Journal of Cybersecurity and Privacy

MDPI

Article

Cybersecurity in Hospitals: An Evaluation Model

Mohammed A. Ahmed *, Hatem F. Sindi and Majid Nour

Electrical and Computer Engineering Department, King Abdulaziz University, Jeddah 22254, Saudi Arabia
* Correspondence: mahmed0101@stu.kau.edu.sa

Abstract: Hospitals have been historically known for their strong risk mitigation policies and designs, which are not becoming easier or simpler to plan and operate. Currently, new technologies and devices are developed every day in the medical industry. These devices, systems, and personnel are in an ever-higher state of connection to the network and servers, which necessitates the use of stringent cybersecurity policies. Therefore, this work aims to comprehensively identify, quantify, and model the cybersecurity status quo in healthcare facilities. The developed model is going to allow healthcare organizations to understand the imminent operational risks and to identify which measures to improve or add to their system in order to mitigate those risks. Thus, in this work we will develop a novel assessment tool to provide hospitals with a proper reflection of their status quo, which will assist hospital designers in adding the suggested cyber risk mitigation measures to the design itself before operation.

Keywords: cybersecurity; cyber-attack; network protection; medical devices; evaluation; hospitals

1. Introduction

Cybersecurity is a set of processes and technologies created to protect computers, software, and data from cyber-threats [1]. Nowadays, many services and procedures depend mainly on the Internet and computers, such as healthcare services [2]. Even though healthcare organizations have strong policies that mitigate most kinds of risks, they are still vulnerable to cyber-threats. This makes cybersecurity an important aspect for many organizations, especially healthcare organizations [2]. Cybersecurity is a relatively new subject in healthcare [3]. It involves the measures taken to secure and protect the electronic equipment and the information saved digitally. The healthcare sector has been advancing rapidly over the past two decades, increasing the use of more advanced technologies [3]. Currently, all patients have their personal identifiable information (PII) and personal health information (PHI) saved in the servers of the hospitals they visit [4]. Even though this rapid incorporation of technology in healthcare improves their services, it also increases the risk of being vulnerable to cyber-attacks [4]. Nowadays, almost every hospital department deals with the PII and PHI of patients using their electronic health records (EHR) and other software such as e-prescription programs [4]. Other than health information, hospitals also use patients' banking and billing information and share them with insurance companies electronically [4]. In addition, hospitals are full of medical devices connected to the network and are subject to cyber-attacks [5]. There are a variety of medical devices that are connected to the network. Some devices are implanted inside patients, which amplify the effects of cyber-attacks. In the case of this happening, the integrity of the medical devices is compromised, which disrupts the services offered by the hospital [5]. Failing to protect hospitals from all types of cyber-attacks to patients' PIIs, PHIs, banking information, and implanted medical devices can result in significant consequences.

On the other hand, finance in healthcare is limited [4]. When a cyber-attack on a hospital takes place, the hospital might be overwhelmed financially due to fines, loss of services, and lawsuits [3]. Hospitals need to implement cybersecurity measures and reduce the costs of their implementation. To decide which measures are more effective than others,

Citation: Ahmed, M.A.; Sindi, H.F.; Nour, M. Cybersecurity in Hospitals: An Evaluation Model. *J. Cybersecur. Priv.* **2022**, *2*, 853–861. https://doi.org/10.3390/jcp2040043

Academic Editor: Steven Furnell

Received: 28 July 2022
Accepted: 19 October 2022
Published: 26 October 2022

an evaluation model will be created to assist hospitals in making such a decision. The model aims to identify and quantify cyber-attack risks and the measures needed to mitigate them.

2. Background

2.1. Cybersecurity in Hospitals

Hospitals are complex organizations that offer services to patients and people in need. Hospitals are technology-saturated environments, making it difficult for their information technology (IT) department to manage all of the devices in their network [3]. The variety of devices the department deals with increases the complexity and difficulty of applying the policies and procedures of the IT department [3]. It is challenging for hospitals to be robust to cyber-attacks due to their complexity [3].

2.2. Cyber-Attack Types in Hospitals

Hospitals are attractive for attackers due to the financial and political gain [6]. Nevertheless, cyber-attacks on hospitals might allow attackers to take lives in the form of cyber warfare [6]. Hospitals are at risk of cyber-attacks in five different ways, according to the US Department of Health [7]. The five threats are email phishing attacks; ransomware attacks; the loss or theft of equipment or data; insider, accidental, or intentional data loss; and attacks against connected medical devices [7]. This section will discuss each of the five threats, along with their causes and impacts.

2.2.1. Email Phishing Attack

An email phishing attack is an attempt to steal information from an employee in the hospital by tricking them into giving information via email [7]. The email appears to the employee as if it is from a legitimate source [8]. An example of a phishing email is receiving an email with an activation link from a known source to acquire the wanted information [7,8]. Then, if the employee clicks the link, it takes them to a website that may steal sensitive information or infect the computer. This type of attacks happens due to a lack of awareness, a lack of IT resources to manage suspicious emails, and a lack of protection software. This type of attacks leads to stolen access credentials that could be used to access sensitive data. It also might affect the reputation of the hospital [7].

2.2.2. Ransomware Attack

A ransomware is a malware that works by encrypting data saved in computers or the network itself [9]. A ransomware attack is a malicious software that eliminates access to user data by encrypting them with a key [7]. The attacker (hacker) is the only person who knows the key, meaning that the attacker is the only person with access to the data [7]. The purpose behind this type of attack is eliciting a ransom payment from the owner of the data to the attacker. This type of attack can be the result of email phishing. Weaknesses in the system, such as a lack of system backup, a lack of anti-phishing capabilities, and a lack of network security, may lead to amplified consequences [7].

2.2.3. Loss or Theft of Equipment or Data

The loss of equipment decreases the productivity of hospitals on the one hand and endangers patients on the other hand [10]. Devices such as laptops, tablets, phones, and USBs in hospitals are considered as parts of the hospital's equipment [7]. If this equipment is stolen, it can end up in the hands of attackers who might take advantage of the situation [7]. Those devices might contain sensitive information or data, and the loss might be catastrophic if they are not password-protected. Some vulnerabilities increase the chance of the occurrence of this type of attack, such as a less-frequent assent inventory schedule, lack of physical security practices (i.e., leaving offices open), lack of awareness, and lack of data encryption. In addition, patient safety will be compromised. This type of attack will disrupt the services offered and break the trust between the patients and the organization [7].

2.2.4. Insider, Accidental, or Intentional Data Loss

Advances in the healthcare technology have led to the use of paperless systems [11]. This fact minimizes the availability of data in physical forms and increases its availability in digital forms [11]. This leads to increases in losses of data or attacks to steal data. Insider accidental data loss is considered a type of unintentional loss caused by honest mistakes [7]. Honest mistakes could be because of a degree of negligence or errors due to procedures and policies [7]. On the other hand, intentional insider loss of data is considered malicious loss or theft. This threat is caused by an employee or any person who uses the hospital's technology and network to benefit personally. Some of the reasons for this type of threat are negligence in sharing data, a lack of data monitoring, a lack of access limitations to sensitive data, and a lack of awareness. This threat can affect patient safety if a patent's data are altered somehow, such as an alteration to a prescribed medication [7].

2.2.5. Attacks against Connected Medical Devices

According to the Saudi FDA, a medical device is defined as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or another similar or related article, including a part or accessory, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease" [5,7]. Medical devices have been evolving in the past decades and have been digitalized instead of remaining analog [12]. Modern medical devices depend on software programs that require connections to external devices and servers, which increases the risk of attacks [12]. Attacks against connected medical devices are initiated by taking control of the care provider's computer [7]. This is possible through email phishing and other methods [7]. Once the attacker is in the network, they can control the connected devices, power them off, reboot them, and alter their settings [7]. The system's vulnerabilities that make this threat possible include patches to maintain medical devices not being implemented correctly [7]. Failing to update medical equipment within the required time can be another reason for this type of threat [7]. The unavailability of the cybersecurity information from the medical devices to the hospital is another system vulnerability [7]. Medical devices can be invasive or non-invasive. Most medical devices are connected to a network to function. Cyber-attacks on medical devices can affect patients' safety in several ways. For instance, attacking implanted medical devices, such as implantable cardioverter defibrillators (ICDs), can result in fatalities [13]. In addition, patients might not receive the desired outcome from the medical device due to cyber-attacks [7]. This can happen when patients' data in their medical records are altered or changed, causing inaccurate assessments or treatments [13]. A threat to medical devices in a hospital causes broad hospital operational impacts due to medical devices being unavailable [7].

2.3. Protecting Hospitals from Cyber-Attacks

There are many practices and measures hospitals can include in their cybersecurity management plans to avoid cyber-attacks. Cybersecurity must be included in the risk management process [6]. Hospitals should move toward achieving the goal of cyber resilience. Table 1 summarizes the measures that can be followed to improve cybersecurity in a hospital.

Table 1. Summary of the measures taken by hospitals to improve cybersecurity.

Seq	Cybersecurity Measure	Description	Threat
1	Regular Staff Training	This indicator makes sure that every employee has cyber security and threat training once yearly	Email Phishing Intentional, accidental, and unintentional data loss
2	Email Protection System	This indicator calculates how many spam filters are used for each received email	Email Phishing Ransomware

Table 1. *Cont.*

Seq	Cybersecurity Measure	Description	Threat
3	Endpoint Protection Systems	This indicator accounts for the size of unauthorized data transfers	Loss or theft of data
4	Access Management Policy	This indictor accounts for unauthorized access to the network	Ransomware Intentional, accidental, and unintentional data loss
5	Backup System	This indicator makes sure data are continuously backed up and that the size is increasing in every backup	Ransomware
6	Updated Equipment	This indicator accounts for every computer in the organization and their update status	Loss or theft of equipment
7	HIS access control	The health information system should not be accessed by unauthorized personnel [14]. This indicator accounts for unauthorized access.	Loss or theft of data
8	Implementing Cybersecurity Policy	This indicator accounts for the availability of a policy that discusses cybersecurity	All threats
9	Medical Devices Security	This indicator accounts for every medical device that is connected to the network and makes sure it is updated	Attacks against connected medical devices
10	Limiting Access to Medical Devices	This indicator accounts for unauthorized access to medical equipment	Attacks against connected medical devices

3. Objective

The main objective of this research is to protect hospitals from most types of cyber-attacks that directly relate to patients' well-being and the privacy of their information. This is achieved by creating a model that evaluates hospital cybersecurity systems. The model will inform hospitals of the most effective measures needed to improve their cybersecurity systems. This model should improve the efficiency of cybersecurity measures in hospitals and their financial standing. There are many measures that are implemented in cybersecurity plans in hospitals, and for the sake of being thorough and covering most types of attacks, we chose the 10 most important measures according to the literature review. The chosen measures are listed in Table 1.

4. Methodology

In this research, we aimed to evaluate hospital cybersecurity measures. This was done by following a number of steps and performing a number of simulations:

1. Choosing the indicators that make up the evaluation model;
2. Creating the model;
3. Writing the model as a code in MATLAB;
4. Testing the model using a set of data from three different hospitals;
5. Analyzing the results and adjusting the model if needed;
6. Validating the model and adjusting it as needed.

The first step, choosing the indicators, was already achieved in the previous section. The indicators that were selected are the ones listed in Table 1. The evaluation model is discussed in detail in the following section of the paper. Then, a set of data is presented and tested using the evaluation model that is created in MATLAB. Finally, the results will be presented and discussed in the paper. Then, the model will be validated by comparing it to existing models to ensure it is as accurate as it can be.

5. Evaluation Model

In this research, we aimed to evaluate the effectiveness of cybersecurity systems in hospitals in general, regardless of their size and scope. In order to do this, a cybersecurity evaluation model was developed. The threats and measures taken to prevent them were taken into account when creating the model. To simplify the model, the measures taken

to prevent threats are grouped into several groups, which are added together in the main model. This grouping is based on how similar they are. The weights included in the equations are variables assigned a value between 0 and 1.

First, user training (*UT*), access management (*AM*), and backup systems (*BU*) can be grouped together, as they all involve the hospitals' employees and their education (1):

$$W_1\ UT + W_2\ AM + W_3\ BU = \omega \quad (1)$$

Then, email (*PP*) and endpoint (*EP*) protection systems are grouped together, since those two measures basically protect the data sent, received, and shared (2):

$$W_4\ PP + W_5\ EP = \tau \quad (2)$$

In addition, updating non-medical equipment (*UD*) in the hospital and updating medical equipment (*MU*) can be grouped into one equation. This grouping is due to the fact that both measures require an inventory of the equipment and periodic maintenance (3):

$$W_6\ UD + W_7\ MU = \sigma \quad (3)$$

Limiting access to medical devices (*MD*), controlling the network *(NS*), and implementing a cybersecurity policy (*CP*) are all measures that can be grouped into one Equation (4). This is because these measures are directly related to patient safety and to patient data:

$$W_8\ CP + W_9\ NS + W_{10}\ MD = \gamma \quad (4)$$

Finally, those four equations are added together to create our model. Our evaluation model, which is used in the hospital evaluation step, is Equation (5):

$$W_{11}\ \omega + W_{12}\ \tau + W_{13}\ \sigma + W_{14}\ \gamma = \Omega \quad (5)$$

6. Dataset

In order to test the evaluation model, three different hypothetical hospitals will be evaluated using the data in Table 2.

Table 2. Datasets from three different hospitals that will be used to test and validate the evaluation model.

Measure / Hospital	A	B	C
Number of Employees	1500	700	4000
Cyber Training Sessions yearly	6	2	0
Capacity of Sessions	200	150	0
Number of Data backups yearly	12	2	6
Size of Data in first backup of the year (GB)	480	150	1000
Increment of data every month (%)	10%	5%	15%
Number of Spam filters applied (Up to 3)	1	0	2
Number of approved data transfers yearly	100	50	650
Average size of data in each transfer (MB)	250	200	300
Total size of transferred data yearly (MB)	40,000	8000	785,000
Number of approved network access instances	1500	600	3850
Total network access	2300	1200	6500
Number of non-medical electronic devices	1700	900	6000
Number of inventories of non-medical devices	12	6	12

Table 2. *Cont.*

Measure	Hospital	A	B	C
Average number of Up-to-date non-medical devices in every inventory		150	80	600
Number of electronic medical devices		3200	1600	10,000
Number of inventories of medical devices		12	4	12
Average number of Up-to-date medical devices in every inventory		300	250	550
Number of employees who can access HIS		1000	450	3000
Actual access to HIS		1300	500	2800
Number of employees that access medical devices		700	350	3600
Actual access to medical devices		500	400	3800
Availability of Cybersecurity policy		Yes	No	Yes

7. Results

The model that was developed in this paper was implemented as a MATLAB code that was used to run the datasets. The datasets introduced in the previous section determined which hospitals had the highest and lowest scores. The results for the three hospitals are available in Table 3.

Table 3. The results of the evaluation model using the three hospitals' data.

Hospital	Minimum Indicator	Maximum Indicator	Final Score
A	Email Protection System	Medical device access, Updating Medical and non-medical devices, and Cybersecurity Policy	80.9%
B	Cybersecurity Policy and Email Protection System	Endpoint Protection System	50.2%
C	Cybersecurity Training	Non-medical device Update and Access Management	65.5%

8. Discussion

Before discussing the results obtained from compiling the datasets into the evaluation model, the weights used in the equations of the model were assigned a value of 0.1 to ensure every indicator has the same importance. Those weights can be altered in the future depending on the importance of the indicators for each hospital. Regulatory agencies can also alter the weights according to their standards if the model is being used in their accreditation process. In addition, the final score that is assigned to hospitals is a value between 0 and 100%. The score determines how strong the hospital's cybersecurity system is.

According to Table 3, hospital "A" achieved the highest score among all three hospitals. The score the hospital received was 80.9%. This score means that the hospital is fairly strong in the area of cybersecurity. The model identified the hospitals' weak and strong measures. The only weak measure was their email protection system. The hospital is not implementing enough spam filters to filter the received emails. As mentioned previously, there are three different types of spam filters that can be used in an email protection system.

On the other hand, the hospital is strong enough in four different areas. The hospital has a great inventory policy or system that makes sure all electronic devices (medical and non-medical) are updated at least once a year. Additionally, the hospital prevents unauthorized personnel from accessing medical devices, which prevents any harm being caused to the patients, as well as preventing patient privacy violations. Finally, the hospital implements a cybersecurity policy that instructs employees on dealing with any cybersecurity aspect.

The hospital that achieved the second highest score was hospital "C" according to Table 3. This score, 65.5%, means that the hospital is moderately vulnerable against cyber-

attacks. This score indicates that the hospital needs to improve more than one measure in order to improve their cybersecurity. The hospital's weakest measure is training employees on cybersecurity measures and cyber-attacks. In other words, having cybersecurity training as the weakest measure indicates that the hospital either does not perform training sessions or does not train every employee at least once a year. On the other hand, the hospital's strongest measures are updating non-medical devices and access management. This proves that the hospital's maintenance and inventory system is working as desired and does not currently need improvement. Otherwise, according to the evaluation model, the hospital has a great access management system, which prevents unauthorized access to the health information system (HIS).

The hospital that had the lowest score of 50.2% was hospital "B" according to Table 3. This score shows us that the hospital is moderately vulnerable to cyber-threats and attacks, even more then the previously discussed hospital. According to the model, in order for the hospital to improve its cybersecurity, it needs to improve most of its measures, especially the cybersecurity policy and email protection systems. The model indicates that the hospital has not implemented a cybersecurity policy, which increases the risk of email phishing and ransomware attacks. In addition, the hospital has another weak measure, which is its email protection system. This means that the hospital does not filter the emails the employees receive with enough filters, which increases the rate of received spam emails and email phishing links. On the contrary, the hospital has strong endpoint protection systems that do not need to be improved in the meantime. This result means that the hospital minimizes unauthorized transfers of data. The hospital authorizes most of the data transferred using any method.

8.1. Model Validation

In this section, we will compare our model to two models from the literature in terms of the structures, types of results, and numbers of factors and trials. A previous paper [15] discussed the development of a security evaluation model that focused on a specific type of threat, which is not similar to our model focusing on five types of threats. However, they used 26 indicators to create their model, which gave promising results [15]. Our model included ten indicators, meaning it is not similar to what their model used. However, the number of indicators in our model fully covers all types of cyber-threats. Increasing the number of indicators could result in different results, but not necessarily better results. Their model did not result in a clear number that defines a specific score or percentage of the tested methods, instead it resulted in factors that organizations can use to prevent information leakage. On the other hand, our model does give a score that defines the vulnerability of the hospital to cyber-attacks.

A previous paper [16] developed a model that evaluates the security of virtual learning websites using six indicators only. The paper gave promising results as well. The number of indicators we included in our model was more than the number they used in their model, which is six indicators. They tested their model on two applications only while we tested our model on three different hospitals [16]. This model resulted in percentages that determine the security of the applications. The two models along with our model are compared in Table 4.

Table 4. Comparison between the two models from the literature and our model.

Model	Model 1	Model 2	Our Model
Number of factors	26 indicators	6 indicators	10 indicators
Number of trials	3 Validation methods	2 Systems	3 Hospitals
Type of results	The results are the factors that they use	Percentage	Percentage(score)

8.2. Model Limitations

There are several points that can be followed to improve our model. First of all, the model has not been applied to actual hospitals to find out whether it is applicable or not. The model can be applied to existing hospitals to evaluate its results and to validate them. The data used in this paper were from three random hospitals, which is why using the model with actual hospitals can provide great feedback to improve it. In addition, due to the lack of models in the literature that focus on our topic and give clear instructions and steps for replicating the model, the hospitals evaluated by our model were not evaluated using other models to compare the results. However, our model has been compared to a couple of models that evaluate the security of applications and organizations to determine its validity and accuracy. This comparison revealed that our model is valid and accurate, as it gives exact values that can be used to quantify the cyber-attack vulnerability of a given hospital, while the model developed in [15] did not provide similar results. The other model developed in [16] gave similar results to our model.

9. Conclusions and Future Works

Many services that are offered worldwide are dependent on the Internet, including services such as banking and healthcare. The Internet has become an essential tool that allows us to perform our daily activities successfully. This fact makes cybersecurity a necessary tool to be incorporated. Cybersecurity involves a set of technologies and processes that protect the organizations from any of the five types of cyber-threats, such as email phishing and ransomware attacks. Cybersecurity systems in organizations are not always perfect, which makes it necessary to improve them. In this paper, we proposed an evaluation model that evaluates a system and identifies the weaknesses that need improvement in the cybersecurity system. This model successfully evaluated three different hospitals and identified their weak and strong measures. This model recommends the necessary measures to be improved for an organization instead of improving all measures and spending their finances on unnecessary measures that are already being implemented and working perfectly. This model can be used as an improvement tool as well as an evaluation and accreditation tool.

In the future, this model will be evaluated using the same data with a different model developed by other researchers to prove it is valid and accurate. The model can be used to evaluate existing hospitals and improved to ensure it gives optimal results. This model can in the future incorporate the use of artificial intelligence in the healthcare industry and can mitigate its risks by increasing the number of indicators to cover all aspects. It can also be edited to evaluate different organizations, increasing its uses and objectives. In addition, this model has inspired us to create similar models that evaluate different security and safety systems instead of cybersecurity systems.

Author Contributions: Conceptualization, M.A.A. and M.N.; methodology, M.A.A.; software, M.A.A.; validation, M.A.A. and M.N.; formal analysis, M.A.A.; investigation, M.A.A.; resources, M.A.A.; data curation, M.A.A.; writing—original draft preparation, M.A.A.; writing—review and editing, M.N. and H.F.S.; visualization, M.A.A.; supervision, M.N.; project administration, M.N.; funding acquisition, M.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

Symbol	Definition
UT	User Training
AM	Access Management
BU	Backup System

PP	Endpoint Protection
EP	Email Protection
UD	Updating Equipment
MU	Medical Device Update
CP	Cybersecuirty Policy
NS	Hospital Network (HIS) Access
MD	Medical Device Access
$W_{1–14}$	Weights between 0 and 1 assigned according to measured importance in the required hospital

References

1. Goutam, R.K. Importance of Cyber Security. *Int. J. Comput. Appl.* **2015**, *111*, 4.
2. Dummanaboyina, K.S.C. Cyber Security and Its Importance. Available online: https://www.researchgate.net/publication/347439655_CYBER_SECURITY_AND_ITS_IMPORTANCE (accessed on 23 March 2022).
3. Jalali, M.S.; Kaiser, J.P. Cybersecurity in hospitals: A systematic, organizational perspective. *J. Med. Internet Res.* **2018**, *20*, e10059. [CrossRef] [PubMed]
4. Argaw, S.T.; Troncoso-Pastoriza, J.R.; Lacey, D.; Florin, M.-V.; Calcavecchia, F.; Anderson, D.; Burleson, W.; Vogel, J.-M.; O'Leary, C.; Eshaya-Chauvin, B.; et al. Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 1–11. [CrossRef] [PubMed]
5. Saudi Food and Drug Authority (SFDA). *Guidance to Medical Devices Cybersecurity for Healthcare Providers*; SFDA: Riyadh, Saudi Arabia, 2019; pp. 1–9.
6. Coventry, L.; Branley, D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas* **2018**, *113*, 48–52. [CrossRef] [PubMed]
7. US Department of Health and Human Services. *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*; US Department of Health and Human Services: Washington, DC, USA, 2020.
8. Syiemlieh, P.; Khongsit, G.M.; Sharma, U.M.; Sharma, B. Phishing—An Analysis on the Types, Causes, Preventive Measuresand Case Studies in the Current Situation. *IOSR J. Comput. Eng.* **2015**, *9*, 2278–8727.
9. Imaji, A.O. Ransomware Attacks: Critical Analysis, Threats, and Prevention Methods. Available online: https://www.researchgate.net/publication/332551447_Ransomware_Attacks_Critical_Analysis_Threats_and_Prevention_methods (accessed on 23 March 2022).
10. Cheung, A.; Clayden, N.; Ocampo, W.; Kiplagat, L.; Kaufman, J.; Baylis, B.; Conly, J.M.; Ghali, W.A.; Ho, C.H.; Stelfox, H.T.; et al. Documentation and investigation of missing health care equipment: The need to safeguard high priced devices in health care institutions. *J. Hosp. Adm.* **2017**, *6*, 10. [CrossRef]
11. Seh, A.H.; Zarour, M.; Alenezi, M.; Sarkar, A.K.; Agrawal, A.; Kumar, R.; Ahmad Khan, R. Healthcare Data Breaches: Insights and Implications. *Healthcare* **2020**, *8*, 133. [CrossRef] [PubMed]
12. Skierka, I.M. The governance of safety and security risks in connected healthcare. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT—2018, London, UK, 28–29 March 2018; pp. 1–12. [CrossRef]
13. Tabasum, A.; Safi, Z.; AlKhater, W.; Shikfa, A. Cybersecurity Issues in Implanted Medical Devices. In Proceedings of the 2018 International Conference on Computer and Applications (ICCA), Beirut, Lebanon, 25–26 August 2018; pp. 1–9. [CrossRef]
14. Almunawar, M.N.; Anshari, M. Health Information Systems (HIS): Concept and Technology. *arXiv* **2012**, arXiv:1203.3923.
15. Kim, J.; Lee, C.; Chang, H. The Development of a Security Evaluation Model Focused on Information Leakage Protection for Sustainable Growth. *Sustainability* **2020**, *12*, 10639. [CrossRef]
16. Callejas-Cuervo, M.; Alarcon-Aldana, A.C.; Lopez, A.B. Security evaluation model for virtual learning environments. In Proceedings of the 2016 XI Latin American Conference on Learning Objects and Technology (LACLO), San Carlos, Costa Rica, 3–7 October 2016; pp. 1–6. [CrossRef]