Escola Nacional de Saúde Publica

Universidade Nova de Lisboa

Relatório de investigação de Mestrado em Saúde Pública

Avaliação do impacto económico do ciberataque no SESARAM: Hospital Dr. Nélio Mendonça

Mestrado em Saúde Pública

Aluno: Diana Portela

Orientação: Prof. Teresa Magalhães

Agosto, 2025

Índice

Introdução

A digitalização dos cuidados de saúde transformou profundamente a forma como os serviços são prestados, geridos e monitorizados. (1) Os sistemas de informação hospitalares e os registos eletrónicos de saúde são hoje ferramentas indispensáveis para assegurar qualidade, eficiência e continuidade de cuidados. No entanto, essa mesma dependência tecnológica aumentou a vulnerabilidade das instituições a ciberataques, que podem comprometer tanto a segurança do paciente como a sustentabilidade organizacional. Na última década, assistiu-se a um crescimento significativo da frequência, sofisticação e impacto destes incidentes em hospitais e organismos públicos de saúde, expondo fragilidades críticas e a necessidade de estratégias de ciber-resiliência. (2)

Apesar de reconhecida a gravidade destes riscos, a literatura científica nacional sobre o impacto económico de ciberataques em saúde é muito limitada. A maioria dos estudos disponíveis centra-se em análises de incidentes em contexto internacional, como o ataque WannaCry de 2017, ou em revisões narrativas que destacam ameaças, vulnerabilidades e recomendações gerais. (3) No entanto, faltam estudos de caso em Portugal que quantifiquem o impacto económico direto de um ciberataque, de modo a fornecer evidência robusta e sustentada que apoie decisões de investimento em cibersegurança e planeamento de contingência no setor da saúde.

Esta lacuna é particularmente relevante numa altura em que a União Europeia tem vindo a reforçar o seu enquadramento legislativo nesta área, através da Diretiva NIS2 e do Regulamento Europeu de Cibersegurança (*Cybersecurity Act*). (4) Este último constitui um marco fundamental ao atribuir à ENISA um mandato permanente e ao estabelecer um quadro europeu de certificação para produtos, serviços e processos de TIC, reconhecido em todos os Estados-Membros. O mecanismo introduz diferentes níveis de garantia e visa promover a adoção de soluções mais seguras e resilientes em setores críticos. Assim, no caso da saúde, os hospitais assumem particular relevância enquanto infraestruturas críticas altamente dependentes de tecnologias digitais, como registos eletrónicos de saúde, dispositivos médicos conectados e plataformas de telemedicina. (5) Tal dependência torna-os alvos preferenciais de ciberataques, cujas consequências podem implicar disrupções severas nos serviços, riscos acrescidos para a segurança do doente e perda de confiança pública. (5, 6)Assim, o enquadramento europeu complementa as práticas recomendadas pela literatura ao fornecer uma base normativa que

sustenta a necessidade de reforço da ciber-resiliência hospitalar, harmonizando práticas e elevando os padrões de segurança em toda a União Europeia.

Face a este contexto, este estudo foi desenvolvido com os seguintes objetivos principais:

- Identificar e sistematizar as datas e eventos-chave relacionados com o ciberataque ocorrido em agosto de 2023 na Região Autónoma da Madeira, que afetou de forma crítica os sistemas do SESARAM.
- Estimar o impacto económico direto do incidente no Hospital Dr. Nélio Mendonça, construindo cenários baseados em diferentes graus de inatividade e recursos afetados, com recurso a dados públicos disponíveis.
- Discutir as implicações dos resultados, reforçando a necessidade da implementação de melhores práticas nacionais, reforçando a relevância da ciber-resiliência hospitalar enquanto dimensão essencial da segurança do paciente e da sustentabilidade dos sistemas de saúde.

A novidade científica deste estudo reside no facto de reforçar e aprofundar uma linha de investigação ainda incipiente em Portugal sobre a quantificação dos custos diretos de ciberataques em contexto hospitalar. Recorrendo a um modelo exploratório baseado em dados secundários e análise de sensibilidade, e tomando o Hospital Dr. Nélio Mendonça como estudo de caso, o trabalho não só contribui para consolidar a evidência já existente, como também oferece um exemplo metodológico passível de replicação noutras instituições e contextos, fortalecendo a base empírica nacional nesta área.

A relevância para a área científica do Mestrado em Saúde Pública é dupla: por um lado, reforça a necessidade de integrar a cibersegurança como dimensão estratégica da gestão e qualidade em saúde e da política pública; por outro, fornece evidência que pode apoiar a formulação de planos de contingência e investimentos sustentáveis em tecnologia da informação.

Este estudo contribui ainda para os Objetivos de Desenvolvimento Sustentável (ODS) definidos pelas Nações Unidas. Relaciona-se com o ODS 3 (Saúde de Qualidade), ao promover a continuidade e segurança dos cuidados de saúde; com o ODS 9 (Indústria, Inovação e Infraestruturas), ao enfatizar a importância de infraestruturas digitais resilientes e seguras; e com o ODS 16 (Paz, Justiça e Instituições Eficazes), ao reforçar a confiança nas instituições públicas de

saúde através de práticas de cibersegurança robustas.

Em síntese, este estudo responde a uma necessidade urgente de evidência científica aplicada ao contexto português, fornecendo um contributo relevante tanto para a prática da gestão hospitalar como para a formulação de políticas públicas de cibersegurança em saúde.

Resumo

Contexto: Na última década, a frequência e a dimensão dos ciberataques na indústria de cuidados de saúde aumentaram, variando entre violações de processos ou redes e encriptação de ficheiros que restringem o acesso aos dados. Estes ataques podem ter várias consequências para a segurança do paciente, uma vez que podem, por exemplo, visar os registos eletrónicos de saúde, o acesso a informações críticas e o suporte a sistemas essenciais, causando assim atrasos nas atividades hospitalares. Os efeitos das violações de segurança cibernética não são apenas uma ameaça à vida dos pacientes, mas também têm consequências financeiras devido à inatividade causada nos sistemas de saúde. No entanto, a informação pública disponível sobre esses incidentes, que quantifique o seu impacto, é escassa. Com este estudo, pretendemos, utilizando dados disponíveis publicamente em Portugal, (1) identificar datas chave durante o evento do ciberataque na Região Autónoma da Madeira (RAM) e, dada disponibilidade de informações públicas disponíveis na Região, (2) medir o impacto económico usando o cenário do ataque ao Hospital Nélio Mendonça como estudo de caso.

Métodos: Recolhemos dados de várias fontes nacionais e locais sobre o ciberataque na RAM em 2023, e construímos uma linha temporal dos eventos chave. Posteriormente, perante a disponibilidade informações públicas sobre os ciberataques (quedas de atividade relatadas e tempo de inatividade) foram estimados os custos diretos do evento. Os dados foram produzidos com base na atividade planeada através do programa de contratualização hospitalar. Utilizamos uma análise de sensibilidade para ilustrar uma faixa potencial de valores com base em suposições.

Resultados: Os impactos financeiros foram obtidos do ponto de vista dos custos, onde os valores estimados variaram de um mínimo de € 113.011,88 a um máximo de € 2.260.237,60, dependendo das percentagens de recursos afetados e do número de dias úteis de inatividade. Estas estimativas consideraram os custos de consultas externas, hospitalização e clínicas ambulatórias durante o período de inatividade, para um máximo de 5 dias úteis.

Conclusões: Para melhorar as capacidades de cibersegurança nos hospitais, é importante fornecer informações robustas que sustentem a tomada de decisão. O nosso estudo fornece informações valiosas e *insights* preliminares que podem ajudar as organizações de saúde a

compreender melhor os custos e riscos associados às ameaças cibernéticas e a melhorar as suas estratégias de cibersegurança. Além disso, demonstra a importância da adoção de estratégias preventivas e reativas eficazes, como planos de contingência, bem como o aumento do investimento em melhorar as capacidades de cibersegurança nesta área crítica, com o objetivo de alcançar a ciber-resiliência.

Palavras-chave: cibersegurança; informática médica; impacto económico; custos; segurança; privacidade; ciberataque; violação de dados; sistema de saúde.

Artigo submitido: Frontiers In Digital Health

Abstract

In the past decade, the frequency and magnitude of cyberattacks in the healthcare sector have increased, ranging from network intrusions to ransomware incidents that encrypt files and restrict data access. Such attacks can severely compromise patient safety by targeting electronic health records, critical clinical information, and essential support systems, thereby delaying hospital activities such as surgeries and medication delivery. Beyond threatening lives, cyber incidents also have substantial financial consequences due to service disruptions. However, publicly available information that quantifies their economic impact remains scarce.

This study aimed to *(1)* identify key dates and events associated with the 2023 cyberattack in the Autonomous Region of Madeira, Portugal, and *(2)* estimate its economic impact using Hospital Dr. Nélio Mendonça as a case study. Data were collected from national and local sources to reconstruct a timeline of events. Based on publicly available information on activity disruption and downtime, we estimated direct costs using the hospital's contractual activity plan. A sensitivity analysis was performed to illustrate a potential range of outcomes under varying assumptions.

Estimated financial losses ranged from a minimum of €113,011.88 to a maximum of €2,260,237.60, depending on the percentage of affected resources and the number of working days disrupted. These estimates accounted for outpatient consultations, hospitalizations, and ambulatory services over a maximum of five working days.

Our findings highlight the importance of robust information to support decision-making in hospital cybersecurity. This study provides valuable preliminary insights into the costs and risks associated with cyber threats and underscores the need for effective preventive and reactive strategies, such as contingency planning and sustained investment, to enhance cyber-resilience in healthcare.

Keywords: cybersecurity; health informatics; economic impact; costs; patient safety; privacy; cyberattack; data breach; healthcare system

Introduction

In recent years, the delivery of healthcare services has become increasingly digital, in part due to the widespread adoption of information systems (IS). (1) While these systems have significantly reshaped the quality and efficiency of healthcare provision, their adoption has also introduced inherent risks. (2, 7-9) Indeed, this growing digitalization has made healthcare institutions particularly vulnerable to cyberattacks. Recent years have witnessed a significant increase in the frequency, sophistication, and impact of cyber incidents targeting hospitals and public health organizations. (10)

Healthcare is considered an attractive target for cybercrime, largely due to the vast amount of personal and sensitive data stored within hospital information systems. (11) Over the past decade, the frequency and scale of cyberattacks in healthcare have grown, ranging from network intrusions to file encryption that restricts data access. (2, 12) For example, the global WannaCry ransomware attack in 2017 was unprecedented in scale and significantly disrupted services at Hospital Garcia de Orta in Portugal's National Health Service. (3) Although not directly aimed at healthcare institutions, the incident exposed the fragility of these systems and demonstrated how health infrastructures worldwide remain highly susceptible to cyber threats. (3, 13-15)

Cyberattacks in healthcare are critical not only because of the type of information at risk but also due to their potential consequences for patient safety. Unauthorised access to electronic health records, manipulation of critical clinical information, or disruption of essential support systems can delay surgeries, medication administration, and other treatments. Such risks may paralyse healthcare systems, expose personal data of multiple stakeholders, erode patient trust, and ultimately threaten human lives. (16, 17) According to the European Union Agency for Cybersecurity (ENISA) (10), cyberattacks on healthcare institutions go beyond service interruptions; they directly affect patient safety, clinical operations, and public trust in health systems. In this context, cyber-resilience is understood as the ability of organizations to effectively prepare for, respond to, and recover from cyber incidents. The literature highlights several recommended practices, including contingency planning, regular incident response testing, redundancy of critical systems, and continuous training for healthcare and IT professionals. In addition, systematic audits based on established frameworks, such as NIST and

COBIT 2019, are considered essential for assessing system maturity and identifying vulnerabilities in a structured way. (18)

The European Cybersecurity Act (Regulation (EU) 2019/881) represents a key milestone in consolidating the European Union's cybersecurity policy, by granting ENISA a permanent mandate and establishing a European cybersecurity certification framework for ICT products, services, and processes (4). This mechanism, recognised across all Member States, stratifies assurance levels and aims to foster the adoption of more secure and resilient solutions in critical sectors. In the health domain, hospitals play a central role as critical infrastructures, highly dependent on digital systems to ensure clinical care, sensitive data management, and continuity of services (5, 6). Such vulnerability makes them attractive targets for cyberattacks, whose consequences may result in service disruptions, increased risks to patient safety, and loss of public trust (5). In this context, the European framework complements existing literature by providing a normative basis that underpins the need to strengthen the cyber-resilience of health systems, harmonizing practices and raising security standards across the European Union.

The consequences of cyberattacks extend beyond risks to patient safety and include significant financial implications. (7) It is estimated that a single cyber incident can cost a hospital up to USD 7 million, and alongside reputational damage, such events may jeopardise long-term operations and revenue. (7, 19) Given the strong dependence of healthcare delivery on information systems, it has become increasingly challenging to quantify the true economic impact of such events. Moreover, although cybersecurity is critical for patient safety, it has historically been undervalued. Even though cyber incidents must be reported and recorded, the resulting data are rarely processed or systematically evaluated, representing a missed opportunity to understand vulnerabilities, risks, and threats. (20, 21) Media reports have documented delays in outpatient follow-up consultations, diagnostic testing, and elective surgeries due to difficulties accessing clinical data. (18) Nevertheless, a recent review of cyber incidents during the COVID-19 pandemic found only six well-documented cases with detailed information available. (22)

At the national level, empirical research on the costs of cyber incidents in the public healthcare sector remains limited. Yet, there is growing recognition of the need for studies that quantify economic impacts in order to support investment decisions in cybersecurity and contingency planning. (17) In Portugal, Portela et al. (2022) conducted a descriptive case study simulating the

economic impact of ransomware attacks on public hospitals, estimating costs between €115,883 and €2.3 million depending on downtime and affected services. (17) While valuable, this work relied on hypothetical scenarios due to limited availability of detailed operational data. By building on this evidence, the present study examines the real-world case of the SESARAM Hospital Dr. Nélio Mendonça cyberattack, providing empirical data to complement previous estimates and further highlight the need for strengthened cyber-resilience in healthcare.

On August 6, 2023, the Madeira Regional Health Service (SESARAM) suffered a large-scale cyberattack that compromised information systems and disrupted essential services across hospitals and primary care centers in the region. This incident caused significant service interruptions and required a comprehensive response to mitigate its impacts. (23)

The European Commission and the OECD have emphasised the importance of collaborative approaches among governments, healthcare institutions, and cybersecurity experts to promote integrated policies and sustainable investments. (24)

Therefore, this study aims to use publicly available data in Portugal to (1) identify key dates during the cyberattack in the Autonomous Region of Madeira and (2) measure its economic impact, using Hospital Dr. Nélio Mendonça as a case study.

Methods

To estimate the direct economic impact of the cyberattack that occurred at Hospital Dr. Nélio Mendonça (SESARAM), an exploratory approach based on publicly available secondary data was used. The methodology aimed to reconstruct the event from official and media sources, identify the period of greatest service disruption, and, based on the hospital's contractual values, estimate the costs associated with inactivity. Thus, 1) we collected the available data from various national and local sources (e.g., Jornal da Madeira, Público, Diário de Notícias, official SESARAM documentation, IASaúde, among others) covering the cybersecurity episode during 2023, to construct a timeline of the identified key events. To analyse the economic impact, 2) we developed a hypothetical scenario based on the costs related to affected resources, percentages of inactivity, and the duration of the disruption. This approach was based on publicly available hospital data, using information from the hospital contractual program. However, the absence of detailed official data on losses by service category justified the construction of a counterfactual scenario, complemented by a sensitivity analysis. (17). This made it possible to assess the potential variation of direct costs according to different percentages of activity affected and duration of disruption, thus contributing to a broader understanding of the possible economic effects of incidents of this nature. For the simulation scenario, data were obtained from public domain sources and organised as follows:

Care Category	**Contractual program value (€)**
Outpatient care [a]	8.345.400,00
Inpatient care [b]	46.767.790,00
Ambulatory care [c]	30.089.300,00
Emergency care [d]	26.976.350,00
Day hospital [e]	833.040,00

Source: JORAM(25); [a] Hospital medical consultations – first and follow-up visits; [b] Hospital inpatient

care for acute patients, inpatient care in the Surveillance Unit (UDV), and inpatient care in health centers; [c] Medical consultations in primary care (in-person), clinical acts, and Complementary Diagnostic and Therapeutic Tests (CDTT) performed in primary care; [d] Hospital emergency and emergency care in health centers; [e] Sessions carried out in day hospital.

These values represent the productive capacity contractually assigned to the hospital and served as the basis for building the revenue loss scenarios due to inactivity during the cyberattack.

Estimates and construction of the impact scenario

An interval of 1 to 5 working days of inactivity was assumed, based on the official calendar of working days in Portugal, reflecting the possible estimated period of greatest hospital disruption reported in public sources. To estimate the degree of impact on healthcare activity, different levels of disruption were defined — 25%, 50%, 75%, and 100% — representing progressively more severe scenarios. The choice of these percentages was guided by a quintile logic, allowing systematic exploration of gradual variations in economic impact without resorting to arbitrary values. This approach facilitates comparison with similar studies (13) and supports the formulation of mitigation strategies adjusted to different levels of severity.

The impact estimate was calculated based on the percentage of service disruption, number of days, and contract value. The sensitivity analysis was included to compensate for the lack of direct empirical data on the exact downtime per service, which is common in cyberattacks due to confidentiality and lack of detailed public audits.

This method makes it possible to:

- Represent realistic impact scenarios with different levels of severity;
- Provide minimum and maximum ranges of values that support cybersecurity investment decisions;
- Illustrate how small variations in time or in the percentage of activity affected can have major economic implications.

Results

This section presents the main results of the analysis of the direct economic impact of the cyberattack that occurred at SESARAM. First, the timeline of critical events related to the incident is described, to contextualise the service interruption. Then, the direct costs associated with the suspension of healthcare activities are estimated, based on contractual program values and planned daily output. Finally, a sensitivity analysis is performed to illustrate the variation of the economic impact according to different scenarios of disruption duration and percentage of activity affected. This approach makes it possible to explore the potential magnitude of losses, even under uncertainty about the exact extent of the disruption.

Timeline of key events identified

On August 6, 2023, the attack was detected at 08:11 a.m., resulting in a generalised malfunction of SESARAM's IT network. This compromise required the adoption of manual procedures in several healthcare units, which made access to patients' clinical records difficult. (26) On the following day, August 7, 2023, SESARAM confirmed the severity of the incident and announced the suspension of all non-urgent clinical activities, including routine consultations, scheduled surgeries, and laboratory tests, in order to prioritise urgent services. (27) One week after the attack, on August 11, 2023, SESARAM communicated the gradual restoration of essential services, starting on August 14, 2023, with the support of specialised cybersecurity teams. However, some critical functionalities remained compromised. (28) Only on November 18, 2023, did SESARAM relaunch its official website, marking an important milestone in the recovery of affected systems and restoring an essential communication platform for patients and healthcare professionals. (29)

Figure 1 – Key events of the cyberattack in Madeira

Case study: Hospital Dr. Nélio Mendonça

Based on SESARAM's hospital contractual program (Contract No. 134/2023), it was possible to determine the annual financial values allocated to different components of the healthcare activity of Hospital Dr. Nélio Mendonça. These data were mainly collected from publicly available official sources, using a snowball sampling method until evidence saturation. The values were aggregated into five major categories: outpatient consultations, inpatient care, ambulatory care (including diagnostic and therapeutic services), emergency care, and day hospital. Assuming a total of 250 working days per year, the average contractual daily value was calculated, totalling approximately €452,047.52 per day.

This daily value was used as the basis for calculating the direct costs of hospital inactivity caused by the cyberattack. From the dates identified in the timeline and the confirmation of the suspension of non-urgent clinical activity, a baseline scenario was defined with three working days of partial interruption (50%) of activity, amounting to €678,071.28, representing significant losses for the institution.

This value represents a conservative estimate of operational losses, corresponding only to unperformed activity and not accounting for other indirect costs, such as crisis management, acquisition of external cybersecurity services, administrative response time, or reputational repercussions. (27)

Given the absence of precise data on the duration and severity of the disruption by service category, a sensitivity analysis was conducted to explore different impact scenarios. This analysis assumed combinations of two critical factors:

- Number of working days affected (from 1 to 5);
- Percentage of healthcare activity compromised (25%, 50%, 75%, 100%).

The objective was to illustrate the plausible range of direct financial impacts of the attack, providing hospital management and policymakers with a practical tool for planning and prevention.

The values ranged from a minimum of €113,011.88 to a maximum of €2,260,237.60, depending on the percentage of resources affected and the number of working days of inactivity. For example, a 75% disruption over four working days would result in direct losses exceeding €1.35 million, highlighting the economic risk associated with digital dependence and the absence of functional redundancy – Figure 2.

% of activity affected (assessed via impact on the total contracted value in the programme contract)	Working days of hospital activity (based on 250 working days/year)				
	1	2	3	4	5
25%	113,011.88 €	226,023.76 €	339,035.64 €	452,047.52 €	565,059.40 €
50%	226,023.76 €	452,047.52 €	678,071.28 €	904,095.04 €	1,130,118.80 €
75%	339,035.64 €	678,071.28 €	1,017,106.92 €	1,356,142.56 €	1,695,178.20 €
100%	452,047.52 €	904,095.04 €	1,356,142.56 €	1,808,190.08 €	2,260,237.60 €

Figure 2 – Sensitivity analysis of a cyberattack considering the contractual base cost (23), including outpatient care[a], inpatient care[b], ambulatory care[c], and emergency care[d]. Legend – [a] Outpatient consultations (first and follow-up); [b] Inpatient care (acute hospital, USV, and primary care centers); [c] Primary care medical consultations, clinical acts, and diagnostic services, plus day hospital; [d] Hospital emergency and primary care emergency services.

Discussion

The results of this study reinforce the need to invest in cybersecurity measures to protect hospital infrastructures. Despite SESARAM's efforts to modernise its systems, the cyberattack revealed significant gaps in preparedness for responding to cyber incidents and was considered one of the most severe ever recorded in the Autonomous Region of Madeira. (27, 30)

The impact of the incident was reflected in the temporary suspension of several non-urgent clinical services, with direct effects on the continuity of care provided to patients. In addition, cyberattacks of this kind have the potential to cause substantial financial losses, affecting not only immediate operations but also institutional reputation.

System recovery began gradually about one week after the incident, with the support of specialised companies in mitigating cyber threats and restoring critical healthcare systems. (23) However, full normalization was a prolonged process, symbolically marked by the relaunch of SESARAM's official website on November 18, 2023; an important milestone in restoring the institution's digital operations. The sensitivity analysis demonstrated that even under conservative scenarios of partial hospital activity disruption lasting only a few days, the direct costs associated with a cyberattack can reach substantial values, easily exceeding €500,000. These findings are consistent with international estimates. For example, Jalali and Kaiser (2018) (7) estimated that the average cost of a hospital cyberattack can reach USD 7 million, considering not only operational losses but also reputational damage and mitigation costs. Similarly, studies conducted in the United Kingdom following the WannaCry attack (31) indicated financial losses of approximately £92 million, of which around £20 million corresponded to the suspension of clinical activities. Although the present study focuses only on direct costs and relies on simulated data, the results are coherent with these findings and reinforce the urgency of robust cyber-resilience strategies. The sensitivity analysis thus proved to be a useful tool to anticipate impacts under different levels of severity, enabling contingency planning tailored to the reality of each institution.

It is important to highlight that even short-term service disruptions can have significant financial consequences if they affect a substantial portion of hospital activity. Therefore, it is essential to implement preventive measures such as redundant backups, regular incident response testing, and effective contingency plans.

The lack of detailed public information on downtime across different services - such as emergency care, outpatient consultations, or administrative processes - reveals an important gap in transparency and crisis communication. Furthermore, the scarcity of available data on cybersecurity incidents in healthcare institutions highlights the need for greater transparency and systematic, detailed reporting. Nevertheless, since this is highly sensitive information with the

potential to expose critical vulnerabilities of healthcare infrastructures, disclosure must be carefully considered. It is crucial to strike a balance between the need for transparency and the duty to protect strategic data that could be exploited by malicious actors. To this end, the creation of secure mechanisms for information sharing between public entities, healthcare professionals, and cybersecurity experts is recommended, ensuring both confidentiality and institutional preparedness.

Our findings align with the cost ranges previously simulated by Portela et al. (2022), who estimated that ransomware incidents in Portuguese hospitals could generate losses exceeding €2 million under severe disruption scenarios. (17) Unlike their study, which was necessarily based on hypothetical assumptions, our analysis relies on real-world SESARAM data. Together, these complementary case studies reinforce the growing evidence base on the economic risks of hospital cyberattacks and underscore the urgency of investment in preventive and reactive cybersecurity measures across European health systems.

Finally, although the focus of these studies was on direct economic impacts, it is crucial to acknowledge indirect effects not accounted for, such as loss of patient trust, prolonged reputational damage, and the technical and human costs associated with recovery. To address these challenges, the Regional Government announced an additional €15 million investment in SESARAM's cybersecurity, aimed at modernizing technological infrastructure and implementing preventive measures to strengthen the digital resilience of the regional health system. (28)

Conclusions

The growing dependence on information systems in healthcare makes institutions particularly vulnerable to cyberattacks, with significant financial and operational consequences. This study provides support on the literature and preliminary insights that can support organizations in risk assessment and in developing strategies to mitigate the impact of future cyber incidents.

Our results highlight the importance of robust data to support decision-making and cybersecurity planning, as well as the need for greater transparency and information sharing among stakeholders.

Based on these findings, we recommend strengthening IT infrastructure, including the implementation of regular automated backups and ensuring redundancy across systems to

safeguard operational continuity. It is also essential to invest in workforce capacity-building through regular cybersecurity training sessions focused on threat detection and response. Furthermore, the development of a comprehensive incident response plan is suggested, encompassing detailed protocols for rapid reaction to cyberattacks, along with periodic simulations to test their effectiveness. Finally, continuous security monitoring should be prioritised, with the adoption of systems capable of detecting suspicious activity in real time and the establishment of a team dedicated exclusively to cybersecurity.

In summary, this study highlighted the economic and operational impacts of a cyberattack on SESARAM, demonstrating the importance of preventive and reactive strategies in hospital cybersecurity. The direct costs, combined with the broader implications for public trust, underscore the urgency of strategic investments in technological infrastructure, workforce training, and incident response planning.

Conclusion (short version)

This study demonstrates that cyberattacks on healthcare institutions can generate substantial direct economic losses, even under conservative scenarios of disruption. Strengthening IT infrastructure, enhancing staff training, and implementing robust contingency and incident response plans are essential to achieve cyber-resilience. The findings highlight the urgency of strategic investments to protect both patient safety and the financial sustainability of healthcare systems.

References

1. JPL. KCL. Management Information Systems: Managing the Digital Firm. 16th edition ed2019.
2. The Lancet Respiratory M. Digital health: balancing innovation and cybersecurity. Lancet Respir Med. 2021;9(7):673.
3. Noticias Dd. Tentativas de ataque a hospitais de norte a sul continuaram mesmo após alerta no Garcia de Orta 2022 [Available from: https://www.dn.pt/sociedade/tentativas-de-ataque-a-hospitais-de-norte-a-sul-continuaram-mesmo-apos-alerta-no-garcia-de-orta-14835607.html.
4. Union E. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification. 2019.
5. ENISA. Health Threat Landscape 2023 [Available from:

https://www.enisa.europa.eu/publications/health-threat-landscape.
6. WHO. Global strategy on digital health 2020-2025 2020–2025 [Available from: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf.
7. Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. J Med Internet Res. 2018;20(5):e10059.
8. Ghafur S, Grass E, Jennings NR, Darzi A. The challenges of cybersecurity in health care: the UK National Health Service as a case study. Lancet Digit Health. 2019;1(1):e10–e2.
9. Dönmez E, Kitapçı N, Kitapçı OC, Yay M, Aksu PK, Köksal L, et al. Readiness for Health Information Technology is Associated to Information Security in Healthcare Institutions. Acta Inform Med. 2020;28(4):265–71.
10. Centre ECC. ENISA Threat Landscape 2023 2023 [Available from: https://ec.europa.eu/newsroom/ECCC/items/806536/.
11. Cyberattacks Cripple Dozens of U.S. Hospitals. AJN The American Journal of Nursing. 2021;121(2):18.
12. Journal H. Healthcare Data Breach Statistics [Available from: https://www.hipaajournal.com/healthcare-data-breach-statistics/.
13. SAPO. Piratas informáticos atacam hospital Garcia de Orta 2017 [Available from: https://sol.sapo.pt/artigo/549734/piratas-informaticos-atacam-hospital-garcia-de-orta-.
14. SPMS. Circular Normativa n.º 01 - SPMS: Medidas excepcionais ciber-segurança 2017 [Available from: http://spms.min-saude.pt/wp-content/uploads/2017/05/Circular-Normativa-n%C2%BA1-SPMS-medidas-ciber-seguran%C3%A7a-v.2.pdf.
15. Publico. Hospital Garcia de Orta alvo de ataque informático. No Litoral Alentejano houve uma tentativa de ciberataque 2022 [Available from: https://www.publico.pt/2022/04/26/sociedade/noticia/hospital-garcia-orta-alvo-ataque-informatico-2003841.
16. DBE MJ. Public Health Informatics and Information Systems: Springer International Publishing; 2020.
17. Portela D, Frade S, Patrício P, Cruz-Correia R. Perspectives on the Present and Future of Electronic Health Records in Portugal. 2022. 2022.
18. HIMSS. 2022 HIMSS Healthcare Cybersecurity Survey 2022 [Available from: https://www.himss.org/sites/hde/files/media/file/2023/04/03/2022-himss-cybersecurity-survey.pdf.
19. Claunch D, McMillan M. Determining the right level for your IT security investment. Healthc Financ Manage. 2013;67(5):100–3.
20. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018;113:48–52.
21. Zarocostas J. Health under cyberattack. Lancet. 2021;398(10303):829–30.
22. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin M-V, Calcavecchia F, Anderson D, et al. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making. 2020;20(1):146.
23. Um mês depois do ciberataque que condicionou o serviço regional de saúde da Madeira [press release]. 2023.
24. OECD. OECD Policy Framework on Digital Security 2021 [Available from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf.
25. JORAM. Contrato n.º 134/2023. In: CIVIL SRDFEDSEP, editor. 2023.

26. Ciberataque força suspensão de actividade clínica no Serviço de Saúde da Madeira [press release]. 2023.
27. SESARAM confirma ciberataque e suspende atividade não urgente desta segunda-feira [press release]. 2023.
28. Saúde da Madeira continua a repor "serviços fundamentais" uma semana após ciberataque [press release]. 2023.
29. SESARAM relança site após ataque informático [press release]. 2023.
30. Ciberataque ao SESARAM foi dos maiores registados na Região e já foi reivindicado [press release]. 2023.
31. WannaCry ransomware attacks cost the NHS £92m. Computer Fraud & Security. 2018;2018(11):1–3.