AUCTORES
Globalize your Research

Clinical Research and Clinical Trials

Cheryl Ann Alexander *

Open Access

Review Article

The Importance of a Business Continuity Plan: Cybersecurity Case Study of a Large Medical Center

Cheryl Ann Alexander [1]* and Lidong Wang [2]

[1] Institute for IT innovation and Smart Health, Mississippi, USA

[2] Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA

***Corresponding Author:** Cheryl Ann Alexander, 1Institute for IT innovation and Smart Health, Mississippi, USA.

Received date: January 11, 2024; Accepted date: January 31, 2024; Published date: February 20, 2024

Citation: Cheryl A. Alexander, and Lidong Wang, (2024), The Importance of a Business Continuity Plan: Cybersecurity Case Study of a Large Medical Center, *Clinical Research and Clinical Trials*, 9(3); **DOI:10.31579/2693-4779/177**

Abstract:

A medical center must conduct business with an awareness of the possibility of cybercrime attacks or the loss of computer control because of criminal attacks on the server resulting in the compromise of patient information. Patient information can be more valuable than a personal social security number and banking information. Third-party agencies can use patient information to make decisions that can deny patients insurance and other treatment. A business continuity plan can be used to provide procedures for sustaining business operations in the medical center while recovering from a considerable disruption of the information system during a pandemic of infectious disease, a cybercrime attack, or in the case when servers break down. Information security in the medical center is critical. The information security team is responsible for the information security that is also related to the hospital infrastructure and the behaviors of stakeholders such as physicians, nurses, patients, etc. The information security team tries to maintain a secure network, for example, by installing and maintaining a firewall configuration. Strong access control is usually required, especially during a pandemic. Restricted access to cardholder data by business need-to-know works well in most sectors. Ethics and recovery criticality are also critical to the function of the medical center.

Keywords: cybersecurity; network structure; business impact analysis; information security; risk management; recovery priorities

Introduction

Charleston Regional Medical Center in the US practices robust cybersecurity for 4,683 employees and all patient visits (yearly over 960,000). The key patient population of the regional hospital includes patients from a radius of the central to western parts of Mississippi. It also serves as the only Level One Trauma Center in the state, accepting all kinds of patients from the state. It is very important to develop a business continuity plan for the Medical Center to find all kinds of disruptions or disasters, for example, information system disruption due to attacks and the pandemic of infectious diseases such as COVID-19. The pandemic left the Medical Center vulnerable to attacks such as Ransomware, malware, and other schemes such as phishing attacks (Khan et al., 2020a; Khan et al., 2020b; Naidoo, 2020). Patient information is highly sought-after and is more valuable than a personal social security number. The right business continuity plan and plan for cyberattacks is essential for any hospital, but more so for the larger ones.

1.1 The General Goals and Business Objectives

The general goals and business objectives are: 1) to provide procedures for sustaining business operations in the Medical Center while recovering from a considerable disruption of the information system during a pandemic of infectious disease; 2) to provide the best hospital care in the region and be the number one choice for hospital care by stakeholders and patients. Charleston Regional Medical Center also wants to be able to function as a business well by practicing solid business practices. These business practices include collecting patient payments promptly and paying for supplies promptly. One business objective is to remain in the black.

1.2 A Stakeholder-Focused Mission Aligning Security Functions to Business Strategy, Goals, Mission, and Objectives

Stakeholders of the Medical Center include physicians, nurses, patients, suppliers, administrators and staff, the information security team, other hospitals that transfer patients in, and research facilities that cooperate with the Medical Center in research projects. All stakeholders should collaborate on emergency management, risk analysis, and preparedness and response. Caregivers (physicians, nurses, etc.) in the Medical Center should be protected by surveillance of post-travel for temperature and acute respiratory illness (ARI). The cybersecurity of their computer systems or tablets, their data, or signs of patients should be protected. Patients should be checked and treated in time; masks and vaccinations should be provided if necessary. Understanding the outbreak and risk of infectious disease is very important for patients. Administrators work on standardized reports and documentation and return-to-work assessment for staff who are sick. The information

security team provides procedures for detecting abnormal behavior of the network or the system, mitigating and correcting cyberattacks, such as a virus, worm, or Trojan horse; provides procedures for relocating information systems operations to an alternate location; provides procedures and capabilities for recovering the information system.

1.3 The Information Security Governance Structure in the Medical Center

The information security in the Medical Center is critical. The information security team is responsible for the information security that is also related to the hospital infrastructure and the behaviors of stakeholders such as physicians, nurses, patients, etc. The information security team tries to maintain a secure network, for example, by installing and maintaining a firewall configuration. Strong access control is usually required, especially during a pandemic. Restricted access to cardholder data by business need-to-know works well in most sectors of the Medical Center, but fingerprint scanning or iris scanning works better for verification or authentication in important sectors. Encrypted transmission of cardholder data across public networks is needed in some critical situations. Tracking and monitoring all access to network resources is necessary for information security (Warsinske et al., 2019).

1.4 Requirements for Legal and Regulatory Compliance

Many compliance expectations in the Medical Center come from regulatory expectations. But compliance expectations regarding patient medical data and privacy are possibly related to legal expectations. Most compliance, both legal and regulatory, descends from government agencies such as the Center for Medicare Services (CMS), the American Hospital Association (AHA), OSHA (Occupational Safety and Health Administration), and others. These services combined with observing care in the Medical Center to make sure it is exceptional and safe. They also serve to keep stakeholders satisfied that the Medical Center maintains an accurate record of patient care, correct ICD-10 records (Adams et al., 2023), and that the Medical Center maintains its running in the black.

1.5 The Established Standards of Ethical Conduct

Ethical decision-making is essential to professional information security practice in the Medical Center. Not only do nurses and physicians adhere to a strict code of ethics, but other staff members in the Medical Center are also held to high moral and ethical standards. Some examples of ethical standards are when a patient is brain-dead and on life support, the nurse, management, family, and physicians must make the most ethical decisions based on the status of the patient. Doing so requires knowledge of the state's legal and ethical standards, as well as the hospitals. An ethics board meeting is required to make the best decision for the patient based on their condition.

Ethical decision-making requires a solid understanding of the moral, legal, and organizational expectations against which individuals apply their ethical standards (Warsinske et al., 2019). When faced with an ethical dilemma, the hospital must form an ethics committee to determine the right course of action. On occasion, there must be legal counsel involved and outside stakeholders involved. One of the most famous cases of this involved the choice to place a feeding tube in a paralyzed patient. The ethics case went before the Superior Court. Bouvia v. Superior Court in 1983 was an ethics case about a woman who went before the Superior Court to win the ability to starve herself. She suffered from Cerebral Palsy and was completely dependent on others to live. After going before the court in 1983, she was allowed to make the decision not to have a feeding tube and starve herself to death. Therefore, many cases go before the ethics committee (Fisher, 1987).

American Health Information Management Association (AHIMA) is active in advancing informatics, data analytics, and information governance for healthcare. The Ethics Code of AHIMA addresses in detail the privacy and security responsibilities that AHIMA's members must address in their professional roles. Their Code of Ethics consists of 11 principles, including support for privacy, confidentiality, a commitment to service before self-interest, efforts to protect health information, and ethical requirements. Like other codes, it also seeks to advance the profession and to ensure that practitioners represent the profession well throughout their work.

2. Business Impact Analysis

Business impact analysis (BIA) can include the following steps (Warsinske et al., 2019; Kodaka et al., 2020): 1) identify prioritized activities (PAs); 2) analyze and evaluate the internal and external impacts of PAs; 3) estimate the maximum tolerable period of disruption (MTPD) and the recovery time objective (RTO); 4) list resources needed for the selected Pas; and 5) identify resources as internal, essential, and external.

2.1 Mission/Business Processes and Recovery Criticality

The mission of the Medical Center includes the need to be the primary choice for patients in their region. The mission states the Medical Center strives to be the best Level One hospital and the choice of patients in the region. The mission also states that all the employees work hard, and all business processes use professional manners to make the Medical Center the choice of stakeholders.

When a disaster or pandemic like COVID-19 happens, the recovery criticality includes communication and network, medical devices and equipment, caregivers (e.g., physicians and nurses), etc. When there is an information system outage or disruption in the Medical Center, Electronic Medical Records/Electronic Health Records (EMRs/EHRs), the network infrastructure (devices, equipment, or hardware for network, storage, and computing, etc.) are the recovery criticality.

2.2 Resource Requirements

During a pandemic like COVID-19, staff (physicians, nurses, etc.), network devices, vaccines, masks, gowns, testing supplies, testing equipment, and other medical devices and equipment are basic resource requirements. For the information system in the Medical Center, the Internet (connecting outside) and the Intranet (only for staff inside the Medical Center) are very important for business operations. When the Internet does not work, Intranet might work, and general operations might continue inside the Medical Center. In addition, hardware for the network infrastructure, software supporting various applications (e.g., software for medical image processing, software for AI-based data analytics), and medical data files like ICD-10 are also resource requirements.

2.3 Recovery Priorities for System Resources

An example of Business Impact Analysis (BIA) is shown in Table 1. It lists anomaly events, their impacts, Recovery Time Objective (RTO), and recovery priorities (Warsinske et al., 2019; Swanson et al., 2010). In the table, staff abusing patient data is one kind of violation of the Health Insurance Portability and Accountability Act (HIPPA).

Events	Impacts	RTO	Recovery Priorities
Sever off-line	Network stops working	12 hours	1
Network intrusion	Regaining network access	12 hours	2
Ransomware of patient data	The Medical Center must pay to get control of patient data	24 hours	3
Staff abusing patient data	HIPPA violation	8 hours	4

Table 1. Business Impact Analysis for the Information System in the Medical Center

3. Annotated Network Diagram

Network components in the information system of the Medical Center mainly include the infrastructure layer, the control layer, and the application layer. Two types of interfaces are used to communicate between the layers: one is for the communication between applications and controllers; the other is for the direct communication between the controllers and the data route network elements in the infrastructure layer. Figure 1 shows the network components in the Medical Center. The infrastructure layer consists of physical hardware, and it may include network devices, servers, storage devices, computing hardware, Internet of Things (IoT), Internet of Medical Things (IoMT), and other items such as barcoding scanners, fingerprint scanners, radio frequency identification (RFID) scanners, etc. IoMT can include medical devices, nurses' stations, medical security systems, etc. (Arista, 2021). The infrastructure layer is mainly responsible for handling data traffic (data capture or collection, transfer, drop, etc.).

The control layer monitors, controls, and manages the hardware in the infrastructure layer. It integrates infrastructure service identification and reporting, software-defined network (SDN) controllers, network, etc. The application layer provides various applications and services via application programming interfaces (APIs). The applications can be access controls, e-health, telehealth, patient monitoring, AI-driven applications (such as situational awareness analysis, threat detection & response), Big data analytics, intrusion/attack detection, etc. Situational awareness deals with profiling, tracking, and finding medical devices and personnel in the Medical Center.

Digital health applications that are based on artificial intelligence (AI) and machine learning (ML) play an important role in the Medical Center. The applications cover telemedicine (remote consults, care management & coordination), health information (digitalized records, diagnostics, dashboards), predictive analytics, decision-making-based AI/ML, etc. Cybersecurity and privacy are major obstacles to digital health applications, continue to erode patient trust and reinforce health systems' reluctance to share data (Abernethy et al., 2022).

Ensuring robust cybersecurity in the Medical Center is critical, and the application layer maintains solid functions in cybersecurity and provides various services in time. Specifically, gathering huge amounts of data into a secure platform (Mastaneh & Mouseli, 2020) is performed, and Big data analytics can be implemented; threat detection is performed all the time to detect intrusions and attacks in the information system; mutual authentication is employed to prevent impersonation attacks on certain devices (Tan et al., 2020); training programs and materials such as linking attacks, spoofing attacks, Denial of Service (DoS), Distributed DoS (DDoS) (Zhang & Wu, 2020) are available for employees in the Medical Center.

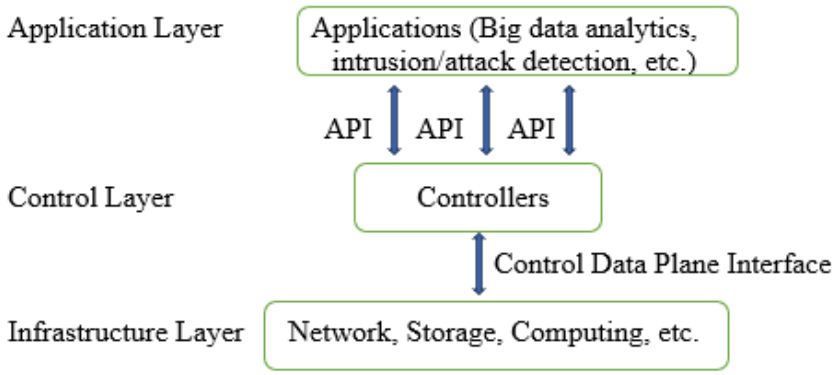

Figure 1. Network Components in the Medical Center

4. Conclusion

Having a business continuity plan is essential to a thriving business in this era of comprehensive information security. A strong risk assessment plan is important to a comprehensive business impact analysis. Recovery priorities include network priorities and cybersecurity priorities such as protection from cyberattacks and internal attacks. Infrastructure for medical care can include networks, storage, data, computers, barcoding, facial recognition, etc. Protecting and maintaining ethics and a strong control layer such as information security professionals and healthcare staff. Training of healthcare staff should include training about cybersecurity issues.

Ethics and a strong moral, legal, and regulatory framework are crucial to a healthcare facility as most healthcare facilities face significant ethical, legal, and regulatory issues at some time throughout the lifetime of the facility. Significant legal and ethical issues have been always identified throughout the courts and the need to form an ethics committee may be necessary at some point, especially for a larger healthcare facility. Ensuring a robust cybersecurity program is essential to a strong healthcare facility.

Acknowledgements

Authors thank Technology & Healthcare Solutions, Mississippi, USA for support.

Conflicts of Interest

There is no conflict of interest.

References

1. Abernethy, A., Adams, L., Barrett, M., Bechtel, C., Brennan, P., Butte, A., ... & Valdes, K. (2022). The promise of digital health: then, now, and the Future. *National Academy of Medicine (NAM) perspectives*, 27-1-24.
2. Adams, M. A., Kerr, E. A., Dominitz, J. A., Gao, Y., Yankey, N., May, F. P., ... & Saini, S. D. (2023). Development and validation of a new ICD-10-based screening colonoscopy overuse measure in a large integrated healthcare system: a retrospective observational study. *BMJ Quality & Safety*, *32*(7), 414-424.
3. Arista (2021) Tenets of a Healthy Hospital Infrastructure, White paper, Arista Networks, Inc., 1-6.
4. Fisher, L. J. (1987). Suicide Trap: Bouvia v. Superior Court and the Right to Refuse Medical Treatment, The. *Loy. LAL Rev.*, *21*,219.
5. Khan, N. A., Brohi, S. N., & Jhanjhi, N. Z. (2020a). UAV's applications, architecture, security issues, and attack scenarios: A survey. In *Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS* 753-760. Springer Singapore.
6. Khan, N. A., Brohi, S. N., & Zaman, N. (2020b). Ten deadly cyber security threats amid COVID-19 pandemic. TechRxiv Powered by IEEE: 394-399.
7. Kodaka, A., Ono, T., Watanabe, K., Leelawat, N., Chintanapakdee, C., Tang, J., ... & Kohtake, N. (2020, October). A dependent activities elicitation method for designing area business continuity management. In *2020 IEEE International Symposium on Systems Engineering (ISSE)* 1-6.
8. Mastaneh, Z., & Mouseli, A. (2020). Technology and its Solutions in the Era of COVID-19 Crisis: A Review of Literature. *Evidence-Based Health Policy, Management and Economics*, 4:138-149.
9. Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306-321.
10. Swanson, M. M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems. NIST Special Publication 800-34 Rev.1, National Institute of Standards and Technology & U.S. Department of Commerce.
11. Tan, H., Kim, P., & Chung, I. (2020). Practical homomorphic authentication in cloud-assisted vanes with blockchain-based healthcare monitoring for pandemic control. *Electronics*, *9*(10), 1683.
12. Warsinske, J., Henry, K., Graff, M., Hoover, C., Malisow, B., Murphy, S., ... & Vasquez, M. (2019). *The Official (ISC) 2 Guide to the CISSP CBK Reference*. John Wiley & Sons.
13. Zhang, J., & Wu, M. (2020). Blockchain use in IoT for privacy-preserving anti-pandemic home quarantine. *Electronics*, *9*(10), 1746.

DOI:10.31579/2693-4779/177