


Chapter 10

Code Blue:

A Case Study of a Hospital Data Breach Response, Remediation, and Organizational Change

Eleanor J. Thompson

 <https://orcid.org/0009-0009-2661-4469>

Marymount University, USA

ABSTRACT

When data are breached in a healthcare setting, the risks and threats are borne by both the impacted medical institution and its patients/customers. For patients, not only is confidential medical information leaked, but their financial data and even their health and wellbeing may be jeopardized. Using scenario-based problem solving, a case study is presented to explore the elements and dynamics of a hospital's breach of medical and financial data and to strategize the organization's responses and remediation to an internal cybersecurity incident in accordance with laws applicable to both financial and healthcare institutions. Recommendations regarding organizational change to address enterprise risk management (ERM), an incident response plan, a compliance program, and ethical leadership practices are outlined to restore the hospital's reputation and prevent or mitigate further data breach incidents.

INTRODUCTION

In just one year, from 2022 to 2023, the number of data breaches globally increased by 20% and the number of victims doubled (Madnick, 2024). In the healthcare space, data breaches in 2023 hit a new high with over 133 million patient records

DOI: 10.4018/979-8-3693-8562-3.ch010

compromised, more than double the prior year (Bruce, 2024). For the patients of a healthcare organization, the exposure carries the compounded threat of having not only personal medical information leaked, but also financial data. Such breaches require responses and remediation on both fronts, in accordance with laws applicable to financial and healthcare institutions. Additionally, the effort, attention, and money that go into addressing healthcare data breaches divert resources from patient care, possibly negatively impacting patient outcomes. To address all the necessary components of a risk management and response plan for medical institutions, a case study of a hospital data breach triggering organizational change is presented, analyzed, and discussed in the context of a healthcare facility in need of ethical corporate culture, internal compliance, data security, and incident preparedness through the introduction of a comprehensive enterprise risk management (“ERM”) program. This paper examines (1) the cybersecurity needs of a healthcare organization, and (2) methods of implementing organizational change to introduce ERM and an ethical, compliant culture.

Problem Statement and Background

When data from a healthcare institution are breached, both medical and financial information are at risk, resulting in greater possible negative impact on the patients and customers and larger damages to the health facility. Medical data breaches could result in reduced hospital efficiency and, at worst, loss of life (Lee et al., 2024). The time and effort it takes a medical facility to remediate data breaches could adversely impact patient care; according to Choi, Johnson, and Lehmann (2019), data breach remediation efforts in healthcare institutions were shown to reduce time-to-electrocardiogram rates and increase myocardial infarction death rates by disrupting or delaying healthcare providers' workflows. For many people, visits to medical facilities represent a time of vulnerability, fear, or uncertainty as healthcare issues, some life-threatening, are treated; compounding these events with breaches of personal data, threats of identity theft or financial loss, and potentially compromised levels of care can be devastating on several levels. Healthcare institutions owe an extra duty of care to their patients and other stakeholders, beyond medical services, to ensure the safety and security of their data through appropriate risk mitigation, management, and response programs.

22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/code-blue/363818

Related Content

An Assessment of the Saudi Entrepreneurial Ecosystem

Mustafa Almuzeland Timothy R. Anderson (2021). *Journal of Business Ecosystems* (pp. 1-9).

www.irma-international.org/article/an-assessment-of-the-saudi-entrepreneurial-ecosystem/300327

Digital Skill Evolution in an Industrial Relationship: Professional Figure in Online Communities

Lucia Aiello (2019). *International Journal of R&D Innovation Strategy* (pp. 1-15).

www.irma-international.org/article/digital-skill-evolution-in-an-industrial-relationship/234350

The Use of Sustainable Business Model Archetypes in the Design of Circular Business Models in the Digital Economy

Marek Jaboski (2020). *Networked Business Models in the Circular Economy* (pp. 1-18).

www.irma-international.org/chapter/the-use-of-sustainable-business-model-archetypes-in-the-design-of-circular-business-models-in-the-digital-economy/236216

Common Pitfalls and Shortcomings of Lessons Learned Programs: Evidence from an Online Survey

Ian Fry (2015). *Utilizing Evidence-Based Lessons Learned for Enhanced Organizational Innovation and Change* (pp. 221-233).

www.irma-international.org/chapter/common-pitfalls-and-shortcomings-of-lessons-learned-programs/117335

Legal and Ethical Aspects of CSR: Potential in New Business Models Development

Ewa Barbara Wójcikand Katarzyna Olejko (2020). *Networked Business Models in the Circular Economy* (pp. 200-223).

www.irma-international.org/chapter/legal-and-ethical-aspects-of-csr/236224