The Rising Frequency of IT Blackouts Indicates the Increasing Relevance of IT Emergency Concepts to Ensure Patient Safety

U. Sax[1]*, M. Lipprandt[2]*, R. Röhrig[2]
[1] Department of Medical Informatics, University Medical Center Göttingen, Göttingen, Germany
[2] Institute of Medical Informatics, Carl von Ossietzky University, Oldenburg, Germany
* both authors contributed equally

Summary

Introduction: As many medical workflows depend vastly on IT support, great demands are placed on the availability and accuracy of the applications involved. The cases of IT failure through ransomware at the beginning of 2016 are impressive examples of the dependence of clinical processes on IT. Although IT risk management attempts to reduce the risk of IT blackouts, the probability of partial/total data loss, or even worse, data falsification, is not zero. The objective of this paper is to present the state of the art with respect to strategies, processes, and governance to deal with the failure of IT systems.

Methods: This article is conducted as a narrative review.

Results: Worst case scenarios are needed, dealing with methods as to how to survive the downtime of clinical systems, for example through alternative workflows. These workflows have to be trained regularly. We categorize the most important types of IT system failure, assess the usefulness of classic counter measures, and state that most risk management approaches fall short on exactly this matter.

Conclusion: To ensure that continuous, evidence-based improvements to the recommendations for IT emergency concepts are made, it is essential that IT blackouts and IT disasters are reported, analyzed, and critically discussed. This requires changing from a culture of shame and blame to one of error and safety in healthcare IT. This change is finding its way into other disciplines in medicine. In addition, systematically planned and analyzed simulations of IT disaster may assist in IT emergency concept development.

Keywords

Equipment Failure, Patient Safety, ITIL, Electronic Medical Records, Clinical Information System

Yearb Med Inform 2016:130-7
http://dx.doi.org/10.15265/IY-2016-038
Published online November 10, 2016

1 Introduction

1.1 Motivation and State of the Art

Clinicians are currently in a dilemma: on the one hand, the clinical working environment is increasingly digital in nature; on the other hand, digital natives[1] have never learned how to deal with a paper and pencil situation in case IT fails. Many processes in hospitals are now software-driven. Data and information from medical instruments and devices are transferred automatically as one aspect of rather complex documentation structures. In general, the clinical user does not need to know about the complexity under the hood of such system. However, we are now seeing the first generation of digital natives entering the workforce as doctors and nurses in clinic. They expect easy-to-use interfaces – perhaps driven by successful form factors derived from the consumer industry. As such, the acceptance of IT support in clinical processes rises.

We therefore face a certain "learned carelessness" [1] and unrealistic expectations towards fault tolerance and the availability of systems. If then an error does occur in software, users frequently do not realize this as an error. As we already are aware, people tend not to memorize data that they know are stored on a computer [2]. If for example a system "always" warns of a drug-drug interaction, the user often concludes there is no interaction if the warning does not appear as a result of some system failure (Expectation conformity).

Workflows frequently include several distinct specialists and the corresponding information systems provide the communication platform between disciplines, professions, and roles. Therefore the single user has to trust the data and information provided, because he/she cannot really prove their correctness (digital Taylorism[2]). This leads to an immense dependence on IT systems, not only in the daily clinical routine. Therefore an IT blackout can lead to hazardous situations, in which critical incidents can occur and harm can result. A disaster concept may reduce any potential risk, thus enhancing patient safety in the case of an IT disaster.

1.2 Shortcomings

Given the complexity of IT systems, their flexibility in terms of customization, the web-driven interaction with other systems, as well as the rather short update and patch cycles, errors, accidents and system failures can never be ruled out.

A system failure may lead to non-availability of IT components, IT systems, partial or total loss of data, or worst case, the loss of data integrity [3]. The literature and error reporting systems only portray the tip of the iceberg. A scenario such as a successful virus attack can cause serious damage to the IT infrastructure and compromise patients' safety [4–6].

The dependency of clinical staff on the availability and the correct function of IT

[1] https://en.wikipedia.org/wiki/Digital_native

[2] https://en.wikipedia.org/wiki/Digital_Taylorism

systems pose a severe threat to the patients, when such systems fail ("hostage situation").

Therefore every clinic needs an emergency plan, which is both feasible and known to the employees, as well as regularly practiced in drills. It is of utmost importance that the additional steps relating to IT emergency and disaster recovery plans be part of the overall quality assessment/assurance and certification procedures. The current approaches and literature aim at making plans to avoid potential IT blackouts rather than describing processes to establish any emergency plan.

1.3 Objectives

The objective of this narrative review is to present the state of the art with respect to strategies, processes, and governance to deal with the failure of IT systems, from a simple blackout via loss of data to the loss of data integrity. We combine an overview of the recent literature with our longstanding personal experience in the operation and use of information systems at the actual point of care.

2 Understanding IT Disaster and Safety Aspects

2.1 Review of the Literature

Disaster recovery refers often to earthquakes, flooding, and fire. Many papers focus on the technical requirements to prevent data loss in case of disasters especially in PACS [7]. The solutions and suggestions mostly refer to a redundant copy of the data or archives at different physical locations [8–10].

A conceptual framework is given in [11], in which the involved users factors are adapted to disaster recovery planning (DRP) by health maintenance organizations (HMO). Patient safety is directly coupled with data reliability and computer system downtime [12]. Furthermore, the security issues relating to access to data are important in disaster management [13]. To detect impending failures, a surveillance system is tested in [14]. Overall, the importance of safe health IT for patient safety is stated in [15]. Many IT problems, such as doublets in patients [16], confusion of patient identification [3], missing data, design flaws, or lack of usability [17] are discussed as crucial factors in health IT systems.

Generally, the literature addresses technical solutions to prevent IT blackouts or the consequences of IT blackouts as a whole. Patient safety was specifically discussed as a result of the malfunctioning of IT systems. However, a clinical process-oriented review of the effects of an IT disaster in terms of patient safety was not the focus of any discussion. The aim of this paper is to discuss approaches to the development of a plan for IT disasters with regard to patient safety.

2.2 Classification of Severe Critical IT-Incidents

After a number of severe denial of service attacks on public infrastructure, governments all over the world have established computer emergency response teams (CERT), such as the European Union Agency for Network and Information Security (ENISA) [18] and the EU CERT website [19].

The German National Research and Education Network (Deutsches Forschungsnetz, DFN) have also set up a computer emergency response team (CERT) service [3] and informs the community and public on security problems with exploits in browsers and so on, whereas the German KRITIS initiative[4] has a more strategic view on the availability of critical infrastructure in different sectors, such as aviation, energy, and health.

Nevertheless, these services mostly lack specific recommendations as answers to questions like: (a) how to deal with an actual incident, and more severely (b) how to revert back to normal operation after such an incident.

The IT Infrastructure Library (ITIL®) continues a little further down the line of - incident - problem (error, solving) - change processes [20]. IT service continuity management (ITSM[5]) covers the steps from prioritizing the severity of a system failure along with business continuity planning (BCP). However, ITIL® does not present a clear and simple concept as to how to classify IT incidents.

From the user perspective, there are only three types of IT problem: (1) lack of system availability, (2) loss of data, and (3) loss of data integrity (Figure 1).

Such IT problems are logically intertwined with patient safety. A lack of system availability is immediately noticed by the user. The recovery process can start as soon as the flaw arises. However, the partial loss of data or loss of data integrity is more difficult to observe. A lot of valuable time may elapse before the recovery process starts. All newly recorded data in the meantime will be lost on data restoration using the last (assumed integer) backup.

2.2.1 Lack of System Availability

If clinical staff cannot use or access a system supporting their process or decision, for example in order to obtain a specific lab result prior to treatment, they may lack the necessary information required for dosing, adjustment, or even contraindication of the medication or treatment regimen selected. The resulting inability to act in an informed fashion is potentially dangerous to patients' lives causing perhaps irreversible damage if not fatal.

System availability is therefore of paramount importance. Key users require a certain level of system availability, which is usually around 99.5% uptime, excluding scheduled down times. However, precautions have to be taken for the remaining 0.5%. This translates to a maximum total of 43.8 hours per year that a system is acceptably unavailable to the user. It is therefore more pertinent to define a limit for the longest acceptable down time (recovery time objective, RTO).

If this limit is exceeded, an alternative device, application, or combination of both should be set up and run to make up for the lack of availability of the main system. An equal data flow of important information

[3] https://portal.cert.dfn.de/adv/archive/
[4] http://www.kritis.bund.de/SubSites/Kritis/EN/Home/home_node.html
[5] https://en.wikipedia.org/wiki/ITIL#IT_service_continuity_management

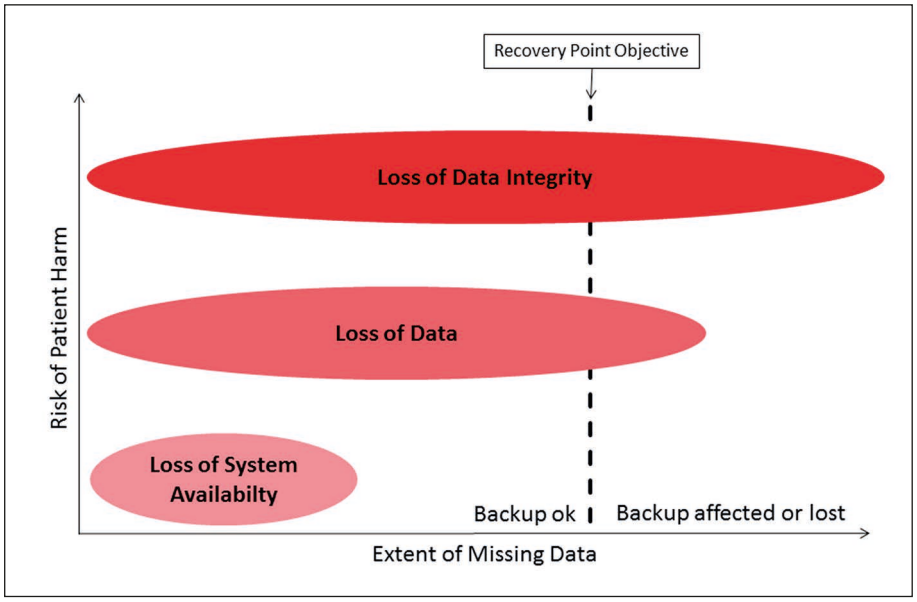

Fig. 1 Classification of IT problems as a function of the risk of patient harm and extent of missing data The Recovery Point Objective (RPO) defines the line between temporary and permanent loss.

can be achieved through e.g. hardcopies or different analog communication media.

The causes of such failures are manifold – from water, to fire, to cooling failure, sabotage etc. However, most are caused by simple things, such as patches, updates, or other logical system failures.

2.2.2 Loss of Data

After a system blackout, the situation may arise that some data cannot be restored any more during the recovery process or the data are lost following a storage, database, or system failure. This is bad enough in the finance sector, but turns out to be much worse in healthcare, as the lost data may include billing information. Data loss can lead to the administering of unnecessary multiple doses of medication. Lost findings and images in radiology may lead to an avoidable and costly repeat of an examination, as well as the potential increase in exposure to ionizing radiation. This can result in a reduction in patient safety and as such needs to be addressed as a particularly hazardous situation. In legal terms, one has to deal with the potentially criminal personal injury resulting from what may be deemed as unnecessary interventions.

In an ideal world, the loss of data should not occur. Nevertheless, we must face the fact that we cannot guarantee 100% safety. Furthermore, it will always have to be a management decision to define any recovery point objective (RPO) as well as the accepted timespan for the recovery of data.

2.2.3 Loss of Data Integrity

The most severe incident though and the one the most difficult to detect is the loss of data integrity. Confusion in patient identification [3] leads to the presentation of incomplete or incorrect data. Furthermore, users have no chance to recognize this failure. As clinical decisions are based more and more on information systems, the more clinicians have to trust their systems in a world of digital Taylorism. They are often unable to detect systematic error, especially if the errors occur rarely or are not reproducible. Flaws in data integrity can lead to failures in decision making, because the calculation of data or their precision can prove incorrect over long periods of time.

In addition to incidents based on incorrect data, the loss of data integrity can lead to data loss, if the corrupted records cannot be identified and corrected.

Some prominent examples of critical IT incidents may be found more frequently in the Critical Incident Reporting System (CIRS) archives[6].

2.3 Understanding Chains of Events Leading From Hazard to Harm

Perhaps it is a philosophical question as to whether to assess an incident from the point of view of an IT service provider or that of a doctor, nurse, or patient.

Figure 2 explains ISO 14971, describing a chain of events: If one or more events (indicating a hazard) occurring with the probability P1 lead to a hazardous situation and an additional event or events with the probability P2 then occur, then we may talk of an incident having occurred, which may even be critical. A third event may then take place with probability P3, such as the failure to act on the incident, perhaps resulting in patient harm. If the event actually occurs, we define this as the adverse event. Should the event not occur, we then talk of a near miss [21].

To avoid misunderstanding, it is necessary to define the term "incident". From an IT technician's point of view, an incident is an IT failure, whereas an incident is a failure in diagnostics or therapy in the eyes of patients or users (nurses, physicians, and medical staff), and hospital risk management staff. With respect to patient safety, it would prove more pertinent to take the patients' and users' aspect.

Therefore, on the assumption that most information systems in hospitals have no immediate effect on patients, an IT blackout or IT disaster "only" leads to a hazardous situation (e.g. necessary data are false or not available) and not directly to an incident. Therefore, there is still a chance to prevent the critical incident (such as a false decision or an error in the administration of medication) from occurring through technical and organizational measures (figure 2, P2). Only the failure of IT systems controlling medical equipment such as ventilators or syringe pumps leads to a (critical) incident

[6] http://www.kh-cirs.de/faelle/ (German only)

immediately. In such cases, clinical staff will need to act quickly in order to avoid any harm to their patients (figure 2, P3).

In both cases, the user is the key in the prevention or mitigation of patient harm. The user's point of view is therefore essential to the emergency concept. We need to ask ourselves how the user can detect that systems are not running. The following questions need to be addressed from the user's point of view:

- How may a user detect the validity of the information presented?
- How can we inform all relevant users of corrupted data or compromised systems?
- Do users know what to do and how to work without the assistance of IT systems?

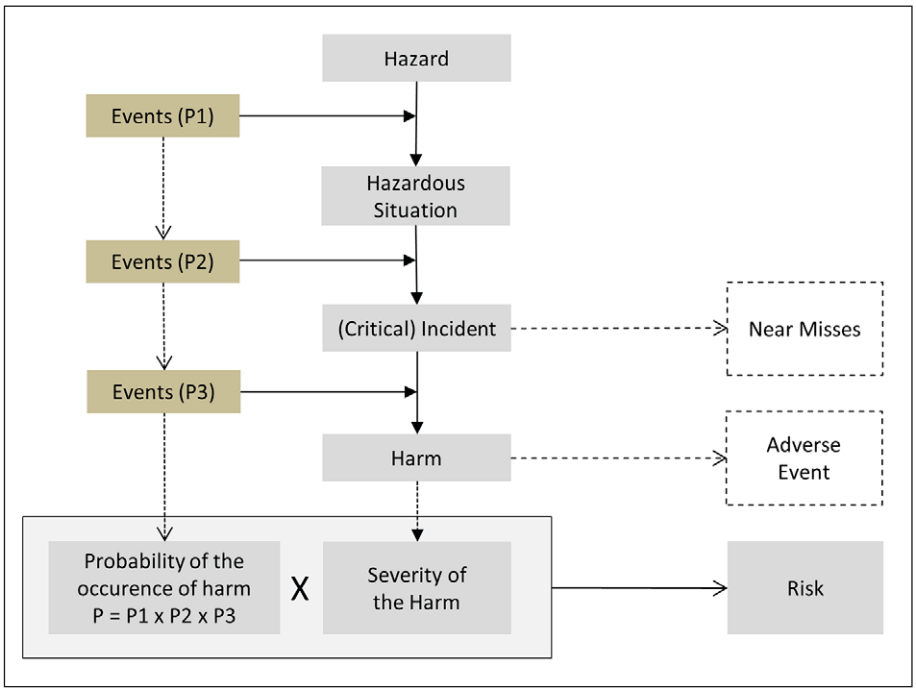

Fig. 2 Chain of events leading from a hazard to harm. A combination of the concepts of technical [21] and medical [22–25] risk management. (p = probability)

3 Developing an Emergency Concept for IT Disaster

The following recommendations are based on concepts from different sources: ITIL [20], London Protocol for Clinical Incidences [26], Clinical Risk Management [21, 27], Human Factors and Patient Safety activities [22–25], unpublished case reports of IT disasters, recommendations for emergency task forces, and the authors' individual experience in task forces. This is an approach to combine these concepts and cultures.

3.1 The Process of Developing an Emergency Concept

In addition to the strategy of enabling IT security and availability, it might prove useful to develop an emergency concept of dealing with IT disasters from the point of view of users. When aiming for a practical concept, we would like to propose the following four steps:

- Identification of information needs: Where does (medical) decision making depend on the information provided by information systems? Which systems are involved?
- Prioritization of critical processes (incl. the periodization of tasks)
- Defining of measures
- Rollout and training of the concept

Each of these steps is described below.

3.2 Risk Assessment

Risk assessment comprises the analysis, estimation, and evaluation of risk. In risk analysis, all potential hazards to which a patient may be exposed have to be identified. Risk estimation involves the classification of hazards and hazardous situations based on the extent of the damage that may be caused and the probability of a hazardous event occurring. The combination of harm and the probability of an adverse event occurring comprise the risk to which a patient is exposed. Risk evaluation is the interpretation of whether a risk is acceptable or not.

The proposed process is a specialized method in the development of IT emergency concepts.

3.2.1 Identification of Information Needs

If an IT disaster strikes, it is important to know where the hazards are. To locate the hazard, it is necessary to understand the (real) usage of the information systems. A formal method of cataloguing all hazards is to explore the information needs, defined as information (presented by an information system) necessary in order to make a (medical) decision [28]. To catalogue these needs, users have to be interviewed with respect to their use of the systems. This must be completed in all organizational units and with all kinds of user. The information needs should be assigned to clinical processes.

3.2.2 Prioritization of Critical Processes

The information needs and clinical processes need to be categorized and prioritized according to the respective problems in delivery of care and the corresponding effect on patient safety. The users must be involved in this step directly. An emergency concept is required for all the tasks presenting potentially serious problems in delivery of care resulting from missing or incorrect data.

3.3 Measures of Risk Control

3.3.1 Infrastructure

Modular and redundant infrastructure gives both users and technicians the ability to switch over to a different medium and/or modality in case of a technical breakdown. When developing the emergency plan, it is particularly important to consider what would happen if essential components (servers, databases, electrical power, and/or the network…) are also involved. Furthermore, decisions must be made on whether such fully independent and redundant systems or procedures are both necessary and feasible.

For example, this could be a local computer connected to an uninterruptable power supply (UPS) and a local printer, on which patients' current medication plans are stored in pdf files.

3.3.2 Organizational Concept

The organizational requirements inform the higher level incident management processes. The respective responsibilities of both the IT department and the various medical departments and institutes need to be defined clearly to improve communication as well as optimize processes. This approach must also be integrated into existing disaster plans. The new process should not be separate to the other plans. A more integrated view of plans for prevention on the one side and plans for IT failures on the other is necessary.

When a serious systematic IT failure occurs, the establishment of a single point of communication (SPOC) plays a crucial role. Errors need to be reported to the SPOC first. The SPOC then has to estimate the consequences of and the hazards associated with the error [20]. Prioritization needs to be carried out based on the assessment of any associated risk emanating from further processing of the error and any possible escalation required. The decision in favor of escalation and the following task to inform an emergency task group can be supported by rules (standard operating procedures, SOPs) basing on the risk analysis of the information needs and critical processes (part of the Support Knowledge Base).

If escalation proves necessary, an IT emergency task force (ITEF) should be set in place. The ITEF follows two approaches, the first of which is to deal with the incident (see 3.3.2.1), to ensure patient safety, and enable workflows as soon as and as normally as possible. The second approach involves a problem management team (see 3.3.2.2) analyzing the root cause, solving the problem, and returning everything to normal operation. This whole process needs to be carried out by two closely cooperating teams, whose activities are best coordinated by supervisors located in the same office when possible.

In addition to the IT managers and systems administrators of the affected systems, representatives of both management and the users should also be represented in the ITEF. Depending on the complexity of the error, it may even prove necessary to involve external experts in the team.

If it is foreseeable that a relevant loss of data or any patient harm caused by the IT failure or a sustained blackout leads to a restriction or reduction in patient care, the institutional press officer should be involved or be instated as a member of the ITEF to avoid any loss of reputation as a result of insufficient external communication.

The importance of having two teams becomes greater, the greater the damage is. One team is on the front line to deal with the situation. Providing an overview, searching for solutions, and communication are main aspects of incident management. The second team can search for the cause of the problem without being interrupted by the effects of the error. Time-critical processes cannot be solved by the same team while working on both fronts.

3.3.2.1 Incident Management Concept

The main objective of the incident management team is to ensure patient safety and enable workflows as soon as possible to be "as normal as possible". To guarantee this, workflows should be described for various failure scenarios. This includes the persons responsible, the tasks, the competencies needed, and resources available. It should be noted that if a larger or longer outage occurs, measures must be in place to deal with items such as replacement, shift changes, or personnel breaks.

The incident management team will need to answer for example the following questions:

- Which department(s) / organizational units are affected by the failure?
- Who is the responsible contact or coordinator in the departments?
- How can the department (responsible contact) be informed?
- What communication channels are available when the network or telephone (voice over IP) systems fail?
- Can numbers of staff be increased to ensure at least emergency service cover? (e.g. telephone communication of lab results if the network or LIS fail?)
- Are sufficient resoures available for emergency use? (e.g. are there enough telephones in the lab?)
- Is the contact person capable of carrying out the necessary measures? (e.g.: Does the contact person have access to a local emergency computer or know where the key is located?)

3.3.2.2 Problem Management Concept

Problem management focuses on analyzing the root cause of incidents, fixing the problem, and returning to the routine workflows. The measures of problem management are often complex and can often lead to further damage in the case of incorrect decisions or execution. Therefore, an important task of the incident management team is to keep the problem management team separated from the communication processes, so that they can focus solely on the time-critical, safety-related tasks.

An often underestimated task after restoring system function is the return to routine operation. In the case of downtime, information may have been noted on paper or alternative media, which has to be (re-) sent or re-entered later. In this transition period, the user cannot be expected to recognize the state of the system (e.g. incomplete data or fully operational). Thus, there should be a specific communication concept in place governing the return to normal workflows.

3.4 Implementation: Rollout, Training, Tests

Thankfully, IT disasters are very rare. However, this also means that both the required infrastructure is rarely used and the

procedures are rarely implemented. This can lead to errors, which can aggravate an already critical situation.

Therefore, SOP's should be in place (and known to the relevant people) for all critical processes, such as database recovery from a backup. In addition, these measures should be practiced regularly. Nevertheless, it is often not possible to perform the needed training and exercises with production systems. Furthermore, the effort required to maintain training environments sufficiently up to date is extremely high. Support contracts with equipment manufacturers or specialized IT service providers comprise an alternative to in-house experience.

A greater challenge lies in the qualification and development of users' skills and competencies. SOP's must not only be available in the case of an IT disaster. We also need to ensure that users know there are SOP's for the respective situation and where they are stored. An established concept is the training of key users. However, it is not certain that trained key users are on duty at the time of an incident. In many cases, respectively qualified staff is scarce overnight, during holiday periods or weekend shifts. Therefore, the storage location of the SOP's as well as possibly a backup copy should be made available centrally. Thus the incident management team is able to advise the users of the SOP's and answer their questions accordingly.

4 Discussion

Nowadays, hospitals are the frequently targets of virus attacks and ransomware [29]. Hospitals are highly dependent on IT systems. IT blackouts have severe consequences for the continuity of healthcare as well as patient safety. The rapid implementation of electronic health records (EHRs) only increases the threat of cyber-crime. New approaches to security are therefore of paramount importance and needs. The four steps suggested by Sittig et al. [30] include a system protection strategy (e.g. backups), an adaptation of users' behavior (e.g. not opening e-mail attachments thoughtlessly), the monitoring of suspicious activities, as well as a recovery and learning strategy following an attack. The recovery strategy described a multidisciplinary team to manage the adverse event and identify the root cause. Furthermore, consultation with other external IT experts should be considered. Last year, the reports on IT problems in hospitals increased and have thus been brought very much into the public eye. This might have different reasons: A larger accumulation of IT failures with the rise of ransomware, the increasing dependence of medical care on IT systems or changes to the information policy of hospital management [29, 30, 31]. The increase in IT attacks on hospitals has led to a more open discussion on the advantages and disadvantages of fully digital documentation. Beside IT attacks, only a small amount of software is legally designated as "safe" for use as a medical product. Most software currently employed is unregulated. Although the guidelines and standards are in place to ensure their safe design, build, implementation, and use, the issue of patient safety is not addressed explicitly [32].

Most of the literature addresses the prevention of IT blackouts, which is of prime importance. The handling and procedure, should an IT blackout occur, are not currently the explicit focus of any discussion. Therefore this narrative review should be viewed as groundwork for further discussion. It should raise awareness of the importance and complexity of IT failures and the need to be prepared when an IT disaster does occur.

Dealing with the prevention of IT failure is slightly different from dealing with an occurred IT-failure and its consequences. Various recommendations for IT security and service delivery such as ITIL® are available [33, 34]. In a survey of hospitals in five European countries in the year 2011, 43 (55%) of 75 participants reported feeling familiar with the term / concept ITIL®. Seven (16%) of 43 participants indicated that their institution had ITIL® certified employees [35]. Although the dissemination of ITIL® has increased in recent years, particularly in Europe, there are still only few publications for use in hospitals and healthcare providers [35, 36].

The focus of most of the recommendations is on service quality and on the prevention of IT blackouts and disasters. Despite the undisputed relevance of the measures to avoid risks, experience and current events indicate that IT disasters just happen despite all measure of good prevention [3, 37, 38]. In such cases, the only help is to be prepared for the worst case scenario [39–41].

Sittig et al. [30] mentioned the importance of a recovery strategy. Evidence of the development of IT emergency concepts is limited to reports on individual cases, individual experience, or the transfer of concepts from other areas of emergency management in healthcare. A detailed plan with different teams for adverse events and a root cause analysis is still missing. Recommendations on the control of an IT blackout have not been discussed sufficiently. Precisely because of the progress of digitization, new threats through e.g. ransomware are ubiquitous. This paper is thus the first step in starting a discussion on consolidated plans in case of an IT blackout.

Risk management concepts in hospitals and concepts geared to patient safety should be adapted to IT failures. In particular, concepts geared towards patient safety are more focused on socio-technical systems and human factors. A combination of different methods from different domains, such as those suggested here, might be reasonable. However, the difficulties lie in bringing the concepts together. This starts with a seemingly simple problem of using the same terminology with different meanings in the various domains. An important task will be to standardize the various terms and definitions.

The recommendation is to divide the CERT into two groups, one in control of incident management and one focused on problem management. This recommendation is based on the analysis of the events when IT failures or IT blackouts occurred, combined with the authors' own experience and principles of mission control in other domains. Nonetheless, most hospitals will find themselves challenged to ensure that members of both teams are always on duty. Given the rate of employee turnover, constant training must be available and the teams must remain open to adaptation. Therefore, research is needed to provide the necessary evidence to underline recommendation.

5 Conclusion

It is highly expected that the relevance of IT emergency plans will rise in the near future. On the one hand, the number of relevant IT disasters is rising, even with the large number of cases of known IT outages and disasters (probability of occurrence) going unreported. On the other hand, the likelihood simply increases with the increasing use of IT systems, as does the level of damage occurring.

Currently, recommendations on dealing with hospital IT disasters can only be made on the basis of evidence through expert opinions or case reports. To improve evidence, two things are needed:

First, only if errors are reported openly can we learn from them. Therefore, all incidents need to be analyzed systematically and published in critical incident reporting systems [24, 42–45], in order to build up the culture of error. Only the courage of hospitals in Los Angeles [4, 5] and Neuss (Germany) [38] to inform the public of their IT disaster caused by ransomware has encouraged a number of hospitals to go public on their past problems with malware as well as unsolved problems and risks.

Secondly, we need research on IT blackouts in healthcare. This should include the systematic development of recommendations for the ITEF, as well as the evaluation of these concepts through simulations and disaster exercises.

Detailed risk management and emergency plans are already established in clinical medicine as well as in IT service management. This paper demonstrates how the fundamental pillars of different emergency plan concepts can be merged and adopted in clinical information systems.

To enable the continuous evidence-based improvement of recommendations for IT emergency concepts, it is essential that IT blackouts and disasters are reported, analyzed, and discussed critically.

This requires changing from the current culture of shame and blame to one of error and safety in healthcare IT. This change is also finding its way into other disciplines in medicine. This requires research into IT disaster management in hospitals, including well-planned and analyzed simulations of scenarios causing IT blackouts.

Contribution to the Authors

US, ML, RR conducted and drafted this study; all authors reviewed this paper substantially.

We are indebted to Andrew Entwistle, who supported us as an excellent proof reader with his profound IT-background.

Conflict of Interests

The authors declare no conflict of interests.

References

1. Frey D, Schulz-Hardt S. Eine Theorie der gelernten Sorglosigkeit. [A theory of learned carelessness] (German) Mandl H, editor. 1997;40:604–11.
2. Sparrow B, Liu J, Wegner DM. Google effects on memory: cognitive consequences of having information at our fingertips. Science 2011;333:776–8.
3. Botta J, Walliser P. Die fatalen Folgen der Implementierung einer HL7-ADT-Schnittstelle. Swiss Medical Informatics 2014;30.
4. Dobuzinskis A. Cyber attack snarls Los Angeles hospital's patient database. Internet; 17.02.2016.
5. Dalton A. Hospital paid 17K ransom to hackers of its computer network. Internet; 17.02.2016.
6. Flade F, Frigelj K, Grabitz I. Cyber Attacks On Hospitals, A New Kind Of Deadly Virus. Internet; 23.02.2016.
7. Avrin DE, Andriole KP, Yin L, Gould R, Arenson RL. Simulation of disaster recovery of a picture archiving and communications system using off-site hierarchal storage management. J Digit Imaging 2000;13:168–70.
8. Mansoori B, Rosipko B, Erhard KK, Sunshine JL. Design and implementation of disaster recovery and business continuity solution for radiology PACS. J Digit Imaging 2014;27:19–25.
9. Colpas P. DR underscores the importance of security. Regardless of the selected solution, experts agree the most important criteria for a disaster recovery (DR) back-up system is that it is secure. Health Manag Technol 2013;34:6-8, 10-1.
10. Poelker C. Don't roll the dice on data loss. Implement smart recovery to reduce disaster recovery costs in healthcare. Health Manag Technol 2012;33:14–5.
11. Bandyopadhyay K, Schkade LL. Disaster recovery planning by HMOs: theoretical insights. Health Care Manage Rev 2000;25:74–84.
12. Bagalio SA. When systems fail: improving care through technology can create risk. J Healthc Risk Manag 2007;27:13, 15-8.
13. Lindeman J, Grogan J. Beyond disaster recovery. Disaster recovery has refocused healthcare organizations from "always being ready" to "always being on". Healthc Inform 2007;24:72.
14. Ong M-S, Magrabi F, Coiera E. Syndromic surveillance for health information system failures: a feasibility study. J Am Med Inform Assoc 2013;20:506–12.
15. Warden GL. Health IT and patient safety: Building safer systems for better care. Washington, DC: National Academies Press; 2012.
16. Just BH, Proffitt K. Do you know who's who in your EHR? Healthc Financ Manage 2009;63:68–73.
17. Bowman S. Impact of electronic health record systems on information integrity: quality and safety implications. Perspect Health Inf Manag 2013;10:1.
18. The European Union Agency for Network and Information Security (ENISA). https://www.enisa.europa.eu.
19. General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee. Computer Emergency Response Team (CERT-EU). https://cert.europa.eu/cert/clusteredition/en/latest.html.
20. Stych C, Zeppenfeld K. ITIL. Berlin: Springer; 2008.
21. DIN ISO 14971. DIN EN ISO 14971:2013-04: Medizinprodukte - Anwendung des Risikomanagements auf Medizinprodukte (ISO 14971:2007, korrigierte Fassung 2007-10-01); Deutsche Fassung [Medical devices - Application of risk management to medical devices; German version] EN ISO 14971:2012.
22. Mellin-Olsen J, Staender S, Whitaker DK, Smith AF. The Helsinki Declaration on Patient Safety in Anaesthesiology. Eur J Anaesthesiol 2010;27:592–7.
23. Diller T, Helmrich G, Dunning S, Cox S, Buchanan A, Shappell S. The Human Factors Analysis Classification System (HFACS) Applied to Health Care. Am J Med Qual 2014;29:181–90.
24. Neuhaus C, Röhrig R, Hofmann G, Klemm S, Neuhaus S, Hofer S, et al. Patientensicherheit in der Anästhesie. [Patient safety in anesthesiology: Multimodal strategies for perioperative care] (Germman) Anaesthesist 2015;64:911–26.
25. Thomeczek C, Rohe J., Ollenschlager G. Das unerwünschte Ereignis in der Medizin. [Adverse events in medicine] In: Madea B, Dettmeyer R, editors. Medizinschadensfälle und Patientensicherheit. [Medical Failures and Patient Safety] (German) Köln: Deutscher Ärzteverlag; 2007. p. 13–20.
26. Taylor-Adams S, Vincent C. Systems analysis of clinical incidents: The London protocol. Clinical Risk 2004;10:211–20.
27. DIN EN 80001-1:2011-11. DIN EN 80001-1:2011-11 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten (IEC 80001-1:2010); Deutsche Fassung [Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities; German version] EN 80001-1:2011.
28. DAkkS Deutsche Akkreditierungsstelle. Leitfaden Usability. 2010. http://www.dakks.de/sites/default/files/71_sd_2_007_leitfaden_usability_1.3_0.pdf.
29. Tom Sullivan. More than half of hospitals hit with ransomware in last 12 months. April 07, 2016. http://www.healthcareitnews.com/news/more-half-hospitals-hit-ransomware-last-12-months. Accessed 2 Aug 2016.
30. Sittig DF, Singh H. A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. Appl Clin Inform 2016;7:624–32.
31. Olenick D. The Ottawa Hospital fends off ransomware attack. 14 March 2016. http://www.scmag-

azine.com/the-ottawa-hospital-fends-off-ransomware-attack/article/482921/. Accessed 2 Aug 2016.
32. Magrabi F, Aarts J, Nohr C, Baker M, Harrison S, Pelayo S, et al. A comparative review of patient safety initiatives for national health information technology. Int J Med Inform 2013;82:e139-48.
33. ISO/IEC 20000–1:2011. ISO/IEC 20000–1:2011 Information technology -- Service management -- Part 1: Service management system requirements.; 2011.
34. Kabachinski J. Have You Heard of ITIL?: It's Time You Did. Biomedical Instrumentation & Technology 2011;45:59–62.
35. Hoerbst A, Hackl WO, Blomer R, Ammenwerth E. The status of IT service management in health care - ITIL® in selected European countries. BMC Med Inform Decis Mak 2011;11:76.
36. Lapão LV, Rebuge A, Silva M<M, Gomes R. ITIL Assessment in a healthcare environment: the role of IT governance at Hospital São Sebastião. Stud Health Technol Inform 2009;150:76–80.
37. Gamble KH. Weathering the storm. Having a disaster recovery plan can mean the difference between scrambling for a quick IT fix and smooth sailing in the storm. Healthc Inform 2008;25:32, 34, 36-8.
38. NGZ-Online. Computer-Virus legt das Lukaskrankenhaus lahm.
39. Genes N, Chary M, Chason KW. An academic medical center's response to widespread computer failure. Am J Disaster Med 2013 Spring;8(2):145-50.
40. Mazzoleni MC, Baiardi P, Giorgi I. Lesson learnt from a halt of the hospital information system. Stud Health Technol Inform 1999;68:102–5.
41. Kilbridge P. Computer crash--lessons from a system failure. N Engl J Med 2003;348:881–2.
42. World Health Organization (WHO). WHO draft guidelines for adverse event reporting and learning systems. 2005. http://osp.od.nih.gov/sites/default/files/resources/Reporting_Guidelines.pdf. Accessed 26 Feb 2016.
43. European Commission, Patient Safety and Quality of Care working group. Key findings and recommendations on Reporting and learning systems for patient safety incidents across Europe. 2014. http://ec.europa.eu/health/patient_safety/policy/index_en.htm. Accessed 26 Feb 2016.
44. Cooper JB, Newbower RS, Kitz RJ. An analysis of major errors and equipment failures in anesthesia management: considerations for prevention and detection. Anesthesiology 1984;60:34–42.
45. Cooper JB, Newbower RS, Long CD, McPeek B. Preventable anesthesia mishaps: a study of human factors. Anesthesiology 1978;49:399–406.
46. Vincent C. How to investigate and analyse clinical incidents: Clinical Risk Unit and Association of Litigation and Risk Management protocol. BMJ 2000;320:777–81.

Correspondence to:
Prof. Dr. Rainer Röhrig
Carl von Ossietzky University
Department of Medical Informatics
26111 Oldenburg
Germany
E-mail: Rainer.Roehrig@uni-oldenburg.de

Glossary

Average	Blackout, loss of data or loss of data integrity
Blackout	Lack of system availability
Care Delivery Problems	Unsafe acts in healthcare (Definition according to the London Protocol) [26] [46]
CERT	Computer Emergency Response Team
Disaster	loss of data, destruction of data (recovery is needed) or loss of data integrity
Incident Management	Sum of all measures necessary to ensure patient safety and enable clinical workflows as normal as possible. (This definition does not match the definition of incident management in ITIL)
Incident Management Team	Team to coordinate and execute the measures of incident management
Information needs	The information required to reach a (medical) decision.
ITEF	IT emergency task force
ITIL®	IT Infrastructure Library
ITSM®	IT service continuity management
Loss of data integrity	especially: loss of data correctness. Important: Recovery can be also corrupted
Problem management	Sum of all measures to analyze the incident, fix the problem, and return to routine workflows. (This definition does not match the definition of incident management in ITIL)
Problem Management Team	Team to coordinate and execute the measures required for problem management.
Patient safety	The prevention of errors and adverse effects to patients associated with health care (WHO)
RTO	Recovery time objective: Accepted timespan for system downtime
RPO	Recovery point objective: Accepted timespan for loss of data
SOP	Standard operating procedure
SPOC	Single point of communication