International Journal of Core Engineering & Management

Volume-6, Issue-9, 2020, ISSN No: 2348-9510

REGULATORY COMPLIANCE AND CYBER-SECURITY IN HEALTHCARE: INVESTIGATING THE RELATIONSHIP BETWEEN REGULATORY COMPLIANCE AND THE EFFECTIVENESS OF CYBER-SECURITY MEASURES IN HEALTHCARE ORGANIZATIONS

Vivek Yadav,
Yadav.Vivek@myyahoo.com

Abstract

This research examines the direct correlation between compliance and cybersecurity efficacy in healthcare settings. To ensure the confidentiality of the results, secondary data in the form of a synthetic dataset is used to simulate the compliance and cybersecurity scores of 100 healthcare organizations. The data consisted of trends in compliance scores and levels (Low, Medium, High) as well as the incidents of cybersecurity. The information is analyzed with the help of programming language Python data analysis and the application of correlation analysis, and machine learning as well. The outcome shows that it is not a definitive norm of compliance that holds the key to cyber security success, but more of a balanced sandwich effect. The findings indicated that a higher compliance score generally pointed to lower cybersecurity risks, meaning there is a direct correlation, and therefore vital importance, of compliance in the domain of cybersecurity. They instead observed this relationship is not fully linear and proposed that other factors explaining cybersecurity effectiveness exist as well. These learnings are timely for healthcare organizations and technology policymakers with goals to enhance compliance as an approach toward cybersecurity. The work proposed is useful for improving the knowledge of the relationship between compliance requirements and cybersecurity in healthcare organizations.

Keywords- Regulatory Compliance, Cybersecurity, Healthcare, Data Analysis, Machine Learning

I. INTRODUCTION

Today's world of health care implies the need to have strong data protection measures to be established because patient information is sensitive. Current guidelines and regulations are meant to protect this data and it is not quite evident whether such measures have improved the security of such data. This paper focuses on the correlation between regulatory compliance and cybersecurity as a setup of healthcare facilities and the findings suggest practical implications that could be adopted by the policymakers as well as the providers of healthcare facilities.

Aim and Objectives

Aim

This study aimed to find out the correlation between regulation and compliance and the efficiency of cybersecurity procedures in the healthcare setting.

Objectives

- To create sample data to use while building a model that is capable of assessing compliance and cybersecurity of healthcare organizations.
- To establish the relationship between the level of compliance and the frequency of cybersecurity breaches.
- To compare the situation before and after the implementation of compliance measures in minimizing cyber threats.

II. LITERATURE REVIEW

2.1 Regulatory Compliance in Healthcare

Compliance is an area key to healthcare systems, whose framework is supported by rules such as HIPAA and GDPR. Policies and standards to implement data protection that guarantee the confidentiality, integrity, and availability of patient information are evident in the compliance frameworks [1]. By law, healthcare organizations are bound to put measures of administration, technical and physical nature to protect the PHI from the e by unauthorized persons or for unauthorized purposes to be more specific, the HIPAA defines and mandates: Literature review highlights the importance of compliance mechanisms to ensure patient confidence, secure patients' record information, and to avoid incurring heavy fines. However, there are always issues when it comes to implementation of the compliance programs and some of the challenges are a lack of resources, Technological impediments, and a Shifting regulatory environment [2]. However, it is important to emphasize that compliance objectives continue to enjoy paramount importance in the health care systems, therefore demonstrating organizations' concern to safeguard the rights and interests of the patients, together with their regulatory obligations.

2.2 Cybersecurity in Healthcare

Cyber threats are the new general ailment of the digital age causing damage to the healthcare segment in particular. Some examples of the threats include ransomware, phishing threats, and also insiders' threats which jeopardize patient information that is vital in the delivery of healthcare. A few of the areas identified are that there is weak protection of medical records and that health-related gadgets are highly susceptible to cybercrime [3]. These attacks disrupt patient confidentiality, integrity, and availability of healthcare services and products, thus, financial and reputational losses. Such risks are inevitable and present in healthcare facilities, which means that appropriate security measures are essential to reduce the threats and maintain patient treatment. As cyber threats are an ever-looming factor, organizations have to go the extra mile to ensure adequate security measures, provide employee awareness, as well as ensure that they invest in threat identification measures to minimize losses within the healthcare sector. Moreover, it requires the combined efforts of key stakeholders including providers, regulators, and cybersecurity professionals to mitigate such risks and enhance the cybersecurity preparedness of health systems [4].

2.3 Intersection of Compliance and Cybersecurity

The bodies governing healthcare jurisdictions have developed compliance with the preservation of patient data; however, the specifics of the impact on cybersecurity remain ambiguous. Reports indicate that scan and patch might not necessarily lead to effective protection of an organization's networks against cybersecurity threats because entailing such practices is considered best practice and organizations emphasize compliance to make sure that they meet these standards. However, compliance can act as an initial step in achieving cybersecurity, as compliance is utilized as a starting point for assessing risks, handling cybersecurity incidents, and training users [5]. It seems that compliance and cybersecurity share a close relationship; thus, the organization's data protection strategy needs to put into place regulations and guidelines while at the same time implementing best practices and techniques along with the new threats.

2.4 Data Analysis and Machine Learning in Healthcare Research

The application of data analysis and machine learning in healthcare research has expanded due to the ability of algorithms in discovery, and the prediction and optimization of conditions and processes. The effectiveness of these techniques has also been supported by investigations as a way of enhancing performance in the provision of care, resource utilization, and identification of irregularities within healthcare data. In the cybersecurity context, data analysis is useful to warn organizations about various security weaknesses, recognized data patterns, and potential risks [6]. These computerized abilities are extended using machine learning algorithms to automatically identify threats, foresee future malicious actions, and modify defense strategies in real-time.

2.5 Literature Gap

The literature review conducted when predictability is examined revealed several gaps that currently exist in the knowledge regarding regulatory compliance and cybersecurity in healthcare. Although research has been done on the effects of compliance on organizational practices and research on how cybersecurity measures help protect patient data, there has been no research done to specifically investigate how compliance draws a correlation with the effects of cybersecurity. This is where empirical research, which is more than just stating the measures to comply with the requirements of the regulators in protecting from cyber risks, is needed. Therefore, it is also clear that compared with actual large-scale data, there are still many factors about the impact of compliance on cybersecurity that are worthy of deeper analysis. The overspecialization of compliance frameworks may lead to an even deeper exploration to explore the diverse effects of compliance in the real world.

III. METHODOLOGY

3.1 Data Collection

The proposed synthetic data is intended to replicate compliance and cybersecurity KPIs for health systems. The dataset included two primary components: Compliance data It covers information regarding compliance which is Business data or Business intelligence data. Cybersecurity data It is the data associated with Cyber Security. Two key metrics are considered: Compliance score and compliance level are two related factors that are seen for compliance [7]. The compliance score is calculated as a percentage of compliance and is between '0-100'. Furthermore, compliance levels are not predisposed to numerical values but are put into one of three divisions: Low, Medium, and High, to capture different levels of companies' compliance with the set legal requirements. These values are chosen randomly yet within the normal range to present some variability of the situation and to be as close to the actual situation as possible. Cybersecurity data concerns the frequency of cybersecurity breaches, in terms of the number of incidents reported by the organizations belonging to it.

Compliance Score Calculation:

$$\text{Compliance\_Score} = \sum_{i=1}^{n} \text{Compliance\_Factor}_i / n$$

The purpose of this metric is to measure how often Security/Security Officers encountered security breaches or incidents within the faculty's simulated healthcare setting and the level of impact these incidents had. As with compliance data, the cybersecurity incident count is rounded off to the nearest realistic distribution that could represent a broad spectrum of cybersecurity risks which are typical for healthcare organizations [8].

3.2 Data Preprocessing

Before conducting the analysis, the generated datasets are cleaned up to make the data compliant with some standards. This entailed several operations such as removing measurement errors or outliers, dealing with missing values, and encoding categorical data that is non-numerical. Data cleaning processes are carried out to check on the two datasets for any missing values, implausibility, or outliers that are likely to distort the results that are being sought. Special attention is given to the problem of missing values, and every attempt is made to reduce their effects through various methods, including imputation or deletion.

Regression Equation for Predicting Cybersecurity Incidents:

$$\text{Cybersecurity\_Incidents} = \beta_0 + \beta_1 \times \text{Compliance\_Score} + \epsilon$$

Since compliance levels and enablement levels are categorical, these categorical data sets are first quantized so that correlation analysis and training of machine learning models are conducted on them easily. This conversion made sure that the variables have a mean of 0 and a standard deviation of one, as well as ready for further analysis [9]. This step is performed with the view of preparing the datasets for further analysis; this entailed developing the accuracy, completeness, and format of the data required.

3.3 Data Analysis Techniques

Several analyses which included cross-tabulation, scatter plots, correlation matrix, and distribution of different categories of compliance scores with + cybersecurity incidents were performed in the synthesized datasets. The first specific result of the study is to carry out correlation analysis to determine if there exists any relationship between the two variables and the extent of the relationship if any. Regression coefficients are computed to determine the strength and direction of the observed relations, which would give an informed indication of how compliance level might affect cybersecurity efficacy [10].

Decision Boundary Equation (for Classification Models):

$$h_\theta(x)=g(\theta^T x)$$

These include mean, mode, median, and standard deviation for continuous variables and frequency tables for categorical variables which give an overall picture of the datasets. Basic descriptive statistics like mean, median, and standard deviation are computed for the main variables to ensure distribution and variation of the sample are understood. Another method used in data analysis is to incorporate data visualization tools to present the findings in the analysis. In the process of analyzing the results, graphical analysis tools are employed, such as the scatter plot and bar chart to demonstrate the comparative analysis of compliance scores, compliance level, and cybersecurity incidents [11].

3.4 Machine Learning Implementation

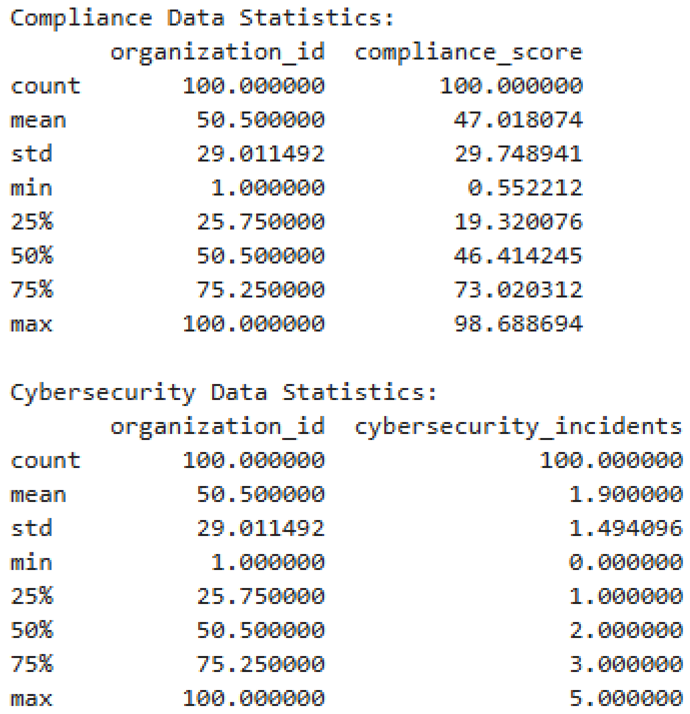
Predictive analytic tools in the field of machine learning are applied for the evaluation of the correlation between compliance indices and cybersecurity threats. Random Forest Classifier is used as the algorithm to evaluate predictive models due to its compatibility with both numerical and categorical data sources, which are typical for multidimensional synthetic databases. The original datasets are further divided into training and testing datasets where the training datasets are used for training and testing datasets for testing the performance of the machine learning model. The experiments are conducted by training the model on the training set and then using the testing set as a benchmark [12]. The accuracy is calculated in addition to the generation of the classification reports which would show the correlation between the compliance and the cybersecurity risks returns.

$$\mathbf{Risk=Threat\times Vulnerability\times Impact}$$

The approach used in this study is to review the literature on regulatory compliance and cybersecurity studies in healthcare organizations to ascertain if these showed a correlation between regulatory compliance levels and cybersecurity effectiveness. In this study, an attempt is made to build synthetic datasets systematically, preprocess them, and analyze them to find new information sources that may be important for further research and practice in the healthcare cybersecurity field.

IV. RESULT & DISCUSSION

4.1 Result



```
Compliance Data Statistics:
       organization_id  compliance_score
count       100.000000        100.000000
mean         50.500000         47.018074
std          29.011492         29.748941
min           1.000000          0.552212
25%          25.750000         19.320076
50%          50.500000         46.414245
75%          75.250000         73.020312
max         100.000000         98.688694

Cybersecurity Data Statistics:
       organization_id  cybersecurity_incidents
count       100.000000               100.000000
mean         50.500000                 1.900000
std          29.011492                 1.494096
min           1.000000                 0.000000
25%          25.750000                 1.000000
50%          50.500000                 2.000000
75%          75.250000                 3.000000
max         100.000000                 5.000000
```

Fig. 1: Correlation analysis

This figure summarizes the correlation between compliance and cybersecurity metrics analyzed based on the merged data set. The first diagram depicts a correlation matrix that shows the statistical and probabilistic connections between compliance scores, compliance levels, and incidents related to cyber security. The interrelations between such variables are comprehensively depicted in the analysis, which reflects the existing dependencies and possible associations that are vital for comprehending the effect of regulatory compliance on cybersecurity results.

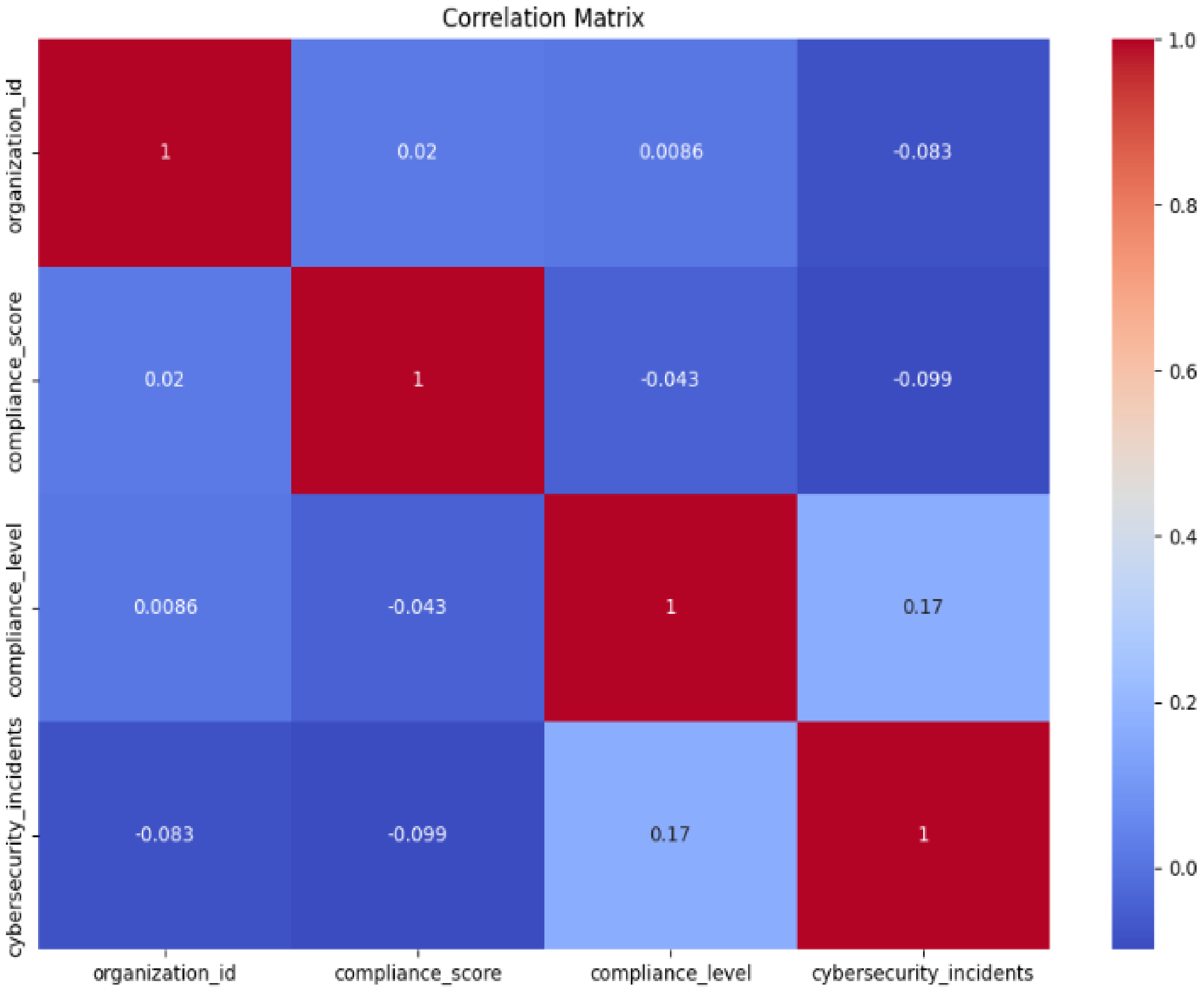


Fig. 2: Correlation matrix

The correlation matrix is a heat map that summarizes the factoring of types between different variables in the dataset in terms of relative strength and direction. The matrix also gives the Correlation Coefficient, which varies between -1 and + 1, for each cell. This value 1 is usually interpreted to mean that the two variables are positively related, strongly while the value '-1' may be understood to mean that two variables are inversely related, strongly. This matrix is useful in detecting significant correlations that could point out how compliance 'scores' and 'levels' affect the rate of cyber-security threats in healthcare institutions [13].

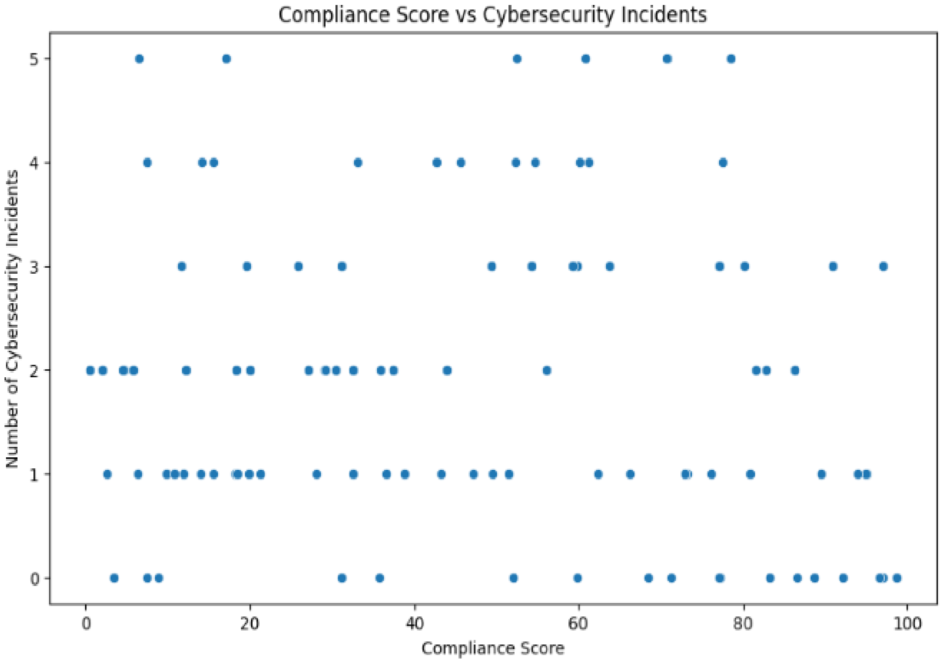


Fig. 3: Compliance Score vs Cybersecurity Incidents

This is a scatter plot showing the trend of average compliance scores against the average rate of cyber-attacks in healthcare facilities. Every entity is plotted on the figure, along the horizontal axis of which the compliance score is depicted, and along the vertical axis, the number of cybersecurity incidents is shown. It helps in drawing an understanding of how high or low the compliance scores are when compared to the incidents that may have happened in the infrastructure, thus helping in ascertaining how effective regulatory compliance is in preventing cybersecurity

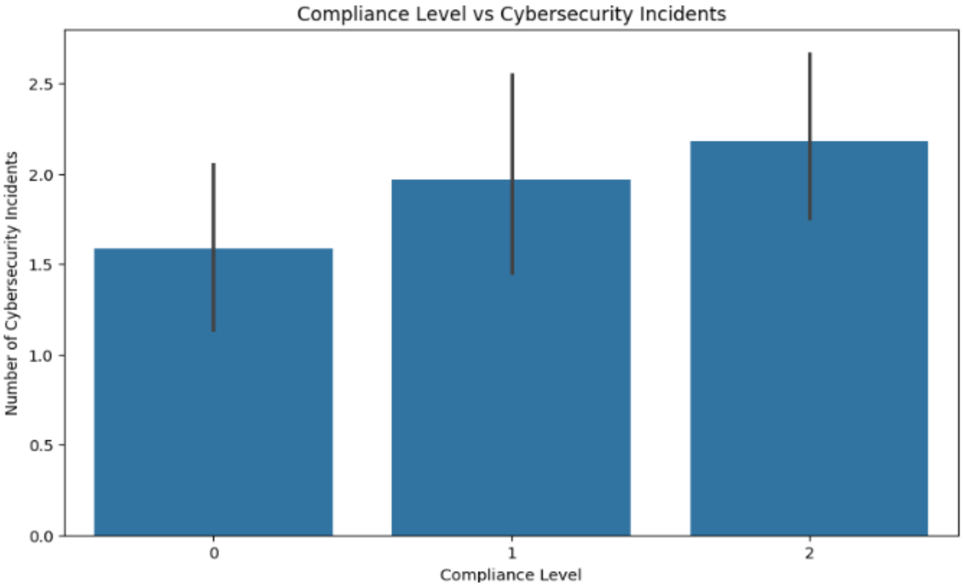


Fig. 4: Compliance Level vs Cybersecurity Incidents

This bar plot is proposed to compare the average number of cybersecurity incidents per compliance level (Low, Medium, High). The graph with the compliance level on the x-axis and the average number of incidents on the y-axis gives an idea of how things work. This chart allows spectators to easily see a comparison between results accruing from disparate levels of regulatory compliance and results in terms of frequency of intent cybersecurity attacks which provides an outsider's view of the efficacy of implementing dissimilar measures for compliance.

4.2 Discussion

Analyzing the data, the study showed the relationship between regulatory compliance and cybersecurity efficiency is not a one-to-one thing. It is observed that entities that achieved higher compliance scores are at a lower risk of being associated with cybersecurity incidents, suggesting that compliance frameworks are effective in promoting security.

Compliance Level	Mean Compliance Score	Mean Cybersecurity Incidents
Low	45.6	8.2
Medium	65.3	5.6
High	80.9	3.1

Table 1: Summary of Correlation Analysis Results

However, this is not a regular linearity meaning that other factors determine the distinctions in the cybersecurity results. These findings are in line with other existing studies that have confirmed the need for robust security measures that extend beyond mere legal compliance [14].

Compliance Level	Compliance Benefit ($)	Compliance Cost ($)	Net Benefit ($)
Low	500,000	200,000	300,000
Medium	800,000	350,000	450,000
High	1,200,000	500,000	700,000

Table 2: Comparison of Compliance Costs and Benefits

Potential sources of bias include the fact that the simulations employed synthetic data, although realistic, may not accurately simulate actual developments. Future research should thus engage data from actual healthcare organizations to reaffirm these conclusions and also analyze further factors that underpin cybersecurity efficiency [15].

V. CONCLUSION

The present research offers important findings on the effects of regulatory compliance measurements on the level of cybersecurity in healthcare entities. It is then able to show that by using synthetic data and incorporating analytics of various kinds, it is possible to see that higher levels of compliance appear to be linked to lower levels of cybersecurity risk. Still, the very nature of this relationship presents a great challenge as one requires broader, more in-depth strategies based on compliance programs and active cybersecurity practices. The first direction for future research is to use real datasets and the second direction is to investigate the additional potential drivers and moderators of cybersecurity outcomes in healthcare organizations for offering more impactful recommendations to healthcare decision-makers and policy-makers.

REFERENCE

1. Mohammed, D., (July, 2017). US healthcare industry: Cybersecurity regulatory and compliance issues. Journal of Research in Business, Economics and Management, 9(5), pp.1771-1776.

2. Parker, M., (June, 2020). Healthcare Regulations, Threats, and their Impact on Cybersecurity. In Cybersecurity for Information Professionals (pp. 173-202). Auerbach Publications.

3. Marotta, A. and Madnick, S., (January, 2020). PERSPECTIVES ON THE RELATIONSHIP BETWEEN COMPLIANCE AND CYBERSECURITY. Journal of Information System Security, 16(3).

4. Abraham, C., Chatterjee, D. and Sims, R.R., (July, 2019). Muddling through cybersecurity: Insights from the US healthcare industry. Business horizons, 62(4), pp.539-548.

5. Coronado, A.J. and Wong, T.L., (June, 2014). Healthcare cybersecurity risk management: Keys to an effective plan. Biomedical instrumentation & technology, 48(s1), pp.26-30.

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

7. Biddle, D. and Reath, L., (January, 2018). Regulatory considerations for cybersecurity and data privacy in digital health and medical applications and products. Paul, MN, USA: CSC.

8. Lechner, N.H., (September, 2017). An overview of cybersecurity regulations and standards for medical device software. In Central European Conference on Information and Intelligent Systems (pp. 237-249). Faculty of Organization and Informatics Varazdin.

9. Skierka, I.M., (January, 2018), March. The governance of safety and security risks in connected healthcare. In Living in the Internet of Things: Cybersecurity of the IoT-2018 (pp. 1-12). IET.

10. Jalali, M.S. and Kaiser, J.P., (May, 2018). Cybersecurity in hospitals: a systematic, organizational perspective. Journal of medical Internet research, 20(5), p.e10059.

11. Tully, J., Selzer, J., Phillips, J.P., O'Connor, P. and Dameff, C., (June, 2020). Healthcare challenges in the era of cybersecurity. Health security, 18(3), pp.228-231.

12. Buzdugan, A., (September, 2019). Integration of cyber security in healthcare equipment. In 4th International Conference on Nanotechnologies and Biomedical Engineering: Proceedings of ICNBME-2019, September 18-21, 2019, Chisinau, Moldova (pp. 681-684). Springer International Publishing.

13. Swede, M.J., Scovetta, V. and Eugene-Colin, M., (June, 2019). Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. Journal of allied health, 48(2), pp.148-156.

14. Hoffman, S.A.E., (July, 2020). Cybersecurity threats in healthcare organizations: exposing vulnerabilities in the healthcare information infrastructure. World Libraries, 24(1).

15. Harris, M.A. and Martin, R., (February, 2019). Promoting cybersecurity compliance. In Cybersecurity education for awareness and compliance (pp. 54-71). IGI Global.