sensors

MDPI

Article

A Risk Assessment Framework Proposal Based on Bow-Tie Analysis for Medical Image Diagnosis Sharing within Telemedicine

Thiago Poleto [1,*], Maisa Mendonça Silva [2], Thárcylla Rebecca Negreiros Clemente [3], Ana Paula Henriques de Gusmão [4], Ana Paula de Barros Araújo [2] and Ana Paula Cabral Seixas Costa [2]

1 Department of Business Administration, Federal University of Pará, Belém 66075-110, Brazil
2 Department of Management Engineering, Universidade Federal de Pernambuco, Recife 50670-901, Brazil; maisa@cdsid.org.br (M.M.S.); anapaula.araujo@ufpe.br (A.P.d.B.A.); apcabral@cdsid.org.br (A.P.C.S.C.)
3 Department of Management Engineering CAA, Universidade Federal de Pernambuco, Caruaru 55002-970, Brazil; tharcylla.clemente@ufpe.br
4 Department of Management Engineering, Universidade Federal de Sergipe, São Cristóvão 49100-000, Brazil; anapaulagusmao@cdsid.org.br
* Correspondence: thiagopoleto@ufpa.br

Abstract: The purpose of this paper is to propose a framework for cybersecurity risk management in telemedicine. The framework, which uses a bow-tie approach for medical image diagnosis sharing, allows the identification, analysis, and assessment of risks, considering the ISO/TS 13131:2014 recommendations. The bow-tie method combines fault tree analysis (FTA) and event tree analysis (ETA). The literature review supported the identification of the main causes and forms of control associated with cybersecurity risks in telemedicine. The main finding of this paper is that it is possible, through a structured model, to manage risks and avoid losses for everyone involved in the process of exchanging medical image information through telemedicine services. Through the framework, those responsible for the telemedicine services can identify potential risks in cybersecurity and act preventively, recognizing the causes even as, in a mitigating way, identifying viable controls and prioritizing investments. Despite the existence of many studies on cybersecurity, the paper provides theoretical contributions to studies on cybersecurity risks and features a new methodological approach, which incorporates both causes and consequences of the incident scenario.

Keywords: image and diagnosis medical security; bow-tie analysis; cyberattack; cybersecurity; decision-making

Citation: Poleto, T.; Silva, M.M.; Clemente, T.R.N.; de Gusmão, A.P.H.; Araújo, A.P.d.B.; Costa, A.P.C.S. A Risk Assessment Framework Proposal based on Bow-Tie Analysis for Medical Image Diagnosis Sharing within Telemedicine. *Sensors* **2021**, *21*, 2426. https://doi.org/10.3390/s21072426

Received: 9 December 2020
Accepted: 11 January 2021
Published: 1 April 2021

1. Introduction

Information technology (IT) has been gaining wide use in the generation of information and in the decision support process in different contexts. One of the IT resources of greatest investment in recent years is the set of multimedia features that allows the sharing of texts, documents, sounds, and images in high resolution, being able to describe, reproduce, create, represent, and simulate several systems. In general, IT multimedia resources are indicated as facilitators of communication and content transmission, especially via the Internet and remote devices, and have ensured the availability and accessibility of different data formats for many organizational processes. As an example, it is possible to consider the widespread use of IT multimedia resources to support medical diagnoses and treatments promoted by health institutions worldwide [1–3].

Medical information contains specific and personal details about patients and their health status. In many situations, images are used as essential sources of information and play a fundamental role in the composition of medical diagnosis [4,5]. The storage of images in medical databases is widely recognized as a procedure that facilitates access to images by several doctors and health centers around the world, offering the sharing

of information and knowledge about different health conditions [6]. In particular, via the Internet and distributed databases, patient reports can be downloaded quickly in order to streamline the response to the healthcare service and real-time monitoring using data from vision-based sensors [7].

The process of transferring medical images is included in the telemedicine resources that comprise several types of imaging tests used in medical diagnostics, such as computed tomography, magnetic resonance, radiography, mammography, nuclear medicine, and ultrasound [8,9]. One of the main storage environments for medical images, the picture archiving and communication system (PACS), allows images and results of treatments to be accessed and shared by several health centers around the world, which speeds up the development of exams, medications, and surgical techniques, in order to support research and discoveries that increase the life expectancy of the population, improve quality of life, and reduce mortality indicators [10,11]. However, in addition to images, personal and confidential data about patients are often shared on the network, which highlights the system's vulnerability [12].

In general, the vulnerability of the system is related to the communication protocols and sharing of medical content via the Internet and distributed databases [13]. Researchers emphasize the concern regarding the implementation of techniques of data hiding, protection, and integrity of medical diagnosis, especially because this type of information is highly sensitive and, if corrupted or modified by cyberattacks, can lead to costly litigation and fines [14,15].

Despite the different techniques used by telemedicine to protect the information shared, cyberattacks can cause huge losses, leading to changes in diagnoses and an increased risk of spreading an incorrect report. Therefore, cybersecurity of medical data is critical in telemedicine solutions because the damage caused by cyberattacks can create serious problems in the diagnosis decision for any individual during the transfer of this data, given that cybersecurity can be considered as a non-cooperative game in which, on one hand, a hacker is trying to find vulnerabilities to exploit sensitive data or perform malicious actions, and on the other hand, the defender is continuously restricting the attack if a threat to the system occurs [16,17]. This process can be considered complex due to the lack of complete information about how or when a cyberattack will occur. However, it is opportune to develop analyses that may make it possible to understand the uncertain context.

The advancement of solutions in the cybersecurity area is driven by business growth in the digital age. Recent research has considered aspects of risk analysis to analyze the operational and strategic conduct of organizations in relation to the uncertainty of the impact of cyberattacks in organizational environments [18–27]. The study of the risks involved in cyberattacks is an opportunity to explore potential failure modes in the image and content archiving system, which can be considered motivators for investing in cybersecurity in telemedicine.

Therefore, the present work aims to address the problem related to cybersecurity within telemedicine with a focus on image and diagnosis sharing using a bow-tie approach. The contributions of this paper are threefold: (i) identification of potential risk factors and risk events; (ii) prioritization of actions that minimize the impact of cyberattacks on telemedicine resources; and (iii) recommendations for the construction of efficient security policies. To the best of our knowledge, this is the first paper that uses a qualitative–quantitative approach to perform a risk analysis regarding online images and online diagnosis within the telemedicine context.

This paper is structured as follows. Section 2 presents a background on telehealth services and infrastructure, cyberattacks in telemedicine services, cybersecurity regarding medical images, and the bow-tie analysis. Section 3 is dedicated to the proposed framework for cybersecurity in telemedicine. Section 4 provides an illustrative example using the proposed framework. Finally, Section 5 shows the theoretical and practical implications of the paper, and Section 6 draws some conclusions.

2. Background

2.1. Telehealth Service and Infrastructure

According to the American Telemedicine Association (ATA), telehealth can be understood as the natural evolution of healthcare in the current digital world because it uses telecommunications technologies and services to provide medical care. In this sense, telehealth can be defined as the use of a technology-based virtual platform to provide various forms of medical care and services at-a-distance, and telemedicine—telehealth's largest segment—is the use of a remote electronic interface to provide the practice of medicine [28]. Therefore, a doctor in one location can use a telecommunication infrastructure to deliver care to a patient at a distant site.

The benefits of telehealth, as related by the ATA, include: (i) value creation for payers, patients, and providers (doctors and clinicians), since it is possible to manage more information about the health status of individuals; (ii) increased patient access to medical reports; (iii) enhanced reach of healthcare services because distance care can be an effective alternative; (iv) 24/7 coverage, which represents the total availability of healthcare services online; (v) higher customer satisfaction due to a high level of communication with the doctor and reduced waiting time for the diagnosis of illnesses; and (vi) reduced cost structure due to the growing offer of technological products and infrastructure that ensure data processing in virtual scales.

A telehealth service can be identified by the communication types and resources that support the telemedicine in different contexts. Table 1 shows the communication types, telemedicine tools, and services.

Table 1. Communication types in telemedicine services [29].

Communication Types	Telemedicine Tools	Telemedicine Services
Doctor to Doctor or Medical Center	E-mail and/or video	Dermatology, radiology, surgical peer mentoring, emergency trauma, and ICU care
Doctors to Patient	Video, phone, e-mail, remote wireless monitoring, Internet	Care for chronic conditions, medication management, wound care, counseling, post-discharge follow-up, mental health
Patient to Mobile Health Technology	Wearable monitors, smartphones, mobile apps, video, e-mail, web portals, games	Health education, monitoring of physical activity, monitoring of diet, medication adherence, cognitive fitness

The functional requirement of the communication infrastructure that allows to obtain the benefits of telehealth is the proposal to integrate remote devices with electronic medical records [30]. The distribution of databases allows the storage and sharing of texts, documents, sounds, and medical images in high resolution, being able to describe, reproduce, create, represent, and simulate several diagnostics about potential diseases by doctors and clinical professionals worldwide [31].

Medical data can be structured, semi-structured or unstructured, or discrete or continuous. As a result, these features need to be considered in data analytics processing. In particular, data analytics processing in healthcare enables the analysis of large datasets from thousands of patients using various intelligent computational techniques to define standards that can assist in the development of medical reports and diagnostics, supporting resources of bioinformatics, medical imaging, medical informatics, and health informatics [32].

In recent years, experts have turned their attention to the growing risks and negative impacts that the lack of cybersecurity has caused in the evolution of business in cyberspace [33]. The lack of cybersecurity has negatively affected the trust of customers and suppliers, service efficiency, the availability of operations, the credibility of the business, and the image of the company. Considering the impact of these attacks, the cyberattacks related to medical services will be addressed in the next section.

2.2. Cyberattacks in Telemedicine Services

The lack of training, in turn, is often due to the fact that managers have not well mapped the processes inherent to telemedicine services and the respective risks to privacy and the security of the inherent information [34]. Consider the situation where the patient's medical information is transferred from one doctor to another doctor for a better solution and health treatment and classification of android malware images [35]. Several possibilities of threats, provided by the transmission of data through a communication channel, can severely affect their authenticity, integrity, and confidentiality [36].

Clinical professionals face a challenge in protecting the privacy of patients in the process of transferring the medical image diagnosis. Information management in telemedicine is a domain that requires proactive actions using techniques such as cryptography, digital signature, and anonymity. However, the scenario can be even more complex when it comes to cyberattacks. Some of these failures can be accidental, or they can be a general neglect to guarantee confidential information in telemedicine services. Figure 1 shows a cyberattack related to the communication using IT devices among clinical professionals in medical centers and patients.

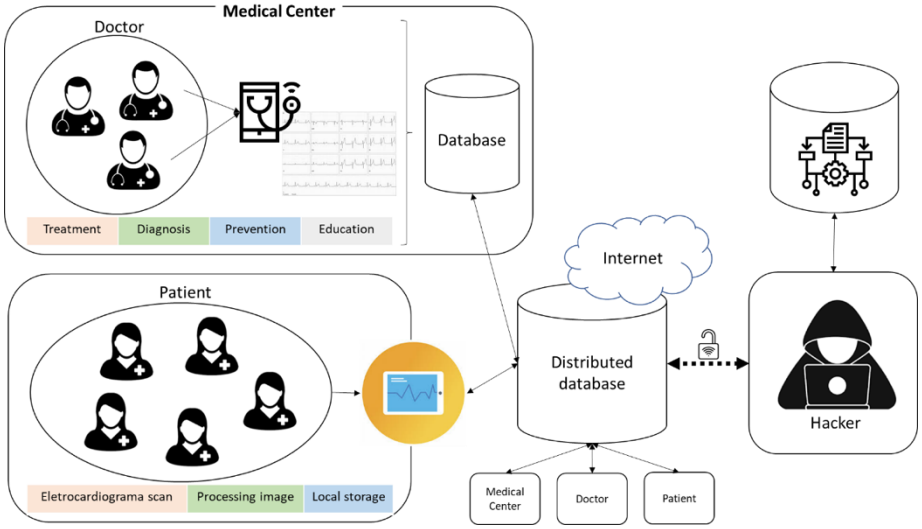

Figure 1. Cyberattacks in telemedicine services.

Effective communication in telemedicine services is supported by the infrastructure of distributed databases that, via the Internet, allows the sharing of data, texts, documents, sounds, and images. However, despite the benefits that this structure offers, there are vulnerabilities that can threaten the integrity of the stored data and cause enormous harm to patients. According to [37], four types of attacks can occur during communication established in telemedicine services: interruption, interception, modification, and fabrication.

In general, vulnerabilities are inserted into the system due to inefficiency or lack of adequate information security policies. Such vulnerabilities allow threats such as hacker actions to manipulate, steal, remove, disable, interrupt, or corrupt data, texts, documents, sounds, and images of the distributed database, causing large-scale damage and compromising the evolution of the business. Hackers, as shown in Figure 1, consider the organization's behavior, as well as vulnerable services and applications to create convincing e-mail messages to entice users to open an attachment, to visit an infected website, or to disclose security credentials in response to a contrived message. These actions are frequent attack mechanisms that have been proven to be very successful.

The risk, which is the probability that a threat exploits a certain vulnerability in a system, is associated with the manifestation of the threat [18,38,39]. Often, the risk identification is not completely known due to a lack of knowledge about when or how the threat will manifest itself in the system. For example, there are no precise standards for

identifying when a hacker will act and corrupt images in a medical database. However, it is possible to classify risks by the different causes of losses or their impacts or consequences in a given system. Particularly, in telemedicine services, there are concerns about the integrity of medical images and diagnoses.

It is worth stating that the analysis of cybersecurity risk regarding medical images is highlighted by normative documents to IT managers in reducing or eliminating adverse events in telemedicine services. Therefore, the next subsection is dedicated to the topic of cybersecurity risk regarding medical images including information about norms and techniques in which cybersecurity in telemedicine can be based on to minimize risks.

2.3. Cybersecurity Risk Regarding Medical Images

Despite the advantages conferred by telehealth, attention must be paid to information security issues. When healthcare practices are performed using the Internet and all information is electronic, ensuring the security and privacy of clinical information becomes more complex. As previously mentioned, this is partly because most health professionals are not trained in protecting the security and privacy of patients in cyberspace. To make things worse, there are many methods that can be used to break into the electronic system and gain unauthorized access to a large amount of health information.

Due to the negative impact that cyberattacks can have on telemedicine services, there are some methods and techniques to ensure the protection of medical images, including discrete wavelet transform (DWT) [40–42] chaos system (CS) [43,44] zero watermarking [45] SDGOEF (Shearlets and DRPE-based generalized optical encryption framework) [46], support vector machine (SVM) [47,48], fuzzy C-means clustering (FCM) [26,48]; Internet of Medical Things–security assessment framework (IoMT-SAF) [49], fuzzy chaotic maps [42], neural network (NN) [41,50], RSA encryption [41]; quantum walks [51], and Multiple Image Owners with Privacy Protection (MIPP) [52].

In recent years, various safety parameters and standards have been developed by agencies, institutes, and researchers to protect medical information in telemedicine services [53]. For instance, in 2008, the first safety standard for medical images, known as ISO 27799:2008, was created by the International Organization for Standardization (ISO). Although the ISO rules provide a standard for regulating the collection and dissemination of health information, several countries have developed their own safety standards for medical imaging. For example, in the USA, in addition to the use of ISO standards, the Health Insurance Portability and Accountability Act (HIPAA) was created to provide privacy and security rules and regulations to protect PHI (protected health information) available to insurance providers as properly governed. The European Union (EU) launched the GDPR (General Data Protection Regulation), which protects all personal data belonging to users residing in the EU and meets the challenges of personal health data protection.

With a focus on risk management in telemedicine service, ISO/TS 13131:2014 [54] stands out for being the most used standard. This norm provides advice and recommendations on how to develop quality objectives and guidelines for telehealth services that use information and communications technologies (ICTs) to deliver healthcare over both long and short distances by using a risk management process. Due to these factors, ISO/TS 13131:2014 will be used as a reference for the framework proposed herein.

Finally, the main control measures adopted to provide security to medical images in telemedicine are watermarking, digital fingerprinting, encryption, and digital signature algorithm. The adoption of these techniques is associated with the main objectives of ensuring the security of medical information. In this sense, Ref. [55] argue that in the process of ensuring information security in telemedicine services, three characteristics related to the types of attacks covered in Section 2.2 are mandatory: confidentiality; reliability which addresses integrity and authentication; availability.

Besides the technical aspects of medical image cybersecurity, it is worth stating the importance of using a risk assessment method to deal with cybersecurity within telemedicine.

Thus, the bow-tie analysis is presented in the next section along with the reasons why this methodology is suitable for the telemedicine context.

2.4. Bow-Tie Analysis

Many risk assessment methods including qualitative and quantitative techniques, such as checklists, hazard and operability study (HAZOP), fault tree analysis (FTA), event tree analysis (ETA), failure mode and effect analysis (FMEA), and hazard indices, have been designed for risk assessment in several contexts. In a general way, the bow-tie approach was created for security management and used mainly to identify threats, analyze barriers, and assess operational risks. In this sense, bow-tie analysis, which is a combination of FTA and ETA, is very popular because it incorporates both the causes and consequences of the incident scenario and can be used to assess all kinds of risks such as the ones regarding gas and oil pipelines [56,57], occupational risks [58], and industrial risks [59,60].

The bow-tie diagram is designed in a way that the fault tree (FT) is placed on the left side and the event tree (ET) is placed on the right side. On the one hand, the FT starts with the critical event (top risk event) [61] and goes to the left side until the intermediate causes are described in terms of basic events with the use of logical connections of type "AND" and "OR". On the other hand, the ET starts with the same critical event (top risk event) and follows the sequence of events to the right side using "AND" connections until it reaches the final outcome events. Figure 2 shows a general FT, and Figure 3 shows a general ET.

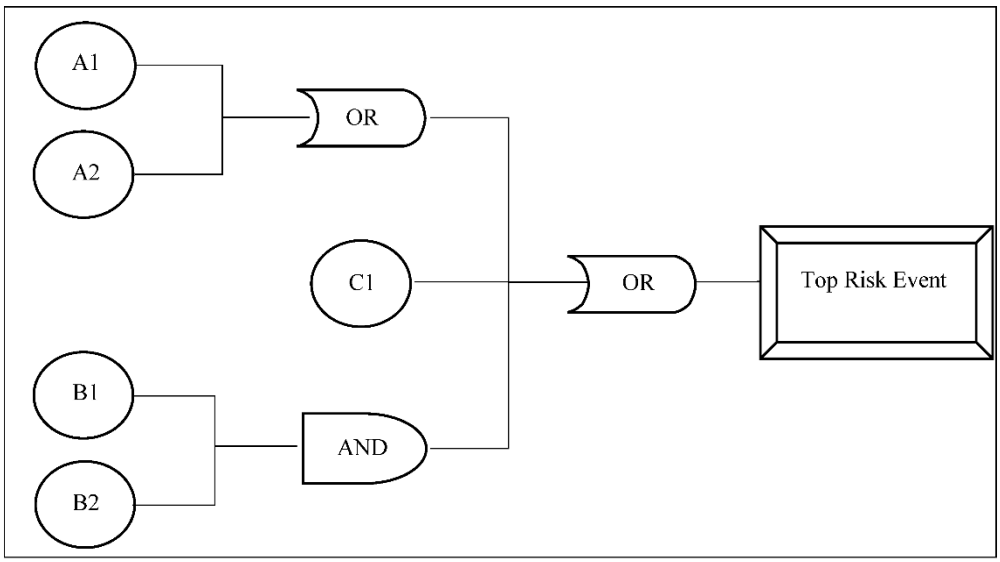

Figure 2. General fault tree.

With regard to an FT, the output of an *OR* gate occurs if some input occurs, and the output of an *AND* gate occurs if all inputs occur. Therefore, given the estimated probabilities of occurrence for risk factors and using the FT of the corresponding bow-tie diagram, the probability of occurrence for the risk event can be calculated assuming that the risk factors are independent. This is the default assumption of a traditional bow-tie analysis. However, several approaches can be used to assume that there are relationships among failure events such as correlation [56] and conditional probability [60]. Thus, the probabilities of an *OR* gate and an *AND* gate are calculated, respectively, as:

$$P_{OR} = \sum_{i=1}^{n} p_i \,, \tag{1}$$

$$P_{AND} = \prod_{i=1}^{n} p_i, \tag{2}$$

where i is a specific basic event, n is the total number of basic events which generate the risk event under analysis, and p_i is the probability of occurrence of the basic event i. For instance, the probability of occurrence of the top risk event in Figure 2 is:

$$P_{RE} = (P_{A_1} \times P_{A_2}) + P_{C_1} + (P_{B_1} \times P_{B_2}). \quad (3)$$

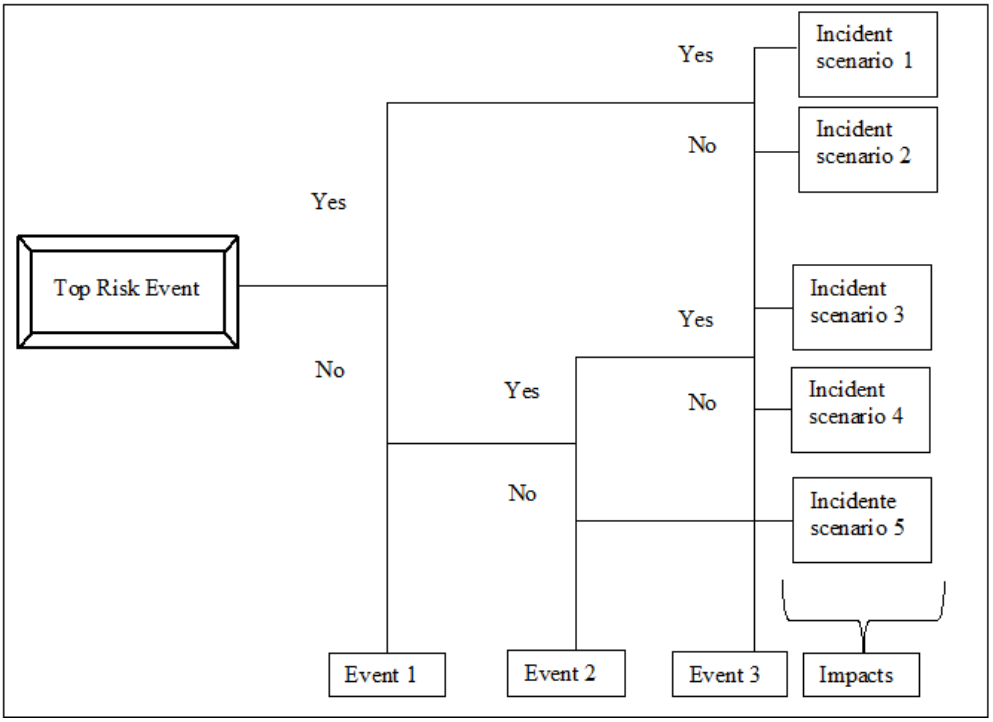

Figure 3. General event tree.

With regard to an ET, different incident scenarios may result from a combination of events following a top risk event. Moreover, the ET considers binary situations such as "Yes" and "No" to propagate the intermediate events until all possible output events are represented in the bow-tie diagram. The severity of the outcomes can be calculated according to the impacts that they can generate. Normally, the impacts are regarding economic, environmental, social, and political aspects (among others).

3. Proposed Framework for Cybersecurity in Telemedicine

According to [54], which provides advice and recommendations on how to develop quality objectives and guidelines for telehealth services that use ICTs, and based on ISO 31100:2018, which provides general guidelines for risk management, the risk management process involves: (i) the systematic application of policies, procedures, and practices for the communication and inquiry activities related to risks; (ii) the establishment of context and evaluation of risks; and (iii) the treatment, monitoring, critical analysis, recording and reporting of risks. Moreover, with a focus on (ii), the risk assessment process comprises the identification of risks, risk analysis, and risk evaluation as shown in Figure 4.

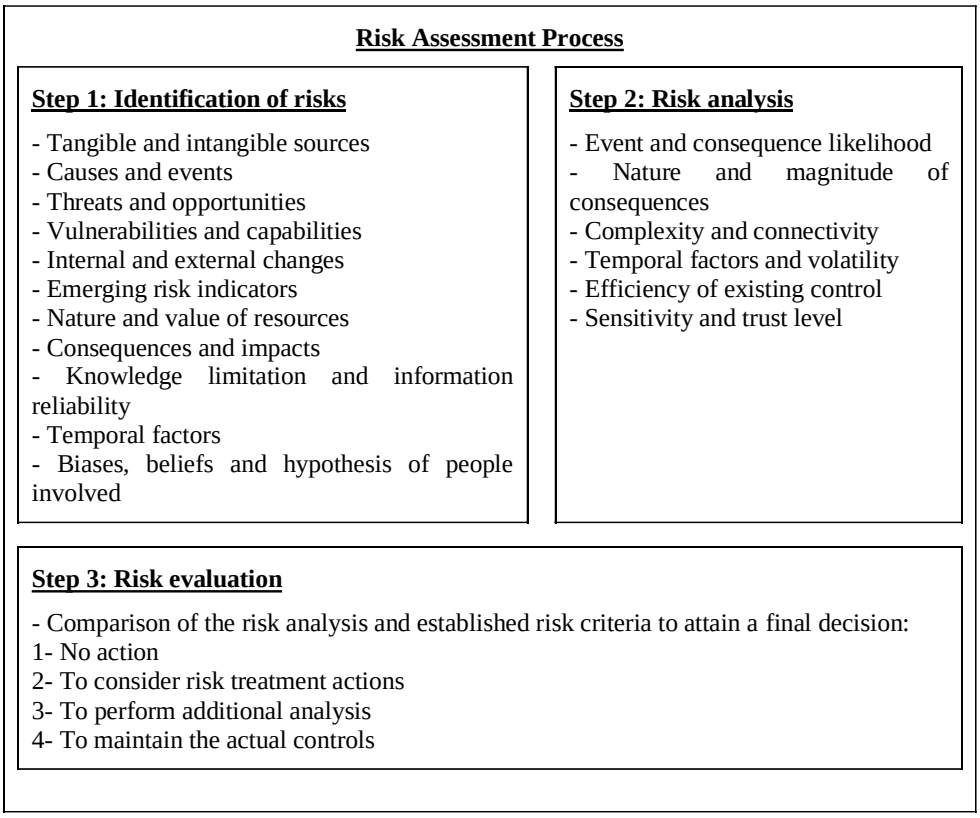

Figure 4. Three steps of the risk assessment process (Source: ISO/TS 13131:2014).

Following the steps of the risk assessment process proposed in ISO/TS 13131:2014, the framework for cybersecurity in telemedicine proposed in this paper comprising three steps is shown in Figure 5.

In Step 1, the identification of risk is conducted using a bow-tie analysis. This step is very critical because it is responsible for the identification of causes (which can be of three types: primary, intermediate, and top), preventive barriers, mitigating barriers, consequences, and the connections among them. In Step 2, the risk analysis is performed using likelihood of causes and severity of consequences. The likelihood of causes can be obtained by using past data regarding incident or expert knowledge. Finally, in Step 3, the risk evaluation is made integrating the risk analysis of Step 2 into a risk matrix where the two axes are: x—severity of consequences and y—probabilities of causes. Then, the established ranking criteria for risk are used to recommend a final decision which can be: (i) to take no action; (ii) to consider risk treatment actions; (iii) to perform additional analysis; and (iv) to maintain actual controls. The next section presents an illustrative example of how the proposed framework can be used for risk management in telemedicine.

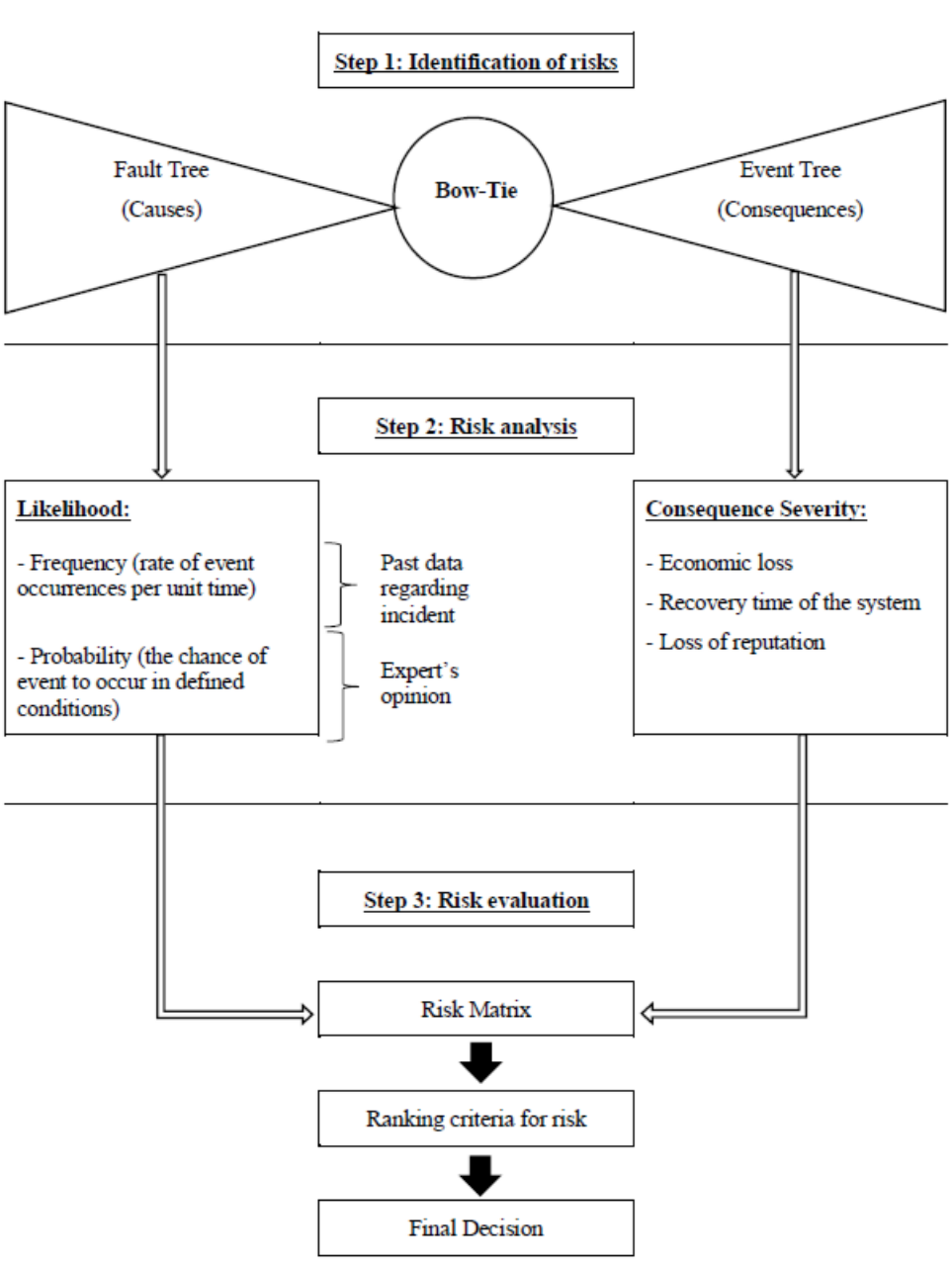

Figure 5. Proposed framework for cybersecurity in telemedicine.

4. Results and Discussion

The idea of this section is to show how the proposed model can assist managers in identifying risks to information security when providing health services. Based on the framework proposed (Figure 5), managers will be able to develop preventive and mitigating actions to be implemented by numerous health professionals. Therefore, a bow-tie analysis for cybersecurity in telemedicine is performed based on Figure 5, as follows.

4.1. Step 1: Identifications of Risks

Cyberattacks can cause serious consequences such as information dissemination, falsification, service failure, server congestion, and changes in medical image resolution. In this way, the bow-tie methodology contributes to improve cybersecurity practices in telemedicine, which is affected by several factors including training rate, security policies, security certification, risk management capacity, IT governance, and management security costs [60]. The bow-tie model for cybersecurity in telemedicine is based on the related

literature (which are shown in Tables 2 and 3). The main critical elements in telemedicine cybersecurity can be divided according to Figure 6: causes (and/or gates, basic and intermediate failure events) consequences (events and incident scenarios), preventive cybersecurity, and mitigating cybersecurity.

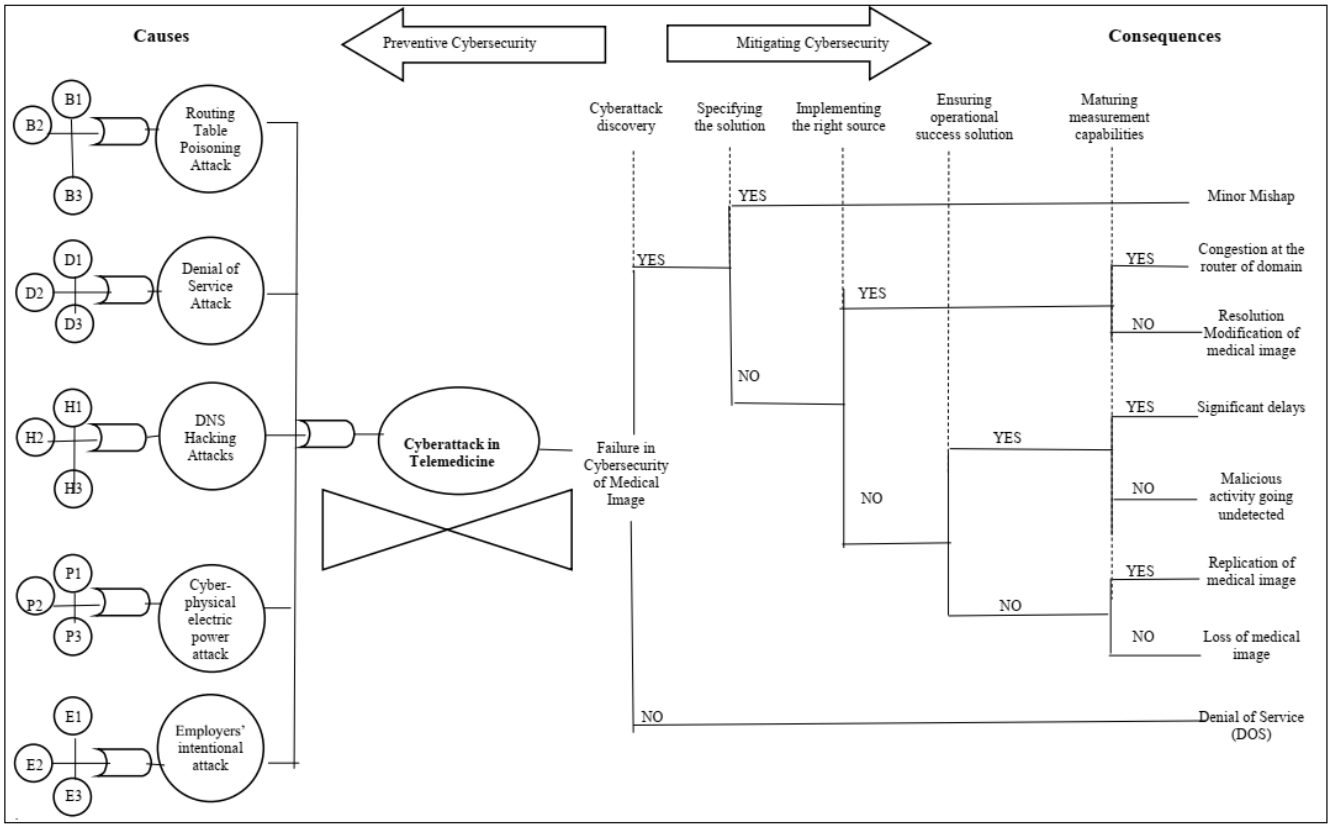

Figure 6. Bow-tie risk analysis for cybersecurity in telemedicine.

Table 2. Failure events of cyberattacks in telemedicine.

Causes	References	Index	Failure Events of Cyberattacks in Telemedicine
Routing Table Poisoning Attacks	[24,59]	B1	Lack of node authentication
		B2	Updating routing table
		B3	Lack of verifying peers in index table
Denial of Service Attack	[60,61]	D1	Smurf attack
		D2	SYN flood
		D3	Botnets
DNS Hacking Attacks	[62,63]	H1	Cybersquatting
		H2	Human attacks
		H3	Authentication vulnerability
Cyber-Physical Electric Power	[61,64]	P1	Inadequate periodic security audits
		P2	Inadequate incident response process
		P3	Insufficient redundancy
Employers' Intentional Attacks	[17,19,23]	E1	Insufficient trained personnel
		E2	Inadequate security awareness program
		E3	Third party as an agent of the utility having access to patient

Table 3. Preventive and mitigating cybersecurity.

Category	References	Preventive and Mitigating Cybersecurity	Description
Access Control	[61–65]	Notification of System Use	Granting access to the system that provides privacy and consistent security notices.
		Previous Logon (Access) Notification	Applicable to logons to information systems via human user interfaces.
		Session Termination	System automatically terminates a user session
		Remote Access	Establishes usage restrictions, configuration/connection requirement, privileged commands, monitoring for unauthorized connections, disable access.
Awareness and Training	[32,33]	Security Awareness Training	Provides basic security awareness training to information system users.
		Role-Based Security Training	Provides role-based security training to personnel with assigned security roles and responsibilities.
Audit and Accountability	[32–37]	Audit Events, Review, Analysis, and Reporting	Generates audit records containing information that establishes what type of event occurred, when the event occurred, and where the event occurred.
		Monitoring for Information Disclosure	Organization monitors evidence of unauthorized disclosure of organizational information.
Security Assessment and Authorization	[35]	System Interconnections	Control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as e-mail and website browsing.
		Security Authorization	Management decisions, conveyed through authorization decision documents.
		Continuous Monitoring	Programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.
		Penetration Testing	Specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries.
Configuration Management	[21,65]	Information System Component Inventory	Control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities.
		Software Usage Restrictions	Provided under software license agreements that permit individuals to study, change, and improve the software.
		Security Impact Analysis	Organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Table 3. *Cont.*

Category	References	Preventive and Mitigating Cybersecurity	Description
Identification and Authentication	[61,62]	Device Identification and Authentication	Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device.
		Service Identification and Authentication	Architectural approaches requiring the identification and authentication of information system services.
		Cryptographic Module Authentication	Information system implements mechanisms for authentication to a cryptographic module.
Physical and Environmental Protection	[48,60]	Physical Access Authorizations	Control applies to organizational employees and visitors; individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors.
		Fire Protection	Fire suppression and detection devices/systems for the information system that are supported by an independent energy source.
		Emergency Power	Provides a short-term uninterruptible power supply to facilitate in the event of a primary power source loss.
		Temperature and Humidity Controls	Control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms
System and Communications Protection	[16]	Trusted Path	Information system establishes a trusted communications path between the user and the following security functions of the system.
		Cryptographic Protection	Establishes and manages cryptographic keys for required cryptography employed within the information system.
		Mobile Code	Information systems are based on the potential for the code to cause damage to the systems if used maliciously.

Traditional information security assessments provide only a simple analysis of a critical event and do not effectively reveal the causes and consequences necessary to improve the transfer of medical images. Therefore, selecting appropriate cybersecurity control actions for telemedicine is an important task that requires a fundamental understanding of the organization's business priorities. This understanding can demonstrate how to ensure more confidentiality, integrity, and availability of information effectively.

In this work, we analyze a critical event—a cyberattack in telemedicine—using the bow-tie methodology, to identify: (i) the causes (to act preventively) and (ii) the consequences (to provide a correction plan) of telemedicine cybersecurity. First, preventive cybersecurity (left part of Figure 6) can be performed by outlining the main causes of a cyberattack in telemedicine and the failure events from which they originate. This information is shown in Table 2 along with literature references and the index used in Figure 6.

Second, organizations that adopt telemedicine practices must adequately mitigate the risks arising from the use of IT in the execution of their business functions while keeping their commitment to patients. Thus, mitigating cybersecurity (the right part of Figure 6) can also be done to provide a continuity plan for the health provider. In this way, the control analysis prescribes actions related to cybersecurity to be performed in telemedicine. The specification provides safety capability instructions to: (i) add control functionality/specificity; and/or (ii) increase the control force, due to possible adverse organizational impacts based on organizational risk assessments (Table 3). These instructions include both preventive and mitigating barriers.

4.2. Step 2: Risk Analysis

Based on Figure 6 and in possession of available data regarding likelihood of failures and severity of consequences, a risk analysis can be performed. First, as shown in Figure 5, the likelihood of failures can be obtained by two ways: past data regarding past failure events or expert knowledge. The probability of each intermediate failure cause can be calculated by using Equations (2) and (3). Table 4 shows these probabilities.

Table 4. Probability of causes that lead to cyberattacks in telemedicine.

Intermediate Causes	Index	Basic Failure Events	Gate Type	Probability
Routing Table Poisoning Attacks	B1 B2 B3	Lack of node authentication Updating routing table Lack of verifying peers in index table	*OR*	$P_{B1} + P_{B2} + P_{B3}$
Denial of Service Attack	D1 D2 D3	Smurf attack SYN flood Botnets	*OR*	$P_{D1} + P_{D2} + P_{D3}$
DNS Hacking Attacks	H1 H2 H3	Cybersquatting Human attacks Authentication vulnerability	*OR*	$P_{H1} + P_{H2} + P_{H3}$
Cyber-Physical Electric Power	P1 P2 P3	Inadequate periodic security audits Inadequate incident response process Insufficient redundancy	*OR*	$P_{P1} + P_{P2} + P_{P3}$
Employers' Intentional Attacks	E1 E2 E3	Insufficient trained personnel Inadequate security awareness program Third party as an agent of the utility having access to patient	*OR*	$P_{E1} + P_{E2} + P_{E3}$

Second, the severity of consequences can be estimated according to some criteria such as economic loss (in monetary units), recovery time of the system (in time units), and loss of reputation (number of dissatisfied patients). For instance, the impact of each incident scenario according to each criterion can be calculated by the expected value, which is the product of the probability of each event and the estimated loss in the corresponding units.

The aggregation of each impact into a unique measure can be done as in [19]. Table 5 presents how the severity of consequences of incident scenarios can be calculated.

Table 5. Failure events of cyberattacks in telemedicine.

Incident Scenarios	Incident Events	Gate Type
Minor mishap	• Cyberattack discovery • Specification of a solution	*AND*
Congestion at the router of domain	• Cyberattack discovery • Implementation of the right source • Maturation of measurement capabilities	*AND*
Resolution modification of medical image	• Cyberattack discovery • Implementation of the right source	*AND*
Significant delays	• Cyberattack discovery • Ensuring operational success solution • Maturation of measurement capabilities	*AND*
Malicious activity undetected	• Cyberattack discovery • Ensuring operational success solution	*AND*
Replication of medical image	• Cyberattack discovery • Maturation of measurement capabilities	*AND*
Loss of medical image	• Cyberattack discovery	*AND*
Denial of service (DoS)	• Failure in cybersecurity of medical image	*AND*

4.3. Step 3: Risk Evaluation

After the calculation of the probability of causes and severity of consequences, a risk matrix can be obtained (Figure 7), and the risks can be classified into levels ranging from very low to very high. For instance, as can be seen in Figure 7, risks can be classified as being low if the probability of occurrence of causes are low or medium and the severity of consequences are low or medium. Finally, a final decision can be recommended as a result of risk evaluation (Figure 4).

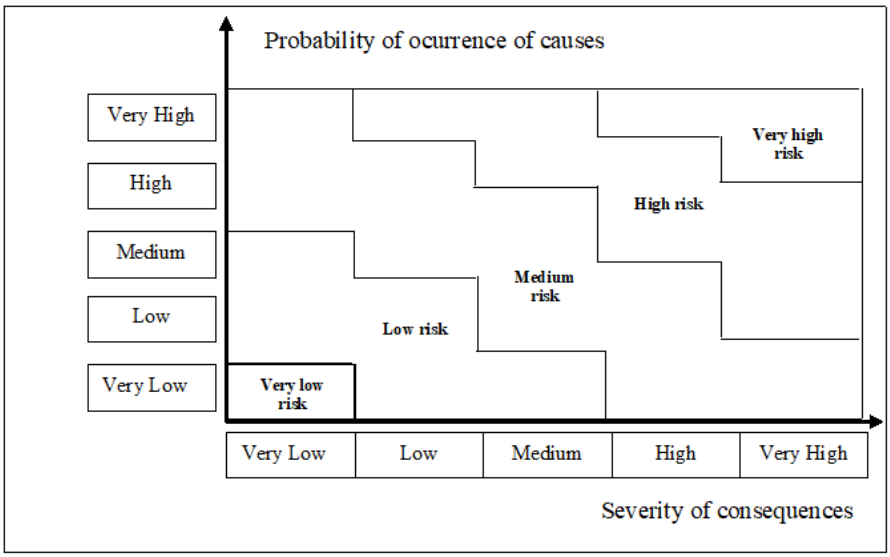

Figure 7. A 5 × 5 risk matrix for cybersecurity in telemedicine.

5. Theoretical and Practical Implications

This paper has both theoretical implications for the cybersecurity literature and practical implications for IT managers. First, the existing cybersecurity literature mainly focuses on: (i) individual solutions to improve the automatic detection system [21,22,61]; (ii) presentation of cybersecurity architecture and standards [23,62,63], and (iii) development of algorithms for medical image encryption [64–66]. Therefore, despite the existence of many studies on cybersecurity, this study provides theoretical contributions to cybersecurity literature because it is the first paper that incorporates a qualitative–quantitative methodological approach designed for medical image security.

The causes related to the problems of routing table poisoning attacks, denial of service attacks, DNS haching attacks, cyber-phsical eletric power, employer's intentional attacks. These factors, if not controlled, generate increased costs. The study by [18] identified some causes related to human error. They justified, in a function of current attacks that are more exposed to risks and uncertainties due to complexity in planning and design. Barriers were also established in telemedicine, in order to neutralize or minimize it. The main barriers were directed to investment in technology and operations monitoring actions. The use of performance indicators allows to verify how the process is behaving and, therefore, allows its flaws to be identified.

The remaining suggestions audit, security assessment, access control, provide cybersecurity advancement in telemedicine, such as the use of software. These solutions may not be low-cost or are complicated to implement but are worth investigating further to enhance the current controls in place for the hazards considered.

Second, with regard to the practical implications, the present study presents a framework with an integrated view to identify potential risks in cybersecurity related to the provision of telemedicine services that can be implemented in practice and that at the same time helps IT managers in clarifying the role of cybersecurity actions in real risk situations.

Given this context, safety guidelines help the flow of reports and improve efficient communication, consequently enhancing IT risk management and the efficiency of the medical center in carrying out more accurate diagnoses. More precisely, the results from this study generated some insights that allow IT managers to improve cybersecurity policies in order to provide privacy guidelines to help organizations ensure confidentiality, availability, and integrity in telemedicine services.

Another important point is that, currently, organizations do not always adopt defined and regulated cybersecurity standards, which can result in negative consequences for the remote healthcare system. In this sense, this study may help organizations in establishing a systematic way to perform cybersecurity within telemedicine. Thus, it is yet another contribution to the healthcare industry.

Finally, this study can also be valuable for patients when it helps to clarify important aspects to ensure the privacy of personal data by promoting value in the provision of remote medical care and encouraging patients to become users of telemedicine services. The next section draws some conclusions and presents limitations and future works.

6. Conclusions, and Future Works

In general, identifying effective actions for operational cybersecurity prevention is a challenge for organizations that design, implement, and operate complex information systems with several integrated hardware and software components. In many cases, cyberattacks occur due to the lack of adequate information security policies and the lack of understanding of IT resources by users.

In the context of healthcare services, telemedicine solutions are, by nature, an integration of different parts and environments using remote devices and the Internet, to maintain efficient communication between the agents involved in the process of distance healthcare. Thus, there is a concern that IT managers must be able to understand the threats and risks during the process of developing cybersecurity policies to ensure the protection of patients' personal data. From this perspective, the most relevant contribution of this paper is the

identification of causes, consequences, and preventive and mitigating measures for threats that in some situations are neglected due to the complexity of a cybersecurity system in telemedicine services.

In particular, although the transmission of medical images online is arousing great interest, the images are vulnerable when they are stored in hospital storage or when they are transferred over an open transmission medium in various telemedicine applications. Cyberattacks are a problem that affects the health sector and can be life-threatening due to vulnerabilities in the telemedicine system. So, when implementing risk assessment measures in cybersecurity, it is possible to design an IT service level that ensures the security and privacy of information and maintains the reputation of healthcare organizations.

Therefore, our proposed framework focuses on a multidimensional view of prevention to be applied to the context of telemedicine and consists of a set of policies and procedures to implement cybersecurity controls that prevent breaches of privacy and misuse or malicious use. It also emphasizes the importance of understanding cyberattack threats and allows structured visualization to help IT managers to better plan and improve the security of telemedicine systems regarding vulnerabilities. More particularly, the bow-tie approach was applied to identify the most critical causes of cyberattack scenarios and to quantify their consequences regarding medical image sharing.

Hospital companies, do not invest in cybersecurity training their staff to train their employees in all necessary processes, especially when there is a high turnover of manual labor, but also in the management. In general, these professionals lack adequate training during the work, but they have little or no knowledge about the physical, and characteristics of each type of software. In addition, investment in cybersecurity training is fundamental to change general behavior in changing organizational culture.

Therefore, we suggest that the main obstacles to implementing cybersecurity in telemedicine are: lack of planning for a cybersecurity project; lack of compliance with pre-established technical standards; choosing inappropriate software; lack of technical knowledge of the physical telemedicine about operations and services; lack of incentives and regulations aimed at cybersecurity

The proposed structure encourages the use of historical data or the knowledge of experts to carry out an analysis on the occurrence of risks and to indicate the relationship between the probability of causes and the severity of the consequences of cyberattacks. Thus, the risk matrix is integrated to provide the classification of the estimated risk and indicate the best recommendation for the decision on mitigating threats to telemedicine services. The applicability of the new framework proposal was done by means of an illustrative example. The main suggestion for future research is real-time implementation of data hiding techniques using new watermark techniques based on machine learning algorithms.

Author Contributions: Conceptualization, T.P., T.R.N.C. and A.P.d.B.A.; investigation, T.R.N.C.; methodology, M.M.S.; validation, T.P., A.P.H.d.G., and M.M.S.; resources, T.P.; supervision, A.P.C.S.C.; visualization, T.P.; writing, original draft preparation, T.P., M.M.S., T.R.N.C., and A.P.H.d.G.; writing, review and editing, T.P., M.M.S., T.R.N.C., and A.P.H.d.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The authors would also like to thank the Federal University of Pará (UFPA) and and GPSID–a decision and information systems research group supporting this research project. The authors would like to acknowledge FACEPE, the scientific foundation of the state of Pernambuco, and the Brazilian National Research Council (CNPq) for their financial support.

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

References

1. Shah, N.H.; Bhansali, P.; Barber, A.; Toner, K.; Kahn, M.; MacLean, M.; Kadden, M.; Sestokas, J.; Agrawal, D. Children with Medical Complexity: A Web-Based Multimedia Curriculum Assessing Pediatric Residents Across North America. *Acad. Pediatr.* **2018**, *18*, 79–85. [CrossRef] [PubMed]
2. Wolbrink, T.A.; Burns, J.P. Internet-Based Learning and Applications for Critical Care Medicine. *J. Intensive Care Med.* **2012**, *27*, 322–332. [CrossRef] [PubMed]
3. Lv, Z.; Wang, J.J.; Yin, T. Editorial: Recent research in medical technology based on multimedia and pattern recognition. *Neurocomputing* **2017**, *220*, 1–4. [CrossRef]
4. Ahmed, O.B.; Benois-Pineau, J.; Allard, M.; Catheline, G.; Amar, C. Ben Recognition of Alzheimer's disease and Mild Cognitive Impairment with multimodal image-derived biomarkers and Multiple Kernel Learning. *Neurocomputing* **2017**, *220*, 98–110. [CrossRef]
5. Hao, S.; Wang, W.; Yan, Y.; Bruzzone, L. Class-wise dictionary learning for hyperspectral image classification. *Neurocomputing* **2017**, *220*, 121–129. [CrossRef]
6. Wisniewski, R.; Grobelna, I.; Karatkevich, A. Determinism in Cyber-Physical Systems Specified by Interpreted Petri Nets. *Sensors* **2020**, *20*, 5565. [CrossRef]
7. Wong, T.C.; Ngan, S.C.; Chan, F.T.S.; Chong, A.Y.L. A two-stage analysis of the influences of employee alignment on effecting business-IT alignment. *Decis. Support Syst.* **2012**, *53*, 490–498. [CrossRef]
8. Doi, K. Computer-aided diagnosis in medical imaging: Historical review, current status and future potential. *Comput. Med. Imaging Graph.* **2007**, *31*, 198–211. [CrossRef]
9. Osteaux, M.; Van den Broeck, R.; Verhelle, F.; de Mey, J. Picture archiving and communication system (PACS): A progressive approach with small systems. *Eur. J. Radiol.* **1996**, *22*, 166–174. [CrossRef]
10. Kapoor, D. Picture Archiving and Communication Systems (PACS)—A New Paradigm in Healthcare. *Apollo Med.* **2010**, *7*, 181–184. [CrossRef]
11. Whiteman, I.A. The decline of medical confidentiality medical information management: The illusion of patient choice. *Clin. Ethics* **2015**, *10*, 47–58. [CrossRef]
12. Li, D.; Liao, X.; Xiang, T.; Wu, J.; Le, J. Privacy-preserving self-serviced medical diagnosis scheme based on secure multi-party computation. *Comput. Secur.* **2020**, *90*, 101701. [CrossRef]
13. Guo, W.; Shao, J.; Lu, R.; Liu, Y.; Ghorbani, A.A. A Privacy-Preserving Online Medical Prediagnosis Scheme for Cloud Environment. *IEEE Access* **2018**, *6*, 48946–48957. [CrossRef]
14. Akkasaligar, P.T.; Biradar, S. Selective medical image encryption using DNA cryptography. *Inf. Secur. J.* **2020**, *29*, 91–101. [CrossRef]
15. Zhang, Y. The fast image encryption algorithm based on lifting scheme and chaos. *Inf. Sci.* **2020**, *520*, 177–194. [CrossRef]
16. Anand, A.; Singh, A.K. An improved DWT-SVD domain watermarking for medical information security. *Comput. Commun.* **2020**, *152*, 72–80. [CrossRef]
17. Diaz, A.; Sanchez, P. Simulation of Attacks for Security in Wireless Sensor Network. *Sensors* **2016**, *16*, 1932. [CrossRef]
18. Liginlal, D.; Sim, I.; Khansa, L. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Comput. Secur.* **2009**, *28*, 215–228. [CrossRef]
19. Henriques de Gusmão, A.P.; Mendonça Silva, M.; Poleto, T.; Camara e Silva, L.; Cabral Seixas Costa, A.P. Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *Int. J. Inf. Manag.* **2018**, *43*, 248–260. [CrossRef]
20. Anwar, M.; He, W.; Ash, I.; Yuan, X.; Li, L.; Xu, L. Gender difference and employees' cybersecurity behaviors. *Comput. Hum. Behav.* **2017**, *69*, 437–443. [CrossRef]
21. Cruz, T.; Rosa, L.; Proenca, J.; Maglaras, L.; Aubigny, M.; Lev, L.; Jiang, J.; Simões, P. A Cybersecurity Detection Framework for Supervisory Control and Data Acquisition Systems. *IEEE Trans. Ind. Inform.* **2016**, *12*, 2236–2246. [CrossRef]
22. Foroutan, S.A.; Salmasi, F.R. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method. *IET Cyber-Phys. Syst. Theory Appl.* **2017**, *2*, 161–171. [CrossRef]
23. Santos, J.R.; Haimes, Y.Y.; Lian, C. A framework for linking cybersecurity metrics to the modeling of macroeconomic interdependencies. *Risk Anal.* **2007**, *27*, 1283–1297. [CrossRef]
24. Timmers, P. Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds Mach.* **2019**, *29*, 635–645. [CrossRef]
25. Ten, C.W.; Ginter, A.; Bulbul, R. Cyber-Based Contingency Analysis. *IEEE Trans. Power Syst.* **2016**, *31*, 3040–3050. [CrossRef]
26. Mahmood, Y.A.; Ahmadi, A.; Verma, A.K.; Srividya, A.; Kumar, U. Fuzzy fault tree analysis: A review of concept and application. *Int. J. Syst. Assur. Eng. Manag.* **2013**, *4*, 19–32. [CrossRef]
27. Poleto, T.; de Oliveira, R.C.P.; da Silva, A.L.B.; de Carvalho, V.D.H. Using Fuzzy Cognitive Map Approach for Assessing Cybersecurity for Telehealth Scenario. In *World Conference on Information Systems and Technologies*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 828–837.
28. Herland, M.; Bauder, R.A.; Khoshgoftaar, T.M. Approaches for identifying U.S. medicare fraud in provider claims data. *Health Care Manag. Sci.* **2020**, *23*, 2–19. [CrossRef] [PubMed]
29. Mechanic, O.J.; Kimball, A.B. *Telehealth Systems*; StatPearls: Treasure Island, FL, USA, 2019.
30. Tuckson, R.V.; Edmunds, M.; Hodgkins, M.L. Telehealth. *N. Engl. J. Med.* **2017**, *377*, 1585–1592. [CrossRef] [PubMed]

31. Watzlaf, V.J.M.; Zhou, L.; DeAlmeida, D.R.; Hartman, L.M. A Systematic Review of Research Studies Examining Telehealth Privacy and Security Practices Used By Healthcare Providers. *Int. J. Telerehabilit.* **2017**, *9*, 39–58. [CrossRef] [PubMed]
32. Ristevski, B.; Chen, M. Big Data Analytics in Medicine and Healthcare. *J. Integr. Bioinform.* **2018**, *15*. [CrossRef]
33. Cabaj, K.; Domingos, D.; Kotulski, Z.; Respício, A. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Comput. Secur.* **2018**, *75*, 24–35. [CrossRef]
34. Enamamu, T.; Otebolaku, A.; Marchang, J.; Dany, J. Continuous m-Health Data Authentication Using Wavelet Decomposition for Feature Extraction. *Sensors* **2020**, *20*, 5690. [CrossRef] [PubMed]
35. Zain, J.; Clarke, M. Security in telemedine: Issues in watermarking medical images. In Proceedings of the 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, Susa, Tunisia, 27–31 March 2005.
36. Silva, M.M.; De Gusmão, A.P.H.; Poleto, T.; Silva, L.C.E.; Costa, A.P.C.S. A multidimensional approach to information security risk management using FMEA and fuzzy theory. *Int. J. Inf. Manag.* **2014**, *34*, 733–740. [CrossRef]
37. De Gusmão, A.P.H.; E Silva, L.C.; Silva, M.M.; Poleto, T.; Costa, A.P.C.S. Information security risk analysis model using fuzzy decision theory. *Int. J. Inf. Manag.* **2016**, *36*. [CrossRef]
38. Arunkumar, S.; Subramaniyaswamy, V.; Vijayakumar, V.; Chilamkurti, N.; Logesh, R. SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. *Measurement* **2019**, *139*, 426–437. [CrossRef]
39. Nagpal, S.; Bhushan, S.; Mahajan, M. An Enhanced Digital Image Watermarking Scheme for Medical Images using Neural Network, DWT and RSA. *Int. J. Mod. Educ. Comput. Sci.* **2016**, *8*, 46–56. [CrossRef]
40. Lakshmi, C.; Thenmozhi, K.; Rayappan, J.B.B.; Amirtharajan, R. Encryption and watermark-treated medical image against hacking disease—An immune convention in spatial and frequency domains. *Comput. Methods Programs Biomed.* **2018**, *159*, 11–21. [CrossRef]
41. Ismail, S.M.; Said, L.A.; Radwan, A.G.; Madian, A.H.; Abu-ElYazeed, M.F. A novel image encryption system merging fractional-order edge detection and generalized chaotic maps. *Signal. Process.* **2020**, *167*, 107280. [CrossRef]
42. Liu, H.; Kadir, A.; Liu, J. Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system. *Opt. Lasers Eng.* **2019**, *122*, 123–133. [CrossRef]
43. Roček, A.; Slavíček, K.; Dostál, O.; Javorník, M. A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters. *Biomed. Signal. Process. Control* **2016**, *29*, 44–52. [CrossRef]
44. Chen, M.; Ma, G.; Tang, C.; Lei, Z. Generalized optical encryption framework based on Shearlets for medical image. *Opt. Lasers Eng.* **2020**, *128*, 106026. [CrossRef]
45. MingRu, K.; Zheng, Q.; Kui Yan, S.; Arunkumar, N. Medical image classification algorithm based on principal component feature dimensionality reduction. *Future Gener. Comput. Syst.* **2019**, *98*, 627–634. [CrossRef]
46. Marwan, M.; Kartit, A.; Ouahmane, H. Security Enhancement in Healthcare Cloud using Machine Learning. *Procedia Comput. Sci.* **2018**, *127*, 388–397. [CrossRef]
47. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Int. Things* **2019**, *8*, 100123. [CrossRef]
48. Fourcade, A.; Khonsari, R.H. Deep learning in medical image analysis: A third eye for doctors. *J. Stomatol. Oral Maxillofac. Surg.* **2019**, *120*, 279–288. [CrossRef]
49. Jafari Barani, M.; Yousefi Valandar, M.; Ayubi, P. A new digital image tamper detection algorithm based on integer wavelet transform and secured by encrypted authentication sequence with 3D quantum map. *Optik* **2019**, *187*, 205–222. [CrossRef]
50. Shen, M.; Cheng, G.; Zhu, L.; Du, X.; Hu, J. Content-based multi-source encrypted image retrieval in clouds with privacy preservation. *Futur. Gener. Comput. Syst.* **2018**. [CrossRef]
51. Thanki, R.; Borra, S. *Medical Imaging and its Security in Telemedicine Applications*; SpringerBriefs in Applied Sciences and Technology; Springer International Publishing: Cham, Switzerland, 2019; ISBN 978-3-319-93310-8.
52. ISO. *ISO/TS 13131 Health Informatics—Telehealth Services—Quality Planning Guidelines 2014*; ISO: Geneva, Switzerland, 2014.
53. Mahmood, A.; Hamed, T.; Obimbo, C.; Dony, R. Improving the Security of the Medical Images. *Int. J. Adv. Comput. Sci. Appl.* **2013**, *4*, 137–146. [CrossRef]
54. Shahriar, A.; Sadiq, R.; Tesfamariam, S. Risk analysis for oil & gas pipelines: A sustainability assessment approach using fuzzy based bow-tie analysis. *J. Loss Prev. Process Ind.* **2012**, *25*, 505–523. [CrossRef]
55. Wei, G.; Shao, J.; Xiang, Y.; Zhu, P.; Lu, R. Obtain confidentiality or/and authenticity in Big Data by ID-based generalized signcryption. *Inf. Sci.* **2015**, *318*, 111–122. [CrossRef]
56. Jacinto, C.; Silva, C. A semi-quantitative assessment of occupational risks using bow-tie representation. *Saf. Sci.* **2010**, *48*, 973–979. [CrossRef]
57. El Hajj, C.; Piatyszek, E.; Tardy, A.; Laforest, V. Development of generic bow-tie diagrams of accidental scenarios triggered by flooding of industrial facilities (Natech). *J. Loss Prev. Process Ind.* **2015**, *36*, 72–83. [CrossRef]
58. Aqlan, F.; Mustafa Ali, E. Integrating lean principles and fuzzy bow-tie analysis for risk assessment in chemical industry. *J. Loss Prev. Process Ind.* **2014**, *29*, 39–48. [CrossRef]
59. de Ruijter, A.; Guldenmund, F. The bowtie method: A review. *Saf. Sci.* **2015**, *88*, 211–218. [CrossRef]
60. Ahmed, Y.; Naqvi, S.; Josephs, M. Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019; pp. 1–9.

61. Hong, J.; Liu, C.C.; Govindarasu, M. Integrated anomaly detection for cyber security of the substations. *IEEE Trans. Smart Grid* **2014**, *5*, 1643–1653. [CrossRef]
62. Samtani, S.; Yu, S.; Zhu, H.; Patton, M.; Matherly, J.; Chen, H. Identifying SCADA systems and their vulnerabilities on the internet of things: A text-mining approach. *IEEE Intell. Syst.* **2018**, *33*, 63–73. [CrossRef]
63. Ten, C.W.; Manimaran, G.; Liu, C.C. Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Trans. Syst. Man Cybern. Part ASyst. Hum.* **2010**, *40*, 853–865. [CrossRef]
64. Khari, M.; Garg, A.K.; Gandomi, A.H.; Gupta, R.; Patan, R.; Balusamy, B. Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, *50*, 73–80. [CrossRef]
65. Khan, J.; Li, J.P.; Ahamad, B.; Parveen, S.; Ul Haq, A.; Khan, G.A.; Sangaiah, A.K. SMSH: Secure Surveillance Mechanism on Smart Healthcare IoT System with Probabilistic Image Encryption. *IEEE Access* **2020**, *8*, 15747–15767. [CrossRef]
66. Sivaprakash, A.; Rajan, S.N.E.; Selvaperumal, S. Privacy Protection of Patient Medical Images using Digital Watermarking Technique for E-healthcare System. *Curr. Med. Imaging Former. Curr. Med. Imaging Rev.* **2019**, *15*, 802–809. [CrossRef]