Corporate Governance

Integration of the Cyber Resilience Strategy at Ramsay Health Care

[Student Name]

[School]

[Course/Number]

February 11, 2021

[Instructor Name]

Integration of a Cyber Resilience Strategy at Ramsay Health Care

Introduction

In the globalized world, technological advancements have emerged to be core pinnacles of organizational growth and competitiveness as they allow efficiency and convenience to thrive. Different industries and sectors rely on the internet for communication, service delivery, commerce, and storage of data. The shift to the electronic approaches of delivering services and operations ensures that companies have a competitive advantage, and offer a variety of services remotely. Although technology offers vast opportunities, it also tags along with myriad risks and threats that have colossal consequences to an organization and its customers. These risks underline the essentiality of cyber-security in any organizational setup. Mitigating and averting threats and risks associated with technology use has become a critical part in the implementation of technological applications, digital systems, and programs.

In the healthcare sector, electronic systems have substantially changed the dynamics of operations, record keeping, and billing. At Ramsay Health Care (RHC), we serve over 3 million patients annually and have a network of 253 hospitals globally as well as manage over 60,000 employees. Within our national borders, the organization is an industry leader in healthcare provision and serves close to one million patients on an annual basis. The industrial position of the company has been advanced by the implementation of the health applications such as MyHealth as well as the network systems that support health records keeping, billing, communication, customer care services, accounting, and human resource applications. As a result, organizational data contains critical customer personal information, health records and financial details, employee details, corporate research data, as well as a magnitude of data on the operations of the company nationally and internationally. Defined as Non- Public Data (NDA),

we are entrusted with a lot of sensitive information that needs to be sufficiently secured from known and unknown threats.

Cybersecurity has evolved to provide and assure the safety of critical, critical organizational systems and data. With the changing tactics of attackers, cybersecurity has to be a multifaceted agenda supported by all functions of the organization. IBM News Room (2018) reports that in 2015, the healthcare industry was the most attacked sector with over 100 million records being compromised globally. The healthcare industry is a top target because of the high demand for medical data on the black market and given the fact that medical identity is much valuable. Also, tactics such as ransomware may paralyse the operations of the company and cost the organization much damage as estimates indicate unplanned downtimes in healthcare institutions can cost the company close to $8,000 a minute per incident (IBM News Room, 2018). The diversity, volatility, and unprecedented nature of cyber-attacks make cyber hygiene and safety of RHC a top priority. Cyber-Attacks have a reputational risk, result to substantial financial loses, and may cripple operations of the organization for days. Therefore, RHC has to integrate a cyber-resilience strategy that eliminates the real risks and vulnerabilities, accounts for future wealth of threats, and spans beyond cybersecurity to business continuity, operations fluency, data protection, and user empowerment.

Integrating the Cyber Resilience Strategy

Cyber resilience can help mitigate all these risks that RHC faces presently and in the future. The World Economic Forum (2017) understands cyber resilience strategies to be long-term actions that that go beyond protection and make use of new technological opportunities. While the concept of cyber-security is more of immediate protection and reaction-driven response, cyber resilience is a long-term action led by key decision makers that shape the choice

of systems and supports the best cautionary and long-term practices (Coventry & Branley, 2018). Primarily, it involves preparation for the known and unknown, in the present environment and future space. The magnitude of this task calls for a corporate board level approach that not only plans but also ensures integration of the cyber resilience strategies.

For RHC to be cyber resilient, we have to acknowledge that securing the virtual environment is not enough due to the inevitability of breaches. Nonetheless, early detection, qualified incidence response plans can assure limited disruptions as a result of cyber-attacks. Comprehensive long-term resilience actions need to address the top risks and threats to continued business survival and also improved the ability of the organization to provide quality and reliable healthcare solutions to our ever increasing client population. However, the success of this integration extensively relies on culture change, the cooperation of all departments and active and unwavering board support which combine to ensure that new custom security practices receive the correct amount of resources and the buy-in of managers and employees (Rothrock et al., 2018).

The integration practices of cyber resilience protocols begin with proper alignment with the overall organizational strategy at the RHC. Significant Board engagement is one of the fundamental methods that assure effective cyber-security integration. The corporate board should spearhead this activity and ensure that all entities of the organization are well aware of the companies approach to cybersecurity. Aligning overall goals and plans with organization cyber security and resilience protocols begins with the creation of a cyber-security risk committee (Hult & Sivanesan, 2014). The World Economic Forum endorses the practice of having a board committee tasked with the duty of evaluating cyber risk which includes IT risk, network

vulnerabilities, and third-party risks. The committee should be in charge of risk assessment of the organization and ensure the implementation of day to day cyber resilience practices.

Through the committee, the corporate board takes ownership of the cyber resilience strategy and ensures that protocols are reviewed on a regular basis. Having a commendable and safe cyber hygiene highly relies on the ability of the organization to maintain, monitor and test installed internal controls and systems (World Economic Forum, 2017). Through the committee, the board can ensure accountability of these protocols. The Australian Securities and Investment Commission (ASIC) (2018) notes that the board should periodically assess progress through measurable risks such as time of detection, the speed of response and recovery process. By directly managing cybersecurity, the board will have a better understanding of the risk status and hence make informed investment decisions on cyber risks. Board ownership of cybersecurity and resilience protocols ensures that they can anticipate security scenarios and cater for the future cybersecurity needs of the organization.

Best Practices

Cyber safety high relates to awareness of how networks operate and the different faces used by attackers. One of the potent approaches of averting risks is through education on how cybersecurity operates and the practical strategies to use to safeguard the organization. Cyber resilience fluency should ensure that board members become more educated and well positioned to understand the core structures of a network protocol. Although this knowledge should be widespread in the organization, it is imperative to ensure that as top decision makers, there is an active understanding and discussion on the cyber threat landscape, involvement in planning, and response scenarios. Cyber resilience fluency plays an integral role in ensuring the support and participation of the corporate board.

To successfully prepare and have a resilient virtual environment, risk management and threat assessment should be established in the cyberculture of the organization. The board has the capability of installing responsible cyberculture that will guide the actions of employees and their practices. Cyber risk management and threat assessment are one of the core principles of cybersecurity that has to be incorporated into the resiliency plan and also in the cyberculture of the organization (Hills & Atkinson, 2016). Risk and threats associated with cyber disruptions are robust, and the best way to mitigate them is to conduct risk assessment continually. The approach enables early discovery of breaches and hence allow a quick response to damage. Cyber risk management should be continuous, and new technology and applications are enabling real-time automation process that integrate a variety of sources of risks. The practice of risk management and threat assessment should guide the cyber resilience efforts of the organization.

Compromise to a single portion of a network can affect the entire system and cause huge losses. Hence, it is of crucial importance that the organization manages third-party risk. RHC collaborates and works with many partners from all the six countries where it operates. To business, this is a sign of success, however, on cybersecurity terms, it increases the points of vulnerabilities in the organization's network. The practice of third-party risk management is one that RHC has to pick up to attain cyber resilience and assure the confidentiality, integrity, and availability of our data (Pate-Cornell et al., 2018). This practice involves developing a risk analysis protocol for all suppliers and partners linked to RHC's comprehensive network. This analysis will look into ethical and legal compliance of the third party entity and the information security program used as well as its vulnerabilities. Loose endpoints of a third party can cause an infiltration on the organizational network that could cause massive and in-depth damages.

After internal, external and third-party risks have been identified, the board should be briefed, and in turn, the chances are discussed in the Board Cyber Risk Framework (ASX Corporate Governance Council, 2014). Through the framework, the board should be able to assess the cyber incident impact assets as well as loss of critical information. Further, the system also looks into the vulnerabilities and threats associated with the risk. Risk and threat briefing should be included in board meetings and discussions on the framework conducted. This practice will ensure that board members understand the necessary steps taken consider data collected by action teams.

Cyber resilience should be an agenda of the board from the creation, implementation, testing, improvement and continuous detection of threats and vulnerabilities. Resilience plans are a permanent long-term and more influential to RHC's success more than the perceived role. Active involvement of the board in cyber resilience offers a pathway for other organizational instruments to follow (ASX Corporate Governance Council, 2014). It defines the fluency and corporate commitment of the organization to the protection of customer data. Furthermore, it fulfils the ethical and legal obligations of the organization. However, for RHC to attain this level of cyber resilience, the board needs to orchestrate changes in the current cyberculture and introduce delegation, responsibility, and accountability.

Recommendations

The current organizational setup and responsibility status of the board can be addressed by utilizing suggested practices. However, it would be imperative to take critical steps to ensure that decision-makers, implementers, and users are empowered to fulfil this task. I would recommend a cyber-workshop that trains and empowers board members to cyber fluency beyond the basic network understanding. In-depth awareness ranges from the specifics of RHC's

network to what the responsibility of oversight entails. The knowledge of board members will ensure that the organization sets up programs that educate and train employees on the system and good practices that provide safety (Deloitte, 2016).

However, comprehensive training may not be conducted for the whole institution but selected few who will be designated the opportunity to chair the committee. Having a competent and well informed cyber security committee is plausible than having entire board discussions on crucial security issues (ASX Corporate Governance Council, 2014). Instead, the board should form a new committee, select 3-5 members, pay for their continuous training and define the responsibility of the board in ensuring cyber resilience. The committee should periodically report to the entire board, seek counsel and have the access of critical human and capital resources. I would also vouch for the presence of contracted experts in the committee in-charge different areas of the organization. As for the other board members, orientation to the RHC's organizational cyber resilience approach.

Furthermore, I would recommend a routine risk assessment through third-party experts. Outsourcing of threat assessment will ensure that all areas of the network are routinely monitored and vulnerabilities identified by experts with adept knowledge of current trends and threats (Hult & Sivanesan, 2014). Due to the extensive nature of the web, the board can set up fusion centres where IT specialist is located and offer real-time monitoring of the RHC's entire system. Real-time monitoring enables early detection and isolation of threats before they affect the whole system. Ideally, in the fusion centre, teams will be working continuously in monitoring the system and managing the existing applications.

Although the organization can ensure proper structures and everyday testing and monitoring, without appropriate accountability cyber resilience efforts may fail to be entirely

sufficient. The board can create the office of Cybersecurity accountability headed by the accountable officer. The mandate of this office will be to strategically mitigate the risks of a cyber-attack and ensure that all cyber resilience efforts of the organization are operational. With direct access to the board, the accountable officer should brief the board on cybersecurity efforts, the expectations of customers and investors, the challenges of an acquisition or a merger and the details of the technologies that could safeguard the organization better (ASX Corporate Governance Council, 2014). It should be the responsibility of the accountable officer to ensure the organization fully complies with legal and ethical standards on the national and international level. Having this office will to a great extent enhance the oversight role of the board and ensure that the board is aware of the cyber hygiene efforts in the organization.

The strength of the mechanisms put in place by the organization hugely depends on tests, reviews, and monitoring of applications and systems. I recommend the establishment of a program of penetration tests that includes a full scope of attacks similar to the approaches used by attackers. These tests should consist of wireless, client-based, and web application attacks that looks into the network. This will include the development of a Red Team exercises as advised by the Centre of Internet Security (CIS) which take on vulnerabilities in the entire network, the organization's policy, and defences in a bid to improve readiness, improve the quality of systems, enhance training of defines personnel, and check performance levels of the organization (Hills & Atkinson, 2016). Through the penetration tests and the Red team program, RHC will be able to improve its preparedness and also increase efficiency within the organization.

Conclusion

Moving forward, RHC needs to define its information security policy fully. Even though we have a comprehensive strategy and plan in place, we need to clearly define the roles of every position in the organizational framework. Cyber resilience is a team effort, and the board, CEO, top managers, mid-level managers and different levels of staff need to understand their role. These efforts begin with a cultural focus by the board before transcending to the entire organization. The engagement, buy-in, and discussion of cybersecurity issues ensure the creation of effective and sustainable cyber resilience plans. Delegation should ensure that details are discussed in committees with board members and specialists and staff representatives. Frameworks will guarantee that the board has custom practices of assessing risks and realizing the probable effects. The efficiency of reviewing, monitoring, and maintenance of critical organizational systems and infrastructure will ensure that the organization is secure and also identify areas that improve the performance of the organization and make RHC future ready. All this will have the combinative action of ensuring that people are indeed caring for people.

References

ASIC. (2018). Cyber resilience good practices | ASIC - Australian Securities and Investments Commission. Retrieved from https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/

ASX Corporate Governance Council. (2014). Corporate Governance Principles and Recommendations. Retrieved from https://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-3rd-edn.pdf

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52.

Deloitte. (2016). Cyber Resilience: Health Care's Best Defense. Retrieved from https://deloitte.wsj.com/cio/2016/10/11/cyber-resilience-is-health-cares-best-defense/

Hills, M., & Atkinson, L. (2016). Towards cyber-resilient & sustainable SMES: the case study of added value from a large IT reseller.

Hult, F., & Sivanesan, G. (2014). What good cyber resilience looks like? *Journal of business continuity & emergency planning*, *7*(2), 112-125.

IBM News Room. (2018). IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses. Retrieved from http://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses

Pate-Cornell, M. E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber Risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis*, *38*(2), 226-241.

RHC. (2018). About Ramsay Health Care. Retrieved from http://www.ramsayhealth.com/About-Us/Overview

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The Board's Role in Managing Cybersecurity Risks. *MIT Sloan Management Review*, *59*(2), 12-15.

World Economic Forum. (2017). Advancing Cyber Resilience Principles and Tools for Boards. Retrieved from http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles- Tools.pdf