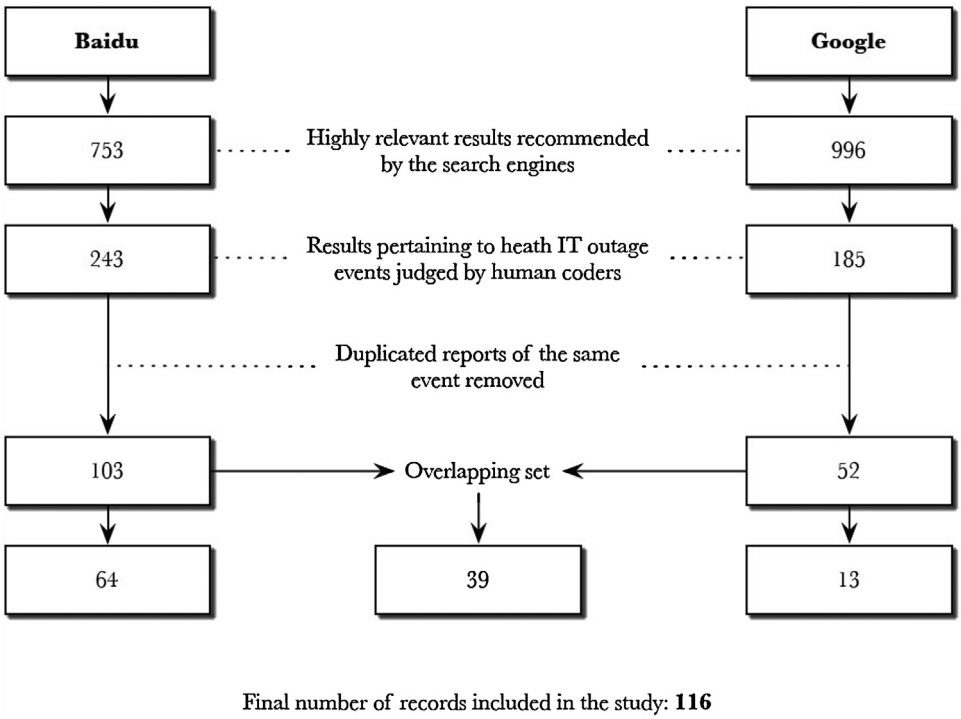

Fig. 1 – The review process based on the initial results returned by the two search engines.

3. Results

3.1. *Retrieval of news articles and incident reports*

The searches were performed on October 16, 2012. Baidu found over 4.3 million web pages of potential interests; Google found 1.2 million. By default, Baidu only returned the first 753 records; the rest were deemed by the search engine as either repetitive or irrelevant and were omitted from the results returned. Google behaved in a similar matter and only returned the first set of 996 matches. In this study, we only included those 'highly relevant' records recommended by the two search engines. We did not make the effort to retrieve the omitted ones even though it is technically feasible.

The two graduate student research assistants then manually reviewed the highly relevant results recommended by the two search engines. 243 and 185 records were selected from the results returned by Baidu and Google, respectively, which were deemed truly pertinent to health IT outage incidents. After consolidating duplicated reports of the same event, a total of 116 distinct health IT outage events were identified. Fig. 1 illustrates this process. As a side note, Baidu seems to outperform Google by a large margin in the particular context of this study. Among the 116 distinct events, 39 were found in both Baidu and Google. Baidu, however, contributed an additional set of 64 matches while Google only contributed additional 13. It is also interesting to note that the two search engines behaved distinctly in how 'relevance' of a webpage was determined. Google's page ranking appears to be more consistent with human judgments, whereas Baidu's ranking, illustrated in Appendix 3, is not.

3.2. *Descriptive statistics*

All health IT outage incidents occurred during the 2001–2012 timeframe. Table 1 presents their overall characteristics. Note that in some sections the numbers may not add up to 116 as certain information, such as time of the day when the outage event occurred, was not disclosed in all reports. Also note that in the Chinese healthcare system there are very few outpatient-only health centers. The majority of healthcare facilities in China provide both inpatient care as well as ambulatory care. For simplicity, we call all of them "hospitals" in this paper.

In China, all hospitals are classified by a government board into three classes: primary (roughly equivalent to community-based health centers in the U.S.), secondary (county- and municipal-level healthcare facilities), and tertiary (large, advanced general or specialty hospitals; often times academic medical centers). There are 5636 primary, 6468 secondary, and 1399 tertiary hospitals in China as of 2011 [19]. Regardless of classes, all hospitals have electronic billing systems because of a government mandate. Not all hospitals have advanced health IT capabilities such as EHRs, however. According to a national survey conducted in 2012, 57.2% of the tertiary hospitals in China have adopted EHRs. This rate drops to 38.8% among the primary and secondary hospitals [14].

As shown in Table 1, the average duration of the health IT outage incidents was 18 h and 6 min. A vast majority of them (69.8%) took place in the morning, possibly due to overcapacity issues, vulnerable hardware or software components breaking down during booting/rebooting, or security patches and software upgrades that are often applied overnight. Furthermore, incidents that occurred in tertiary hospitals accounted

Table 1 – Descriptive statistics.

Measure	Statistics
Number of distinct outage incidents	116
Date range	July 2001 to September 2012
Duration	15 min to 720 h (mean: 18.1 h, median: 2 h)
Time of the day when the outage incidents occurred	
Morning (7am–12pm)	81
Noon (12–1pm)	7
Afternoon (1–6pm)	5
Evening (6pm–7am)	7
Not reported	16
Number of hospitals affected	>102[a]
Distribution by hospital class (number of incidents)[b]	
Primary	3
Secondary	15
Tertiary	80
Not reported	4
Top five provinces/autonomous cities where outage events were most frequently reported	Beijing (37), Guangdong (24), Shanghai (18), Fujian (6), Hubei (5)
Patient care areas affected	
Outpatient	93
Inpatient	12
Entire hospital	8
Not reported	1
Incidents that affected multiple hospitals	14

[a] 14 incidents affected all hospitals in a city or region.
[b] Incidents affecting multiple hospitals were not counted.

Table 2 – Risk components.

Hospital functions affected[a]	Frequency
Registration	61
Billing	68
Patient-provider encounter	29
Pharmacy	33
Laboratory	8
Admission, discharge, transfer (ADT)	10
Entire hospital	8

[a] A single outage incident may be counted multiple times if it affected more than more hospital functions.

for over 80% of the outage events. We do not know, however, if the tertiary hospitals indeed have a higher rate of health IT failure or whether this observation was an artifact of their more advanced stage of health IT adoption or better monitoring and reporting mechanisms. Similarly, a large number of health IT outage events was reported in Beijing, Guangdong, and Shanghai, the three most economically developed regions in China. This is also likely a reflection of their more advanced stage of health IT adoption and more thorough reporting mechanisms rather than poorer IT risk management capabilities.

The last few rows in Table 1 show a breakdown of the scope of impacts by area of care. A majority of the incidents affected ambulatory settings; eight had a hospital-wide impact; 14 involved multiple hospitals. Most of the incidents involving multiple hospitals were caused by the malfunction of municipal-level public insurance payment systems that disrupted the operation of all hospitals in a city or in a region.

Fig. 2A and B depict the distribution of the health IT outage events by year and by calendar month, respectively. Despite some fluctuations, outage incidents seem to occur more and more often over the past eight years. Based on a simple linear regression, it may be predicted that in year 2016 the number of health IT outage incidents in China will exceed 30. By 2020, this number will grow above 40. These are, of course, only the tip of the iceberg as it may be reasonably assumed that only a small number of health IT outage incidents ever get widely publicized. As shown in Fig. 2B, the incident rate in February is remarkably low. This is likely due to the fact that the Chinese New Year holidays usually take place from late January through most of February. Seeking care during this period of time is generally advised against as in most hospitals a majority of the staff will not be on active duty. Of course, it is also possible that the outage events occurring during this period of time might be underreported.

3.3. *Analysis based on the synthesized IT risk model*

Tables 2–4 show the results based on the synthesized IT risk model. Each of the three tables summarizes the results related

Table 3 – Risk factors.

Factor	Description	Frequency
Hardware malfunction	Computer workstation breakdown	18
	Server breakdown	9
Software malfunction	Malfunction after applying security patches and/or system upgrades	11
	Failure of database management systems	8
	Software failing to respond for unknown reasons [a]	30
Loss of network connectivity		12
Human error		4
Virus/hacker attack		2
Natural disaster [b]		4
Electronic power outage		5
Causes unknown or not disclosed		13

[a] Software hanging due to known reasons (e.g., loss of network connectivity) was not counted in this category.
[b] Mainly due to fire or electricity surge during thunderstorms.

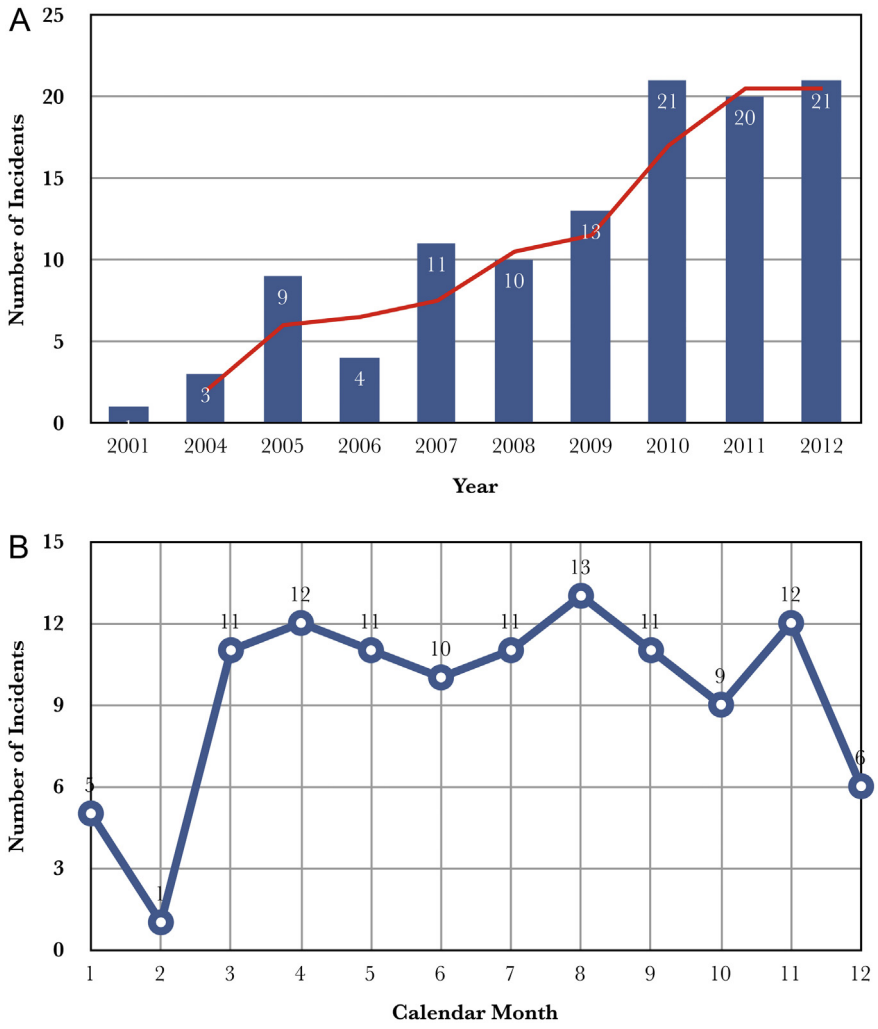

Fig. 2 – The distribution of the health it outage events overtime (note that not all incident reports explicitly mentioned when the events occurred: three reports did not provide the year in which the events took place; four reports did not specify month.).

Table 4 – Negative outcomes.

Measure	Frequency
Number of patients affected	
>1000	9
500–999	3
100–499	30
<100	5
Not reported	68
Patient safety events/risks resulted	
Death	1
Patient care delayed/canceled	109
Patients forced to seek care in other hospitals	21
Unrecoverable data losses	8
Direct financial losses [a]	35

[a] Costs associated with hardware replacements and software repair are not considered.

to risk components, risk factors, and probability of negative outcomes, respectively.

IT outages that brought down the registration and billing functions of a hospital constitute the majority of the incidents reported (Table 2). As mentioned earlier, most of the incidents that affected multiple hospitals were also related to the cascading effect of the failure of billing systems at the municipal level. Of course, it is very possible that outage incidents associated with registration and billing are disproportionally represented in our data. Because patients experienced such events first-hand, the likelihood of their becoming widely publicized could be much higher than those affecting only the internal processes of a hospital.

Table 3 shows the sources (risk factors) of the health IT outage incidents. Nearly two thirds (65.5%) of them were related to malfunctioning software or hardware. The single largest category, "software failing to respond for unknown reasons," accounts for more than a quarter (25.8%) of the total number of incidents identified—many were reportedly linked to overcapacity issues (e.g., "system crashed due to unknown reasons

Table 5 – Risk management measures.

Measure	Frequency
Field emergency response teams	35
Backup systems activated	
'Hot swapping' failover backup systems	7
Fallback manual processes	21
Post-crisis remedy measures	18

during peak time"). Most of the incident reports, however, only mentioned very vaguely that the health IT failure was caused by software defects (bugs or design issues); very few provided a diagnosis of what the exact cause was. Notably, about 10% of the breakdowns occurred after security patches and/or system upgrades were applied. Thirteen of the 116 reports did not mention at all the reason(s) for the health IT failure.

All health IT outage incidents identified in the data resulted in some kind of negative outcome with varied degrees of severity, including a patient's death reported in 2009. A summary is shown in Table 4. Among them, eight caused unrecoverable data losses; 35 resulted in direct financial costs to the healthcare institution where the event occurred. Most of the financial losses were in the form of lawsuits, monetary compensations, free services provided for the patients affected, and opportunity costs associated with patient care services that could not be rendered during health IT outage (e.g., due to patient care canceled or patients alternatively seeking care in other hospitals). None of the incident reports provided an explicit estimation of the magnitude of the financial losses, however.

Table 5 describes countermeasures reportedly taken to mitigate the adverse effects of the health IT outage incidents. Our data show that field emergency response teams were deployed in 35 cases to manage the crises. The field teams' work included informing patients about the system blackout, providing triage and consultation services, and helping to transfer critically ill patients to nearby hospitals. In 28 cases, backup systems were activated in a timely manner to support the affected processes. Seven of them used 'hot swapping' failover systems (e.g., mirror servers and redundant power supplies); Twenty one rolled back to manual, paper-based routines that had existed prior to computerization. In 18 cases, post-crisis remedy measures were used to compensate patients such as waiving registration fees or providing free care. It is important to note that 54 out of the 116 outage incidents we reviewed in the study (46.6%) did not mention the use of any risk management strategies.

4. Discussion

Unexpected downtime of health IT systems could cause chaos in today's extensively wired healthcare environments. The consequences, either in terms of patient safety risks, financial costs to provider institutions, or damage to clinicians' trust in health IT [13], can be devastating. In a recent Institute of Medicine report concerning new types of patient safety hazards associated with technology use, robust IT infrastructures that "cause no unanticipated downtime" are regarded as a critical requirement for building safer health IT systems for better care [20,21].

Risk identification and risk assessments are essential steps to developing preventive measures to reduce risks to an acceptable level [22]. Equally important is institutionalization of contingency plans in anticipation of emergency situations as not all failures of health IT can be predicted, and thus effectively prevented. In this study, we used publicly available incident reports as a source of information to investigate the nature of historical health IT outage events. We believe that drawing insights from the past is an indispensable means to inform future risk prevention measures, emergency response plans, as well as remedy strategies in the aftermath.

The most significant learning from this study is perhaps not about the health IT outage incidents we analyzed, but the recognition of the scarcity of research and the lack of data supporting scientific investigations and knowledge accumulation. First, the health IT incident reports we were able to identify very likely represent only a small percent of outage events that have occurred. Second, most of the publicly available incident reports lacked necessary clarity and detail to support in-depth comparison and research analyses. These point to the need of establishing a systematic mechanism for healthcare institutions to report unplanned health IT downtime events, including symptoms, causes, impacts and, in hindsight, possible prevention and emergency response strategies that could have been used to prevent or minimize the adverse impact.

The Institute of Medicine, in the aforementioned report, puts forth a similar proposal calling for the establishment of a mechanism for vendors and users to systematically report health IT related deaths, serious injuries, and unsafe conditions [20,21]. The work discussed in this paper represents a preliminary attempt to characterize common characteristics of adverse patient safety events and workflow disruptions as a result of unexpected health IT downtime. Significant future work is needed to develop regulations, incentive strategies, and privacy protection measures to encourage provider institutions and health IT vendors to report such events. Also needed are guidelines, standards, and nomenclature/classification systems to formalize the reporting of health IT outage events so they can be more effectively analyzed, better understood, and better managed [8,23].

Several findings in the specific contexts of this study are noteworthy. First, a vast majority of the outage events occurred in the morning. Even though the nature of our data did not allow us to derive a definitive explanation for this observation, there were indications that (1) in ambulatory care clinics, patient care demands were much higher during mornings; (2) software and hardware issues were more likely to manifest during computer workstations' booting and rebooting processes; and (3) security patches and software upgrades applied overnight accounted for most of the early morning breakdowns. Therefore, IT departments and emergency response teams should be on high alert during mornings when most unexpected outage events, close to 70% according to our data, tend to occur.

Second, many of the health IT outage events we reviewed, including most of the registration and billing system failures, were directly linked to overcapacity issues (e.g., network congestion and server hanging due to large volume of concurrent accesses). Such issues are usually difficult to replicate

in simulated laboratory testing settings and thus can be difficult to detect and prevent. As the demands for healthcare grow rapidly in many countries, so does the amount of clinical and administrative data being stored and exchanged, it is imperative to have forward-thinking to accommodate future data manipulation, storage, and network traffic needs when health IT infrastructures are designed and implemented.

Third, the failure of municipal-level public insurance payment systems brought down many hospitals' billing functions. This again points to the need for provider institutions to develop contingency plans for today's highly interconnected health IT environments, since there can be many external factors affecting a hospital's operation that are out of a local institution's control. Preparing field teams to be deployed to work with patients during crises, training staff periodically about the use of paper-based backup systems, and having in place post-crisis remedy measures, are commonly adopted contingency plans to minimize the adverse impact of unexpected health IT downtime.

This study has several limitations. First, as mentioned earlier, the only data available to us were news articles and publicly accessible incident reports, which may have only captured a small number of health IT outage events that occurred. Further, the nature of this dataset prohibited in-depth research analyses, and the data might be biased toward certain types of events that were more likely to get publicized widely (e.g., registration and bill system failures that affected patients directly). Second, not all findings from this China study can be generalizable to other countries where structure of healthcare systems and use cases of health IT may be very different. Therefore, caution must be used when applying the findings of this research to other healthcare settings.

5. Conclusion

Health IT failures are inevitable. With proper planning and preparation healthcare organizations can meet the vitally important challenges involved in providing high-quality healthcare in and efficient and effective manner using the latest health IT tools and techniques. In this study, we retrieved and analyzed news articles and incident reports publicly available on the internet describing health IT outage events that occurred in China. The results showed several informative patterns, and pointed to the critical need for establishing a systematic reporting mechanism for the healthcare industry, in China and in other countries more broadly, to document unplanned health IT downtime events in order to promote

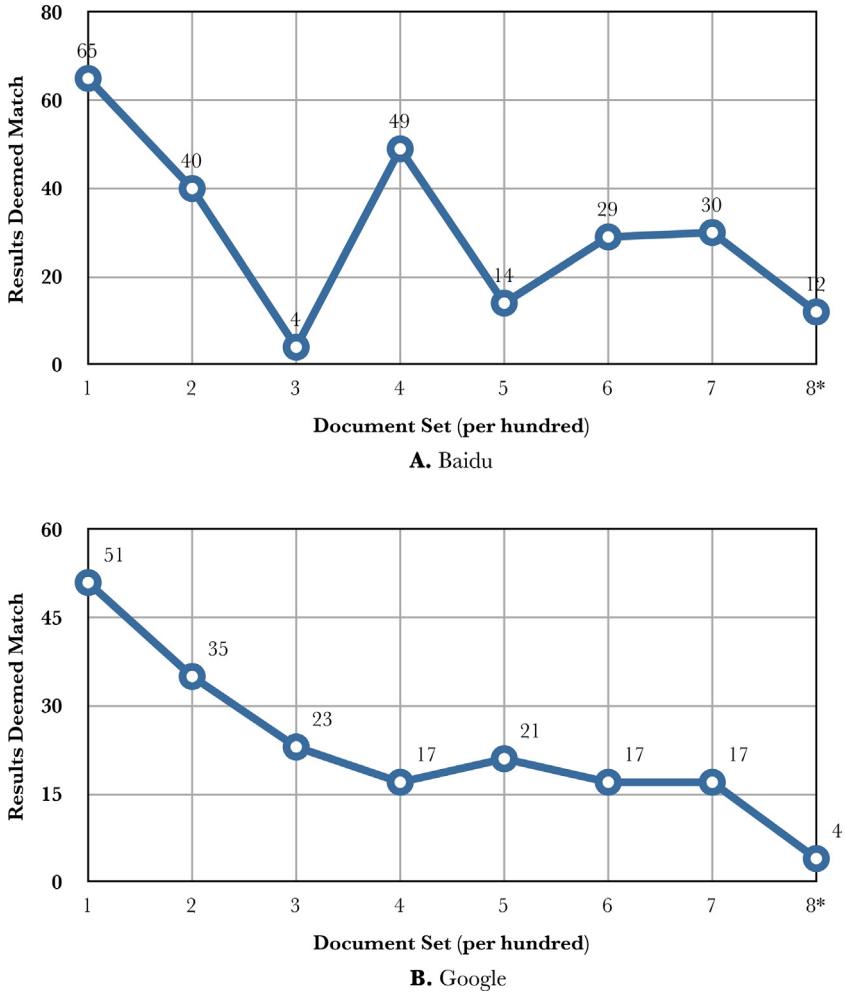

Fig. A1 – Ranking of relevance of retrievals by Baidu and Google: Webpages Deemed Relevant by Human Coders (per hundred documents returned; for fair comparison, only the first 753 documents were used).

transparency and accountability and inform more effective prevention and emergency response practices. The work discussed in this paper attempted to characterize commonalities of unexpected health IT downtime, and may represent an initial step toward the systematic health IT outage incident reporting mechanism proposed.

Authors' contributions

KZ and JL developed the conceptual framework and research protocol for the study. JL drafted the manuscript and KZ made major revisions. Masters students PG, XL, and KG conducted the literature and internet search, information extraction, and preliminary data analyses. DFS and YC helped with the study design and made revisions to the manuscript. JZ, QM, and YL supervised the study and provided comments on the manuscript. All authors read and approved the final manuscript.

Conflicts of interest

None.

Acknowledgement

This study was partly supported by the National Natural Science Foundation of China (NSFC) Grant # 81171426.

Appendix 1. Keywords used to search in literature databases

The following English keywords and their Chinese translation were included in the literature search: "Hospital information system" or "hospital electronic medical record" and "system paralysis" or "system dysfunction" or "network dysfunction" or "computer dysfunction" or "network paralysis" or "computer paralysis" or "system downtime" or "system crashes."

Appendix 2. Keywords used to search in Baidu and Google

The Chinese translation of the following key words and combination of keywords was included: "hospital" and "system paralysis" or "system dysfunction" or "network dysfunction" or "computer dysfunction" or "network paralysis" or "computer paralysis." Note that some keywords used to search in literature databases were not included in the Baidu and Google searches. This was either because these keywords are technical terms not commonly used in everyday language in Chinese, or because they were accommodated through the Chinese translation of some other terms included.

Appendix 3. Ranking of relevance of retrievals by Baidu and Google

Fig. A1. Webpages Deemed Relevant by Human Coders (per hundred documents returned). Note that: (1) For fair comparison, only the first 753 documents returned by each search engine were included. Hence, the denominator of the eighth data point on each graph (marked by asterisk) is 53 instead of 100. (2) The proportion of webpages deemed relevant based on manual review is erratically distributed on the first graph, which indicates that the page ranking results provided in Baidu were not consistent with human judgments. By contrast, the proportion of webpages deemed relevant decreases steadily on the second graph, which indicates that Google's page ranking results were in better agreement with the human coders' judgments.

Summary points

What was already known?

- The healthcare industry has become increasingly dependent on using information technology (IT) to manage its daily operations.
- Unexpected downtime of health IT systems could wreak havoc and result in catastrophic consequences.
- There have been no systematic mechanisms for provider organizations and health IT vendors to report unexpected health IT outage events.

What this paper adds:

- While limited in nature, news articles and incident reports publicly available on the internet can be a valuable data source informing common characteristics of unexpected health IT downtime and more effective prevention and emergency response practices.
- Risk identification and risk assessments are essential steps to developing preventive measures. Equally important is institutionalization of contingency plans as not all failures of health IT can be predicted and thus effectively prevented.
- There is a critical need of establishing a systematic mechanism for healthcare institutions to report unplanned health IT downtime events, including symptoms, causes, impacts and, in hindsight, possible prevention and emergency response strategies that could have been used to prevent or minimize the adverse impact.
- Significant future work is needed to systematize the reporting of health IT outage incidents in order to promote transparency and accountability.

REFERENCES

[1] G.F. Anderson, B.K. Frogner, R.A. Johns, U.E. Reinhardt, Health care spending and use of information technology in OECD countries, Health Aff. (Millwood) 25 (3) (2006) 819–831.
[2] A.K. Jha, D. Doolan, D. Grandt, T. Scott, D.W. Bates, The use of health information technology in seven nations, Int. J. Med. Inform. 77 (12) (2008) 848–854.
[3] China Hospital Information Management Association, The White Paper on China's Hospital Information Systems, 2008,

http://www.chima.org.cn/pe/DataCenter/UploadFiles_8400/200812/20081219115545203.pdf (accessed 26.01.13).
[4] E.M. Campbell, D.F. Sittig, J.S. Ash, K.P. Guappone, R.H. Dykstra, Types of unintended consequences related to computerized provider order entry, J. Am. Med. Inform. Assoc. 13 (5) (2006) 547–556.
[5] E.M. Campbell, D.F. Sittig, K.P. Guappone, R.H. Dykstra, J.S. Ash, Overdependence on technology: an unintended adverse consequence of computerized provider order entry, AMIA Annu. Symp. Proc. 9 (2007) 4–8.
[6] T. Hoff, Deskilling and adaptation among primary care physicians using two work innovations, Health Care Manage. Rev. 36 (4) (2011) 338–348.
[7] D.F. Sittig, H. Singh, Electronic health records and national patient-safety goals, N. Engl. J. Med. 367 (19) (2012) 1854–1860.
[8] R.B. Myers, S.L. Jones, D.F. Sittig, Review of reported clinical information system adverse events in US Food and Drug Administration databases, Appl. Clin. Inform. 2 (1) (2011) 63–74.
[9] D.F. Sittig, H. Singh, Defining health information technology-related errors: new developments since to err is human, Arch. Intern. Med. 171 (14) (2011) 1281–1284.
[10] S. Sharma, G. Dhillon, IS risk analysis: a chaos theoretic perspective, Issues Inform. Syst. 10 (2) (2009) 552–560.
[11] S. Alter, S.A. Sherer, A general, but readily adaptable model of information systems risk, Commun. Assoc. Inform. Syst. 14 (1) (2004) 1–28.
[12] T.L. Hanuscak, S.L. Szeinbach, E. Seoane-Vazquez, B.J. Reichert, C.F. McCluskey, Evaluation of causes and frequency of medication errors during information technology downtime, Am. J. Health Syst. Pharm. 66 (12) (2009) 1119–1124.
[13] L.A. Huryk, Factors influencing nurses' attitudes towards healthcare information technology, J. Nurs. Manag. 18 (5) (2010) 606–612.
[14] China Hospital Information Management Association, Survey of Health Information Technology Adoption Status among Chinese Hospitals, 2011–2012, 2012.
[15] Analysys International, Baidu, Google China and Sogou Got Top3 in China Internet Search, 2012, http://english.analysys.com.cn/article.php?aid=136839 (accessed 26.01.13).
[16] Alexa Internet, The Top 500 Sites on the Web, 2012, http://www.alexa.com/topsites (accessed 26.01.13).
[17] K. Charmaz, Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis, Sage, Thousand Oaks, CA, 2006, ISBN 978-0761973539.
[18] S.A. Sherer, S. Alter, Information systems risks and risk factors: are they mostly about information systems? Commun. Assoc. Inform. Syst. 14 (2) (2004) 29–64.
[19] Center for Statistics and Informatics, Ministry of Health, China, China Health Statistics, 2012, 2012, http://www.moh.gov.cn/publicfiles/business/cmsresources/mohwsbwstjxxzx/cmsrsdocument/doc15055.pdf (accessed 26.01.13).
[20] Committee on Patient Safety and Health Information Technology; Institute of Medicine, Health IT and Patient Safety: Building Safer Systems for Better Care, The National Academies Press, Washington, DC, 2011, ISBN 978-0309221122.
[21] U.S. Office of the National Coordinator for Health Information Technology, The Health IT Patient Safety Action and Surveillance Plan for Public Comment, 2012, http://www.healthit.gov/sites/default/files/safetyplanhhspubliccomment.pdf (accessed 26.01.13).
[22] G. Stoneburner, A. Goguen, A. Feringa, Risk Management Guide for Information Technology Systems. The U.S. National Institute of Standards and Technology Special Publication 800-30, 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp 800-30.pdf (accessed 26.01.13).
[23] F. Magrabi, M.S. Ong, W. Runciman, E. Coiera, Using FDA reports to inform a classification for health information technology safety problems, J. Am. Med. Inform. Assoc. 19 (1) (2012) 45–53.