Towards an Incident Response Framework for Database Management Systems: the Case of a Tertiary Hospital in South-South Nigeria

Leton Rebecca Nsereka and Irene Govender

March 2, 2023

Towards an Incident Response Framework for Database Management Systems in a Tertiary Hospital in South-South Nigeria

Leton Rebecca Nsereka[1][0000-0001-7746-6173] Irene Govender[2][0000-0002-4499-1091]

1 School of Management, IT and Governance, College of Law and Management Studies, Information Systems and Technology, University of KwaZulu-Natal Durban, South Africa
rebecca.nsereka@uniport.edu.ng

2 School of Management, IT and Governance, College of Law and Management Studies, Information Systems and Technology, University of KwaZulu-Natal, Durban, South Africa
Govenderi4@ukzn.ac.za

Abstract. Health-providing institutions can no longer handle cyber security issues associated with using Hospital Database Management Systems (HDMS) with kid gloves. Data breaches in HDMS are a serious threat to the underlining business objective. The damaging effects of data breaches result in loss of sensitive data, operational downtime, financial losses, and reputational harm. Often, this leads to stigmatization, discrimination, insurance loss, employment loss and, in extreme cases, legal action. This study investigates the Hospital Database Management system in a selected hospital in South-South Nigeria for the possibility of a medical record data breach. A concise penetration test was carried out on the hospital database to expose instances of data breaches from the network. Findings from the Pentest proved that systems could be affected by inherent threats and vulnerabilities. The study designed an incident response framework according to the NIST.SP.800-61R2 standard, which was later implemented and evaluated on the existing HDMS for data breach mitigation (in the selected hospital). The designed incident response framework (IRF) serves as a paradigm for hospitals where a proper incident response plan is lacking. The study recommends that hospitals carry out penetration tests on their information systems from time to time to uncover red flags for data breaches. The IRF should be implemented on systems to mitigate breaches.

Keywords: Incident response framework, Hospital database management system, Computer security incidents, Data breach, Penetration testing.

1.0 Introduction

Medical records contain one of the most sensitive personal identifying information (PII) about individual patients (Smith, 2016). The application of advances in information systems and technology has led to the implementation of hospital database management systems (HDMS). These innovations connect medical research, clinical records, diagnosis, operational and financial systems to the central network infrastructure for large hospital databases. Accordingly, the hospital largely depends on the network for its day-to-day service delivery.

Irrespective of the benefits, the severity of cyber security associated with HDMS cannot be understated". cyber security issues associated with using HDMS cannot be handled with kid gloves. Data breaches in HDMS are a severe threat to the underlining business objective. The damaging effects of data breaches result in the loss of sensitive data, operational downtime, financial loss, reputational harm, and in extreme cases, legal action (Meta_Compliance, 2020), not to mention the privacy of individuals. Choi (2021) have established that data breaches constitute a continuous threat to hospitals.

The security of patient and research data related to the hospital system must receive top priority (Czeschik, 2018). The complexity of hospital systems and technological practices involved has exposed the systems to several vulnerabilities (Branch, 2018). Daramola *et al*. (2019) revealed that medical identity fraud, theft, and impersonation are currently the primary concern of healthcare systems in Nigeria. Recent studies indicate that many investigations on incident response were often based on event studies, reviews of papers and works of literature, interviews, etc. (Abernathy & McMillan, 2018; Burkhead, 2014; Line, 2015). In this study, however, the researcher based the findings on practically applied tests using the population of the study.

Feedback from this application will be the basis for improvement on the existing recommendations for handling cybersecurity incidents in a threatened healthcare-providing database management system.

1.2 Contribution to knowledge base

This work will generate a well-defined Incident Response Model that can curb the activities of hackers in a automated hospital environment. Findings reached will help protect valuable patient data in a hospital. The model will significantly enhance data protection and privacy in the hospital database management systems. More importantly, the model will serve as an Incident Response tool a threatened hospital DBMS.

2.0 Research Background and Objectives

The protection of medical records is of great importance in healthcare-providing institutions (Smith, 2016). Towbin (2019) reported a phishing attack against a health insurance company. Hackers had access to download over 80 million patient records, including names, birthdates, Social Security numbers, email addresses, and phone numbers. Neprash's *et al*. (2022) study revealed that 374 ransomware attacks launched on the United States Healthcare institutions exposed close to 42m personal health information (PHI) of patients from 2016 to 2021. In 2020 alone, HIPAA healthcare data breach report indicated over 500 data breaches at more than 1.76 per day from the healthcare providers and their associates (HIPAA, 2020). More specifically, it has been shown that Nigeria has become a significant source and target of harmful internet activities, with a vast majority of well-educated and technologically knowledgeable yet unemployed youth spending valuable time and energy on diverse online activities Ofusori (2019).

Hence the study is guided by the following research questions:

1. What factors (cyber threats or otherwise) are affecting the HDMS?
2. What does a penetration test of HDMS reveal?
3. How can data breaches and cyber-attacks be mitigated using an incident response model?

2. Related Literature

2.1 Information Security

The NIST.SP.800-12R1 defines information security as the protection of information systems from unauthorized use, access, disruption modification, disclosure, or destruction. Information security enables the safety of operations for system applications and protects organizational data, thereby safeguarding the technological assets in use (Nieles *et al*., 2017). According to Thompson (2018), certain activities that constitutes the ABC of information security must be in place.

2.2 Data Breach

Data, referred to as the "new oil" (Nirmal,2018) with an elevated status, is one of the most important assets in any organization (Juma'h & Alnsour, 2020). Hence, companies like Google, Amazon, Alibaba, Facebook, Tesla and so on, thrive on data, so do other organizations and individuals the world over. A data breach could be defined as a security incident involving the disclosure, manipulation, destruction, or access to data which could be either intentional or unintentional (Fowler, 2016). The threat of losing control over data is a serious issue that affects everyone. Data breaches expose the inherent internal control deficiencies in an organizations' information system. However, the basis of data breach is usually an existing vulnerability in the system, which could be exploited (Schlackl *et al.,* 2022).

Hence, it is important that companies keep upgrading their IT controls to reduce risks of data breaches and cyber security incidents. Several organizations adopt different guidelines to mitigate the risk of data breaches. Some protection techniques adopted by companies according to Juma'h and Alnsour (2020) include data encryption, system authentication, firewalls and user access controls among others.

2.3 Computer Security Incidents

Security incidents are bound to occur. However, the level of damaging impact on an organization is significantly determined by the strength of the response. It is essential to note that an organization's incident response policies must be well designed, adequately communicated, and followed to address satisfactorily and specifically cyberattack incidents in the organization. According to the NIST.SP.800-61R2 a computer security incident is any event that constitutes a threat to computer security policies and violates standard or normal security practices (Cichonski *et al.,* 2012).
While there is an increase in the complexity of cybersecurity threats in today's society, an organization can respond to and contain the scope of a security attack by employing efficient incident management (Chapple *et al*., 2021) techniques. Regrettably, there is limited capability in applying existing cybersecurity controls (Sabbagh, 2019).

Using defensive measures referred to as incident response in Burkhead's (2014) study, organizations' responses to information security attacks is the key to solving cybersecurity problems. Roberts and Brown (2017) argue that incident response

requires detecting and identifying intrusions, gathering, and developing a proper understanding of such intrusions, and developing executable plans to remove the intruders.

Burkhead (2014) investigated information security incidents from the experience of information security (IT) professionals who provide or respond to security incident reports during information security management in the private sector. He utilized the phenomenal qualitative research approach. He discovered that: information security detection were not accomplished using technical tools and organizations provisioned incident response resources have not developed (at the time of his research) beyond returning the system to service. Also, forensic studies were never done for criminal investigations. Apart from the military, all other organizations did not implement the lessons learned from security breaches or incidents. Burkhead (2014) claimed this was a result of limited or inadequate resources and undeveloped procedures and processes, and since a more significant number of the security incidents experienced had not resulted in substantial breaches of protected data.

The next section describes the conceptual framework for this study.

3.0 Contingency Plan for Data Breach Mitigation Model (CPDBMM)

The conceptual framework for the research is the Contingency Plan for Data Breach Mitigation Model

Diagrammatically, represented as follows:

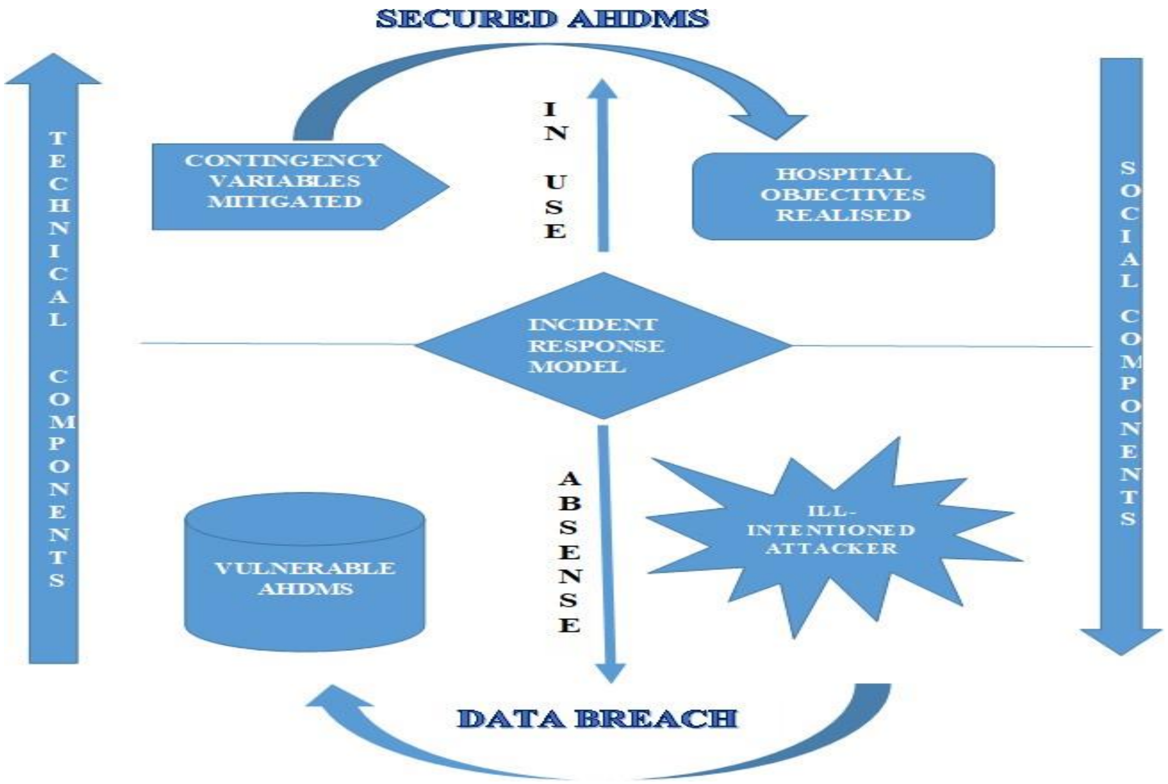


Fig. 1: Combination of Contingency and Routine Activity Theories to achieve a conceptual model (CPDBMM). Author's own design

Starting from the middle of the model is the incident response plan, which indicates the centre of operation. The absence of the incident response plan in the organization paves the way for an ill-intentioned attacker to launch a successful attack on the vulnerable automated hospital database management system. This unfortunate event results in a data breach. On the other lower side of the divide is the incident response plan in use. There are contingency variables on the left side, such as information security threats, vulnerabilities, and so on. With the incident response plan adequately applied, the system experiences a secured HDMS. The hospital's primary objectives (to provide efficient, quality, uninterrupted, modern technological medical services using HDMS and to ensure secured patient/research data and financial and administration records) are realized.

The hospital here is an organization that relies on the processes and procedures of the social and technical components, which include information systems and other infrastructures in use. The implementation of an Incident response plan on an AHDMS is a critical security policy by top management. The aim is to achieve joint optimization – by each data breach mitigation, making the hospital realize its objectives.

3.1. Incident Response

Incident response is a security measure guided by existing and standardized Cybersecurity frameworks such as the US NIST.SP.800-61R2. Incident response is the process applied for identifying, investigating, and resolving various computer security issues with the aim of restoring system to normalcy in case of a data breach. The security incidents include all kinds of malicious activities on a network and PC level, ranging from Denial of Service (DoS) attacks and hacking attempts to malware and compromised systems. According to Roberts and Brown (2017), incident response requires detecting and identifying intrusions, gathering and developing a proper understanding of such intrusions, and developing executable plans to remove the intruders

3.2. The incident Response Process

These recommended plans, according to the US NIST.SP.800-61R2 (Cichonski *et al.*, 2012) include: Preparation, Detection, Analysis, Containment, Eradication and recovery, and Post-incident Activity (lesson learned).Below is a diagram of the NIST recommendation for incident response:

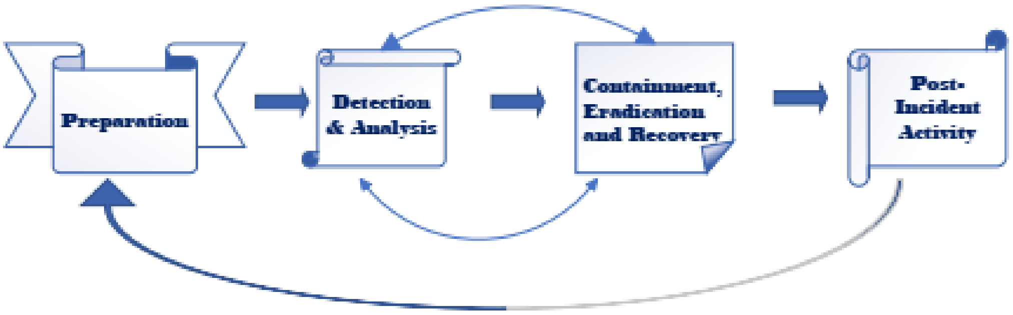


Fig 2. The NIST recommended phases of cybersecurity incident response Source: (Cichonski et al., 2012- Updated by author)

Preparation refers to the readiness to address security issues when they occur. This proactive phase places a lot of demand on the system. The need to prepare channels for communication with primary and secondary contacts such as incident response teams and law enforcement agencies; mechanisms for incident reporting, network mapping (diagrams). Provision of critical assets catalogues, jump kits for the rescue team. Incident handling software and hardware collection, user awareness trainings, malware detection and prevention software installation, general network, and host security.

Detection and Analysis: this involves defining the nature of attack vectors to identify, detecting signs of security incidents by use of intrusion detection programs (IDPs) to constantly watch over the network for indicators of compromise and more. Analysis demands validation and scrutiny of the occurrence of an incidence on the organization's network.

Containment Eradication and Recovery: Containment and recovery is carried out to minimize the adverse effects of a security incident on the system. The impact of an incident must be determined to envisage its recovery. Also, the escalation level must be established in the organization by the parties involved, appropriate notification is expected for prioritized and analyzed incidents (Microsoft, 2023). A successful eradication targets eliminating the root cause of the security incident. In this process, the adversary should be totally evicted from the environment. Also, the vulnerability that exposed the system to such an attack must be mitigated to avoid future re-entry of the attacker.

Recovery: the recovery process is hinged on a proper containment and eradication. The last known configurations or good state of the system must have been saved during the detection phase. The system is gradually brought back to that state by restoring backups until the system becomes functional as expected (Microsoft, 2023).

Post-incident activity. It is often said that "once beaten twice shy". It is enough to suffer a first attack however, subsequent attacks should not be meet one unprepared. The post-activity or lessons learned is a vital phase of the incident response model. The phase require that a lessons learned meeting be held with all the parties involved after handling a major incident (Microsoft, 2023). In such a meeting, a complete review of all that occurred is carried out. Mitigation measures that were adopted, the merits and demerits of the adopted measured must also be discussed. Reports from a lesson learned meeting serves as a training resource for new team members.

4. Methodology

4.1 Research Design

The primary aim of this paper is to solve the problem of security issues regarding the hospital database management systems. To achieve the research objectives, a sequential mixed methods design was employed, using the quantitative design followed by the qualitative (Schoonenboom & Johnson, 2017) approach within the design science research approach.

To determine the views and interactions of staff with the system, a questionnaire was administered to 40 medical record staff selected through a purposive sampling method from the selected hospital. The aim of the questionnaire was to ascertain information security practices of the medical record and IT Unit of the hospital and identify the need for conducting the Penetration test.

A follow-up to this was the deployment of a penetration test on the database management system in use by the hospital by use of Penetration testing tools for monitoring vulnerabilities over the network and ascertain the possibility of data breach occurrence. Using the design science approach, an incident response framework for database management systems was designed. by investigating security issues involved in handling a hospital's database management system (HDMS) and keep track of situations that could result in a data breach so that they can be mitigated

5. Data Analysis and Findings

To ensure brevity, just a set of the study results was presented in this paper. Hence, three research questions were used to address the study's research objectives.

1. **What factors (cyber threats or otherwise) affect the HDMS?**

Forty copies of the questionnaire were administered to medical records staff of the target hospital to identify and rate the severity of the threats to the Hospital Database Management System.

Table 1: Possible Threats to HDMS

	Threats	**Severe**	**Moderate**	**Mild**
1.	Malicious code attacks	**13**	**16**	**11**
2.	Unauthorized access	**13**	**18**	**9**
3.	Computer Misuse	**16**	**17**	**7**
4.	Medical record Theft	**18**	**14**	**8**
5.	SQL Injection	**15**	**13**	**12**
6.	Computer hoaxes	**11**	**20**	**9**
7.	Unauthorized Utilization of Services	**15**	**16**	**9**
8.	Privilege Escalation and Elevation	**13**	**20**	**7**
9.	Excessive Privilege Abuse	**14**	**17**	**9**

10.	Legitimate Privilege Abuse	**21**	**12**	**7**
11.	Storage media Exposure	**18**	**14**	**8**
12.	Malware	**13**	**17**	**10**

Effect of threats on the HDMS

Findings from the respondents indicated that Legitimate Privilege Abuse constituted the highest threat to HDMS as identified by 52. 5% of the respondents. Storage media Exposure and Medical record Theft were identified by 45% of respondents as the second most severe. The implication of the result is that Legitimate Privilege abuse is the greatest threat to hospital database of the hospital database management system.

Research question 2

What does a penetration test of HDMS reveal in an information system?

Penetration Test Reports and Interpretation

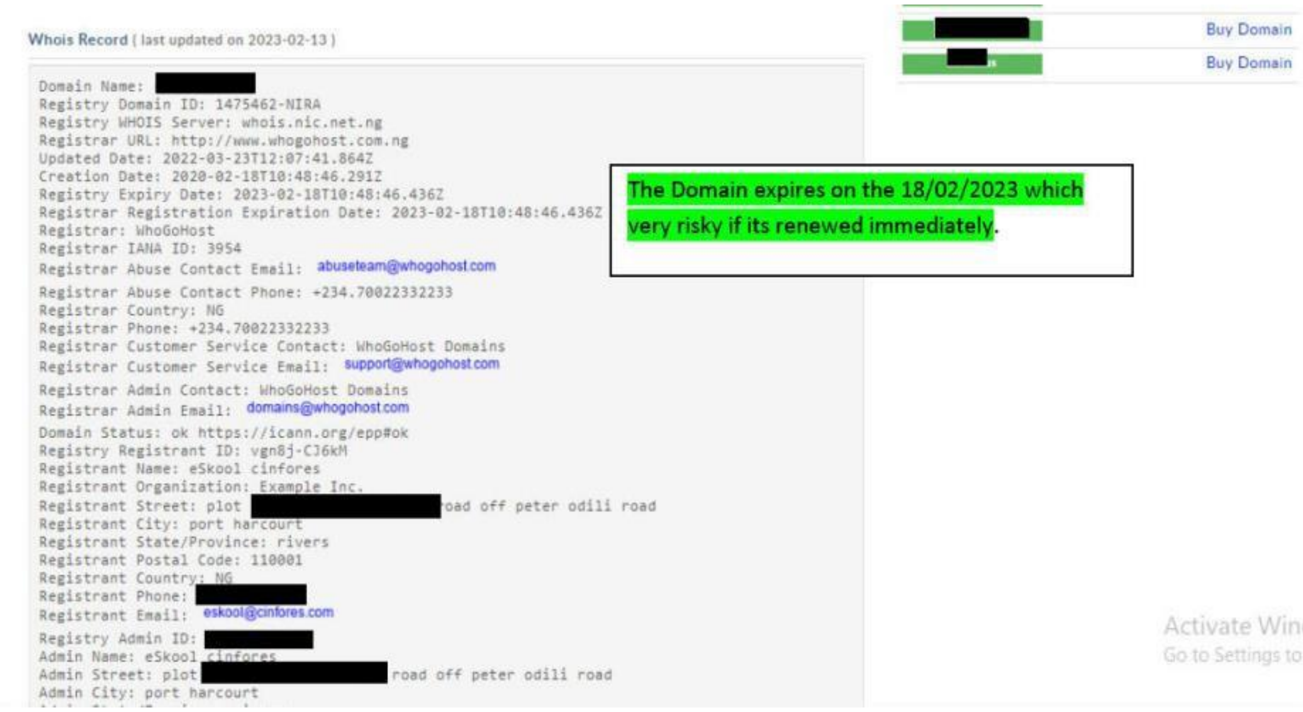
Penetration testing is done by ethically stress-testing the information security infrastructure to identify security issues that were during the software development life cycle. The goal of the pen test is to discover the threats and vulnerabilities before an adversary could take advantage of such to attack the system.

According to Baloch (2015) penetration testing, an aspect of ethical hacking is made up of methods and procedures for testing an organization’s security. To check the possibility of attackers exploiting discovered vulnerabilities to access organization’s access in an unauthorized manner, a pen test must be carried out. This form of offensive security are the techniques used to discover inherent flaws in the information system or network (Syed *et al*., 2020). It is an evaluation of the ability of an organization to protect IT infrastructures such as computer systems, applications, network and other valuable assets against security threats be it external or internal (EC-Council, 2021).

Penetration Test Results Exposing Vulnerabilities in HDMS

Pen Test Scenario 1: Information Pre-engagement or information gathering.

The first stage of penetration test is information gathering. Once the information about the organization has been obtained from an elaborate penetration test, the outcome can be used by hackers to access sensitive information about the organization. Figure 2 below is an output for the information gathering stage of the penetration test. The test reveals a grave vulnerability on the database: the expiration date of the domain hosting the hospital’s site.



[redacted] Buy Domain
[redacted] Buy Domain

Whois Record (last updated on 2023-02-13)

```
Domain Name: [redacted]
Registry Domain ID: 1475462-NIRA
Registry WHOIS Server: whois.nic.net.ng
Registrar URL: http://www.whogohost.com.ng
Updated Date: 2022-03-23T12:07:41.864Z
Creation Date: 2020-02-18T10:48:46.291Z
Registry Expiry Date: 2023-02-18T10:48:46.436Z
Registrar Registration Expiration Date: 2023-02-18T10:48:46.436Z
Registrar: WhoGoHost
Registrar IANA ID: 3954
Registrar Abuse Contact Email: abuseteam@whogohost.com
Registrar Abuse Contact Phone: +234.70022332233
Registrar Country: NG
Registrar Phone: +234.70022332233
Registrar Customer Service Contact: WhoGoHost Domains
Registrar Customer Service Email: support@whogohost.com
Registrar Admin Contact: WhoGoHost Domains
Registrar Admin Email: domains@whogohost.com
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: vgn8j-CJ6kM
Registrant Name: eSkool cinfores
Registrant Organization: Example Inc.
Registrant Street: plot [redacted]oad off peter odili road
Registrant City: port harcourt
Registrant State/Province: rivers
Registrant Postal Code: 110001
Registrant Country: NG
Registrant Phone: [redacted]
Registrant Email: eskool@cinfores.com
Registry Admin ID: [redacted]
Admin Name: eSkool cinfores
Admin Street: plot [redacted] road off peter odili road
Admin City: port harcourt
```

The Domain expires on the 18/02/2023 which very risky if its renewed immediately.

Fig 3 Penetration test out for information gathering phase

What happens when domain hosting expires?

When a domain expires it becomes inactive immediately and all the services attached to it cease to function including updates to the domain. The domain will remain available for reactivation at the regular domain rate under the list of Expired Domains. Domain's expiration can constitute a serious security risk. For instance, Alowaisheq *et al*. (2020) revealed that most expired domains were often repurchased without the consent or control of previous domain owners. This activity is capable of grounding business operations of the affected domain owner, resulting in a failed business development goal. Malicious attackers may leverage on that and access redundant domains to launch a variety of attacks against organizations. Some of such attacks include Phishing and business email compromise attacks, ransomware, and supply chain attacks and more. Taking over an expired domain simplifies almost any compromise in which an attacker uses an ostensibly legitimate identity to circumvent defenses.

Research Question 3

How can data breaches and cyber-attacks be mitigated using an incident response model?

The purpose of this study has been to design an incident response framework according to NIST.SP.800-61R2 standard (Cichonski *et al*., 2012). This section unveils the incident response framework that will be utilized to curb and mitigate instances of data breach that could occur in a hospital data base management system. See figure below.

Data breach Mitigation Framework Design

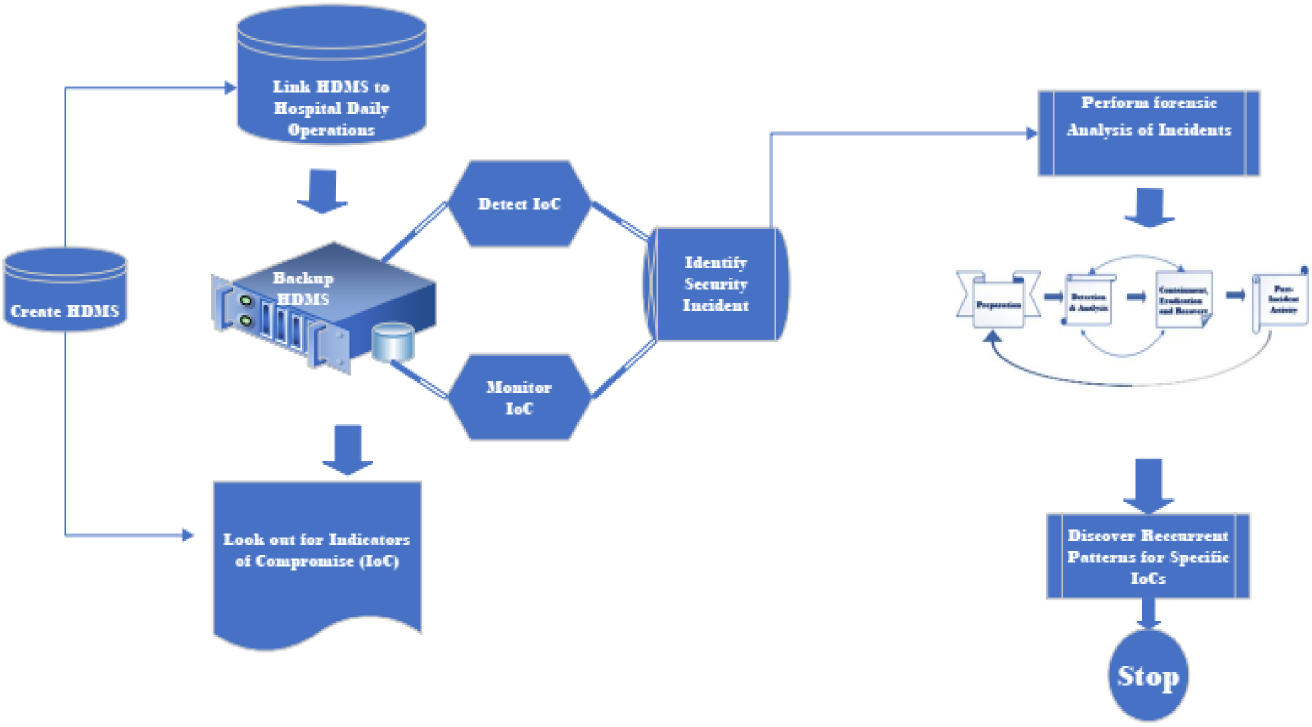

Link HDMS to Hospital Daily Operations
Create HDMS
Backup HDMS
Detect IoC
Monitor IoC
Identify Security Incident
Look out for Indicators of Compromise (IoC)
Perform forensic Analysis of Incidents
Preparation
Detection & Analysis
Containment, Eradication and Recovery
Post-Incident Activity
Discover Recurrent Patterns for Specific IoCs
Stop

Fig 4. Data Breach Mitigation Incident Response Framework

The proposed design above begins with creating a hospital database management system (where such a design is absent) that connects to the hospitals daily operations. A total backup is implemented for the hospital's operational activities. A penetration test is run on the information system (IS) from time to time that can expose inherent threats and vulnerabilities on the IS. This penetration test is in line with Syed *et al*. (2020) that prescribe penetration testing as an offensive security measure for hospital databases to discover flaws or vulnerabilities on the network. The Incident response framework phases (as discussed above) are then deployed on the information system to curb data breaches.

4.0 Conclusion and Recommendations

To overcome cybersecurity issues associated with operational and dynamic databases connected to a network, much preparation must be enforced. The purpose of this study is accomplished by the designed incident response framework (IRF) that serves as a paradigm for hospitals where a proper incident response plan is lacking. The study recommends that hospitals carry out penetration tests on their information systems from time to time to uncover red flags for data breaches. The IRF should be implemented on operational hospital data base management systems to mitigate breaches.

References

Abernathy, R. a., & McMillan, T. (2018). *CISSP Cert Guide, Third Edition*. Pearson Education, Inc. Alowaisheq, E., Tang, S., Wang, Z., Alharbi, F., Liao, X., & Wang, X. (2020). Zombie awakening: Stealthy hijacking of active domains through DNS hosting referrals. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security,

Baloch, R. (2015). *Ethical Hacking and Penetration Testing Guide*. CRC Press Taylor & Francis Group, LLC.

Branch, L. E. (2018). *Cyber Threats and Healthcare Organizations: A Public Health Preparedness Perspective* [PhD Dissertation, West Virginia University]. Morgantown, West Virginia.

Burkhead, R. L. (2014). A phenomenological study of information security incidents experienced by information security professionals providing corporate information security incident management.

Chapple, M., Stewart, J. M., & Gibson, D. (2021). *(ISC)2® CISSP® Certified Information Systems Security Professional Official Study Guide* (Ninth Edition ed.). John Wiley & Sons, Inc. .

Choi, J. L. S. J. (2021). Hospital Productivity After Data Breaches: Difference-in-Differences Analysis. *Journal of Medical Internet Research*, *23*(7). https://doi.org/10.2196/26157

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide Recommendations. *NIST Special Publication*.

Czeschik, C. (2018). Black Market Value of Patient Data. *Digital Marketplaces Unleashed*, 883- 893. https://doi.org/https://doi.org/10.1007/978-3-662-49275-8_78

Daramola, O. E., Abu, J. M., Daramola, L., & Akande, T. M. (2019). Medical Identity Fraud in Health Insurance Schemes: Creating Awareness in Nigeria.

EC-Council. (2021). *Ethical Hacking Essentials Version 1*. EC-Council. Fowler, K. (2016). *Data Breach Preparation and Response:*

Breaches are Certain, Impact is Not. Elsevier Inc.

HIPAA. (2020). *2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020*. HIPAA. Retrieved 08/08/2021 from https://www.hipaajournal.com/2020-healthcare-data-breach- report-us/

Juma'h, A. H., & Alnsour, Y. (2020). The Effect of Data Breaches on Company Performance. *International Journal of Accounting and Information Management (IJAIM), 28*(2).

Line, M. B. (2015). *Understanding Information Security Incident Management Practices: A case study in the electric power industry* Norwegian University of Science and Technology]. Norwegian University of Science and Technology.

Meta_Compliance. (2020). *5 Damaging Consequences of a Data Breach*. Meta Compliance. https://www.metacompliance.com/blog/5-damaging-consequences-of-a-data-breach/

Microsoft. (2023). Risk Assessment Guide for Microsoft Cloud. https://learn.microsoft.com/en-us/compliance/assurance/assurance-sim-containment-eradication-recovery

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum*, *3*(12), e224873-e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

Nieles, M., Dempsey, K. a., & Pillitteri, V. Y. (2017). *NIST Special Publication 800-12 Revision 1An Introduction to Information Security* (C. S. D. I. T. Laboratory, Ed.). US Department of Commerce. https://doi.org/https://doi.org/10.6028/NIST.SP.800-12r1

Nirmal, J. (2018). *BREACH - Remarkable Stories of Espionage and Data Theft and The Fight to Keep Secrets*

Safe. PENGUIN BOOKS.

Ofusori, L. O. (2019). *Three-dimensional security Framework for BYOD*

enabled Banking institutions in Nigeria [PhD, Durban, South Africa]. University of Kwazulu-Natal Roberts, S. J., & Brown, R. (2017). *Intelligence-Driven Incident Response: Outwitting the Adversary*. O'Reilly Media. https://books.google.co.za/books?id=kvkxDwAAQBAJ

Romanosky, S., Hoffman, D., & Acquisti, A. (2011). Empirical Analysis of Data Breach Litigation. WEIS,

Sabbagh, B. A. (2019). Cybersecurity Incident Response : A Socio-Technical Approach.

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, *59*(4), 103638. https://doi.org/https://doi.org/10.1016/j.im.2022.103638

Schoonenboom, J., & Johnson, R. B. (2017). How to Construct a Mixed Methods Research Design. *KZfSS Kölner Zeitschrift für Soziologie und Sozialpsychologie*, *69*(2), 107-131. https://doi.org/10.1007/s11577-017-0454-1

Smith, T. T. (2016). *Examining Data Privacy Breaches in Healthcare* Walden University]. Syed, S., Khuhawar, F.,
Arain, K., Kaimkhani, T., Syed, Z., Sheikh, H., & Khan, S. (2020). Case Study: Intranet Penetration Testing of MUET. In: vol.

Thompson, E. C. (2018). *Cybersecurity incident response: How to contain, eradicate, and recover from incidents*. Apress.

Towbin, R. S. (2019). A Protection Motivation Theory Approach to Healthcare Cybersecurity: A Multiple Case Study. In N. University (Ed.). ProQuest LLC San Diego, California.