Health Policy and Technology 14 (2025) 100955

Contents lists available at ScienceDirect

Health Policy and Technology

journal homepage: www.elsevier.com/locate/hlpt

Original Article/Research

Assessing the impact of technology partners on the level of cyberattack damage in hospitals

Yannik Angler [a,*], Steffen Flessa [a], Emilia Grass [b], Olav Goetz [c]

[a] University of Greifswald, Greifswald, Germany
[b] Karlsruhe Institute of Technology, Karlsruhe, Germany
[c] APOLLON University of Applied Science GmbH, Bremen, Germany

ARTICLE INFO

Keywords:
Technology partnerships
Cybersecurity
Medical devices
Emergency department
Discrete event simulation

ABSTRACT

Objective: Reliable performance of medical devices is crucial for hospitals. However, these devices are increasingly connected with the internet and, thus, prone to cyberattacks resulting in risks for patient safety and financial loss. As the number of specialists in this field is limited in most hospitals, technology partnerships with medical technology manufacturers can be a suitable concept for increasing the level of security or limiting damage in the event of a cyberattack.

Methods: Based on a discrete event simulation model (DES), the effects of security incidents with different degrees of impact on downtime costs, length of stay, staff utilization and lost arrivals in an emergency department of a general hospital were modelled and simulated. The effects of a technology partnership were simulated using what-if scenarios in order to be able to draw conclusions about the benefits by comparing the avoidable damage effects and the investment costs incurred for a technology partnership.

Results: Depending on the scenario, the resulting savings range from €245,579 to €315,768, with a cost-benefit ratio between 4 and 5 over a 21-day period. Non-financial benefit (e.g. shorter lengths of stay or reduction IT resources) can also be achieved.

Conclusion: Our analysis demonstrates that the level of security for hospitals and their medical devices as well as the operational functionality in the event of damage can be increased if such a concept it applied, i.e., patient safety can be increased while costs can be cut.

List of abbreviations

CBA	Cost-benefit analysis
CBR	Cost-benefit ratio
DES	Discrete event simulation
DM	Damage model
ED	Emergency department
FDC	Financial downtime costs
HM	Hospital model
IoMT	Internet of Medical Things
LOS	Length of stay
LPA	Lost patient arrivals
LPR	Lost patient revenue
MD	Medical Devices
MTM	Medical technology manufacturers
MTS	Manchester triage system
OWSA	One-way sensitivity analysis
TP	Technology partnerships
TPM	Technology partnership model

Lay summary

Digital networking in the hospital sector increases the risk of cyberattacks, which can have serious consequences for patient care and the profitability of hospitals. Medical devices in particular are a frequent target of attacks as they are often outdated. Technology partnerships between a medical device manufacturer and a hospital can provide a novel security concept that helps hospitals protect their medical devices. Our research study shows that in the event of a cyberattack, a technology partner's technical expertise and additional human resources can

* Corresponding author at: University Greifswald, Friedrich-Loeffler-Straße 70, 17489, Greifswald, Germany.
E-mail addresses: yannik.angler@stud.uni-greifswald.de (Y. Angler), steffen.flessa@uni-greifswald.de (S. Flessa), emilia.grass@kit.edu (E. Grass), Olav.Goetz@apollon-hochschule.de (O. Goetz).

https://doi.org/10.1016/j.hlpt.2024.100955

Available online 29 November 2024

help contain and recover damage faster than if a hospital were to do so without support. This can prevent lost patient revenue due to lost patient arrivals, reduce the burden on hospital staff and improve patient safety. Based on these results, the concept of technology partnerships should be given greater consideration in practice in the future.

Introduction

Digitalization in the healthcare sector holds value-adding potentials for patient care, but also high risks for possible cyberattacks due to increasing interoperability [1,2]. Threats are also increasingly directed against hospitals (e.g. WannaCry Attack [3], Attack on Düsseldorf University Hospital [4])

Medical devices (MD) are a particularly vulnerable gateway for cyberattacks within a hospital. MD are characterized by the fact that they are used to maintain, improve, diagnose, monitor and treat the state of health of patients (e.g. ultrasonic devices; imaging systems). These devices contain software components and can interact in information networks, e.g. to send or receive data [5]. As soon as MD collects health data and exchange it in connected information networks via various communication channels on the Internet, this is referred to as the Internet of Medical Things (IoMT) [6,7]. According to Stern et al. [8], 17 % of hacker attacks succeed in gaining access to a hospital's internal network via a medical device. This is because many MD are characterized by a long service life due to very robust hardware. Over time, this life cycle introduces the risk that the devices' technical security measures become outdated [9]. Many hospitals have a shortage of IT and financial resources to adequately prepare for or respond to cyberattacks [10,11]. As a result, MD are often used beyond their life cycle [12] and modernization measures are not implemented so that networked MD become susceptible to cyberattacks. The associated damage relates not only to financial downtime costs (FDC) such as lost patient revenue (LPR), but also to restricted access to care services, which is why patient safety is at high risk [13].

One possible approach to mitigating this risk to patient safety and reducing or even avoiding FDC are technology partnerships (TP) between hospitals and medical technology manufacturers (MTM). In this paper, it is assumed that a TP refers to a service partnership for MD between a hospital and a MTM over a long-term period (usually 8–10 years [14]), in which the MTM is responsible for the management of all the hospital's MD. This includes the provision of specialists from the MTM who are responsible for the maintenance, repair, modernisation and troubleshooting of the hospital's MD. From a hospital's perspective it is important to consider that a TP is a long-term and significant investment, as the average investment can be between 6 and 25 million euros, depending on the service area (radiology, laboratory, IT) and duration [14].

With the growing number of MD and the increasing threat of cyberattacks, TPs may be a suitable approach to increase the security level for hospitals and their MD. Several potentially suitable security concepts for MD can be derived from literature (see Appendix 1). To the best of our knowledge, none of the analysed scientific studies refer to the potential benefits of TPs to increase the security level of MD in hospitals. Our research aims to fill this gap and investigates the costs and benefits of a previously unexplored security concept in the form of TPs as a financially worthwhile solution for improving the security level of MD in hospitals. Using an established operations research technique, discrete event simulation (DES) [15], within an emergency department (ED) of a general hospital, we aim to assess the effectiveness of such partnerships for the first time.

In summary, our study provides a novel, evidence-based approach to improving cybersecurity in healthcare that has direct implications for operational practice, strategic planning and patient care outcomes in the face of cyberthreats. In this way, the study provides a practical and strategic approach for hospitals and MTM to increase the security level of MD in collaboration and responsibility through the concept of TP. In addition, our study provides a novel approach for the economically evaluation of a security concept prior to its implementation in a hospital, so that limited financial resources in the healthcare sector can be better utilised.

Methods

Discrete event simulation for TP assessment

The *hospital model (HM)* was created in a previous research project to simulate the processes in an ED of a general hospital in Germany [16]. The hospital is a provider of standard care with 250 beds. The ED focuses on internal medicine, general vascular, urology, orthopaedics, anaesthesia and intensive care. The ED ensures care in a rural region 24 h a day, seven days a week [16]. Based on empirical data obtained through observations, expert interviews, process analyses and time studies, Angler et al. [16] simulate the flow of care in the ED using a stochastic DES model, from which various potential improvements for the processes in the ED are derived. The background material of the HM can be found in Appendix 2–4. For the present work, this HM is extended to the scenario of a security incident caused by a cyberattack using MedModel simulation software (10.0.0.3218, 2017, BigBear.ai, Columbia). For better differentiation, this will henceforth be referred to as the *damage model (DM)*. The patient journey can differ between patients based on the urgency of the treatment (blue, green, yellow, orange, red) and is determined by the initial assessment using the Manchester triage system (MTS). Regarding the MTS levels, only the blue/green, yellow and orange levels are taken into account. The exclusion of red patients is justified by the fact that the time recording of acute emergency patients is not ethically justifiable. The patient pathway ends either with inpatient admission to hospital or discharge from the ED (see Fig. 1).

The modification from HM to DM, took place in several coordination phases together with the stakeholders of the project hospital. Based on this, the model and the resources, ED layout, processes and logics it contained are specified in iterative cycles. The recorded patient arrivals from the time study for the HM by Angler et al. [16] are adopted unchanged for the individual MTS stages in consultation with the project hospital. For the model-based mapping of cyber damage in the ED, the different activity and waiting times (e.g. treatment time – see Appendix 3) are increased in DM (see Appendix 5). This slowing down of processes is a key factor in realistically mapping a security incident in the model, as the failure of digital systems (e.g. electronic triage system) severely restricts data transfer and the process must be completely converted to paper-based operation wherever possible. Due to the different types of cyberattacks, the extent of damage caused by a cyberattack can vary greatly. A cyberattack can only cause partial damage, which is why the emergency room can continue to provide limited care. However, the damage can also be so extensive that an emergency room can no longer accept new patients and ambulances must be turned away. This represents an uncertainty that must be taken into account using the sensitivity analysis method. This refers to dealing with uncertainty in input data as a process that can be carried out through a series of runs with alternative input data [17]. The ISPOR-SMDM Good Modelling Practices series recommends estimating and accounting for uncertainty in model parameters using both deterministic and probabilistic sensitivity analyses for valuations [18]. In order to do justice to this uncertainty, a scenario analysis with three damage scenarios (see Fig. 2) was chosen together with the project hospital in order to carry out a differentiated analysis that takes into account conservative and extremely threatening scenarios [19]. This allows conclusions to be drawn about the effects of fluctuations in the level of damage on the parameters LPR, LOS, LPA and resource utilisation, which can also be easily communicated to the decision-makers of the project hospital [20] (see Fig. 2).

All model parameters (see Appendix 3) are increased by the respective percentage in the DM. In addition, time-dependent downtimes are added to the DM. During these downtimes, no new patients can

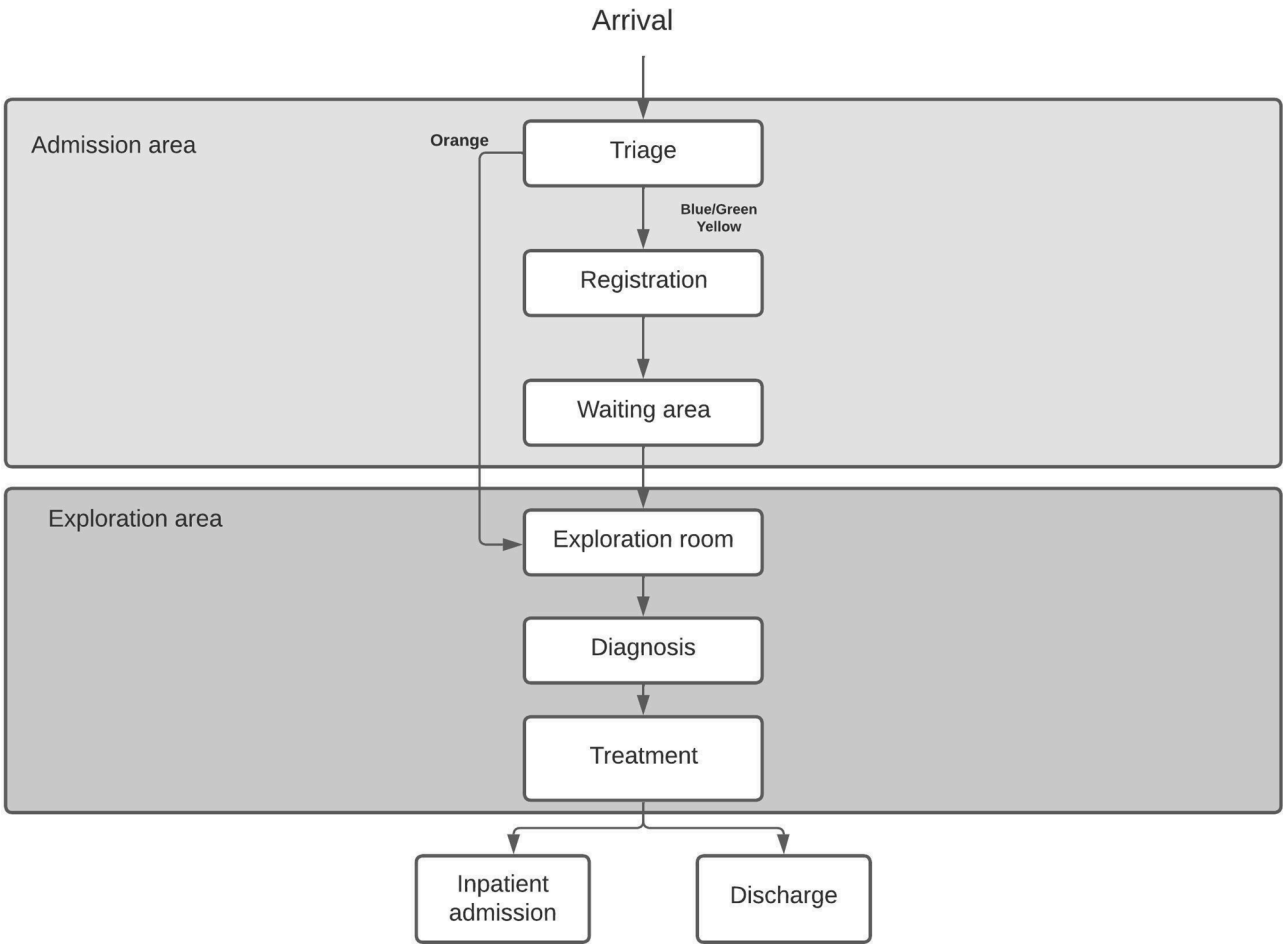


Fig. 1. Patient's journey through the ED [16].

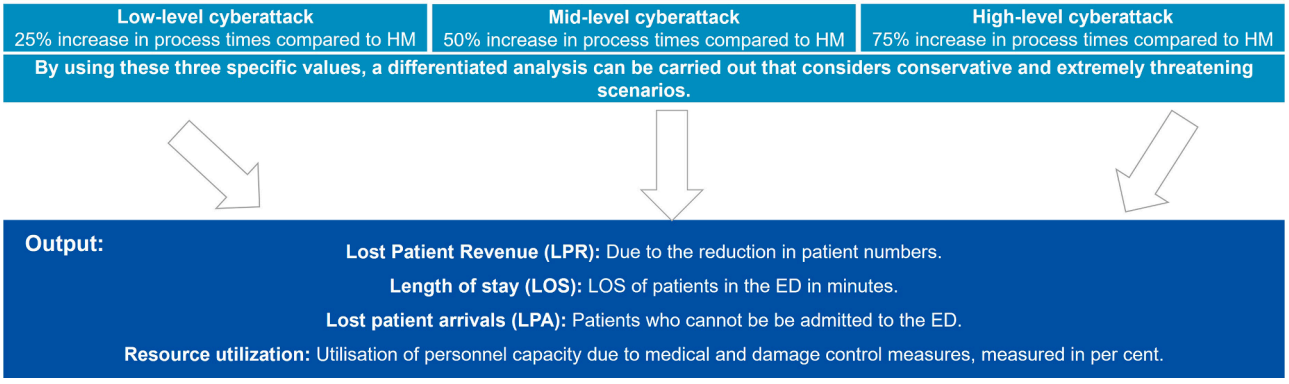


Fig. 2. Damage Scenarios.

enter the system, as the ED is unable to provide care to further patients. These patients are recorded as "LPA". In addition, the "IT" resource is activated during each downtime to restore the EDs operational functions. The duration of IT activity also varies depending on the damage scenario. As a result, the IT resource needs longer to restore normal operations in the event of a high-level incident than in the event of a low-level incident.

Based on the damage scenarios in the DM, a further model is created to analyse the impact of a TP on reducing the extent of damage compared to independent recovery by a hospital. This model is referred to below as the *technology partnership model* (TPM). To quantify the impact of a TP in terms of speeding up the recovery of hospital operations or maintaining partial operations, realistic assumptions about effectiveness have been made based on interviews with 11 experts (see Appendix 6–8). The experts are chief information officers, doctors or MTM. The experts were asked for a quantitative assessment of the impact of TPs on the degree of recovery of care operations in a hospital. Taking into account the already defined threshold values, a degree of impact on the reduction of the level of damage of 25 %, 50 % or 75 % could be selected. Based on the interviews, most experts (5 experts) consider an efficiency level of 25 % to be realistic (see Appendix 8). In consultation with the project hospital, it is agreed to assume the efficiency of 25 % most frequently mentioned by the experts for the impact of a TP on damage reduction compared to the DM. Based on the

interviews, the process times and downtimes in the TPM for each scenario are reduced by the respective impact level of 25 % compared to the respective damage scenario in the DM. The reduction based on the assumption that any damage that occurs can be resolved more quickly with a technology partner due to additional personnel resources and increased medical technology expertise. In addition to IT, another resource is added to the TPM with the name "technology partner". The influence of a technology partner on the restoration of regular operations in the ED can be tracked based on changes to time-dependent variables such as LOS.

To determine the average patient revenue in an ED, the information from Brachmann [21] is used, which defines the average revenue at €1670.73. It should be noted that this research study calculates the amount of damage based solely on the LPR. Other costs that a hospital may incur because of a cyberattack (e.g. ransom fees, legal costs) [22] cannot be determined due to the high variability of individual cases. MedModel's calculation function is used to determine the financial amount of damage per scenario that a hospital loses due to LPR. This function makes it possible to allocate revenues to entities. Entities refer to relevant factors of interest within a system (e.g. patients) [23]. Average patient revenue is calculated based on the daily patient numbers at each MTS level, with total daily revenue calculated by summing all MTS patient revenue. The LPR due to LPA is calculated by multiplying the number of LPA at each MTS level by the average revenue and then summing to the total. To calculate the LPR per day, the total patient revenue from the HM is subtracted from the total patient revenue from the respective DM and TPM scenarios and then the LPR due to LPA is added. The LPR per day for each scenario is then multiplied by 21 days. By calculating the difference between each DM and TPM scenario, the avoidable LPR over 21 days that could potentially be avoided by a technology partner can be derived (see Appendix 9). Next, the extended model is verified and validated. For the verification process, following Banks et al. [23], the debugger functions provided by MedModel are used to ensure that the model scenarios behave as expected. During validation, the model scenarios are accepted as realistic representation of the ED in joint consensus with the project hospital. The duration of a cyberattack until normal operations are restored can vary greatly due to the different effects of the damage. For this reason, the study uses data on the average duration of cyberattack on organisations worldwide from 2020 to 2022 (see Appendix 10). The calculation of the arithmetic mean leads to an assumption of 21 days [24], which is used for the simulation runs.

The simulation runs are started with a one-week warm-up phase to check whether the model works without limitations. Three-week simulation runs are then carried out for each scenario. For the model scenarios, 30 replications are carried out to obtain better information on the average performance of the different scenarios. By conducting several simulation runs and replications, a probability distribution of the target variables is generated as a result, which makes it possible to determine valid parameters despite many random variables in relation to the process times and thus to take parameter uncertainties into account. Due to the scenarios formed in combination with the fact that the present DES model implies a massive use of probabilistic distributions, the authors use a probabilistic scenario sensitivity analysis in this study [20]. The effectiveness of a TP on damage reduction during a security incident is evaluated based on the difference between the damage scenarios and the TP scenarios, focusing on the parameters of LPR, LOS, LPA and resource utilization. A cost-benefit analysis (CBA) [20], is then carried out with the investment required for a TP based on the avoidable LPR caused by a TP.

As cyberattacks and the potential benefits of a TP can occur at different times, it is necessary for the calculation to relate the costs and benefits to a comparable time period using the discounting method. In this context, it is important that the present study focuses on the perspective of the project hospital as a healthcare provider regarding the economic evaluation of a technology partnership using a CBA, in which the term cost refers to economic cost [25]. For discounting, an average TP period of 9 years is assumed based on a TP study that indicates a TP period of 8–10 years based on surveys [14]. The comparison period for discounting is based on the simulation runs (21 days). This study uses a discount rate of 5 % in accordance with the Hannover Consensus, which proposes this discount rate for Germany [26]. Considering the discounting table by Drummund et al. [27], this results in a discount rate of 0.6446 for 9 years (see Appendix 11). In addition to information technology, the ED of the project hospital also operates imaging procedures, but no laboratory. For this reason, only the investment volume for IT (€ 9 million) and imaging (€ 25 million) is included [15]. Calculating the arithmetic mean results in an average investment volume of € 17 million. The following formula is used to derive the present value:

$$PV = X\left[\frac{1}{(1+i)^n}\right]$$

PV = Present Value; X = amount to be discounted; i = interest rate as decimal; n = number of years

We multiply the 17 million by the selected discount value to obtain the present value for 9 years (€10,958,200). This present value is calculated for 21 days (€10,958,200/3287 (9 years in days)*21 days = €70,010). Discounting to a period of 21 days results in a comparative value for the CBA of € 70,010.

Results

Results of LOS, LPA, LPR

In comparison with the HM, the results of various damage scenarios in the DM shows that the LOS for all MTS patients increases significantly (e.g. Scenario 75 % - orange: 497.19 min.; yellow: 240.71 min.; blue/green: 179.60 min.) and the number of patients decreases as the damage level increases, as the ED can only absorb limited capacity into the system due to restricted operations (see Table 1). This leads to limited access to care for patients. These effects are associated with a slowdown in processes due to the failure of important equipment and systems. As a result, various treatment procedures are no longer possible until functionality is restored, which leads to longer waiting times and an overall longer LOS. Furthermore, the damage scenarios in the DM meant that the ED is no longer able to accept new patients in the ED for a certain period of time, resulting in LPA (e.g. Scenario 75 % - orange: 3; yellow: 4; blue/green: 4). It is remarkable that the LPA of critical orange patients increase in the DM scenario 75 %. This can be explained by the fact that the shock rooms, including their medical equipment, could hardly be used for intensive care treatment. This can also have an impact on ambulances, which must transport urgent patients for critical care to an ED that is further away.

In addition to the impairment of the security of care for patients, the hospital incurs high financial losses because of a security incident. The FDC due to fewer patient treatments and LPA also increase with the damage level over a period of 21 days (Scenario 25 %: € 736,792; Scenario 50 %: € 877,133; Scenario 75 %: € 1192,901) (see Table 1). Compared to the DM scenarios, several value-adding improvements were achieved through the TPM scenarios. Table 1 shows that all TPM scenarios lead to a reduction in LPA and a higher number of patients able to pass through the system, while the LOS is significantly reduced (blue/green: from 497.17 min. to 306.26 min.; yellow: from 240.71min. to 167.33 min.; orange: from 179.60 min. to 112.81 min.). This can be explained by the fact that TP provides additional personnel resources with in-depth medical-technical knowledge, so that the effects of damage can be limited to a greater extent (e.g. lower MD downtimes) or normal operation can be restored more quickly (e.g. faster restoration of backups) than if a hospital were to attempt this using only its own IT resources.

Faster provision of required capacities in the ED and the associated

Table 1
Comparison between DM and TPM.

	MTS-Level	Entities	Average LOS (in min.)	Average LPA	Average LPR (in €)
HM	Blue/ Green	20	267.34	0	€ 0
	Yellow	10	129.16	0	
	Orange	5	73.44	0	
DM Scenario 25 %	Blue/ Green	14	316.22	2	€ 736,792
	Yellow	4	155.53	3	
	Orange	2	100.14	1	
TPM Scenario 25 %	Blue/ Green	15	269.44	1	€ 491,195
	Yellow	5	140.45	2	
	Orange	4	84.75	0	
DM Scenario 50 %	Blue/ Green	11	405.02	2	€ 877,133
	Yellow	3	188.01	3	
	Orange	2	138.78	1	
TPM Scenario 50 %	Blue/ Green	12	295.95	1	€ 631,536
	Yellow	4	150.40	2	
	Orange	4	101.20	0	
DM Scenario 75 %	Blue/ Green	7	497.17	4	€ 1,192,901
	Yellow	2	240.71	3	
	Orange	2	179.60	3	
TPM Scenario 75 %	Blue/ Green	9	306.26	3	€ 877,133
	Yellow	3	167.33	2	
	Orange	3	112.81	0	

increase in the number of patients as well as the reduction in LOS and LPA, TP also leads to lower FDC during a security incident (see Fig. 3).

When comparing the avoidable FDC with the discounted investment volume over 21 days, it becomes clear that the financial benefit components significantly exceed the costs that a hospital must incur for TP. The potential savings due to damage limitation through a TP range from €245,597 (factor 4) to €315,768 (factor 5) per scenario (see Table 2).

Table 2
CBR of TP.

	Discount unavoidable damage losses	Discounted investment costs (21 days)	CBR of TP
Scenario 25 %	€ 245,597	€ 70,010	**4**
Scenario 50 %	€ 245,579	€ 70,010	**4**
Scenario 75 %	€ 315,768	€ 70,010	**5**

Results of staff utilization

In relation to resource utilization, it is found that the utilization of medical staff in the various DM scenarios decreases compared to HM. It can be assumed that this decrease is related to the decreasing number of patients and the limited treatment options due to the downtime of necessary medical equipment. At the same time, the utilisation of IT resources increases for each DM scenario as IT attempts to resolve the security incident (see Fig. 4). In addition to the financial effects, the results also show that a better spread of IT resource utilisation could be achieved in all TPM scenarios, i.e. the scarce IT personnel resources can be relieved by TP. As a result, a TP can maintain access to care to a higher degree during a security incident or restore it more quickly in comparison to the damage scenarios, which increases the capacity of the medical staff and relieves the burden on IT resources.

Discussion

Protecting hospitals and their MD is critical as these devices often contain sensitive patient data, so a malfunction can result in widespread harm to patients. This fact is supported by Bracciale et al. [5] who found that many healthcare systems are operating MD with critical vulnerabilities, which is highly dangerous. This study has shown that security incidents can significantly increase the LOS of patients in an ED. Numerous studies indicate that a longer LOS in the ED has a negative impact on clinical outcomes [28–30]. In addition, due to limited ED capacity, access to care is more difficult for patients in need of treatment as they must seek care elsewhere, potentially further extending the time of non-treatment. Furthermore, disrupted ED processes due to a cyberattack can also have an impact on the ambulance service, which may have to transport critical patients for whom every minute counts to more distant EDs. Cyberattacks also have a significant impact on hospitals. Our study shows that, depending on the level of damage, a reduction in

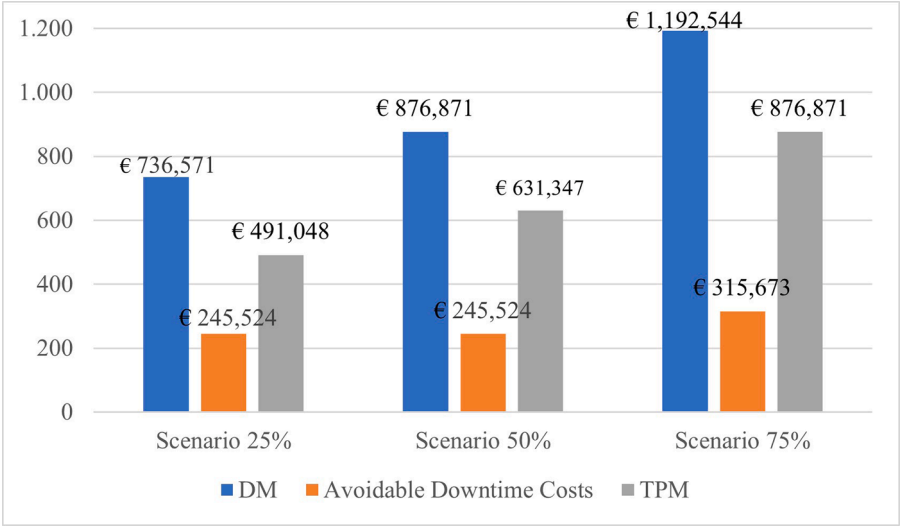
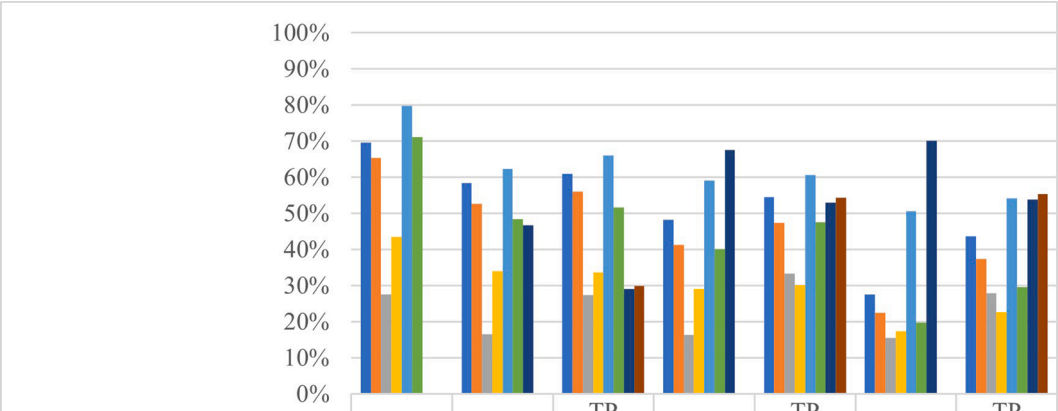


Fig. 3. Comparison of FDC between DM and TPM (in €).



	HM	DM Sce. 25%	TPM Sce. 25%	DM Sce. 50%	TPM Sce. 50%	DM Sce. 75%	TPM Sce. 75%
Nurse Blue/Green/Yellow 1	69.51%	58.38%	60.99%	48.19%	54.47%	27.48%	43.69%
Nurse Blue/Green/Yellow 2	65.40%	52.61%	56.04%	41.18%	47.44%	22.48%	37.38%
Nurse Orange	27.57%	16.47%	27.29%	16.28%	33.32%	15.40%	27.81%
Triage Nurse	43.43%	33.92%	33.70%	29.05%	30.05%	17.34%	22.58%
Physician 1	79.77%	62.32%	66.00%	59.04%	60.67%	50.60%	54.18%
Physician 2	71.17%	48.44%	51.59%	40.09%	47.45%	19.80%	29.61%
IT	0	46.69%	29.10%	67.61%	52.98%	70.03%	53.80%
Technology Partner	0	0	29.94%	0	54.33%	0	55.25%

Fig. 4. Comparison of staff utilization between DM and TPM.

the number of patients treated daily can be expected, leading to LPR. The loss of sensitive patient data, the resulting fines and the potential loss of patient confidence in the reliability of the hospital can also have negative consequences. Due to these consequences, it is important that MD are always protected against cyber threats. According to a Delphi survey by Alanazi [31], most respondents see the biggest challenge in implementing cyber security measures in the time and resource constraints of implementation and the complexity of the systems. Thomasian & Adashi [32] point to the increasing networking of MD and new types of attack vectors. This requires the further development of MD to the latest state of the art [32]. Alami et al. [33] emphasise the importance of raising employee security awareness.

The results of our research study suggest that MTM can provide hospitals with value-adding support in this essential task as part of TP. In addition to additional human resources, technology partners also offer comprehensive technical expertise. These factors help hospitals to increase the security level of their MD and restore normal operations more quickly in the event of damage. Our research study shows that, in addition to the financial effects in terms of avoidable FDC, a TP also has an influence on non-financial effects such as LOS, which can increase patient safety.

In the context of the research study, however, it should be noted that our paper focused exclusively on security incidents involving MD, which corresponds to the scope of a technology partner. This means that the effects of a TP listed above relate exclusively to security incidents on a MD that is managed by a technology partner. However, in addition to MD, a hospital also has many IT systems (e.g. hospital information system), which are also at risk of security incidents. For a holistic security concept, the protection of these applications must also be considered. In this context, the importance of backups as an essential part of a holistic security concept for clinical IT systems and MD should be emphasised. Several scientific studies confirm the importance of backups for the rapid recovery of data in the event of a cyberattack [34, 35]. It should also be noted that the FDC were calculated solely based on LPR. However, it should be noted that a security incident results in a highly number of additional costs for hospitals, which means that the loss of damage is certainly underestimated. Moreover, the calculation of financial losses is based on the volume-oriented Diagnosis Related System remuneration concept, in which the hospital receives a treatment-related payment for each patient treated. The logic of the derived LPR is not transferable to hospitals that are financed via a budgeting system.

The inclusion of other costs (e.g. recovery costs) and remuneration mechanisms (e.g. budgetary scheme) could potentially corroborate the findings of this study and lead to a more accurate estimate of the true FDC and illustrate the financial effects for a wider range of hospitals from different health systems. Furthermore, this study focused exclusively on the ED and not on other departments (e.g. radiology). Besides, the simulation is based on the example of a general hospital, which is why the results cannot be fully transferred to a large university hospital due to the deviating processes and size ratios. DES analysis of the effects of TPs or other security concepts in other departments and a different hospital size could help to substantiate the results of the present study and to generalise the effects of security concepts more to the entire hospital. Nevertheless, the research study has shown that our DES model is suitable for realistically modelling the effects of cyberattacks and security concepts on processes and deriving practical results from them.

The extent to which TPs will be used as a security concept in the future remains to be seen. Many hospitals are under high-cost pressure, which is why the necessary investment in cyber security is lacking [11, 36]. This fact could lead to hospitals remaining reluctant to enter cooperation with a TP. This makes it even more important to apply a suitable CBA procedure, as we have demonstrated in our study, to highlight the value of a security concept like TPs. For practical implementation, a pilot project for a specific device segment can be an option to test a TP and assess the value before making this long-term

investment. In this process, MTM technological expertise can be combined with the hospital's knowledge of clinical processes and critical risk areas for MD cybersecurity to encourage a security-by-design approach.

Regulatory requirements such as the Medical Device Regulation, the NIS2 Directive and the US FDA's Cybersecurity Guidance require a high level of risk management and technical protection for MD [37–39]. TPs offer potential for collaboration between MTM and hospitals to fulfil regulatory requirements and develop practical proposals for their improvement, which can serve as a basis for regulatory decisions.

In this way, we emphasise the potential of TPs for cyber security, which has not yet been recognised by many experts in the healthcare sector.

Conclusion

The paper presents an approach for a future-oriented security concept that is not yet widespread, which should serve as an inspiration for hospitals and MTM. TPs have the potential to provide hospitals with far-reaching support in the face of increasing security threats and an existing shortage of specialists, not only to mitigate or even avoid LPR but also to ensure a high level of patient safety. In this way, TPs represent a strategic shift towards collective action in cybersecurity, encouraging a culture of shared responsibility which could set a precedent for other sectors. As a result, it will be important in the future to consider the value of TPs as part of cybersecurity strategies and measures in healthcare.

Funding

None.

Consent for publication

Not required.

Ethics approval and consent to participate

Not required.

Acknowledgements

The authors would like to thank the project hospital for their comprehensive support in creating the scenarios in the emergency department and for the valuable information from their practical work. The authors would also like to thank all the interviewees for their valuable insights into the value of technology partnerships.

CRediT authorship contribution statement

Yannik Angler: Project administration, Conceptualization, Investigation, Data curation, Formal analysis, Methodology, Validation, Writing – original draft, Writing – review & editing. **Steffen Flessa:** Validation, Writing – review & editing. **Emilia Grass:** Validation, Writing – review & editing. **Olav Goetz:** Supervision, Validation, Writing – review & editing.

Declaration of competing interest

None declared.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.hlpt.2024.100955.

Appendix

Appendix 1. Scientific Studies for cyber security of MD.

Authors	Cyber security of MD	Research Gap
Williams & Woodward (2015) [A1]	The author recommends a standardised assessment and control of cyber security for the future protection of medical devices. This includes technical controls, governance, resilience measures, consolidated reporting, contextual expertise, regulation and standards.	Description: The study identifies cybersecurity vulnerabilities in medical devices and lists a number of selected measures to protect medical devices, but does not analyse the effectiveness of the measures by analysing the cost-benefit ratio. Summary: No cost assessment of security measures for medical devices. No consideration of technology partnerships as a security measure.
Stern et al. (2019) [A2]	The authors recommend more transparency of cybersecurity information in the product summaries of medical devices, which should support doctors and hospitals in the selection of medical devices.	Description: This paper examines the cybersecurity features of digital medical devices using FDA product summaries and also points to closer co-operation between regulators and manufacturers. However, the study does not take into account the further cooperation possibilities between manufacturers and hospitals. Product summaries with cybersecurity content are also essential for hospitals to secure their devices appropriately in daily operations. Summary: No consideration of cooperations between hospitals and medical device manufactures for a better support for hospitals in term of cybersecurity.

(*continued on next page*)

(*continued*)

Authors	Cyber security of MD	Research Gap
Willing et al. (2020) [A3]	Willing et al. (2020) proposes a suitable organisational structure in the form of a joint department for medical technology and information technology as a solution for the secure operation of medical devices.	Description: The study focuses on a suitable organisational structure in the form of a joint department for medical technology and information technology as a solution for the secure operation of medical devices and also provides conclusions on the benefits of this security measure in the form of a success rate for successful or unsuccessful cyberattacks. However, according to the authors, the results on the success rate are exclusively a qualitative statement, meaning that there is no quantitative assessment of the benefits. Furthermore, no potential costs for the organisation of a joint department for medical technology and information technology were focused on. Summary: No quantitative assessment of security measures for medical devices. No consideration of technology partnerships as a security measure.
Thomasian & Adashi (2021) [A4]	As the Internet of Medical Things continues to evolve, the authors recommend additional regulatory guidance to mitigate the risks of the Internet of Medical Things, as well as security awareness measures to increase end-user awareness of the potential dangers of cyberattacks.	Description: This study highlights cybersecurity challenges in the Internet of Medical Things and recommends additional regulatory guidance and measures to promote awareness and security hygiene for end users of medical devices as attack vectors evolve. In terms of expanding cybersecurity guidelines, which are important reference points for both medical device manufacturers and hospitals, the study does not consider the potential for collaboration between medical device manufacturers and hospitals to develop practical suggestions for regulatory guidance enhancements that can serve as a basis for regulatory decisions. Summary: No consideration of co-operation between hospitals and medical device manufacturers as a possible option for the further development of regulatory guidelines to strengthen the security of Internet of Medical Things. No consideration of technology partnerships as a security measure.
Wassermann & Wassermann (2022) [A5]	The authors recommend technical security measures such as network segmentation, patching, data encryption, automated storage of backups, financial measures such as taking out cybersecurity insurance and organisational measures to regularly check devices, networks, user activities and security plans to close vulnerabilities in medical devices.	Description: The article provides a general overview of cyber security risks and gaps (including for medical devices) in hospitals in the form of a structured literature review. In addition to the risks, specific measures to protect critical application systems and medical devices are also mentioned. However, no co-operations or partnerships (e.g. between medical device manufacturers and hospitals) are mentioned with regard to the proposed measures. Summary: No consideration of cooperation or partnership models (e.g. technology partnerships) as a cybersecurity approach to achieve a higher protection level for medical devices.
Baker (2022) [A6]	The author recommends comprehensive patch management for medical devices and that operators start or improve their internal security programme for their medical devices, citing specific guidelines (security section of AAMI's Medical Connectivity FAQs,6 the Center for Internet Security (CIS) Critical Security Controls,13 and NIST SP 1800–88).	Description: The work addresses the paradoxical state of cyber security in medical devices and refers to specific standards for improving security programmes for medical devices (e.g. Critical Security Controls of the Center for Internet Security (CIS) and NIST SP 1800–8), but without naming or discussing specific security measures for medical devices. Summary: No concrete list of measures for more security of medical devices. No consideration of technology partnerships as a security measure.
Cartwright (2023) [A7]	Focus on technical security measures such as regular patching or data encryption and provision of human and financial resources as well as stronger regulation of IoMT as important drivers for increasing the security of medical devices.	Description: The work provides extensive suggestions for measures to improve the protection of medical devices and highlights the need for financial resources for cyber security. However, the work does not consider co-operation or partnerships between medical device manufacturers and hospitals in its proposed measures. It goes on to mention hospitals' financial deficits and the need for cybersecurity funding, but does not suggest ways to overcome this challenge. Summary: No suggestions for solutions to provide financially viable funding for cyber security in hospitals. No consideration of technology partnerships as a security measure.
Javaid et al. (2023) [A8]	Javaid et al. (2023) see an experienced partner as a key factor in protecting against cyberattacks. According to the authors, service providers can, for example, help analyse network environments, identify and eliminate vulnerabilities and advise internal IT on legal compliance	Description: The work provides a comprehensive overview of current practices and trends for cybersecurity in the healthcare sector. The work also proposes several measures for the protection of medical devices. In addition, the work explicitly points out the potential of a reliable and experienced partner to significantly reduce the risk of cyberattacks. However, no specific partnership options and their concrete effects are discussed.

(*continued on next page*)

(*continued*)

Authors	Cyber security of MD	Research Gap
Bracciale et al. (2023) [A9]	Bracciale et al. (2023) recommend, for example, network segmentation, firewalling, efficient recall processes in the event of risks, transparency in the software supply chain with regard to third-party software contained in medical devices, sensitisation of employees and the use of standards (e.g. TR 80,001–2–2:2012).	Summary: No concrete partnership options (e.g. technology partnerships). Description: The study identifies several mitigation measures and improvements for the security of medical devices such as network segmentation and firewalls, improving the efficiency of recalls, raising awareness or promoting the use of standards. However, the study completely ignores the possible effects of cooperation or partnerships on damage limitation and improvements to the security of medical devices.
Mejía-Grand et al. (2024) [A10]	Mejía-Grand et al. (2024) suggest strong passwords, continuous security monitoring of medical devices, the introduction of a secure software development life cycle (SSDLC), regulatory compliance and improved collaboration between medical device operators and manufacturers to increase the security level of medical devices.	Summary: No consideration of technology partnerships as a security measure. Description: The study identifies collaboration, regulatory compliance and continuous safety monitoring as key safety measures for medical devices. The study also aims to encourage industry, research and stakeholders to use these findings to improve safety and ensure patient safety. However, this study does not identify approaches for collaboration options and their concrete potential benefits. Summary: No suggestions for collaboration approaches.

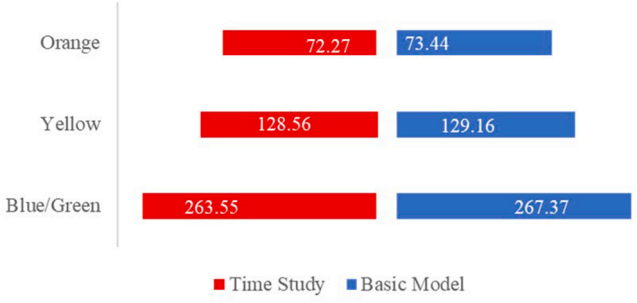
Appendix 2. Resources and activities in the HM [16].

Staff activity in Scenarios	Resources
Triage and admission	Triage Nurse
Collection of blue, green and yellow patients in the waiting area	Nurse Blue/Green/Yellow 1 or Nurse Blue/Green/Yellow 2
Checking the patient's vital parameters	Nurse Blue/Green/Yellow 1 or Nurse Blue/Green/Yellow 2
Receiving the orange patients from the ambulance	Nurse Orange
Inpatient transfer of orange patients	Nurse Orange
Treatment	Physician 1 or Physician 2
Diagnosis	Physician 1 or Physician 2

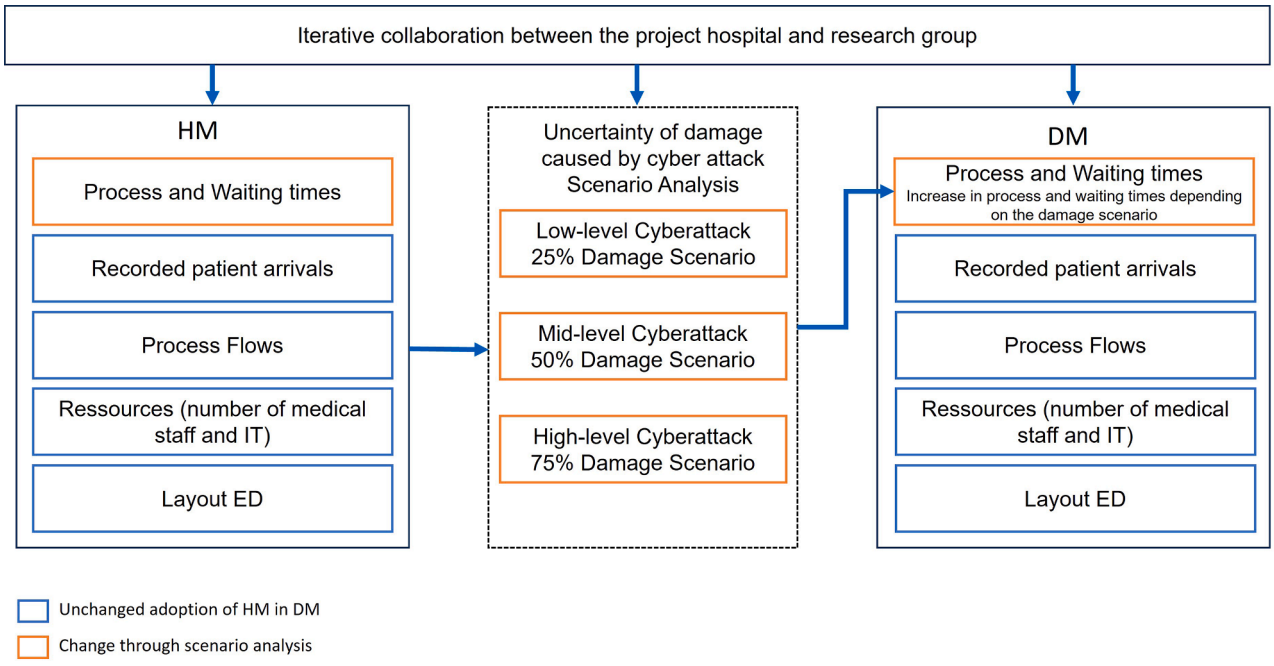
Appendix 3. Process times from time study in mean value and standard deviation in min. [16].

	Blue/Green		Yellow		Orange	
	M	SD	M	SD	M	SD
T1 Time between arrival and triage	3.34	1.51	5.27	3.28	0.0	0.0
T2 Triage & Registration	9.27	1.59	9.51	1.17	8.43	1.45
T3 Time from registration to collection by nursing staff	188.34	70.58	45.54	31.20	0.0	0.0
T4 Collection/reception and transfer of patients to the examination room	4.11	1.43	4.16	1.59	2.51	0.33
T5 Examination of the patient and their vital signs	7.13	2.28	7.59	4.00	0.0	0.0
T6 Time until the doctor arrives	16.29	8.35	9.07	2.33	11.18	3.33
T7 Treatment & Diagnosis	34.27	24.50	46.21	27.22	49.34	1.32
Leaving the ED	263.55	77.09	128.56	48.34	72.27	0.17

Appendix 4. Time comparison between time study and HM according to total mean value in min. [16].



Appendix 5. Transformation HM to DM.

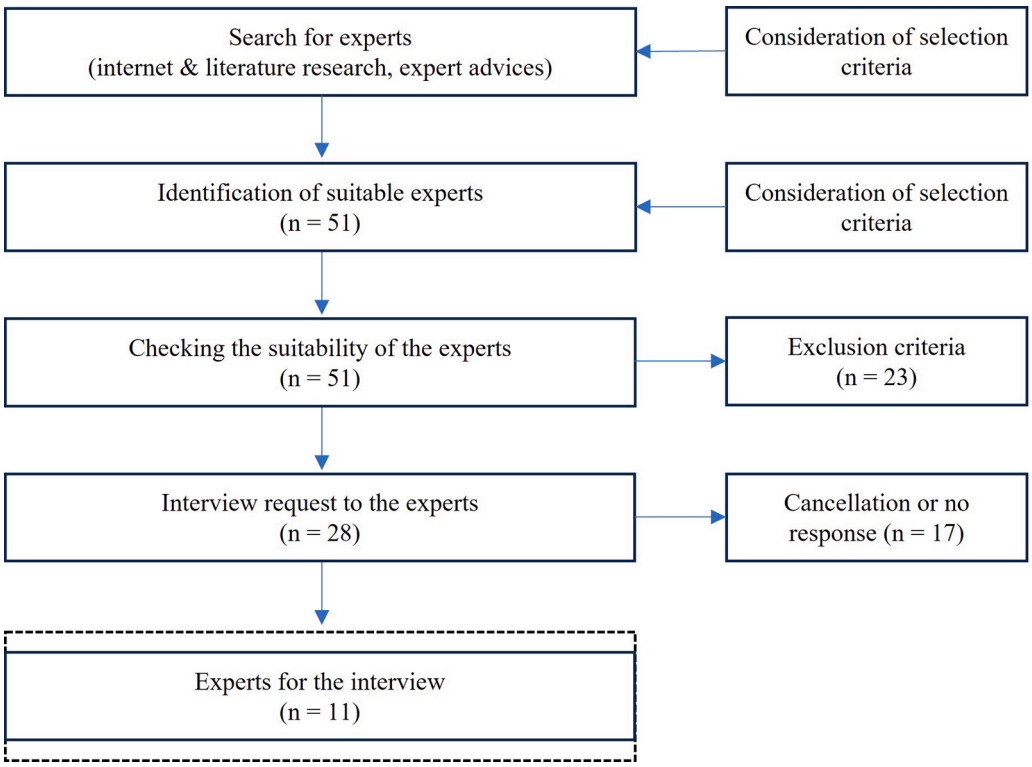


Appendix 6. Inclusion and exclusion criteria for the selection of experts.

Inclusion Criteria	Exclusion Criteria
Experts from the DACH region*	Experts outside of the DACH region*
German and or English-speaking experts	No German and or English-speaking experts
Experts are members of hospital or medical device-related institutions (e.g. Hospitals, MTM, healthcare consulting firms).	Experts are no members of hospital or medical device-related institutions.
Expertise in the use and/or operation of MD.	No expertise in the use and/or operation of MD.
At least five years of practical experience in TPs and/or cybersecurity in the context of MD.	Less than five years of practical experience in TPs and/or cybersecurity in the context of MD.

*DACH stands for three German-speaking countries (D for Germany, A for Austria and CH for Confoederatio Helevtica / Switzerland).

Appendix 7. Process of the expert selection the selection.



Appendix 8. Key content of the interviews.

Institution	Role	Key content	effect estimation
Medical manufacturer	Managing director	Q: From your point of view, what are the main reasons why hospitals enter into a technology partnership?A: Budget security over a long term, gain in expertise, speed of implementation in the course of modernizing the equipment fleet and standardization of the device landscape for improved management.Q: For which hospitals is a technology partnership worthwhile?A: Relevant for every hospital because IT and medical technology are growing ever closer together as a result of increasing networking. For this reason, partnerships are relevant for smaller hospitals that do not have the necessary human resources.Q: What role does cybersecurity play from the perspective of hospitals and manufacturers when entering into a technology partnership?A: An important topic with regard to the secure integration of the devices into the hospital network and the system design of the products.Q: How do you estimate the effectiveness of a technology partnership for a faster recovery of hospital operations in the event of damage compared to recovery measures taken by the hospital alone? • Impact effect on recovery of 25 % possible? • Impact effect on recovery of 50 % possible? • Impact effect on recovery of 75 % possible? A: Estimate is 25 %, because cyberattacks need not be limited to medical devices but also affect clinical application systems that are probably not within the technology partner's area of application. Effects result above all from the partner's gain in expertise.Q: How do you assess the future significance of technology partnerships for cybersecurity?A: High importance because medical devices in hospitals are becoming increasingly outdated, there is ever greater networking between IT and medical technology, medical devices are becoming ever more networkable and hacker attacks on the healthcare sector are on the rise.	25 %
Medical manufacturer	Head of technology partnership division	Q: From your point of view, what are the main reasons why hospitals enter into a technology partnership?A: Many hospitals have limited staff capacity to manage and regularly modernize a large number of medical devices. A technology partner can contribute to greater standardization from a single source. This also creates better visibility of the condition of the equipment.Q: For which hospitals is a technology partnership worthwhile?A: Technology partnerships are relevant for every hospital, as the conditions for a technology partnership can be flexibly adapted.Q: What role does cybersecurity play from the perspective of hospitals and manufacturers when entering into a technology partnership?A: The topic of security is slowly gaining in importance. On the hospital side, this is due to the increasing threat of cyber-attacks on the healthcare sector. On the manufacturer side, the amendment to the Medical Devices Implementation Act (MPDG), which now obliges manufacturers to take	50 %

(*continued on next page*)

(*continued*)

Institution	Role	Key content	effect estimation
		information security into account when developing their devices, has certainly led to manufacturers increasingly promoting security in such partnerships.Q: How do you estimate the effectiveness of a technology partnership for a faster recovery of hospital operations in the event of damage compared to recovery measures taken by the hospital alone? • Impact effect on recovery of 25 % possible? • Impact effect on recovery of 50 % possible? • Impact effect on recovery of 75 % possible? A: 50 % is quite realistic. Medical devices have a complex system structure that has been designed for a specific purpose. Due to this complexity, a technology partner can respond much faster to security incidents as they know exactly what adjustments need to be made. In addition, potential sources of danger can be checked very quickly by manufacturers worldwide - resulting in a faster response time if this threat situation occurs in a hospital. However, a higher impact is unlikely, as information technology can also be threatened by a security incident, for which the hospital is no longer solely responsible, but rather the technology partner.Q: How do you assess the future significance of technology partnerships for cybersecurity?A: Technology partnerships must play an important role in cybersecurity, as medical devices and their operation are sometimes vital and the dangers of cyber-attacks are increasing. For this reason, medical devices must be protected by every conceivable means. This applies to the secure system design, but also to the secure integration and operation of the devices. Close cooperation between the manufacturer and operator of the devices is seen as a key success factor.	
Hospital	Chief Information Officer	Q: From your point of view, what are the main reasons why hospitals enter into a technology partnership?A: The transfer of maintenance work that could generally only be carried out with limited expertise.Q: For which hospitals is a technology partnership worthwhile?A: A technology partnership only makes sense for a hospital if the medical device manufacturer takes over the complete management of the device pool. Only taking over selected devices does not relieve the hospital's IT department in the long term, as it is still occupied with managing other medical devices. This requirement is particularly important for small hospitals as, unlike larger university hospitals, there is often no staff available for medical technology.Q: What role does cybersecurity play from the perspective of hospitals and manufacturers when entering into a technology partnership?A: The topic of cybersecurity is to be seen as a side effect in such partnerships; the main driver for concluding a technology partnership is more likely to be at a financial level.Q: How do you estimate the effectiveness of a technology partnership for a faster recovery of hospital operations in the event of damage compared to recovery measures taken by the hospital alone? • Impact effect on recovery of 25 % possible? • Impact effect on recovery of 50 % possible? • Impact effect on recovery of 75 % possible? A: This is estimated at 25 %, as it is difficult for a hospital with limited human resources and usually no cybersecurity experts to respond quickly to a security incident. This fact alone has the effect of speeding up the restoration of supply operations with the help of a technology partner. However, a major impact is not to be expected, as a security incident usually affects not only medical devices, but also conventional information technology, which is not the responsibility of the technology partner.Q: How do you assess the future significance of technology partnerships for cybersecurity?A: With regard to medical devices, cybersecurity must play an important role in such partnerships. However, there are also other applications in a hospital with critical data that need to be protected. For this reason, the importance of the technology partnership for cybersecurity can only be considered high if the partnership also takes into account the interfaces with information technology.	25 %
Institute for medical products	Expert for Regulatory Affairs for Medical Devices & Medical Devices Software	Q: From your point of view, what are the main reasons why hospitals enter into a technology partnership?A: Possibilities for co-innovation approaches for joint product development and modernization & standardization of the equipment fleet.Q: For which hospitals is a technology partnership worthwhile?A: Larger hospitals have a greater understanding of technology. In addition, both the operator and the manufacturer must contribute their expertise to a partnership. expertise into a partnership, which a large hospital can provide better than a small hospital.Q: What role does cybersecurity play from the perspective of hospitals and manufacturers when entering into a technology partnership?A: It should play a major role in the technology partnership, as the attack surface is becoming ever larger, especially in the area of medical devices, due to increasing networking.Q: How do you estimate the effectiveness of a technology partnership for a faster recovery of hospital operations in the event of damage compared to recovery measures taken by the hospital alone? • Impact effect on recovery of 25 % possible? • Impact effect on recovery of 50 % possible? • Impact effect on recovery of 75 % possible? A: No comment.Q: How do you assess the future significance of technology partnerships for cybersecurity?A: High to moderate importance - due to the digital transformation, the development towards more security in the field of medical technology must generally take place to a greater extent.	No information
Hospital	Physician	Q: From your point of view, what are the main reasons why hospitals enter into a technology partnership?A: Quality assurance and reducing the workload of hospital staff. Otherwise, the limited resources of hospital staff would have to take over the tasks of managing the device pool. Due to the increasing complexity of medical devices, this is difficult for a hospital to achieve.Q: For which hospitals is a technology partnership worthwhile?A: Technology partnerships can be concluded in various models. A leasing model can be relevant even for a	50 %

(*continued on next page*)

(*continued*)

Institution	Role	Key content	effect estimation
		small hospital. Radiology is a prime example. But a technology partnership can also be relevant for intensive care units and emergency departments. Relevant for all departments that work with a large number of medical devices.Q: What role does cybersecurity play from the perspective of hospitals and manufacturers when entering into a technology partnership? A: In my opinion, security is more of a secondary issue in such partnerships, as aspects such as improved financial planning are more of a focus.Q: How do you estimate the effectiveness of a technology partnership for a faster recovery of hospital operations in the event of damage compared to recovery measures taken by the hospital alone? • Impact effect on recovery of 25 % possible? • Impact effect on recovery of 50 % possible? • Impact effect on recovery of 75 % possible? A: The healthcare sector is an interesting target for hackers. The responsibility for securing systems or even restoring supply operations in the event of a cyber-attack is placed on clinics, which is not part of a clinic's core expertise. These capabilities can be covered by a technology partner. Manufacturers are able to provide comprehensive cybersecurity management services - from comprehensive monitoring to regular patching. This means they can also provide valuable support in the event of a security incident. For this reason, the effect can be estimated at approximately 50 %.Q: How do you assess the future significance of technology partnerships for cybersecurity?A: The importance of technology partnerships for cybersecurity will still take some time, as other problems in hospitals, such as the shortage of skilled labour, are still more prominent. Nevertheless, it is essential to address this issue in order to ensure operational security. One problem is that decision-makers are far removed from the topic of cybersecurity. More understanding is needed here to recognize the urgency of cybersecurity and address the issue	
Hospital	Chief Infor-mation Of-ficer	Q: From your point of view, what are the main reasons why hospitals enter into a technology partnership?A: Modernization & standardization of the equipment pool for improved management and administration of medical devices.Q: For which hospitals is a technology partnership worthwhile?A: Every hospital can benefit from the advantages of a partnership, as expert knowledge of medical technology can be made available in addition to personnel. The benefits must be individually agreed and agreed upon.Q: What role does cybersecurity play from the perspective of hospitals and manufacturers when entering into a technology partnership?A: Cybersecurity is not the main issue, but often economic factors. In the future, the importance should also increase due to more frequent cases.Q: How do you estimate the effectiveness of a technology partnership for a faster recovery of hospital operations in the event of damage compared to recovery measures taken by the hospital alone? • Impact effect on recovery of 25 % possible? • Impact effect on recovery of 50 % possible? • Impact effect on recovery of 75 % possible? A: No comment.Q: How do you assess the future significance of technology partnerships for cybersecurity?A: High future significance because cyber-attacks will increase significantly in the future.	No information
Consulting Firm	Manager	Q: From your point of view, what are the main reasons why hospitals enter into a technology partnership?A: First and foremost, to bundle financial planning and procurement. In terms of acquisition and operating investments.Q: For which hospitals is a technology partnership worthwhile?A: A range of services tailored to the individual needs and requirements of a hospital makes sense for all clinics and supports the limited human resources in the IT department.Q: What role does cybersecurity play from the perspective of hospitals and manufacturers when entering into a technology partnership?A: Currently still plays a subordinate role, but it can be assumed that its importance will increase due to the increasing threat to the healthcare system.Q: How do you estimate the effectiveness of a technology partnership for a faster recovery of hospital operations in the event of damage compared to recovery measures taken by the hospital alone? • Impact effect on recovery of 25 % possible? • Impact effect on recovery of 50 % possible? • Impact effect on recovery of 75 % possible? A: Perhaps around 25 % less, because the technology partner can only provide support for recovery within the scope of the medical devices. However, thanks to its expertise or the rapid provision of replacement equipment, hospital operations can be restored much more quickly than if a hospital tries to repair the damage on its own.Q: How do you assess the future significance of technology partnerships for cybersecurity?A: Technology partnerships will not be insignificant for cybersecurity in the future, but it remains to be seen whether such partnerships will find broad application as a security concept.	25 %
Consulting Firm	Manager	Q: From your point of view, what are the main reasons why hospitals enter into a technology partnership?A: Classically, these are financial aspects, as in such a partnership equipment can be modernised without the need for high initial investments, but the investments can be made within a long risk period (e.g. if maintenance and recertification are the legal responsibility of the technology partner).Q: For which hospitals is a technology partnership worthwhile?A: Technology partnerships are associated with a large investment volume - especially for large medical devices - which is difficult for small hospitals to manage. They are therefore more of a model for large hospitals.Q: What role does cybersecurity play from the perspective of hospitals and manufacturers when entering into a technology partnership?A: This is very important, as hospitals need support in the secure integration, secure operation and ongoing modernization of medical devices due to limited personnel resources.Q: How do you estimate the effectiveness of a technology partnership for a faster recovery of hospital operations in the event of damage compared to recovery measures taken by the hospital alone?	25 %

(*continued on next page*)

(*continued*)

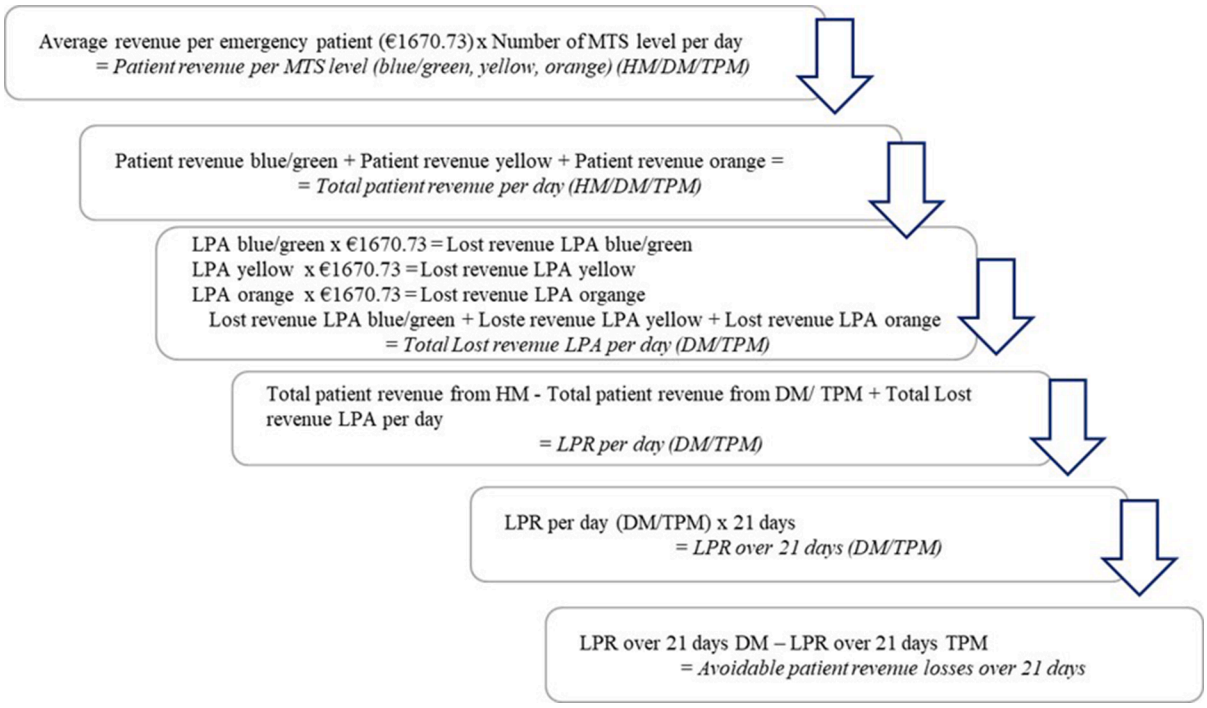
Institution	Role	Key content	effect estimation
		• Impact effect on recovery of 25 % possible? • Impact effect on recovery of 50 % possible? • Impact effect on recovery of 75 % possible? A: 25 %, as medical device manufacturers can contribute their findings and intervention measures based on global experience with safety incidents involving their medical devices. In addition, devices can be replaced quickly if access to the device is no longer possible due to a ransomware attack, for example.Q: How do you assess the future significance of technology partnerships for cybersecurity?A: Very large, as a large number of old medical devices in hospitals will have to be replaced in the near future. This is where a technology partner can provide support and achieve high safety effects through modernization alone. In addition, information technology and medical technology are working more and more in harmony, which means that the secure integration of medical devices into the hospital network will become increasingly important. This requires a high level of expertise in the field of medical technology, which a technology partner can provide.	
Association	Managing director	Q: From your point of view, what are the main reasons why hospitals enter into a technology partnership?A: Relief from tasks through medical partners. Especially in the context of the shortage of skilled labour. Furthermore, ensuring a functioning equipment pool over a long-term period.Q: For which hospitals is a technology partnership worthwhile?A: Technology partnerships must be viewed individually. In general, partnerships are relevant for all companies - they must be customized.Q: What role does cybersecurity play from the perspective of hospitals and manufacturers when entering into a technology partnership?A: Cybersecurity should play a role. Cybersecurity is not the central element of a technology partnership. However, if you decide in favour of a partnership, then cybersecurity should be taken into account. It should always be borne in mind that it is not the individual devices that need to be cyber secure, but the entire network of devices in a hospital.Q: How do you estimate the effectiveness of a technology partnership for a faster recovery of hospital operations in the event of damage compared to recovery measures taken by the hospital alone? • Impact effect on recovery of 25 % possible? • Impact effect on recovery of 50 % possible? • Impact effect on recovery of 75 % possible? A: 25 % because medical devices are only one component of cybersecurity. Nevertheless, the partner can achieve faster recovery through known threat trends and the rapid intervention of medical technology experts compared to recovery attempts by the hospital alone.Q: How do you assess the future significance of technology partnerships for cybersecurity?A: The importance of technology partnerships for cybersecurity will not increase significantly in the future; security is an add-on benefit in such partnerships and is often not seen as a central focus.	25 %
Association	Managing director	Q: From your point of view, what are the main reasons why hospitals enter into a technology partnership?A: Improved financial planning, relief for staff, gain in expertise.Q: For which hospitals is a technology partnership worthwhile?A: It makes more sense for small hospitals, as there is often a lack of resources in IT and medical technology. Larger hospitals can create synergy effects and often have more staff available.Q: What role does cybersecurity play from the perspective of hospitals and manufacturers when entering into a technology partnership? A: The topic is highly relevant in partnerships, as the increasing threat of cyber-attacks is significantly increasing the challenges for the secure operation of infrastructure and medical devices.Q: How do you estimate the effectiveness of a technology partnership for a faster recovery of hospital operations in the event of damage compared to recovery measures taken by the hospital alone? • Impact effect on recovery of 25 % possible? • Impact effect on recovery of 50 % possible? • Impact effect on recovery of 75 % possible? A: 75 % if a comprehensive range of services has been agreed, including consulting services on security and business continuity management.Q: How do you assess the future significance of technology partnerships for cybersecurity?A: Due to the shortage of skilled workers, particularly in technical disciplines, and the increasing challenges posed by digitalization, the need for hospitals to protect themselves against cyberattacks is growing.	75 %
Association	Head of the digital medical products	Q: From your point of view, what are the main reasons why hospitals enter into a technology partnership?A: The lack of qualified labour plays a role. Comprehensive maintenance of various systems from different manufacturers is necessary.Q: For which hospitals is a technology partnership worthwhile?A: It is particularly worthwhile for maximum care providers and university hospitals, as a large number of medical devices have to be managed here. However, small clinics can also benefit from a technology partnership if a contract is tailored to their specific needs.Q: What role does cybersecurity play from the perspective of hospitals and manufacturers when entering into a technology partnership?A: Cybersecurity should be given a great deal of consideration, as cybersecurity is becoming increasingly important in the healthcare sector due to the rising level of digitalization.Q: How do you estimate the effectiveness of a technology partnership for a faster recovery of hospital operations in the event of damage compared to recovery measures taken by the hospital alone? • Impact effect on recovery of 25 % possible? • Impact effect on recovery of 50 % possible? • Impact effect on recovery of 75 % possible? A: 50 % increase when combining technical and organizational levels. It is important here that the medical device's event log can be used to trace how the damage occurred.	50 %

(*continued on next page*)

(*continued*)

Institution	Role	Key content	effect estimation
		Furthermore, the technology partner must guarantee the fastest possible availability in the event of damage.Q: How do you assess the future significance of technology partnerships for cybersecurity?A: The potential for technology partnerships for cybersecurity is very high, as medical device manufacturers offer many services that are helpful for a hospital to comprehensively protect its medical devices.	

Appendix 9. Calculation steps to derive the avoidable patient revenue losses over 21 days.



Appendix 10. Average duration of downtime after a ransomware attack at organizations worldwide from 1st quarter 2020 to 2nd quarter 2022 [24].

Quarter	Average length of downtime (in days)
Q1 2020	15
Q2 2020	16
Q3 2020	19
Q4 2020	21
Q1 2021	23
Q2 2021	23
Q3 2021	22
Q4 2021	20
Q1 2022	26
Q2 2022	24
20.9	

Appendix 11. Discount Table for present value of $1[27].

N	1 %	2 %	3 %	4 %	5 %	6 %	7 %	8 %	9 %	10 %
1	0.9901	0.9804	0.9709	0.9615	0.9524	0.9434	0.9346	0.9259	0.9174	0.9091
2	0.9803	0.9612	0.9426	0.9246	0.9070	0.8900	0.8734	0.8573	0.8417	0.8264
3	0.9706	0.9423	0.9151	0.8890	0.8638	0.8396	0.8163	0.7938	0.7722	0.7513
4	0.9610	0.9238	0.8885	0.8548	0.8227	0.7921	0.7629	0.7350	0.7084	0.6830
5	0.9515	0.9057	0.8626	0.8219	0.7835	0.7473	0.7130	0.6806	0.6499	0.6209
6	0.9420	0.8880	0.8375	0.7903	0.7462	0.7050	0.6663	0.6302	0.5963	0.5645
7	0.9327	0.8706	0.8131	0.7599	0.7107	0.6651	0.6227	0.5835	0.5470	0.5132

(*continued on next page*)

(*continued*)

N	1 %	2 %	3 %	4 %	5 %	6 %	7 %	8 %	9 %	10 %
8	0.9235	0.8535	0.7894	0.7307	0.6768	0.6274	0.5820	0.5403	0.5019	0.4665
9	0.9143	0.8368	0.7664	0.7026	**0.6446**	0.5919	0.5439	0.5002	0.4604	0.4241
10	0.9053	0.8203	0.7441	0.6756	0.6139	0.5584	0.5083	0.4632	0.4224	0.3855

References

[1] Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare challenges in the era of cybersecurity. Health Secur 2020;18(3):228–31.
[2] Vukotich G. Healthcare and cybersecurity: taking a zero trust approach. Health Serv Insights 2023;16:11786329231187826.
[3] Burke G, Saxena N. Cyber risks prediction and analysis in medical emergency equipment for situational awareness. Sensors (Basel) 2021;21(16):5325.
[4] Nadeborn D, Dittrich T. Cybersicherheit in krankenhäusern – Teil 1: iT-compliance als leitungsaufgabe [Cybersecurity in hospitals-Part 1: IT compliance as a management task]. Int Cybersecur Law Rev 2022;3(1):147–61.
[5] Bracciale L, Loreti P, Bianchi G. Cybersecurity vulnerability analysis of medical devices purchased by national health services. Sci Rep 2023;13(1):19509.
[6] Wagan SA, Koo J, Siddigui IF, Attique M, Shin DR, Faseeh Qureshi NM. Internet of medical things and trending converged technologies: a comprehensive review on real-time applications. J King Saud Univ - Comput Inf Sci 2022;34(10):9228–51.
[7] Huang C, Wang J, Wang S, Zhang Y. Internet of medical things: a systematic review. Neurocomputing 2023:557.
[8] Stern AD, Gordon WJ, Landman AB, Kramer DB. Cybersecurity features of digital medical devices: an analysis of FDA product summaries. BMJ Open 2019;9(6):e025374.
[9] Kuehn BM. Pacemaker recall highlights security concerns for implantable devices. Circulation 2018;138(15):1597–8.
[10] Wasserman L, Wasserman Y. Hospital cybersecurity risks and gaps: review (for the non-cyber professional). Front Digit Health 2022;4:862221.
[11] Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Digit Med 2019;2:98.
[12] Mayor S. Sixty seconds on … the WannaCry cyberattack. BMJ 2018;361:k1750.
[13] Cartwright AJ. The elephant in the room: cybersecurity in healthcare. J Clin Monit Comput 2023;37(5):1123–32.
[14] PD - Berater der öffentlichen Hand [Advisor to the public sector]. Evaluation von Technologiepartnerschaften [Evaluation of technology partnerships] [Internet]. 2021 [cited 2023 Aug 12]. Available from: https://www.pd-g.de/assets/Projektreferenzen/201029_Evaluation_Technologiepartnerschaften_Ergebnisse.pdf.
[15] Vázquez-Serrano JI, Peimbert-García RE, Cárdenas-Barrón LE. Discrete-event simulation modeling in healthcare: a comprehensive review. Int J Environ Res Public Health 2021;18(22):12262.
[16] Angler Y, Loßin A, Götz O. Process flows of an emergency department. how process modelling and simulation can help improve the efficiency and quality of patient care. editors. In: Vilka L, Krumina J, editors. 9th International multidisciplinary research conference societY. EDP Sciences; 2024. HEALTH. WELFARE - SHS Web Conf. Riga.
[17] Karnon J, Stahl J, Brennan A, Caro JJ, Mar J, Möller J. Modeling using discrete event simulation: a report of the ISPOR-SMDM modeling good research practices task force-4. Med Decis Making 2012;32(5):701–11.
[18] Briggs AH, Weinstein MC, Fenwick EA, et al. Model parameter estimation and uncertainty analysis: a report of the ISPOR-SMDM Modeling Good Research Practices Task Force Working Group-6. Med Decis Making 2012;32(5):722–32.
[19] Briggs A. Economics notes: handling uncertainty in economic evaluation. BMJ 1999;319(7202):120.
[20] Drummond MF, Sculpher MJ, Claxton K, et al. Methods for the economic evaluation of health care programmes. 4th ed. Oxford: Oxford University Press; 2015. p. 393–7.
[21] Brachmann M. Prozessoptimierung durch Point-of-Care-Testung [Process optimisation through point-of-care testing]. In Von Eiff W, Dodt C, Brachmann M, Niehues C, Fleischmann T, editors. Management der notaufnahme – patientenorientierung und optimale ressourcennutzung als strategische erfolgsfaktor [Emergency department management - patient orientation and optimal use of resources as a strategic success factor]. Stuttgart: Kohlhammer; 2016. p. 323.
[22] Peterson DC, Adams A, Sanders S, Sanford B. Assessing and addressing threats and risks to cybersecurity. Front Health Serv Manage 2018;35(1):23–9. https://doi.org/10.1097/HAP.0000000000000040.
[23] Banks J, Carson II JS, BL Nelson, DM Nicol. Discrete-event system simulation. 4 th ed. Upper Saddle River: Pearson Prentice Hall; 2005.
[24] Petrosyan A. Average duration of downtime after a ransomware attack at organizations worldwide from 1st quarter 2020 to 2nd quarter 2022 [Internet]. 2024 [cited 2024 Apr 18]. Available from: https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack-global/.
[25] Turner HC, Sandmann FG, Downey LE, et al. What are economic costs and when should they be used in health economic studies? Cost Eff Resour Alloc 2023;21(1):31.
[26] Graf von der Schulenburg JM, Greiner W, Jost F, et al. German recommendations on health economic evaluation: third and updated version of the Hanover Consensus. Value Health 2008;11(4):539–44.
[27] Drummond MF, O'Brien B, Stoddart GL, Torrance GW. Methods for the economic evaluation of health care programmes. Oxford: Oxford university press; 1997. Drummond MF, O'Brien B, Stoddart GL, Torrance GW, editors.
[28] Kim YE, Lee HY. The effects of an emergency department length-of-stay management system on severely ill patients' treatment outcomes. BMC Emerg Med 2022;22(1):204.
[29] Wu L, Chen X, Khalemsky A, et al. The association between emergency department length of stay and in-hospital mortality in older patients using machine learning: an observational cohort study. J Clin Med 2023;12(14):4750.
[30] Seo H, Ahn I, Gwon H, et al. Prediction of hospitalization and waiting time within 24 h of emergency department patients with unstructured text data. Health Care Manag Sci 2024;27(1):114–29.
[31] Alanazi AT. Clinicians' perspectives on healthcare Cybersecurity and cyber threats. Cureus. 2023;15(10):e47026.
[32] Thomasian NM, Adashi EY. Cybersecurity in the internet of medical things. Health Policy and Technology 2021;10(3):100549.
[33] Alami H, Gagnon MP, Ahmed MAA, Fortin JP. Digital health: cybersecurity is a value creation lever, not only a source of expenditure. Health Policy and Technol 2019;8(4):319–21.
[34] Javaid M, Haleem A, Singh RP, Suman R. Towards insighting cybersecurity for healthcare domains: a comprehensive review of recent practices and trends. Cyber Security and Applications 2023;1.
[35] Abbou B, Kessel B, Ben Natan M, et al. When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. Front Digit Health 2024;6:1321485.
[36] Dubas-Jakóbczyk K, Kocot E, Tambor M, et al. The association between hospital financial performance and the quality of care - a scoping literature review. Int J Health Policy Manag 2022;11(12):2816–28.
[37] European Parliament. Medical Device Regulation (MDR) 2017/745 [Internet]. 2024 [cited 2024 Aug 07]. Available from: https://eur-lex.europa.eu/eli/reg/2017/745/2017-05-05.
[38] Biasin E, Kamenjašević E. Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. Int Cybersecur Law Rev 2022;3(1):163–80.
[39] U.S. Food and Drug Administration. Cybersecurity in Medical Devices: quality System Considerations and Content of Premarket Submissions [Internet]. 2023 [cited 2024 Aug 07]. Available from: https://www.fda.gov/media/119933/download.