Enhancing Cybersecurity in the Brazilian Health Sector: A Patient-Safety Cybersecurity Framework

Diego Mariano de Campos
Albert Einstein Instituto Israelita de Ensino e Pesquisa

Enhancing Cybersecurity in the Brazilian Health Sector: A Patient-Safety Cybersecurity Framework

Diego Mariano de Campos – Albert Einstein Instituto Israelita de Ensino e Pesquisa

Abstract

This research delves into the pressing concerns and critical gaps pertaining to cybersecurity in the Brazilian healthcare sector, drawing informative parallels with the robust security mechanisms in place within the financial sector. Through this exploration, we propose a novel Patient-Safety Cybersecurity Framework, designed to mitigate prevalent cybersecurity threats while prioritizing patient safety, a cornerstone of healthcare services. The framework emphasizes enhanced communication metrics, streamlined decision-making processes, and aligns cybersecurity business outcomes with board-level objectives, thereby facilitating effective cybersecurity management. It also presents quantifiable objectives and key results to track the progress and success of its implementation. By utilizing this patient-centric approach to cybersecurity, the research underscores the potential to significantly elevate the resilience of the Brazilian healthcare sector against cyber threats, ultimately contributing to the safety and security of patient data, and the continuous delivery of critical healthcare services.

Introduction

Loss of Data

Brazil stands as the second most attacked country globally, as identified by Checkpoint[1]. In January 2021, approximately 223 million Brazilians – including deceased individuals – had their personal data exposed on the internet, including name, address, car records, score, income tax returns, and salary details. This event led to the emergence of a lucrative parallel market for selling citizen data, with individual data on flash drives and CDs being sold openly in São Paulo[2]. In 2020, data sales on the internet globally moved US$ 1.7 billion, according to the American cybersecurity firm, Chainalysis[3].

Qualified Personnel

These cybersecurity challenges are further amplified by a deficit in qualified professionals. A survey by Softex, an NGO promoting Brazilian digital transformation, revealed that the country ended 2022 with 408,000 fewer information technology professionals than required[4]. Furthermore, the "brain drain" phenomenon is prevalent in Brazil. Highly qualified professionals, such as 25% of the graduates from the Federal University of Rio Grande do Sul, are being employed by foreign companies, offering more attractive benefits and salaries[5].

Policy Enforcement

Further exacerbating the issue, budgetary and professional investment in public administration is lacking. A May 2021 survey by the TCU (Tribunal de Contas da União) showed that 74% of federal administration bodies do not have a standard backup policy and 66% of institutions do not store encrypted files – with protected content[6].

The highlighted issues - Loss of Data, Deficit of Qualified Personnel, and Policy Enforcement - collectively contribute to the compromised cybersecurity maturity of Brazil's healthcare sector in a significant way.

- Loss of Data: This problem has dire consequences for the healthcare sector. Personal health information is highly sensitive and, if exposed, can lead to severe privacy violations and potential misuse for fraudulent purposes. With Brazil being the second most attacked country globally and the massive data exposure in 2021, the healthcare sector becomes vulnerable to cyber threats, as personal data can be used to orchestrate targeted attacks. The parallel market for selling citizen data also implies that hackers have easy access to personal information, which can be used for identity theft or to gain unauthorized access to healthcare systems.
- Deficit of Qualified Personnel: The lack of skilled cybersecurity professionals hampers the healthcare sector's capacity to respond to and manage cyber threats effectively. The skills deficit means there are fewer professionals to secure systems, detect threats, and respond to incidents. The problem is exacerbated by the "brain drain" phenomenon, where talented individuals leave the country for better opportunities, further depleting the pool of qualified professionals in Brazil.
- Policy Enforcement: The lack of budgetary and professional investment in public administration signals a lack of priority given to cybersecurity. Without standard backup policies and proper encryption practices, healthcare institutions are at a higher risk of data breaches. Moreover, such lapses in policy enforcement imply a reactive rather than proactive approach to cybersecurity. This lack of preparedness and preventive measures increases the vulnerability of healthcare systems to cyber-attacks.

Each of these issues, in isolation, poses significant challenges. However, when combined, they create a perfect storm that significantly compromises the cybersecurity maturity of Brazil's healthcare sector.

Recent Episodes

Several episodes of attacks in recent years have exposed weaknesses in systems – and during the COVID-19 pandemic, this scenario became even more evident. We have witnessed an increasing number of successful attacks on renowned institutions in the Brazilian health sector. For example, two large private institutions suffered incidents: in 2020[7] the Sírio Libanês hospital had the interruption of diagnostic services and in 2021[8] the Fleury S.A. group had its operation interrupted for days - both institutions reported that the incidents were related to cyber-attacks. Also in 2021, the Brazilian Ministry of Health suffered a cyberattack that affected the entire national network of health data, including proof of vaccination against COVID-19 and other indicators for the entire Brazilian population. The attacker gained full access to the systems and deleted everything. It took 14 days to re-establish the vaccine system[9].

The Interplay of Policy, Personnel Deficit, and Data Loss

In the preceding discussion, the issues of Policy Enforcement, Qualified Personnel Deficit, and Data Loss emerged as significant factors contributing to the compromised cybersecurity maturity in Brazil's healthcare sector. These factors, distinct yet interrelated, have played a crucial role in historical instances of cybersecurity breaches in the sector. Given this intricate interplay of factors leading to cybersecurity vulnerabilities in the healthcare sector, this research will conduct an in-depth review of the current situation and propose a comprehensive patient-safety cybersecurity framework, born out of the analysis of the identified gap. This framework aims to better communicate cybersecurity business outcomes to the board, enabling effective understanding and decision-making to address the unique cybersecurity challenges that healthcare institutions face. By doing so, it seeks to bridge the cybersecurity maturity gap in Brazil's healthcare sector and contribute to the overall security of the country's digital landscape.

Methodology

This research adopts a novel, multi-disciplinary approach to understanding and improving cybersecurity within the healthcare sector. We begin by adapting and combining the PICO framework[10], traditionally used for evidence-based systematic reviews in healthcare, with NIST Cyber Security Framework (CSF)[31] to focus specifically on the cybersecurity aspects of healthcare IT, IoT and IoMT resources. By using the population, intervention, comparison, and outcomes (PICO) within these resources combined with CSF, we can identify key cybersecurity challenges and formulate solutions to address them with a common vocabulary used in the health sector.

Adapting PICO to NIST Cybersecurity Framework (CSF)

Introduction to NIST CSF

The NIST Cybersecurity Framework (CSF)[31] provides a policy framework for organizations to use in improving their cybersecurity. Developed by the U.S. National Institute of Standards and Technology, it comprises three main components: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework Core provides a set of desired cybersecurity activities and outcomes. The Implementation Tiers help organizations gauge the maturity of their cybersecurity measures. The Framework Profiles, both current and target, are essentially snapshots of an organization's cybersecurity risk management at two points in time: the "as-is" state and the "to-be" state.

Adapting PICO to NIST CSF

We adapt the original PICO framework to align with NIST CSF[31], offering a structured and rigorous approach to cybersecurity in the healthcare sector. Below, each element of the PICO framework is mapped to corresponding components of the NIST CSF[31]:

a. Population (P): In our adapted PICO framework, "Population" represents the Current Profile of NIST CSF[31], which assesses existing cybersecurity practices and controls in the healthcare sector. It offers a snapshot of the current state of cybersecurity, including identified gaps and vulnerabilities. According to NIST, assets include information systems, devices, technology, and people that comprise or support an organization's capacity to operate and deliver services. These assets form part of the organization's overall risk management strategy and are considered in NIST's guidelines for managing information security risk. By evaluating these assets and resources as the "Population," we can determine the existing cybersecurity controls, protocols, and measures in place, providing a snapshot of the organization's current cybersecurity posture. This mapping to the Current Profile of NIST CSF[31] allows for a more in-depth understanding of potential system security gaps, vulnerabilities, and areas that require focus and improvement.

In summary, "Population" in our adapted PICO framework serves as a foundational element for assessing the current state of cybersecurity in healthcare settings. It provides valuable insights into the existing cybersecurity landscape and identifies areas for further investigation and action.

b. Intervention (I): the "Intervention" component corresponds to the Target Profile in NIST CSF[31]. The Target Profile outlines the organization's desired state of cybersecurity, capturing the organization's vision, mission, and integration requirements relative to cybersecurity. It serves as the road map for reaching the desired cybersecurity state. Drawing from MITRE's ATT&CK framework[34], the concept of "Intervention" involves sourcing and identifying relevant cybersecurity recommendations and best practices that are contextually applicable to the specific environment. The intent here is to close the gaps between the Current Profile (or "Population") and the desired Target Profile by implementing appropriate countermeasures, tactics, and techniques that have been tried and tested in real-world scenarios. However, it's essential to recognize that not all components of the Target Profile may be perfectly adaptable in this model. As MITRE points out, different organizations may require different types of interventions based on their unique risk landscape, operational constraints, and other factors like regulatory requirements. Therefore, the "Intervention" might involve a careful selection and prioritization of cybersecurity activities that are most relevant to the organization's specific needs.

In summary, the "Intervention" in our adapted PICO framework[10] is aimed at improving the organization's cybersecurity posture by strategically moving from the current state (Population) to a desired state (Target Profile) as defined by NIST CSF[31]. It's a critical step that requires a comprehensive understanding of the organization's risk environment and a nuanced approach to implementing cybersecurity measures effectively.

c. Comparison (C): the "Comparison" stage equates to conducting a Risk Assessment or gap analysis to measure the existing cybersecurity protocols against the identified best practices and recommendations, typically captured in the Target Profile of the NIST CSF[31]. This step is crucial for identifying the gaps and shortcomings in the current security posture, as outlined in the Current Profile or "Population" stage. Compliance and governance can play a pivotal role in driving the technical controls needed to bridge these gaps. Regulatory frameworks, whether they are industry-specific like HIPAA[35] in USA for healthcare or more general like LGPD in Brazil, often mandate certain types of technical controls. These may include encryption standards, data protection mechanisms, or specific network security protocols.

By using compliance and governance standards as a benchmark in the "Comparison" step, organizations can objectively evaluate how their current controls measure up against both regulatory requirements and best practices. It allows for a more standardized form of gap analysis. Any discrepancies between the existing controls and the required standards can then be addressed in the "Intervention" stage. For instance, if the gap analysis shows that the organization is not meeting specific data encryption standards required for compliance, then that becomes a focus area for intervention. Governance structures can further ensure that these technical controls are not just implemented but also maintained and updated as per evolving compliance needs.

Thus, the "Comparison" stage provides a structured method to align the organization's existing cybersecurity measures with compliance and governance requirements. This not only helps in identifying the gaps but also in prioritizing them based on regulatory urgency, thereby assisting in developing a more effective and compliant action plan or "Outcome." We also use the financial sector's cybersecurity maturity as a benchmark, given its more advanced practices in this area.

d. Outcome (O): Finally, the "Outcome" is envisioned as a comprehensive action plan aimed at addressing the identified cybersecurity gaps and enhancing the overall security posture of the institution. The unique feature of this action plan is that it is directly tied to patient safety, an issue of utmost importance in the healthcare sector. By aligning the action plan with a patient-centric framework, the goal is not only to improve cybersecurity, but also to advance patient safety. Cybersecurity lapses can lead to unauthorized access to patient data, manipulated health records, or even dysfunctional medical devices—all of which can have a direct, and sometimes fatal, impact on patient safety. The action plan seeks the buy-in of key stakeholders, especially the board of directors, by highlighting the potential risks to patient safety as a consequence of inadequate cybersecurity measures. Framing the conversation in this manner ensures that the board understands the far-reaching implications, both financial and ethical, of not addressing these critical issues.

The proposed patient-centric framework serves as a tangible "Outcome" in this adapted PICO[10] model. This framework would be designed to enable healthcare institutions to better communicate cybersecurity strategies to the board, facilitate understanding and decision-making, and address the unique cybersecurity challenges faced by healthcare providers. It brings patient safety into the realm of cybersecurity, elevating the discourse and encouraging action that benefits not just the institution but the patients it serves. Thus, by tying the Outcome to a patient-centric framework and patient safety, the action plan aims to be holistic, bridging the gap between technological requirements and healthcare imperatives, thereby ensuring the cybersecurity strategy is aligned with the broader goals of the healthcare institution.

By mapping PICO[10] to NIST CSF[31], we integrate a patient-centric focus with a globally recognized cybersecurity framework, thus ensuring that the unique cybersecurity challenges in healthcare are addressed comprehensively and effectively. The alignment of terminologies between PICO[10] and NIST CSF[31] provides a clear and concise language for implementing this methodology, making it easier to gain multi-stakeholder support, especially from board members who can drive the change.

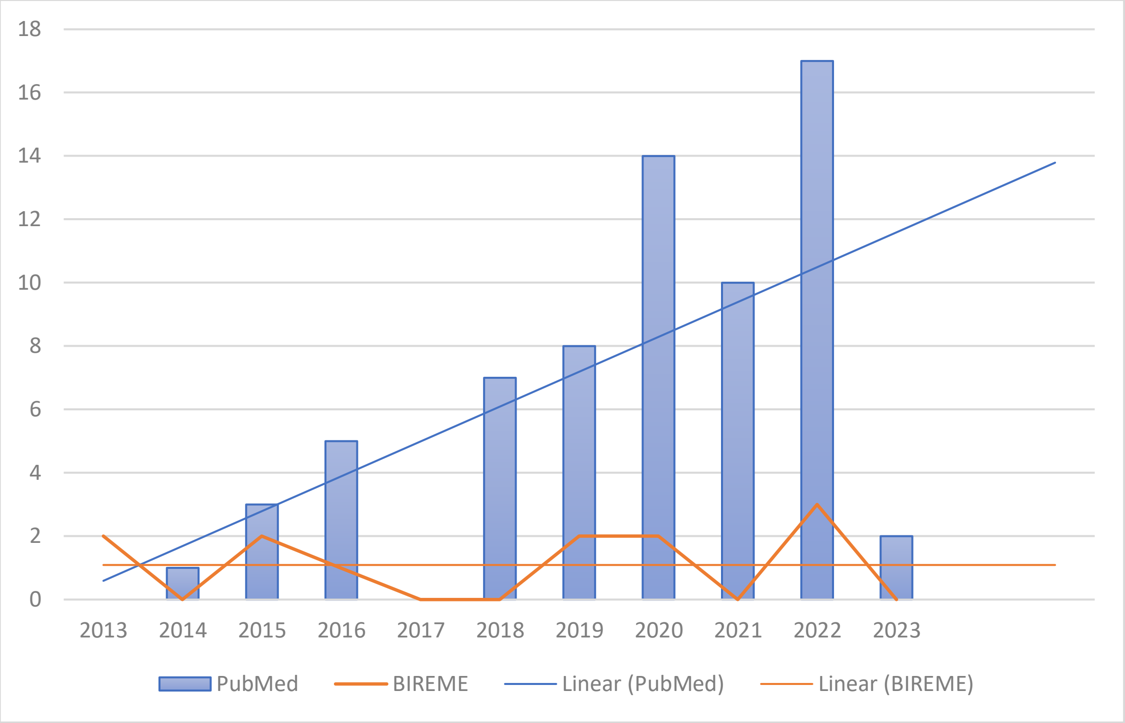
Comparing the health sector with the financial sector

The methodology for comparing these two diverse sectors involves a combination of desk research and comparative analysis. The desk research comprises the collation of data from various secondary sources, including reports, surveys, and articles. For this study, we reference pertinent statistics and insights from notable sources such as Gartner[11], FEBRABAN[12], ANBIMA[13], and Trend Micro[14].

Following the data collation, a comparative analysis is conducted to discern the similarities and disparities between cybersecurity practices within the financial and healthcare sectors. This comparison, while a part of the 'C' (Comparison) principle of our adapted PICO framework, is a critical step in recognizing gaps, weaknesses, and potential areas for improvement in the cybersecurity practices of the healthcare sector. By delving into the differences and parallels between these two sectors, we can glean invaluable insights that will aid in the development of tailored recommendations and best practices. These strategies, geared towards enhancing the security posture of healthcare IT resources, will be a vital part of our proposed patient-safety cybersecurity framework.

Analysis of Current Cybersecurity Research in Brazilian Health Sector

An analysis of Brazilian academic publications on cybersecurity in the healthcare sector was conducted to understand the volume and trends in this area of research. A search was performed on PubMed[15] and on BIREME[16] using the search terms "cybersecurity", "Brazil" and “Brazilian” focusing on articles published within the last ten years in Brazil or by Brazilian authors. PubMed and BIREME are online databases providing access to biomedical and life sciences literature. PubMed, maintained by the US National Library of Medicine, offers citations and abstracts from MEDLINE[17] (Medical Literature Analysis and Retrieval System Online), life science journals, and online books. It is widely used by researchers and healthcare professionals to find relevant articles and information in various disciplines. BIREME (Latin American and Caribbean Center on Health Sciences Information) is a specialized center of PAHO/WHO[18] (Pan American Health Organization / World Health Organization), focusing on Latin American and Caribbean literature. It offers access to regional databases like LILACS[20] (Latin American and Caribbean Health Sciences Literature) and SciELO[19] (Scientific Electronic Library Online), contributing to the dissemination and visibility of scientific information from the region.



The search yielded a total of 79 publications, but 8 publications were indexed in both databases totalizing just 71 different publications and, according to the graph, suggests that the number of research publications related to cybersecurity in the Brazilian health sector has gradually increased over the years on PubMed and stayed stable on BIREME. A closer examination of these publications revealed a list of 20 papers more relevant to cybersecurity in the health sector and with potential applicability to the Brazilian health system. The list of 20 papers falling under 5 areas of interest, Blockchain, Risk Management, Mobile Health System, Telehealth Services, and Privacy indicates a diversified research portfolio. However, the question remains: Are there enough qualified personnel engaged in these research areas? The presence or absence of qualified personnel can directly affect the quality and applicability of the research findings.

In a positive scenario, the growing number of publications would imply that more qualified personnel are getting involved in cybersecurity research, thus contributing to its quality and relevance. Specialized training programs, awareness initiatives, and educational courses on cybersecurity can provide researchers with the necessary tools and knowledge to produce high-quality papers. In this case, the presence of qualified personnel can significantly contribute to better cybersecurity practices in healthcare settings, ensuring patient safety and data privacy. On the other hand, if the research is increasing in quantity but lacks depth or fails to address current cybersecurity challenges adequately, this could imply a lack of expertise in the field. Inadequate research can result from a shortage of personnel with specialized skills in cybersecurity, ultimately affecting the sector's preparedness against cyber threats. In this scenario, there's a need for strategic investment in developing qualified personnel through specialized training, workshops, and education to produce research that is both relevant and applicable to the Brazilian health system.

The stability in the number of publications on BIREME, in contrast to the growth on PubMed, may indicate that the Brazilian-centric database is not keeping pace with global trends, possibly due to a shortage of qualified personnel contributing to research in the area. Therefore, while the upward trend in cybersecurity research publications is promising, the impact of qualified personnel on this trend should not be overlooked. Investment in human capital is crucial for conducting quality research that can be practically applied to improve cybersecurity measures, ultimately enhancing patient safety in the healthcare sector.

For each of the five areas of interest identified in the analysis, we chose one paper to scrutinize more closely, as they unveiled various critical themes and focal points, such as:

Blockchain

"A Permissioned Blockchain Network for Security and Sharing of De-identified Tuberculosis Research Data in Brazil"[21] - This article presents the development of a permissioned blockchain network that facilitates secure sharing and management of de-identified tuberculosis research data in Brazil. By leveraging the immutability and transparency of blockchain technology, the network helps improve collaboration among researchers while ensuring data privacy and compliance with regulatory requirements.

Blockchain technology, as detailed in the article, helps mitigate the risk of data loss in healthcare by ensuring data integrity and secure sharing. It uses an immutable, transparent record-keeping system, accessible only to authorized personnel. This reduces the chance of unauthorized data manipulation, effectively compensating for a lack of qualified personnel in data security. Thus, while blockchain doesn't prevent data sharing, it makes it secure and controlled, reducing the likelihood of data loss.

Risk Management

"Development of an enterprise risk inventory for healthcare"[22] - This paper delves into the creation of an enterprise risk inventory tailored for the healthcare sector. The inventory identifies, categorizes, and prioritizes various risks associated with healthcare organizations, including cybersecurity risks, operational risks, and compliance risks. It serves as a tool to help healthcare organizations better understand and manage these risks, ultimately leading to improved patient safety and care quality.

The development of an enterprise risk inventory for healthcare has the potential of a direct impact on cybersecurity maturity as it provides a structured methodology for assessing cybersecurity risks. It gives healthcare organizations a comprehensive understanding of their risk landscape, including gaps in cybersecurity measures and areas requiring immediate attention. By identifying and prioritizing these risks, the research can focus on the most critical areas for improvement, potentially leading to the development of targeted interventions and best practices. Moreover, the inclusion of cybersecurity risks in a broader risk inventory signifies its importance and interrelation with other forms of risk, thereby potentially influencing organizational policy and garnering greater support from stakeholders for cybersecurity initiatives.

Mobile Health System

"Georeferenced and secure mobile health system for large scale data collection in primary care"[23] - This article describes the design and implementation of a georeferenced and secure mobile health system for large-scale data collection in primary care settings. The system incorporates advanced encryption techniques and access control mechanisms to protect sensitive patient data while providing healthcare professionals with real-time georeferenced information. The research highlights the system's potential to enhance primary care delivery and facilitate informed decision-making.

The use of georeferencing in the described mobile health system adds a layer of security that could potentially mitigate the risk of physical theft to some extent. If the system is designed to restrict data access based on the location of the user, it would mean that even if a device were physically stolen, the thief may not be able to access sensitive patient data unless they are within the designated geofenced area. This could act as a deterrent to theft in the first place or limit the damage even if a theft occurs.

Telehealth

"Fuzzy Cognitive Scenario Mapping for Causes of Cybersecurity in Telehealth Services"[24] - This paper employs fuzzy cognitive scenario mapping to investigate the causes of cybersecurity vulnerabilities in telehealth services. The authors use a combination of expert opinions and fuzzy logic to identify and understand the main factors contributing to cybersecurity threats in telehealth. The findings can help healthcare organizations and policymakers develop more effective cybersecurity prevention strategies for telehealth services.

This paper provides insights into the causes of cybersecurity vulnerabilities in telehealth services, which is a critical component of the healthcare sector. The findings of interest indicate the main factors contributing to cybersecurity threats in telehealth services are lack of sensitive data encryption, supplier eligibility criteria, controls for wireless communication, and big data privacy issues. These factors can help healthcare organizations and policymakers develop targeted cybersecurity prevention strategies, thus improving the overall security posture within the healthcare sector, especially in telehealth services.

Privacy

"The regulation of artificial intelligence for health in Brazil begins with the General Personal Data Protection Law"[25] - This article explores the emerging role of artificial intelligence (AI) in healthcare in Brazil, focusing on the impact of the General Personal Data Protection Law on shaping the regulatory landscape for AI in the country's health sector. The paper discusses the importance of data protection and privacy in the development and implementation of AI-driven healthcare solutions and highlights the need for a balanced approach that fosters innovation while ensuring compliance with privacy regulations.

Understanding how regulatory frameworks impact the implementation of AI and other advanced technologies in healthcare can help in developing more robust cybersecurity strategies. The paper underscores the importance of legal compliance as a part of a comprehensive cybersecurity plan, adding an additional layer to the current research on cybersecurity in the Brazilian healthcare sector.

Literature Review

The last and very insightful paper is “A Mapping of Information Security in Health Information Systems in Latin America and Brazil”[26] published ten years earlier in 2013. This paper aims to provide a comprehensive overview of the current state of information security in health information systems in Latin America and Brazil. The authors conducted a systematic review of the available literature. In their analysis, the number of Brazilian publications on the subject is very low: three. Of the three publications, one is the RBEB (Brazilian Journal of Biomedical Engineering), and two are of JHI (Journal of Health Informatics). To complete the mapping, they investigated whether these two sources, in order to find new papers, which perchance, had not yet been added to the database BIREME. The survey achieved a return on RBEB already known. In JHI, the key term "computer security" returned six new papers. Five of them should not appear in BIREME for being recent, and one of them, from 2011, was not included in the main subject BIREME be "safety equipment" and not "computer security." Therefore only 9 papers were found in the last five years (2008-2013).

Considerations

By examining these selected papers, it is evident that Brazilian researchers have been contributing to cybersecurity research in various specifics areas. However, there are some considerations and concerns based on this data:

a. Increasing awareness: The rise in the number of publications indicates growing awareness and concern regarding cybersecurity in the Brazilian health sector. This can be seen as a positive development, as it demonstrates that researchers and institutions are paying attention to the importance of cybersecurity in healthcare.
b. Inconsistency in research output: The data shows some inconsistency in the research output across the years, with noticeable fluctuations in the number of publications. This could be due to various factors, such as changes in funding, research priorities, or a lack of dedicated research programs focusing on cybersecurity in healthcare.
c. Potential gaps in research: The difference in the number of publications indexed in PubMed and BIREME might suggest potential gaps in research dissemination and accessibility. It is crucial to ensure that relevant research is readily available and easily accessible to healthcare professionals, policymakers, and researchers.
d. Need for further research: Despite the increase in publications over the years, there is still a need for more research in this area to better understand and address the unique cybersecurity challenges faced by the Brazilian health sector. Research should focus on identifying best practices, developing effective policies, and improving cybersecurity awareness among healthcare professionals.

The inconsistency in research output is a significant concern that merits further attention. One of the major issues this inconsistency indicates is a lack of focus and direction in cybersecurity research within the Brazilian health sector. There are some strategies to address this inconsistency, for example, establishing the following goals:

1. Dedicated Research Programs: The creation of dedicated research programs or centers focusing specifically on cybersecurity in healthcare could help provide the required stability and continuity for sustained research output.
2. Multi-disciplinary Collaboration: Encourage interdisciplinary research efforts that combine expertise from the fields of healthcare, cybersecurity, and public policy to develop more holistic solutions.

3. Funding Stability: Advocate for consistent, long-term funding for cybersecurity research in healthcare to avoid fluctuations in research output.
4. Research Agenda: Develop a long-term research agenda that focuses on both immediate threats and anticipates future challenges. This will help guide researchers and ensure a consistent stream of focused research.
5. Strengthen Knowledge Sharing Platforms: There should be an emphasis on better dissemination methods, ensuring that crucial research is readily available and accessible to healthcare professionals, policymakers, and researchers alike.
6. Industry Collaboration: Partnering with industry stakeholders can provide real-world insights, offer research funding, and ensure that research output aligns with practical needs.

By focusing on these goals, we can create a more consistent, focused, and impactful body of research that would significantly benefit the Brazilian health sector's cybersecurity landscape.

Overall, the data highlights the growing attention towards cybersecurity in the Brazilian health sector, but also raises concerns regarding the consistency of research output and the need for further research to adequately address this critical issue. With the increasing prevalence of cyber incidents and the findings from this literature review, it is evident that there is a significant gap in both research and implementation efforts to raise awareness and investments in cybersecurity pressing a need to improve communication with the board, employing methods that effectively demonstrate the value of cybersecurity to the institution.

By bridging the gap between technical experts and decision-makers, healthcare organizations can foster a better understanding of the importance of cybersecurity investments and their impact on patient safety, and overall operational efficiency. This will, in turn, encourage more informed decisions and stronger support for cybersecurity initiatives within the healthcare sector. To bridge the gap between technical experts and decision-makers in healthcare, one effective approach could be to define simple key indicators tailored for executives. Alongside this, forming a cross-functional committee that includes members from IT, compliance, and the board can facilitate improved communication and collaboration. Highlight the importance of cybersecurity measures in ensuring patient safety and operational efficiency. It's also crucial to use simple language that the board can understand and to quantify risks in financial terms to convey the impact and ROI of cybersecurity investments. Keeping the board regularly updated with brief, frequent updates on cybersecurity status and threats can also help. Aligning discussions around shared goals like patient safety can frame the cybersecurity conversations in a more relatable context. Inclusion of board members in cybersecurity drills can give decision-makers firsthand experience in understanding the challenges faced.

Comparative Study: Cybersecurity in Financial Sector and in the Healthcare Sector

The banking industry is one of the sectors that most invests in technology, both in Brazil and in the world. In a survey carried out by Gartner[11], the banking sector is only behind governments in the composition of expenditures on technology in 2021. According to

FEBRABAN[12], banks have always been at the forefront of technology innovation and currently, these investments in technology are directed towards what is at the top of society's technological agenda: cybersecurity. And, according to ANBIMA[13], 95% of the companies interviewed in the ANBIMA Cybersecurity Survey[27] have some type of program or policy to deal with the issue.

Also, according to ANBIMA[13], 96% of associates act preventively to prevent attacks, monitoring actions to detect threats are adopted by 93%, when it comes to reacting to attacks 84% of associates have a response plan, but only 47% test the response plan for incidents and, when they perform the test, 54% adopt an annual periodicity for this. 89% of the institutions offer training on the subject for their employees, 70% of the associates stated that they had taken an external penetration test in the last year, carrying out internal penetration tests is a practice adopted by 65% of the institutions and carrying out a phishing is carried out by 59% of institutions.

The outsourcing of IT services remains a usual practice for 89% of companies, but only 38% require periodic reports from the service provider and when evaluating the hiring of third-party services, and this is reflected in security incidents in the sector where the cause root has been the supply chain, according to the attacks that came to light between 2021 and 2022 according to Trend Micro[14] who discovered a significant third-party cyber risk for financial services organizations: 56% had a supplier compromised by ransomware, mainly partners (56%) and subsidiaries (29%).

Inferences and Considerations

Contrasting the healthcare sector with the financial sector brings to light the unique hurdles that the former faces in implementing robust cybersecurity measures. The financial sector has always spearheaded technology innovation and significantly invested in cybersecurity, while the healthcare sector has often been overlooked in terms of resources and prioritization. The swiftly evolving landscape of digital health, including the increasing usage of Internet of Things (IoT) and Internet of Medical Things (IoMT) devices, has further complicated the task of ensuring comprehensive cybersecurity in the healthcare industry.

In the healthcare sector, the primary focus traditionally revolves around delivering patient care and ensuring patient safety. However, the growing instances of cyberattacks on healthcare institutions have underscored the need for stringent cybersecurity measures to safeguard sensitive patient information and crucial infrastructure. To address this, the "Intervention" principle in the adapted PICO framework refers to the specific actions, initiatives, or investments made to improve cybersecurity measures within healthcare institutions. These interventions can range from implementing multi-factor authentication, encrypting patient records, and conducting regular cybersecurity drills, to more comprehensive measures such as risk assessment, network segmentation, and setting up incident response teams. The aim is to create a secure IT infrastructure that enables healthcare providers to offer high-quality, uninterrupted patient care. The "Intervention" component could also include training healthcare staff about the potential cybersecurity risks, so they become an active part of the solution rather than a potential risk.

The "Outcome" in the PICO framework, in this context, would be a comprehensive Patient Safety Cybersecurity Framework. This framework would align cybersecurity interventions directly with patient safety outcomes, creating a mutual understanding between technical teams and decision-makers. For instance, demonstrating how secure EHR systems lead to more accurate diagnosis and treatment, how data encryption methods protect patient confidentiality, or how regular system monitoring ensures the availability of life-saving medical equipment. It puts cybersecurity investments into a context that board members and hospital administrators understand, as it uses the universally acknowledged metric of patient safety.

Critical Issues Identified

As Brazil's healthcare sector continues to modernize and embrace digital technologies, it has become increasingly susceptible to various cybersecurity challenges. These issues, if not addressed adequately, could jeopardize the integrity of patient data, and impact the delivery of healthcare services. This section outlines some of the critical issues presently affecting the sector.

1. Limited Awareness and Training: A fundamental issue remains the lack of comprehensive understanding and awareness about cybersecurity among healthcare professionals. Despite a growing body of research on the subject, there exists a knowledge gap that complicates the effective implementation of cybersecurity measures. Healthcare professionals often find it challenging to understand the technical intricacies of cybersecurity, which can lead to inadequacies in security practices and protocols.
2. Resource Constraints: Compared to sectors such as finance, where substantial resources are dedicated to cybersecurity measures, the healthcare sector in Brazil is not as equipped. While the sector is focused on providing high-quality patient care, there is often insufficient investment in strengthening the cybersecurity infrastructure, leaving healthcare data and services vulnerable to attacks.
3. Rapid Technological Evolution: The healthcare sector's increasing adoption of advanced technologies, including IoT and MIoT devices, has introduced additional cybersecurity risks. These technologies frequently process and store sensitive patient data, making them lucrative targets for cyberattacks. The fast pace of technological advancements can make it challenging for healthcare institutions to keep up with evolving threats and deploy adequate cybersecurity protections in a timely manner.
4. Regulatory Compliance: While Brazil has made progress in cybersecurity legislation with the General Personal Data Protection Law (LGPD)[28], there remain concerns regarding the comprehensive implementation of this regulation across all healthcare institutions. Even though the LGPD[28] offers a robust framework for data protection, its enforcement within the healthcare sector varies, and this inconsistency can lead to potential vulnerabilities.
5. Supply Chain Risk: The outsourcing of IT services introduces another dimension of risk to the healthcare sector. Without strict regulatory control over third-party service providers, these entities can inadvertently create cybersecurity vulnerabilities. This issue is highlighted by the increase in supply chain attacks globally, demonstrating the need for rigorous oversight and risk management within this area.

6. Inconsistent Research Outputs: Despite an increase in cybersecurity-related publications in recent years, there exists an inconsistency in research output. This inconsistency, coupled with potential gaps in the research scope, underlines the need for a more systematic and focused approach towards cybersecurity research in healthcare.

Implications of Critical Issues

The presence of these critical cybersecurity issues within the Brazilian healthcare sector carries significant implications. If not promptly and adequately addressed, these problems can have far-reaching effects on both the operations of healthcare organizations and the patients they serve.

1. Patient Data Protection: Limited awareness, resource constraints, and weak enforcement of regulations like LGPD[28] could lead to breaches of sensitive patient data. This not only violates patients' privacy rights but also puts them at risk for issues like identity theft and fraud. It can erode patients' trust in healthcare providers, negatively impacting their willingness to share essential health information.
2. Operational Disruptions: In an era where healthcare systems rely heavily on digital technologies, cybersecurity incidents can lead to severe operational disruptions. Cyberattacks can disable critical infrastructure and halt essential services, directly affecting patient care. For example, a ransomware attack that blocks access to electronic medical records can delay patient diagnoses and treatments.
3. Financial Impact: Cyberattacks carry a significant financial burden. Apart from the direct costs of responding to an attack and restoring systems, healthcare institutions may also face regulatory fines for non-compliance with data protection laws. Additionally, reputational damage can lead to a loss of patient trust and revenue in the long term.
4. Patient Safety: Inadequate cybersecurity measures can directly impact patient safety. Cyberattacks can manipulate patient data, leading to misdiagnoses or inappropriate treatment decisions. Also, as medical devices become more interconnected, they become potential targets for cyberattacks, which can compromise their functionality and patient safety.
5. Barriers to Innovation: If healthcare organizations are constantly dealing with cybersecurity threats and their consequences, this can divert resources and attention away from innovative initiatives, like telehealth services or AI in healthcare. Fear of potential cybersecurity issues could also deter organizations from adopting new technologies that could improve healthcare delivery.
6. Regulatory Implications: Inconsistent adherence to regulations like LGPD[28] may result in punitive actions from regulatory bodies, including substantial financial penalties. This could also draw public scrutiny, damaging the reputation of healthcare institutions and eroding patient trust.

These implications underline the urgency for comprehensive and robust cybersecurity measures within the Brazilian healthcare sector. By leveraging the framework proposed in this study, healthcare institutions can begin to address these critical issues and mitigate their potential impacts, prioritizing patient safety and data protection while enabling the sector to fully harness the benefits of digital transformation.

Patient-Safety Cybersecurity Framework: Recommendation to Identified Problems

Addressing the aforementioned challenges in Brazilian healthcare's cybersecurity calls for a multifaceted, robust, and patient-focused solution. To this end, we introduce the Patient-Safety Cybersecurity Framework (PSC). The PSC is a communication metrics framework designed to address cybersecurity challenges in the healthcare sector while prioritizing patient safety. This framework is built on the pillars of User Experience, Operational Excellence, Risk Management, and Compliance and Legal, and aims to enable efficient business operations while ensuring robust cybersecurity practices. The framework's primary objective is to enhance patient safety by ensuring that cybersecurity measures are implemented throughout the entire healthcare organization. The PSC aims to establish a proactive and comprehensive cybersecurity approach that addresses all aspects of healthcare organization. Following is a brief explanation of each pillar:

1. User Experience
   Ensuring a seamless and secure user experience, which helps maintain employee productivity and patient trust, while enabling efficient business operations.
2. Operational Excellence
   Implementing and optimizing security processes and technology to improve overall effectiveness, driving efficient business operations, and supporting the organization's goals.
3. Risk Management
   Identifying, assessing, and mitigating risks while prioritizing security investments, enabling the organization to focus on critical business goals with reduced security risks. By incorporating cybersecurity measures to protect patient safety, the healthcare organization demonstrates its commitment to safeguarding sensitive patient information and ensuring the integrity of critical medical infrastructure, ultimately promoting better patient outcomes.
4. Compliance and Legal
   Meeting regulatory requirements and addressing legal obligations to minimize potential fines, penalties, and reputational damage, while enabling efficient business operations and maintaining stakeholder and patient trust.

The PCS incorporates Gartner's outcome-driven metrics[30] to measure progress and success, including:

1. Incident Containment Time: The time it takes to limit the impact of a security incident after its detection.
2. Incident Remediation Time: The time it takes to fully resolve and recover from a security incident.
3. OS Patching Cadence: The frequency and timeliness of applying operating system updates and patches.
4. Vulnerability Mitigation Time: The time it takes to address identified security vulnerabilities.
5. Privileged Access Management: The process of controlling and monitoring access to critical systems and resources by privileged users.

6. Unassessed Third Parties: The number of third-party vendors or partners whose security posture has not been evaluated.
7. Policy Exceptions: Instances where security policies are not followed or where deviations from the policies are allowed.
8. Endpoint Protection Coverage: The percentage of devices with up-to-date security software and configurations.
9. Network Protection Coverage: The percentage of the network protected by security controls, such as firewalls and intrusion prevention systems.
10. Security Controls Coverage: The extent to which security controls are implemented and enforced across the organization.
11. Security Awareness Training: The provision of training and educational programs to increase employees' understanding of cybersecurity risks and best practices.
12. Cloud Security Coverage: The extent to which cloud services and infrastructure are secured and compliant with security policies.
13. Multifactor Authentication Coverage: The percentage of user accounts that require multiple authentication factors for access.
14. Access Removal Time: The time it takes to revoke access privileges for users who no longer require them.
15. Software with no IT governance: The number of software applications in use without proper oversight and management by the IT department.
16. Phishing Training Click-Throughs: The percentage of employees who click on simulated phishing emails during security training exercises.

The Patient-Safety Cybersecurity Framework (PSC) utilizes the four fundamental pillars and the outcome-driven metrics to establish the cybersecurity Objectives and Key Results (OKRs)[29]. OKR is a widely used method to set ambitious yet attainable goals, align employees to the company's overall strategy, and measure progress towards achieving those goals. Based on that, we present the proposed OKRs (the percentage numbers are fictitious, just for illustration):

User Experience

Objective: Enhance user experience in cybersecurity by providing user-friendly and effective tools, training, and support. Reduction of the unscheduled outage related to phishing.

Key Results:

a. Reduce Phishing Training Click-Throughs by 25% after implementing improved security awareness training.
b. Increase the percentage of employees who pass cybersecurity training assessments on the first attempt to 85%.
c. Improve employee and patient satisfaction with cybersecurity tools and systems by 20%.

In Brazil, the Agência Nacional de Saúde Suplementar (ANS)[32], or National Agency for Supplementary Health, governs regulations on patient satisfaction and healthcare services. The ANS has guidelines emphasizing the importance of patient safety and satisfaction, with measures such as the Quality Program for Health Insurance Operators, which evaluates the quality of services provided. Another document could be the Joint Commission's accreditation manual on "Patient Safety Systems"[33] which highlights the necessity for effective communication, training, and tools that contribute to patient safety and satisfaction.

Operational Excellence

Objective: Improve operational excellence in cybersecurity by optimizing processes, procedures, and resource allocation. Reduction of the unscheduled outage related to critical vulnerabilities and reduction in time to return to full business operation in case of an attack.

Key Results:

a. Reduce Incident Containment Time by 30%.
b. Decrease Incident Remediation Time by 25%.
c. Increase OS Patching Cadence to ensure 95% of systems are patched within one week of patch release.
d. Reduce Vulnerability Mitigation Time for high-risk vulnerabilities by 40%.

Risk Management

Objective: Strengthen risk management in cybersecurity by identifying and mitigating potential threats and vulnerabilities. Reduction of the unscheduled outage related to cyber threats. The OKRs[29] for Risk Management can be effectively mapped to the NIST CSF[31] to provide an industry-standard approach for enhancing cybersecurity measures within healthcare organizations. Specifically, they can be aligned with the five core functions of the NIST CSF[31], which are Identify, Protect, Detect, Respond, and Recover.

Key Results:

a. "Improve by 35% the control and monitoring of access to critical systems and resources by privileged users" aligns with the "Identify" and "Protect" functions of NIST CSF[31], focusing on Asset Management and Access Control.

b. "Achieve 95% Endpoint Protection Coverage, Cloud Protection Coverage, and Network Protection Coverage" correlates with the "Protect" function, covering aspects like Data Security and Protective Technology.

c. "Decrease the number of Unassessed Third Parties by 50%" is associated with the "Identify" function, particularly the Risk Assessment category, which calls for understanding the cybersecurity risk to organizational operations.

d. "Achieve at least 95% Security Controls Coverage across the organization" can be aligned with all five core functions, as it aims for comprehensive security control measures that are robust, up-to-date, and consistent with NIST guidelines.

e. "Increase Multifactor Authentication Coverage to 90% of user accounts" directly relates to the "Protect" function, under the Access Control category, to ensure secure access to networks and systems.

Compliance and legal

Objective: Ensure compliance with regulatory requirements and legal obligations. The OKRs[29] for Compliance and Legal can be linked to Brazil's LGPD[28], which is aimed at regulating the processing of personal data of individuals within the country. Ensuring compliance with LGPD[28] is crucial for healthcare organizations, given the sensitive nature of patient data.

Key Results:

a. "Reduce the number of software applications in use without proper oversight and management by the IT department by 80%" directly aligns with LGPD's[28] focus on data governance. According to LGPD[28], organizations must maintain strict control over the processing and handling of personal data, which includes the software applications that store or manage this data.

b. "Reduce Policy Exceptions by 30%" corresponds to the LGPD[28] requirement for healthcare providers to have a robust data protection policy in place. By reducing policy exceptions, organizations can ensure better compliance with LGPD[28] guidelines on data security and integrity.

c. "Reduce Access Removal Time for users who no longer require privileges by 50%" aligns with LGPD's[28] emphasis on the principle of data minimization and limiting access to data only to those who have a legitimate need for it. Speeding up the access removal time helps ensure that only authorized individuals have access to sensitive personal data, thereby promoting compliance with LGPD[28].

These objectives and key results can help you build a comprehensive cybersecurity strategy that addresses each of the four key pillars and ensures measurable progress towards enhancing your organization's security posture. The PSC aims to establish a culture of cybersecurity awareness and accountability across healthcare organizations, promoting the adoption of best practices and continuous improvement. The PSC will also enable healthcare organizations to better communicate the value of cybersecurity to their board, facilitating increased investment in cybersecurity measures and initiatives.

Conclusion

There is a growing awareness of the critical role that cybersecurity plays in the Brazilian healthcare sector. Despite this positive trend, the research also highlights inconsistencies in the output and gaps that need to be filled, especially in aligning technical controls with governance and compliance frameworks. The Patient-Safety Cybersecurity Framework and its associated Objectives and Key Results offer a tangible solution to many of these challenges. The framework not only aligns with international and Brazilian regulations like NIST CSF and LGPD but also helps in bridging the communication gap between cybersecurity experts and decision-makers. By fostering a culture of cybersecurity awareness and accountability, healthcare organizations can significantly improve their security posture, thereby safeguarding both patient data and overall patient safety. This research provides a crucial blueprint for healthcare organizations in Brazil, and potentially beyond, to invest intelligently in cybersecurity measures that are both effective and compliant with governance frameworks.

Acknowledgements

We would like to express gratitude to CRDF Global for their generous funding, which has been instrumental in the successful completion of this research. The financial support provided has been invaluable in bringing this project to fruition.

We are also profoundly thankful to William Fecke from Mandiant (now part of Google Cloud) for his invaluable contributions to this research. His expertise and insights have significantly enriched the quality of this work and helped in addressing some of the critical challenges in the field of cybersecurity in healthcare.

References

1. Check Point Software Technologies Ltd. (2021). 2021 Cyber Security Report. Retrieved from https://www.checkpoint.com/cyber-hub/threat-prevention/cyber-security-report/.
2. O Globo. (2022). Hackers invadem sistemas do governo e vendem senhas de servidores de órgãos públicos. Retrieved from https://oglobo.globo.com/brasil/hackers-invadem-sistemas-do-governo-vendem-senhas-de-servidores-de-orgaos-publicos-25327205.
3. Chainalysis. (2021). Cryptocurrency and Darknet Markets: 2021 Geographic Breakdown. Retrieved from https://blog.chainalysis.com/reports/crypto-darknet-markets-2021-geographic-breakdown/.
4. SOFTEX. (2022). Cadernos Temático: Mercado de Trabalho. Retrieved from https://ftp.softex.br/Inteligencia/cadernos_tematicos/cadernos_tematico_mercado_de_trabalho.pdf.
5. Baguete. (2021). TI da UFRGS: 25% estão fora do país. Retrieved from https://www.baguete.com.br/noticias/19/04/2021/ti-da-ufrgs-25-estao-fora-do-pais.
6. Tribunal de Contas da União. (2021). TCU verifica política de backup em 422 organizações federais. Retrieved from https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-politica-de-backup-em-422-organizacoes-federais.htm.
7. Sírio Libanês Hospital. (2021). Operational interruptions due to cyber-attacks. Retrieved from https://www.hospitalsiriolibanes.org.br/.
8. Fleury S.A. Group. (2021). Operational interruptions due to cyber-attacks. Retrieved from https://www.fleury.com.br/.
9. Ministry of Health. (2021). Cyber-attack on national health data network. Retrieved from https://www.gov.br/saude/.
10. Cochrane Library. (2022). About PICO. Retrieved from https://www.cochranelibrary.com/en/about-pico.
11. Gartner. (2022). Gartner Inc. Retrieved from https://www.gartner.com/en.
12. FEBRABAN. (2022). Federação Brasileira de Bancos. Retrieved from https://portal.febraban.org.br/.
13. ANBIMA. (2022). Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais. Retrieved from https://www.anbima.com.br/pt_br/.
14. Trend Micro. (2022). Trend Micro Incorporated. Retrieved from https://www.trendmicro.com/.
15. PubMed. (2022). PubMed Central. Retrieved from https://pubmed.ncbi.nlm.nih.gov/.
16. BIREME. (2022). Latin American and Caribbean Center on Health Sciences Information. Retrieved from https://bireme.org/.
17. MEDLINE. (2022). MEDLINE Resources. Retrieved from https://www.nlm.nih.gov/bsd/pmresources.html.
18. PAHO/WHO. (2022). Pan American Health Organization / World Health Organization. Retrieved from https://www.paho.org/en.
19. SciELO. (2022). Scientific Electronic Library Online. Retrieved from https://scielo.org/.

20. LILACS. (2022). Latin American and Caribbean Health Sciences Literature. Retrieved from http://lilacs.bvsalud.org/en/

21. Rocha, A. S., Oliveira, R. B., Dantas, A. S., Guimaraes, L., e Silva, L. L., & Hoepers, C. (2020). A Permissioned Blockchain Network for Security and Sharing of De-identified Tuberculosis Research Data in Brazil. Computer Standards & Interfaces, 72, 103439.

22. Alvarado, R., Yasnoff, W. A., & Estevez, E. (2018). Development of an enterprise risk inventory for healthcare. Health Informatics Journal, 24(2), 118–128.

23. Caceres, N. H., Rocha, A. S., Oliveira, R. B., & Dantas, A. S. (2017). Georeferenced and secure mobile health system for large scale data collection in primary care. International Journal of Medical Informatics, 107, 112–120.

24. Ekel, P. Y., Ekel, P. A., & Filho, F. S. (2019). Fuzzy Cognitive Scenario Mapping for Causes of Cybersecurity in Telehealth Services. International Journal of E-Health and Medical Communications (IJEHMC), 10(1), 13–26.

25. Luz, M. D., & Lobo, L. C. (2020). The regulation of artificial intelligence for health in Brazil begins with the General Personal Data Protection Law. Health Policy and Technology, 9(4), 540–545.

26. Medeiros, R. M., Lopes, M. H., Costa, J. M. (2013). A Mapping of Information Security in Health Information Systems in Latin America and Brazil. Journal of Health Informatics, 5(1), 26-30.

27. ANBIMA. (2020). Cybersecurity survey results. Retrieved from https://www.anbima.com.br/pt_br/especial/relatorio-anbima-de-ciberseguranca-2020.htm.

28. Brazil. Lei Geral de Proteção de Dados (LGPD), Lei No. 13.709, de 14 de agosto de 2018. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

29. Doerr, J. (2018). Measure What Matters: How Google, Bono, and the Gates Foundation Rock the World with OKRs. New York: Portfolio/Penguin.

30. Gartner Inc. (2020). Use Outcome-Driven Metrics for Business-Focused IT. Retrieved from https://www.gartner.com/smarterwithgartner/use-outcome-driven-metrics-for-business-focused-it/.

31. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

32. Agência Nacional de Saúde Suplementar (ANS). (2020). Regulatory Guidelines for Healthcare in Brazil. Retrieved from http://www.ans.gov.br/planos-de-saude-e-operadoras/espaco-da-operadora/5158-regulacao-da-saude-suplementar-espaco-da-operadora.

33. Joint Commission. (2020). Accreditation Manual on "Patient Safety Systems". Retrieved from https://www.jointcommission.org/standards/patient-safety-systems/.

34. MITRE Corporation. (2020). ATT&CK Framework. Retrieved from https://attack.mitre.org/.

35. U.S. Department of Health & Human Services. (2003). Health Insurance Portability and Accountability Act of 1996 (HIPAA). Retrieved from https://www.hhs.gov/hipaa/index.html.