https://doi.org/10.48009/2_iis_2011_49-52

Issues in Information Systems

Volume XII, No. 2, pp. 49-52, 2011

CASE STUDY – TRIPLE JEOPARDY: DATA BACKUP/LOSS, DISASTER RECOVERY, & NETWORK SECURITY

L. Roger Yin, University of Wisconsin-Whitewater, yinl@uww.edu
Lawrence Brown, University of Wisconsin-Whitewater, brownla14@uww.edu

ABSTRACT

In the midst of healthcare reform legislation in the U.S. and HIPAA enforced patient record security issues, it is imperative to enlighten computer software and hardware professionals today and tomorrow worldwide regarding the importance of risk management of healthcare information systems. One way for one to learn a new idea or concept is through storytelling. In this case study, the management and risk mitigation of patient records is portrayed. Consequences of critical data loss at both technical and human sides are examined. Through this applied case, communication and network software developers can learn about information security related issues in the burgeoning healthcare industry globally in general and in the U.S. specifically.

Keywords: network security; case study; healthcare information system; data backup; data loss; disaster recovery planning; HIPAA compliance

CASE SCENARIO

You are the patient record manager at L.A. Clinic, a mid-sized healthcare facility with many specialist and general practice doctors. Your job description consists of maintaining patient records' security and integrity. Additionally, you are charged with the responsibility of making sure doctors, nurses, and medical assistants securely and confidentially handle patient record matters. For many years, operations are running smoothly, and you have just undertaken a major project: converting paper file records to computer-based electronic records; that project has proven to be successful and is promising to save the clinic one-hundred-fifty thousand U.S. dollars by eliminating the necessity of several administrative assistants. Everyone is happy and has been so for the past two years.

A few weeks ago, during a routine security audit of the entire IT system, you hired an independent consulting firm to perform an audit on your companies IT resources. For the most part, the audit went well; operations were efficient, and for the most part, security measures were proper. Currently, you are confident that if the clinic experienced a disaster that you could reasonably recover. However, the audit revealed potential weaknesses in your disaster prevention and backup routines / policies & procedures. You are currently using two Storage Area Networks: One for operations data, one for performing system backups. After reading the audit report, you realize one important, but obvious aspect was left out of your disaster recovery plan: a secure off-site data backup plan and a failover plan – a plan to temporarily mirror and switch data services to so business can sustain and continue during disaster recovery operations with minimal interruptions.
After careful review and deliberation, you decide it would be feasible to hire an outside IT consultant to recommend options for the project. The consultant recommends that your clinic consider on-line cloud-based backup, which is encrypted. In addition, it was recommended L.A. Clinic to have a company host and mirror clinic operations applications and data. The encryption is a necessary service as it guarantees data security over the network connections via leased lines as backup / failover data transmissions occur.

Given constraints, the total cost of the backup plan would cost the clinic approximately $125,000 annually, including communications company fees, cloud-based backup hosting fees, and in-house administrative staff fees. Additionally, the cost of outsourcing a failover hosting of your operations would cost you $15,000 / yr., based on the average of several quotes. On the bright side, your clinic's annual liability insurance premiums would decrease by approximately twenty-thousand dollars. Overall annual cost to the clinic would be an estimated $120,000. Finally, the project would take five business days to implement and five business days to fully document.

There are many controversial interests, however. Many powers to be are questioning issues surrounding options which comprise the best solution for the organization and issues of how to share financial responsibility for the recommended project. Physicians are concerned about the additional costs which affect them indirectly. They argue that some insurance

policy reimbursement rates are not enough where they will have enough overall profits to continue to provide quality services to these patients. Additional political constraints throughout the clinic are also a considerable factor in how fast the project is ramped up to speed; there is much political red tape involved with most procedures at the L.A. Clinic.

As far as he physicians are concerned, the additional costs would be cutting into their clinic's (and therefore, their) profitability. Consequently, they are concerned that this may affect their ability to continue to accept certain insurances, such as Medicare, Medicaid, and many HMO plans. Many government and HMO based health care programs limit their reimbursement amounts to participating health care providers. And many HMO plans constrain coverage by selecting their preferred providers in their covered networks; cost is often a constraining issue when HMO plans decide whether or not to include a provider in their network. Of course, it is not surprising that the physicians do not wish to compromise on their personal incomes either.

At L.A Clinic, the process for approving projects is most extensive for projects not budgeted for. While the clinic has a contingency funding pool, the process for tapping this fund is very complicated, and only projects which are considered an emergency or are mission-critical in nature are approved. *Even if the project falls within a department's budget*, there are several layers of approval needed in order for the project to be approved and to go forward, which may take up to ten to twenty business days. Since this project is considered a high-priority, these projects are most likely to be approved and are expedited, but approval can take three to five business days at best – even under these circumstances.

Complicating matters, clinic staff is feuding over job security issues. The Database Administrator who has tenure recently got wind of the consultant's recommendation and is concerned about losing his job. Consequently, he champions an in-house solution over the provider-based recommendation. Additionally, due to the automation of patient record storage and retrieval, three clerical staff positions were eliminated; there is tension amongst remaining office staff members who are mainly concerned about possibly losing their positions as well. Clerical employees assert that the clinic used to be like a big family working together and have wondered why it was necessary to switch to computerized patient records in the first place. To make matters more interesting for clerical staff lobbying behind keeping their jobs, there are several HIPAA related concerns among office staff. For one, they contend that if anything goes awry with the new system, they could be questioned by government officials as to how information was lost and / or misdirected into wrong hands. Furthermore, they argue that human intervention is the most appropriate solution for patient record storage and retrieval; they argue that a computerized inventory of records is *far more vulnerable, and expensive to operate / maintain* than paper records left under lock, key, and human intelligence behind the desk – especially with legal requirements being volatile in nature.

The feuding continues until legal counsel advises the urgency that an appropriate solution be in place in order for L.A. Clinic to be in compliance with HIPAA requirements. The question isn't whether to go with the plan or not – one single incident or loss could potentially cost many employees their jobs and could send some people in charge of patient record security to jail (especially, the Patient Records and Data Administrators). Speaking of legalities, the firm has received legal threats from two of the patient's lawyers – two patients who have since switched health providers recently after experiencing difficulties concerning their charts while being admitted for inpatient surgery.

You and your clinic now need to turn focus towards approving and implementing the project. Much is at risk and the conversion from paper to data records is a sunk cost. If a patient's data records are lost / compromised, lawsuits could permanently cripple the clinic in terms of finance and in terms of public trust / image. Considering the known backup vulnerability, and compliance requirements under HIPAA, it is the clinic's responsibility to see to it that these records are secured; they also need to be readily available only to the appropriate medical / office staff, and law enforcement agencies, regardless of cost to the firm. To finish the transition, the Data Administrator will need to be trained on any new policies in the coming weeks. Despite the plethora of concerns, political interests, and considerable additional cost, the heat is on! It is up to you to make final recommendations to main management and help soothe political conflicts in order to resolve the underlying problem the clinic faces and time is *not* on your side!

CASE SPECIFICATION

Industry:	Healthcare
Vulnerability at technical side:	Moderate (Equipment / Media Failure)
Vulnerability at human side:	High (Critical data are at stake)
Current loss:	None to date
Potential loss:	Extremely High, with devastating legal / public image ramifications

KEY QUESTIONS

A. What penalties does HIPAA provide if patient data is lost / compromised?

B. I have a smaller clinic using electronic records – such compliance could result in financial hardship. Under these circumstances, I am not obligated under HIPAA, right?

C. I am thinking of managing losses on a per-incident basis. What are the PROs and CONs?

D. What viable data backup options are generally available?

E. What other safeguards / practices should be followed in addition to backing up data?

PROPOSED SOLUTIONS

F. What penalties does HIPAA provide if patient data is lost / compromised?

Civil and Criminal penalties may be imposed on any health care provider who does not comply with HIPAA. Civil penalties are up to $100 per failure to comply, up to $25,000 aggregate annual total; Health and Human Services can seek these penalties [1]. In addition, fines can total up to $250,000 (with prison terms up to five years for personnel involved) if the action was willful and / or negligent. Since data loss is considered negligent in most cases, the clinic would be at high risk for significant legal ramifications and / or loss of public confidence [2].

G. I have a smaller clinic using electronic records – such compliance could result in financial hardship. Under these circumstances, I am not obligated under HIPAA, right?

Incorrect if you said "YES". Regardless of size (physically, or financially), because you are a health care provider, you accept patients' insurance coverage. Additionally, your use of electronic transmission / storage of sensitive patient data bind you into compliance with the Health Insurance Portability and Accountability Act. Specifically, this act requires records be available at ease by the patient or other authorized parties and that the records be secured by necessary technological means [3]. In the e-business world, this means that records be safeguarded with encryption and only proper doctors / medical personnel / IT professionals be in possession of the key.

H. I am thinking of managing losses on a per-incident basis. What are the PROs and CONs?

PROs: Less costly in the short run. It may apply to isolated incidents that do not reoccur often or at all. CONs: Long-term costs will significantly affect the firm negatively in terms of legal costs [2], lost productivity [4], public confidence, and lost business [5].

I. What viable data backup options are generally available?

There are generally a couple of options for a truly safe backup: on-site [4] and off-site backup, using tapes or drives. Technical and equipment options vary between the two [6], however the main concept is that with off-site backup, the backup is safely distanced from the original, helping to ensure that if a disaster did occur, the odds are considerably slimmer that the backup would be destroyed along with the working copies of data. In addition, considering HIPAA laws, a failover plan is the best option while backups are being restored [5].

J. What other safeguards / practices should be followed in addition to backing up data?

Keep a good security policy on the computer and communication network [7]. This policy should include educating users on proper procedures, stringent password changes, monitoring / logging all user activity, and making sure firewall and anti-virus programs are installed and kept up to date. These procedures will help protect data against incidents which would occur as a result of carelessness or unauthorized access to the network [8, 9]. The frequently planned and properly executed network security audits – both internal and external – can reveal communication and network system vulnerabilities hence mitigate risks of data loss due to human errors or intentional intrusions [10]. Of course, social re-engineering tactics can bring even the most secure system to its knees. So, above all, make sure your employees are well educated (do's and don'ts) and understand the importance of keeping their workstations, the environment, and the network secure [11].

ACKNOWLEDGMENT

L.R.Y. thanks College of Business and Economics at University of Wisconsin-Whitewater for the support of the Applied Research Grant and Mini-Grant toward the development of this case study on applied network and internet communication and security.

REFERENCES

1. US Department of Health and Human Services. (2003, May). Summary of the HIPAA Privacy Rule (DHHS Publication – OCR Privacy Summary). Washington, DC: U.S. Government Printing Office. Retrieved December 29, 2010 from http://www.hhs.gov/ocr/privacysummary.pdf.
2. M. Amatayakul (2006, May). HIPAA enforcement rule will more teeth equal bigger bite? Healthcare Financial Management, 60(5), 116,118. Retrieved December 29, 2010, from ABI/INFORM Global database. (Document ID: 1042683421).
3. M. E. Cooper and J. G Brady (2005, March). The HIPAA Privacy Rule: Is Your Health Plan Ready? Findlaw. Retrieved December 29, 2010 from http://library.findlaw.com/2005/Mar/23/172827.pdf.
4. DeFelice (2007, December). Preparing for the Worst. Accounting Technology, 23(11), 14-16,18-19. Retrieved May 4, 2011, from ABI/INFORM Global database. (Document ID: 1402797031).
5. D. Robb (2006, November). Lessons In Business Continuity And Disaster Recovery. Business Communications Review, 36(11), 52-55. Retrieved May 4, 2011, from ABI/INFORM Global database. (Document ID: 1164197621).
6. E. McCarthy (2007, February). Tech Tools for Disaster Recovery. Journal of Financial Planning, 20(2), 28-30,32-34. Retrieved May 4, 2011, from ABI/INFORM Global database. (Document ID: 1232437331).
7. Beliles and D. Twinam. (2008, January). Securing Physical Security Systems on the IP Network. SDM, 38(1), 85-88. Retrieved May 4, 2011, from ABI/INFORM Global database. (Document ID: 1421459791).
8. Vijayan and P. Thibodeau. (2008, April). IT Tries to Keep Internal Users Under Control. Computerworld, 42(15), 14-15. Retrieved May 4, 2011, from ABI/INFORM Global database. (Document ID: 1463035751).
9. K.. Gupta (2008). How to Protect Your Data When You're on the Web. Family Practice Management, 15(4), 29-34. Retrieved December 29, 2010, from ABI/INFORM Global database. (Document ID: 1469228581).
10. Petterson (2005, July). The keys to effective IT auditing. The Journal of Corporate Accounting & Finance, 16(5), 41-46. Retrieved May 4, 2011, from ABI/INFORM Global database. (Document ID: 857256961).
11. Chronister (2008, April). Protecting from Identity Theft? A Good Start. Security, 45(4), 76-77. Retrieved May 4, 2011, from ABI/INFORM Global database. (Document ID: 1470830211).