buildings

MDPI

Article

Prioritising Non-Systematic Risks to the Operational Sustainability of Smart-Building Technologies in Healthcare Facilities: A Best-Worst Method Study

Erman Gedikli [1], Emre Yılmaz [1,*], Rasime Özdil [2] and Yeter Uslu [1]

[1] School of Health Science, Istanbul Medipol University, Istanbul 34815, Türkiye; egedikli@medipol.edu.tr (E.G.); yuslu@medipol.edu.tr (Y.U.)
[2] Institute of Health Science, Istanbul Medipol University, Istanbul 34815, Türkiye; rasime.ozdil@std.medipol.edu.tr
* Correspondence: emreyilmaz@medipol.edu.tr

Abstract

Healthcare facilities depend on smart-building technologies, yet their institution-specific vulnerabilities are difficult to prioritise. Ten purposively recruited experts from hospitals in Istanbul, Türkiye, weighted eight literature-derived risks. The primary analysis used linear Best-Worst Method (BWM) estimation and arithmetic-mean aggregation. Additional judgement-traceability diagnostics, consistency-based reweighting and selection, Bayesian BWM, group omissions and bootstrap resampling were post hoc exploratory robustness analyses. In the primary analysis, privacy and data breach (0.170), crisis response and recovery failure (0.163), loss of data integrity and transparency (0.158) and device and endpoint security (0.142) carried 63.4% of the weight, but their order and group membership were sensitive to analytical choices and panel composition. Improper data disposal policies ranked last (0.030) in the primary analysis and the reported non-bootstrap sensitivity specifications. Crisis response and recovery failure ranked first or second in analyses that weighted or selected experts according to judgement consistency; privacy and data breach did not rank first in these analyses. Recovery failure fell to seventh when the three experts whose comparison vectors prioritised it were omitted. Questionnaire limitations included a missing comparison row, conflicting selections and duplicate comparisons, and a fixed criterion order. The weights describe expert-perceived priorities and require validation against incident and downtime data before guiding resource allocation.

Keywords: smart hospital; facility management; operational sustainability; multi-criteria decision analysis; business continuity; Best-Worst Method; cyber resilience

Check for updates

Academic Editors: Qiuchen Lu and Ya Wen

Received: 8 October 2026
Revised: 27 October 2026
Accepted: 28 October 2026
Published: 2 November 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Healthcare facilities constitute a distinctive class of critical infrastructure. They must sustain uninterrupted operations while simultaneously meeting stringent requirements concerning patient safety, infection prevention, data protection, environmental quality and resource efficiency. Unlike conventional commercial buildings, hospitals depend on the continuous and coordinated functioning of heating, ventilation and air-conditioning (HVAC) systems; electrical and water infrastructure; medical gas networks; access-control and fire-safety systems; clinical information systems; and increasingly interconnected medical devices. A failure in any of these components may extend beyond technical or financial loss to disrupt clinical workflows, compromise sensitive health information, delay

treatment or directly endanger patients. In this context the sustainability of a healthcare facility cannot be reduced to energy efficiency or environmental performance alone. It must also encompass the facility's capacity to maintain critical services, withstand operational disruptions and restore acceptable performance within a clinically tolerable period.

The adoption of smart-building technologies has substantially transformed the management of healthcare facilities. Internet of Things (IoT) devices, sensor networks, building management systems (BMSs), building automation systems (BASs), cloud and edge computing, artificial intelligence, digital twins and advanced analytics increasingly enable real-time monitoring and automated control of building operations. These technologies may support predictive maintenance, energy optimisation, asset tracking, environmental monitoring, space management and more responsive allocation of organisational resources. Smart hospitals, however, should not be understood merely as healthcare buildings equipped with a greater number of digital devices. Their effective operation depends on the integration of physical assets, digital infrastructures, information systems, users and managerial processes within a coherent socio-technical ecosystem [1]. A recent systematic review of digital technologies in healthcare facility management likewise identifies cybersecurity, data privacy, interoperability and organisational adoption as persistent barriers to realising these benefits [2].

Building information modelling and digital-twin applications extend this integration by connecting physical assets with continuously updated operational data. Such systems may improve visibility across the asset lifecycle and support more informed decisions regarding maintenance, energy consumption and facility performance. Building-information-modelling-enabled facility management is strategically relevant to the optimisation of energy, physical assets and information resources in smart hospitals [3]. Sensor-enabled digital twins may similarly support real-time monitoring and decision-making in healthcare environments [4]. The value of these systems nevertheless remains conditional on the accuracy of the underlying data, the reliability of connected devices, the compatibility of different platforms, and the organisation's capacity to interpret and act upon the information produced.

The relationship between smart-building technologies and operational sustainability is therefore neither automatic nor uniformly beneficial. Automated systems may improve efficiency under normal conditions while creating new dependencies and failure pathways: energy-oriented HVAC optimisation, for example, may compromise ventilation rates, pressure differentials or infection control if these are not incorporated into the control logic, and hospital indoor environments must be managed through an integrated approach rather than through energy indicators alone [5]. Operational sustainability is therefore conceptualised here as the capacity to achieve efficiency without compromising safety, reliability, environmental quality or continuity of care.

Digital connectivity introduces an additional layer of complexity. Smart healthcare facilities frequently integrate heterogeneous sensors, legacy equipment, proprietary software, third-party services, building-control networks, hospital information systems and Internet of Medical Things (IoMT) devices. The resulting architecture can enhance situational awareness, yet it also expands the number of potential points of failure. Inaccurate sensor readings, inadequate calibration, software vulnerabilities, communication failures, incompatible data standards and poorly configured access permissions may undermine automated decisions or render critical systems unavailable. A recent systematic review of cyberattacks on healthcare systems identified human error, under-investment, complex network-connected endpoint devices, legacy systems and rapid digitalisation as recurrent sources of vulnerability [6]. The convergence of information technology (IT), operational

technology (OT) and connected medical devices further increases the possibility that a cyber incident will migrate from the digital environment into physical building operations [7–9].

Cybersecurity in smart healthcare facilities must consequently be treated as an operational sustainability concern rather than solely as an information-technology or confidentiality issue. Cyber risks affect the confidentiality, integrity and availability of information and technological assets [10]. Reviews and organisational studies of healthcare cybersecurity show that ransomware and other attacks increasingly target the availability of clinical services as well as the confidentiality of records, and that organisational and human factors condition exposure alongside technical vulnerabilities [11–14]. Within a hospital, compromised availability or integrity may affect not only administrative information but also environmental controls, diagnostic equipment, access systems and other functions upon which clinical services depend. Cyber-risk assessment in connected healthcare environments should therefore account for the interdependencies among people, information, technological assets, facility assets and services [8,15].

1.1. Risk in the Context of Smart Healthcare Facilities

Risk may broadly be understood as the combination of the likelihood of an uncertain event and the severity of its consequences for organisational objectives, assets or processes. In healthcare facilities these consequences may include financial loss, service interruption, impaired clinical performance, unauthorised disclosure of personal health information, deterioration of indoor environmental conditions, reputational damage, or harm to patients and staff. Risk in a smart-building environment is therefore multidimensional and cannot be adequately represented by the probability of device failure alone [8,16].

Systematic and Non-Systematic Risks

For the purposes of this study, risks are differentiated as systematic or non-systematic according to their origin, their scope across institutions and the degree to which an individual organisation can control them. Systematic risks originate predominantly outside the organisation and can affect many institutions simultaneously—economic crises, pandemics, armed conflict, national energy shortages, regional disasters or extensive regulatory change; facilities can prepare for them but cannot eliminate their source. Non-systematic risks arise primarily from the institution-specific configuration of technology, human resources, devices, data governance, internal controls and management practices, so their probability and consequences vary between facilities even where similar technologies are deployed. The classification is analytical rather than absolute: "non-systematic" does not mean insignificant or isolated, because an architectural vulnerability specific to one institution may still disable that institution's entire network. A risk is treated here as non-systematic when its principal source is specific to the facility and materially influenced by decisions taken within it, even when its consequences cascade across internal systems.

1.2. Rationale for Focusing on Non-Systematic Risks

Three considerations motivate this focus. First, non-systematic risks are comparatively actionable: healthcare managers cannot independently prevent a national energy crisis or a pandemic, but they can improve network architecture, strengthen endpoint security, revise access controls, train personnel, verify backup systems and test recovery plans. Second, smart-building configurations are highly heterogeneous; differences in device portfolios, network architecture, legacy infrastructure, organisational capacity, outsourcing arrangements and data-governance practices create institution-specific risk profiles, so that the same technology may improve performance in one facility while creating substantial vulnerability in another. Third, healthcare organisations operate under resource constraints

and cannot address every vulnerability simultaneously; they require a defensible mechanism for determining which controllable risks should receive priority.

Existing studies have frequently examined energy efficiency, building information modelling, IoT, indoor air quality, privacy, device security or cybersecurity as separate domains. Evidence concerning the relative managerial importance of facility-specific technological, human, informational and recovery risks remains comparatively limited, and studies that integrate these domains within a single decision-oriented framework are scarce. This gap constrains healthcare managers who must allocate finite resources across multiple competing vulnerabilities.

Recent syntheses illustrate this fragmentation. Zhang et al. [2] reviewed digital technologies in healthcare facility management and identified cybersecurity, data privacy, interoperability and organisational adoption as persistent challenges; reviews of healthcare cybersecurity catalogue threats, human factors and socio-technical vulnerabilities [6,11,17], and an interview-based system-dynamics study models how hospitals build cybersecurity capability [12]; reviews of networked medical devices concentrate on device-level attacks and countermeasures [9,18]; and the critical-infrastructure and hospital-resilience literature concentrates on the capacity to absorb, adapt to and recover from disruption [19–22]. Multi-criteria studies of smart hospitals have addressed building information modelling and asset and energy management [1,3] rather than the relative priority of competing risks.

Against this background, the study makes three contributions. First, we are not aware of a previous study that quantifies, within a single decision model, the relative priority that experts assign to institution-specific technical, human, informational, governance and recovery risks of smart-building technologies in healthcare facilities. Second, it frames these risks in terms of operational sustainability—the capacity to sustain safe clinical services—rather than energy efficiency or information security alone. Third, it audits the resulting weights for judgement consistency, panel heterogeneity and causal heterogeneity, and translates them into candidate control schemes whose validity remains to be tested against incident data.

The present study therefore addressed the following research question: which non-systematic risks do experts judge to warrant priority in the management of smart-building technologies in order to strengthen the operational sustainability of healthcare facilities? The Best-Worst Method (BWM) was selected because it derives criterion weights from structured comparisons between the most important criterion and all remaining criteria, and between all criteria and the least important criterion. BWM requires fewer pairwise comparisons than complete comparison procedures, tends to produce more reliable comparisons, and provides an explicit mechanism for evaluating the consistency of expert judgement [23,24]. The choice of BWM over the analytic hierarchy process (AHP) and the Decision-Making Trial and Evaluation Laboratory (DEMATEL) is justified in Section 2.4.1.

2. Materials and Methods

2.1. Study Design

A cross-sectional expert-elicitation study using the Best-Worst Method was conducted between 14 May and 30 June 2026, after ethics approval had been granted.

2.2. Development of Risk Criteria

The criterion set was derived from a narrative synthesis of the literature on smart buildings, smart hospitals, IoMT security, health information governance and critical-infrastructure resilience. Candidate risks were consolidated where they described overlapping mechanisms, each retained criterion was given an operational definition and mapped to supporting sources, and the resulting set was reviewed by the research team for non-redundancy and managerial actionability. The final set comprised eight criteria, including

improper data disposal policies, which covers the end-of-life stage of the information lifecycle; all ten experts evaluated the full eight-criterion set. Table 1 distinguishes the sources from which each criterion was derived before the study from additional supporting evidence identified during revision; healthcare-specific reviews were located for criteria C1, C2, C4 and C5 and healthcare breach analyses for C3, whereas the additional evidence for C6-C8 consists of general frameworks and standards.

The eight retained criteria are listed in Table 1. The criteria intentionally encompass risk sources, adverse events and control failures; they should not be interpreted as mutually exclusive constructs located at an identical causal level. Their inclusion in a single model is justified pragmatically: each represents a distinct domain to which healthcare managers may allocate preventive or corrective resources. The model is therefore intended for managerial prioritisation rather than for estimating a single causal pathway.

To make this heterogeneity explicit, each criterion was classified a posteriori by its position in a bow-tie representation of the risk process [25]: threat and vulnerability sources that precede an incident (C1, C2 and C4, the last representing endpoint compromise as an entry pathway); information-compromise events (C3 and C6); and management-control failures that weaken preventive or recovery barriers (C5, C7 and C8) (Table 1). The classification does not alter the single-level elicitation; it is used to describe how the weights are distributed across causal positions (Section 2.5.3) and to qualify their interpretation. Because a source such as personnel negligence can contribute to an event such as a data breach, the criteria are not fully non-redundant, and the weights are interpreted as relative priorities for managerial attention rather than as additive shares of a single risk quantity.

Table 1. Non-systematic risk criteria included in the Best-Worst Method model.

Code	Criterion	Causal Level [1]	Operational Definition	Derivation Sources	Additional Evidence
C1	Infrastructure Design Vulnerability	Source	Architectural defects, inadequate network segmentation, insufficient redundancy, insecure communication protocols or structurally deficient security controls that allow a local incident to propagate across the facility.	[7,26,27]	[6,28]
C2	Personnel Negligence and Misconduct	Source	Weak credential practices, susceptibility to social engineering, inappropriate privilege use, failure to follow procedures, or intentional disclosure by staff.	[8,15]	[6,17]
C3	Privacy and Data Breach	Event	Acquisition, disclosure or use of patient records or personal health information by unauthorised parties, with regulatory, reputational and operational consequences.	[15,16]	[29,30]
C4	Device and Endpoint Security	Source	Compromise, unavailability or corruption of medical devices, sensors, wearables, controllers or gateways, including devices that continue operating while producing inaccurate data.	[4,8,26]	[9,31]
C5	Crisis Response and Recovery Failure	Control failure	Failure to maintain or restore critical systems following a cyberattack, technical failure or disaster, including documented plans that fail under real operating conditions.	[32,33]	[20–22]
C6	Loss of Data Integrity and Transparency	Event	Alteration, deletion, corruption or unverifiability of data during storage or transmission, undermining automated decisions and auditability.	[8,10]	[34]

Table 1. *Cont.*

Code	Criterion	Causal Level [1]	Operational Definition	Derivation Sources	Additional Evidence
C7	Erroneous Risk Assessment and Analysis	Control failure	Incorrect identification or prioritisation of threats, leading to inefficient allocation of financial, technical and human resources.	[8,16,35]	[36]
C8	Improper Data Disposal Policies	Control failure	Inadequate destruction, sanitisation or decommissioning of records, storage media and retired devices, permitting recovery of residual protected information.	[16]	[37]

[1] Causal level (bow-tie position, assigned a posteriori): Source = threat or vulnerability source preceding an incident; Event = information-compromise event; Control failure = failure of a preventive or recovery management barrier. Device and endpoint security is treated as a source (endpoint compromise as an entry pathway); its classification as an event is examined in Section 3.6 and Supplementary Material S1.

2.3. Expert Panel

Ten experts were recruited through institutional connections, professional networks and academic contacts using purposive sampling in Istanbul, Türkiye. Seven experts were affiliated with public hospitals and three with private hospitals. Eligibility required (i) a professional or academic role in healthcare management, healthcare facility and technical services management, health information systems or health information security; (ii) at least three years of relevant experience; and (iii) direct familiarity with smart-building or building-automation applications in a healthcare setting. The panel was sized for depth of domain knowledge rather than statistical representativeness; the consequences of its small size are examined through the leave-one-out, removal and resampling analyses (Section 2.5.2). Data were collected after participants had been informed about the study and provided informed consent. Apart from public or private hospital affiliation, participant characteristics were not recorded; individual data on professional role, sex, age and years of experience are therefore unavailable. The professional composition of the panel cannot be reported, and the analyses of preference groups and concordance described in Section 2.5.2 characterise the heterogeneity of the experts' priorities, not their professional backgrounds.

2.4. The Best-Worst Method

The primary analysis consisted of estimating individual criterion weights using linear BWM and calculating group weights by arithmetic-mean aggregation across all ten experts, normalised to sum to unity. Judgement-consistency traceability, the additional subset-removal tests introduced during revision and Bayesian BWM were post hoc exploratory analyses conducted solely to assess the robustness of the primary findings. They did not replace the primary estimates or provide independent validation of the priorities. The distinction between the original sensitivity analyses and the additional post hoc exploratory analyses is specified in Section 2.5.2.

2.4.1. Choice of Method

Table 2 compares BWM with the two alternatives most often considered. The analytic hierarchy process [38] answers the same question but requires 28 pairwise judgements per expert for eight criteria, against 13 for BWM [23], an important consideration for a paper instrument completed in a single session; BWM was also expected to yield more consistent comparisons [23,39], although the high consistency ratios observed here show that this advantage did not fully materialise on paper. DEMATEL [40] addresses a different question—the causal structure of influence among criteria—and does not by itself

produce importance weights. BWM was therefore the most parsimonious method able to answer the research question, and its consistency diagnostics can be traced to individual comparisons [24,41]. It does not model interdependence among criteria, a limitation that the causal-level classification makes explicit but does not resolve (Section 4.3).

Table 2. Comparison of candidate weighting methods for the present study.

Requirement	AHP [1]	BWM [3]	DEMATEL [4]
Primary output	Priority weights	Priority weights	Cause–effect structure; weights only through extensions such as DANP [5]
Judgements per expert ($n = 8$)	28	13	56
Comparison structure	All pairs of criteria	Best-to-Others and Others-to-Worst vectors	Direct influence of each criterion on every other
Consistency diagnostics	Consistency ratio of the full matrix	$\tilde{\zeta}^{L}$, CR and input-based CR^{I}, traceable to individual comparisons	No intrinsic consistency measure
Interdependence among criteria	Not modelled (requires ANP [2])	Not modelled	Modelled explicitly
Burden on a paper instrument	High	Low	High

[1] AHP: analytic hierarchy process. [2] ANP: analytic network process; [3] BWM: Best-Worst Method; $13 = 2n - 3$ comparisons per expert; the paper form recorded the best-versus-worst comparison twice. [4] DEMATEL: Decision-Making Trial and Evaluation Laboratory, [5] DANP: DEMATEL-based analytic network process.

2.4.2. Estimation Procedure

BWM was implemented in five steps [23,24].

Steps 1–4. After the set of decision criteria $\{c_1, \ldots, c_n\}$ had been defined ($n = 8$), each expert identified the most important (best, B) and least important (worst, W) criterion and expressed, on a 1–9 scale, the preference of the best criterion over every other criterion (Best-to-Others vector, elements a_{Bj}, with $a_{BB} = 1$) and the preference of every criterion over the worst (Others-to-Worst vector, elements a_{jW}, with $a_{WW} = 1$).

Responses were collected on paper forms and transcribed for analysis. The instrument was administered in Turkish and included explanatory descriptions of the criteria. One researcher (R.Ö.) collected the completed paper forms, and another researcher (E.Y.) checked the responses and entered the data into a computer for analysis. Because the forms were completed by hand, three coding rules were applied and are reported here in full. First, for each expert the best criterion was taken to be the criterion receiving a value of 1 in the Best-to-Others vector, and the worst criterion the criterion receiving the maximum value in that vector; this coding coincided with the participant's own tick in the "select the best" and "select the worst" fields for eight of the ten experts, and the vector was given precedence for the remaining two: expert 7 ticked device and endpoint security as best but assigned the Best-to-Others value of 1 to crisis response and recovery failure; expert 10 ticked infrastructure design vulnerability as worst but assigned the largest Best-to-Others value to improper data disposal policies. Second, the instrument contained Others-to-Worst rows for the first seven criteria only. For the nine experts whose vector-coded worst criterion was improper data disposal policies this is immaterial, because that entry equals 1 by definition. For expert 6, whose worst criterion was infrastructure design vulnerability, the comparison of improper data disposal policies against the worst criterion was not elicited; the corresponding constraint was therefore omitted from that expert's optimisation, which was estimated from twelve rather than thirteen comparisons. Third, the form elicited the best-versus-worst comparison twice, once in each vector; the two entries differed for experts

3 (8 and 9), 5 (8 and 7) and 10 (9 and 3). Both entries were retained in the primary model, and a sensitivity model that enters the comparison once, using the Best-to-Others value and thus restoring the standard 2n − 3 comparisons, is reported in Section 3.5.

Step 5. Optimal weights were obtained from the linear BWM model [24]:

$$\begin{array}{ll} \text{minimise} \xi^{L} & \\ \text{subject to } \left|w_B - a_{Bj} \cdot w_j\right| \le \xi^{L;} & \text{for all } j; \\ \left|w_j - a_{jW} \cdot w_W\right| \le \xi^{L} & \text{for all } j; \\ \Sigma_j w_j = 1;\ w_j \ge 0 & \text{for all } j. \end{array} \quad (1)$$

The linear model yields a unique weight vector and a scalar ξ^{L} that can be interpreted directly as an indicator of comparison consistency, with values closer to zero indicating greater consistency [24]. Models were solved with the Excel Solver in Excel (Microsoft 365). The values in Tables 3 and 4 were re-computed in Python 3.12 (*NumPy 2.5*, *SciPy 1.18*) (Supplementary Material S2) independently of the Excel workbook, and all post hoc analyses were performed only in Python. The Python code was prepared with the assistance of a generative artificial intelligence tool (Claude Opus 5.5, Anthropic); it reproduces the Excel Solver results for Tables 3 and 4 to the reported precision, whereas the post hoc analyses have no independent implementation. The role of this tool in preparing the code and the verification procedure are described in Section 2.7.

Table 3. Individual criterion weights and consistency indicators.

Expert	C1	C2	C3	C4	C5	C6	C7	C8	ξ^{L}	CR	CR^{I}
E1	0.095	0.076	0.191	0.127	0.296	0.127	0.064	0.023	0.086	0.472	0.361
E2	0.097	0.129	0.285	0.129	0.078	0.194	0.065	0.023	0.104	0.644	0.571 *
E3	0.078	0.097	0.194	0.097	0.129	0.300	0.078	0.026	0.088	0.505	0.393 *
E4	0.088	0.074	0.110	0.088	0.110	0.147	0.353	0.029	0.088	0.407	0.292
E5	0.131	0.099	0.197	0.275	0.079	0.131	0.066	0.022	0.120	0.722	0.661 *
E6	0.031	0.104	0.138	0.083	0.104	0.138	0.332	0.069	0.083	0.416	0.304
E7	0.106	0.084	0.141	0.141	0.327	0.106	0.070	0.026	0.095	0.472	0.361
E8	0.318	0.099	0.079	0.199	0.132	0.066	0.079	0.026	0.079	0.407	0.292
E9	0.125	0.093	0.075	0.187	0.307	0.125	0.062	0.027	0.067	0.330	0.222
E10	0.061	0.123	0.290	0.098	0.070	0.246	0.082	0.029	0.202	1.058	0.875 *

ξ^{L} = objective value of the linear BWM model; CR = classical consistency ratio (ξ/CI); CR^{I} = input-based consistency ratio. E1–E10 = experts 1–10. * CR^{I} above the threshold of Liang et al. for eight criteria (0.3620) [41], computed with the Best-to-Others a_{BW}; expert 3 is within the threshold with the Others-to-Worst value.

Table 4. Aggregated criterion weights, ranking and robustness checks.

Rank	Code	Criterion	Arithmetic Mean (n = 10)	Geometric Mean (n = 10)	Restricted Sample [1]	Rank Range, Leave-One-Out
1	C3	Privacy and Data Breach	0.1701	0.1739	0.1517	1–2
2	C5	Crisis Response and Recovery Failure	0.1632	0.1555	0.1854	1–3
3	C6	Loss of Data Integrity and Transparency	0.1581	0.1639	0.1504	2–4
4	C4	Device and Endpoint Security	0.1424	0.1491	0.1314	3–5
5	C7	Erroneous Risk Assessment and Analysis	0.1251	0.1088	0.1379	4–7
6	C1	Infrastructure Design Vulnerability	0.1131	0.1082	0.1172	5–7
7	C2	Personnel Negligence and Misconduct	0.0979	0.1086	0.0947	6–7
8	C8	Improper Data Disposal Policies	0.0301	0.0319	0.0312	8

[1] Two least consistent respondents (experts 5 and 10, largest ξ^{L}) excluded, n = 8.

2.5. Consistency Assessment

Three consistency indicators were computed for each expert. The linear-model indicator ξ^{L} was taken from the optimisation above. The classical consistency ratio was computed

as $CR = \frac{\xi}{CI}$, where ξ is the optimal objective value of the original non-linear BWM model, obtained by bisection over feasibility linear programmes, and CI is the consistency index corresponding to a_{BW} [23]. The input-based consistency ratio, which can be calculated directly from the comparison vectors before optimisation, was computed as below [41].

$$CR^{I} = \max_{j}\left(\frac{\left|a_{Bj} \cdot a_{jW} - a_{BW}\right|}{a_{BW}^{2} - a_{BW}}\right) \quad (2)$$

All three indicators are reported because they behave differently under scale compression, which is common when the number of criteria approaches the upper limit of the 1–9 scale. Liang et al. provide reference thresholds for CR^{I} by number of criteria and by a_{BW} [41]; for eight criteria the threshold is 0.3620 when a_{BW} is 8 or 9. The thresholds were not used to exclude experts from the primary analysis, but they define one of the sensitivity specifications below. For experts 3, 5 and 10 the two recorded best-versus-worst comparisons differed, and CR^{I} was computed with the Best-to-Others value. With the Others-to-Worst value (9), expert 3's CR^{I} is 0.292 and within the threshold; experts 5 and 10 remain above it under either coding. Experts 1 and 7 ($CR^{I} = 0.361$) meet the threshold by 0.001.

2.5.1. Judgement Traceability (Post Hoc Exploratory)

The judgement-traceability diagnostics in this subsection were introduced after peer review as post hoc exploratory robustness analyses; the chronology of the other sensitivity analyses is distinguished in Section 2.5.2. Because a high consistency ratio shows that inconsistency is present but not where it originates, three diagnostics were computed for each expert from the raw vectors: the ordinal agreement between the Best-to-Others and Others-to-Worst vectors (Spearman's ρ between the importance orders they imply, and the proportion of criterion pairs strictly reversed between them); the agreement of the two recorded best-versus-worst comparisons; and the triad deviations $a_{Bj} \cdot a_{jW} - a_{BW}$, which identify the comparisons that drive CR^{I} [41]. Others-to-Worst vectors with $\rho < 0.50$ were classified as ordinally incoherent; this threshold, and the related cross-check of more than 25% reversed pairs, were chosen after inspection of the data; expert 5 ($\rho = 0.49$) lies at the cut-off, and the related rule (expert 5: 30% reversed pairs; highest among the seven coherent experts, expert 2: 22%) classifies identically. Because the judgements were collected in a single administration, inconsistent comparisons could not be returned to the experts for revision, and no judgement was edited.

2.5.2. Aggregation and Sensitivity Analysis

The primary group estimates were the arithmetic means of the ten individual linear-BWM weight vectors, normalised to sum to unity. Geometric-mean aggregation, leave-one-expert-out replication and re-estimation after excluding the two respondents with the largest ξ^{L} (experts 5 and 10) were sensitivity analyses reported in the original manuscript. Additional post hoc exploratory robustness analyses introduced during revision comprised (i) consistency-based re-specifications: weighting experts by $1/\xi^{L}$; re-estimating expert 10, the ordinally incoherent experts or all experts from their Best-to-Others vectors; entering the best-versus-worst comparison once; excluding ordinally incoherent experts; and retaining only experts within the Liang et al. thresholds, with two variants testing the fragility of that subset (expert 3 coded with its Others-to-Worst best-versus-worst value; experts 1 and 7 excluded); (ii) Bayesian BWM [42], in which multinomial likelihoods for each expert's two vectors are linked by a Dirichlet distribution centred on the group weights (Gamma(0.01, 0.01) prior on its concentration; flat Dirichlet prior on the group weights), estimated by Metropolis-within-Gibbs sampling with four chains from overdispersed starting values (50,000 burn-in and 1,000,000 iterations per chain, thinned by 100), retaining

both recorded best-versus-worst entries and, for expert 6, renormalising over the observed criteria; convergence required a rank-normalised split potential scale reduction factor ($\hat{R}$) below 1.01 and bulk and tail effective sample sizes (ESS) above 400 for every group weight and the concentration parameter; (iii) leave-one-group-out analysis, grouping experts by the domain of the criterion designated as best in their Best-to-Others vector (information-centred: C3 or C6; resilience-centred: C5; assessment-centred: C7; technical-asset-centred: C1 or C4), benchmarked against all removals of one to three experts; and (iv) a bootstrap over experts (10,000 resamples) [43]. Because the groups are defined by each expert's top priority, (iii) shows dependence on like-minded experts, not the panel's professional composition; with ten purposively selected experts, bootstrap proportions describe sensitivity to panel membership, not population probabilities. Agreement was quantified with Spearman's ρ and, among individual rankings, with Kendall's tie-corrected W [44]; associations across experts are reported descriptively, without adjustment for multiple comparisons. The additional analyses test the robustness of the primary findings; they are not confirmatory tests or independently validated priority models.

2.5.3. Analytical Procedure forCausal-Level Decomposition (Post Hoc Exploratory)

Using the classification in Table 1, the aggregated weights were summed within each causal level and expressed as within-level shares. Because level totals depend on the number of criteria per level, each total is compared with the share expected under equal weights (the number of criteria in the level divided by eight). Two alternative classifications were examined: treating device and endpoint security as an event, consistent with its operational definition, and a five-level split separating inducement, equipment compromise, information events, preventive management failures and recovery failure. The decomposition is descriptive and contains no elicited comparisons between levels.

2.6. Ethics

The study was approved by the Non-Interventional Clinical Research Ethics Committee of Istanbul Medipol University (decision number 872, 14 May 2026; reference E-10840098-50.04-3939). All participants provided written informed consent before completing the instrument. No personal health data were collected, and expert responses were stored in de-identified form.

2.7. Use of Generative Artificial Intelligence

A generative artificial intelligence (GenAI) tool, Claude Opus 5.5 (Anthropic), was used during revision to assist in preparing the Python re-analysis code (NumPy, SciPy). Its role was limited to writing and debugging code that implemented analyses specified by the authors: the independent re-computation of the individual and aggregated linear-BWM weights and consistency indicators reported in Tables 3 and 4 (Sections 2.4.2 and 2.5) and the post hoc exploratory analyses described in Sections 2.5.1–2.5.3. The study design, criterion set, model specifications, analysis parameters and thresholds, and the interpretation of the results were determined by the authors, and the tool was not used to generate, alter or impute any expert judgement. The authors reviewed and executed the code and verified it by confirming that it reproduced the Excel Solver results for Tables 3 and 4 to the reported precision; because the post hoc analyses have no independent implementation, their correctness rests on this review. The complete code is provided as Supplementary Material S2 which, together with the raw comparison vectors in Supplementary Material S1, allows all reported results to be reproduced. Other uses of GenAI in preparing the manuscript (language editing, drafting revised text and checking references) are reported in the Acknowledgments.

3. Results

3.1. Expert Judgements

All ten invited experts completed the instrument, giving a response rate of 100%. Crisis response and recovery failure was designated as most important in the Best-to-Others vectors of three experts, privacy and data breach and erroneous risk assessment and analysis by two experts each, and infrastructure design vulnerability, device and endpoint security and loss of data integrity and transparency by one expert each. Improper data disposal policies was the least important criterion for nine of ten experts; the remaining expert placed infrastructure design vulnerability last. The complete Best-to-Others and Others-to-Worst vectors are reported in Table A1 (Appendix A).

3.2. Individual Weights and Consistency

Individual weight vectors and consistency indicators are reported in Table 3. The linear-model indicator ranged from 0.067 (expert 9) to 0.202 (expert 10), with a median of 0.088. The classical consistency ratio ranged from 0.330 to 1.058 and the input-based ratio from 0.222 to 0.875.

Against the input-based thresholds of Liang et al. for eight criteria [41], six experts (1, 4, 6, 7, 8 and 9) were within the acceptable range and four (2, 3, 5 and 10) exceeded it (seven and three if expert 3 is coded with the Others-to-Worst value); for expert 10 the optimal objective value also exceeded the corresponding consistency index ($CR > 1$). The magnitudes assigned in the Others-to-Worst vectors were systematically larger than the reference comparison a_{BW} would imply; the cardinal information in the individual weights is therefore weak, and the individual weights should be read as indicative rather than precise. This pattern is characteristic of scale compression in eight-criterion problems, where a_{BW} reaches or approaches the upper bound of the 1–9 scale and leaves insufficient headroom for the intermediate products $a_{Bj} \cdot a_{jW}$.

Traceability analysis (Table A2, Appendix A) located the sources of inconsistency. For seven experts the two vectors were ordinally coherent ($\rho = 0.60$–0.98) and inconsistency arose from cardinal inflation: for every expert the largest triad deviations were positive. Experts 5, 6 and 10 met the incoherence rule. For expert 10 the best-versus-worst comparison was recorded as 9 in one vector and 3 in the other, 11 of 28 criterion pairs were reversed ($\rho = 0.16$), and infrastructure design vulnerability was rated almost least important relative to the best criterion ($a_{B1} = 8$) but maximally important relative to the worst ($a_{1W} = 9$); entering the best-versus-worst comparison once reduced this expert's CR from 1.058 to 0.910, but the pattern cannot be corrected by recoding. For experts 5 and 6 the incoherence was concentrated in crisis response and recovery failure and in device and endpoint security and loss of data integrity and transparency, respectively. The two diagnostics capture different problems: expert 6 met the CR^I threshold despite ordinal incoherence, whereas experts 2 and 3 exceeded it with coherent orderings.

3.3. Aggregated Weights and Ranking

Aggregated weights are reported in Table 4. Privacy and data breach obtained the highest weight (0.170), followed by crisis response and recovery failure (0.163) and loss of data integrity and transparency (0.158). These three criteria jointly accounted for 49.1% of the total weight, and together with device and endpoint security (0.142) for 63.4%. Erroneous risk assessment and analysis followed (0.125), then infrastructure design vulnerability (0.113) and personnel negligence and misconduct (0.098). Improper data disposal policies received a markedly lower weight than every other criterion (0.030), less than one-fifth of the leading criterion.

3.4. Heterogeneity Across Experts

Individual weight vectors varied substantially (Table 3). The highest individual weight recorded for any single criterion was 0.353 (erroneous risk assessment and analysis, expert 4) and the lowest was 0.022 (improper data disposal policies, expert 5). Despite this dispersion, improper data disposal policies received the lowest weight in nine of the ten individual models; in the tenth (expert 6) the lowest weight fell to infrastructure design vulnerability, which that expert had identified as the worst criterion, while improper data disposal policies ranked seventh. Personnel negligence and misconduct was placed in the lower half of the ranking by five experts and at the midpoint (tied fourth and fifth) by two more. Agreement among the individual rankings was moderate (Kendall's $W = 0.47$, $\chi^2(7) = 33.0$, $p < 0.001$; pairwise ρ between experts from −0.40 to 0.97). Grouped by the criterion each expert designated as best, the panel contained three information-centred experts (2, 3 and 10), three resilience-centred experts (1, 7 and 9), two assessment-centred experts (4 and 6) and two technical-asset-centred experts (5 and 8).

3.5. Robustness

Leave-one-expert-out replication is summarised in Figure 1. The leading three criteria in the full-sample solution—privacy and data breach, crisis response and recovery failure, and loss of data integrity and transparency—also occupied the first three positions in nine of the ten replications. In the tenth, obtained by omitting expert 3, device and endpoint security displaced loss of data integrity and transparency from third position by a narrow margin. Ordering within the leading group was likewise unstable: privacy and data breach ranked first in seven replications and second in three, whereas crisis response and recovery failure ranked first in three, second in three and third in four. Across all replications these four criteria occupied ranks between 1 and 5, and their observed rank ranges overlap (Table 4). When expert 5 was omitted, erroneous risk assessment and analysis (0.132) displaced device and endpoint security (0.128) from fourth position. Improper data disposal policies ranked eighth in all ten replications.

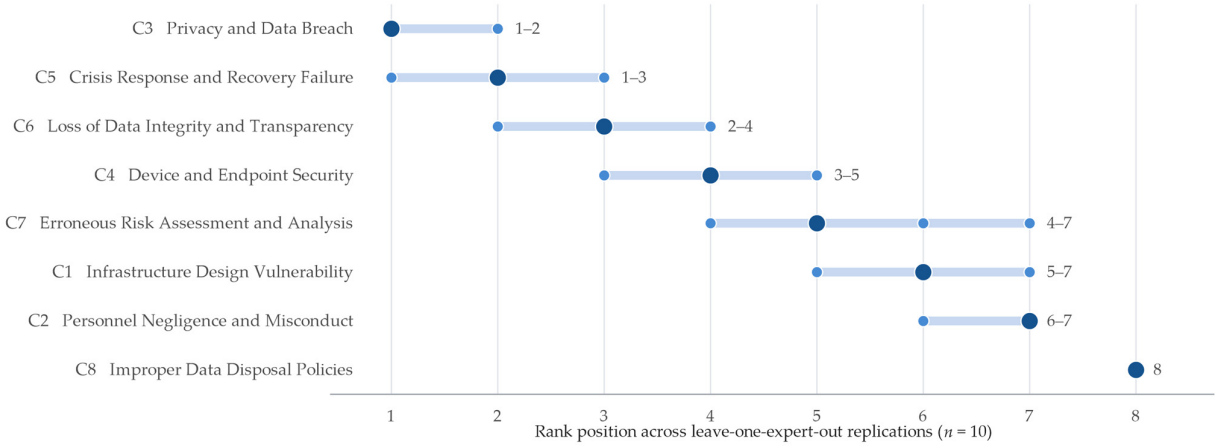


Figure 1. Full-panel rank (large dot) and ranks in the ten leave-one-expert-out replications (small dots); bars show the range.

Changing the aggregation rule from the arithmetic to the geometric mean left the same four criteria at the top and the lowest-ranked criterion in place, although crisis response and recovery failure fell to third behind loss of data integrity and transparency (Spearman ρ = 0.95; Table 4). Excluding the two least consistent respondents shifted crisis response and recovery failure to first position (0.185) ahead of privacy and data breach (0.152), and erroneous risk assessment and analysis (0.138) displaced device and endpoint security

(0.131) from fourth position (Spearman $\rho = 0.95$ relative to the full-sample ranking). Thus, the four highest-weighted criteria in the primary analysis could not be reliably ordered internally, and device and endpoint security left the top four when experts 5 and 10 were excluded. The additional post hoc exploratory analyses below further examine sensitivity to judgement consistency and panel membership.

The additional post hoc exploratory analyses (Table 5) showed that the full-panel ranking changed when experts were weighted or selected according to judgement consistency. Across experts, the weight of privacy and data breach was strongly associated with CR^I (Spearman $\rho = 0.98$; 0.86 if expert 3 is coded with the Others-to-Worst value), whereas that of crisis response and recovery failure was negatively associated with it ($\rho = -0.65$); these associations are descriptive. When every expert was retained and only the comparison inputs were re-specified (Best-to-Others-only and single best-versus-worst models), the ranking was unchanged ($\rho = 1.00$) and privacy and data breach stayed first. Consistency weighting ($\rho = 0.98$; the contribution of expert 10 fell to 4.6%, although the ordinally incoherent expert 6 received an above-average 11.2%), exclusion of the three ordinally incoherent experts ($\rho = 0.95$) and Bayesian aggregation ($\rho = 0.88$) placed crisis response and recovery failure first. Retaining only the six experts within the Liang et al. thresholds changed the ranking substantially ($\rho = 0.52$): crisis response and recovery failure (0.213) led, followed by erroneous risk assessment and analysis (0.160), while privacy and data breach and loss of data integrity and transparency fell to fifth and sixth. This subset is fragile: coding expert 3 with the Others-to-Worst value places that expert within the threshold, and loss of data integrity and transparency and privacy and data breach then rank third and fourth ($\rho = 0.76$); excluding experts 1 and 7, who meet the threshold by 0.001, places erroneous risk assessment and analysis first. In all three threshold-based variants, crisis response and recovery failure ranked first or second, and privacy and data breach did not rank first. Because three of the four experts above the thresholds were the three information-centred experts, inconsistency and preference cannot be separated in these data. Bayesian BWM (split-$\hat{R} \leq 1.001$; minimum ESS 3998) placed crisis response and recovery failure (0.155; 95% credible interval 0.126–0.188) narrowly ahead of privacy and data breach (0.153; 0.123–0.185); the credal probability that the latter outweighs the former was 0.46 (Monte Carlo standard error 0.003).

Membership of the leading group was also sensitive to panel membership. Omitting the information-centred experts displaced loss of data integrity and transparency to sixth ($\rho = 0.67$), omitting the resilience-centred experts moved crisis response and recovery failure to seventh ($\rho = 0.62$), and erroneous risk assessment and analysis entered the top four in three of the four group omissions. The two three-expert omissions are among the most influential possible: across all 120 ways of omitting three experts the median ρ was 0.90 (5th percentile 0.76) and the leading four were reproduced in 52% of subsets. In the bootstrap, the four were reproduced as a set in 46% of resamples (Supplementary Material S1).

Two ordinal statements held in every specification except the bootstrap, including all 175 removals of one to three experts: improper data disposal policies ranked last, and personnel negligence and misconduct did not enter the top four (it did so in 0.4% of bootstrap resamples). A third held in the analyses that weighted or selected experts according to judgement consistency: crisis response and recovery failure ranked first or second; it ranked third under geometric aggregation and in four leave-one-out replications, and seventh when the three experts whose vectors designated it as best were omitted. The first position of privacy and data breach and the membership of loss of data integrity and transparency and of device and endpoint security in the leading group were conditional on the inclusion of particular experts.

Table 5. Post hoc exploratory sensitivity of the aggregated weights to consistency-based re-specifications, Bayesian BWM, group omission and resampling.

Specification	***n***	**C3**	**C5**	**C6**	**C4**	**C7**	**C1**	**C2**	**C8**	**ρ** [2]
Primary: arithmetic mean [1]	10	**0.170**	**0.163**	**0.158**	**0.142**	0.125	0.113	0.098	0.030	-
Consistency-based re-specifications (post hoc exploratory)										
Consistency-weighted ($1/\xi^{L}$)	10	**0.156**	**0.176**	**0.151**	**0.143**	0.129	0.118	0.096	0.031	0.98
BO-only [3]: expert 10	10	**0.181**	**0.162**	**0.154**	**0.141**	0.124	0.112	0.096	0.032	1.00
BO-only: experts 5, 6 and 10	10	**0.177**	**0.160**	**0.151**	**0.147**	0.127	0.112	0.093	0.033	1.00
BO-only: all experts	10	**0.176**	**0.169**	**0.148**	**0.138**	0.128	0.111	0.087	0.044	1.00
Best-versus-worst entered once	10	**0.174**	**0.163**	**0.157**	**0.143**	0.125	0.113	0.097	0.029	1.00
Excluding experts 5, 6 and 10	7	**0.154**	**0.197**	**0.152**	**0.138**	0.110	0.130	0.093	0.026	0.95
Within Liang et al. thresholds (1, 4, 6–9)	6	0.122	**0.213**	0.118	**0.137**	**0.160**	**0.127**	0.088	0.033	0.52
Within thresholds, expert 3 coded $a_{BW} = 9$ (1, 3, 4, 6–9)	7	**0.133**	**0.201**	**0.144**	0.132	**0.148**	0.120	0.090	0.032	0.76
Within thresholds, excluding experts 1 and 7	4	0.101	**0.163**	0.119	**0.139**	**0.207**	**0.140**	0.093	0.038	0.36
Bayesian BWM [4] (posterior mean)	10	**0.153**	**0.155**	**0.139**	**0.147**	0.110	0.123	0.120	0.052	0.88
Leave-one-group-out (post hoc)										
Without information-centred (2, 3, 10)	7	**0.133**	**0.194**	0.120	**0.157**	**0.147**	0.128	0.090	0.032	0.67
Without resilience-centred (1, 7, 9)	7	**0.185**	0.100	**0.175**	**0.138**	**0.151**	0.115	0.104	0.032	0.62
Without assessment-centred (4, 6)	8	**0.181**	**0.177**	**0.162**	**0.157**	0.071	0.126	0.100	0.025	0.93
Without technical-asset-centred (5, 8)	8	**0.178**	**0.178**	**0.173**	0.119	**0.138**	0.085	0.098	0.032	0.95
Bootstrap over experts (10,000 resamples) [5]										
95% percentile interval	10	0.127-0.216	0.106–0.227	0.121–0.201	0.110–0.180	0.069–0.205	0.077–0.165	0.088–0.109	0.025–0.039	-
Proportion ranked first	10	0.39	0.35	0.10	0.05	0.10	0.02	0.00	0.00	-
Proportion ranked 1–4	10	0.95	0.86	0.86	0.75	0.39	0.18	0.004	0.00	-

[1] Weights are normalised arithmetic means of individual weights; columns follow the primary ranking, and the four highest weights in each row are in bold. [2] ρ = Spearman rank correlation with the primary ranking. [3] BO-only = weights re-estimated from the Best-to-Others vector alone. Groups are defined by the domain of each expert's best criterion. [4] Bayesian BWM: posterior means of the group weights (four chains, 40,000 retained draws; 95% credible intervals in Supplementary Material S1). [5] The leading four were reproduced as a set in 46% of bootstrap resamples.

3.6. Causal-Level Decomposition (Post Hoc Exploratory)

Under the three-level classification, level totals were similar (sources 0.353, events 0.328, control failures 0.318; Table 6), but this partly reflects the number of criteria per level. Relative to equal weighting, information-compromise events received 1.31 times their uniform share (0.164 per criterion), against 0.94 for sources (0.118) and 0.85 for control failures (0.106). The decomposition is sensitive to classification: treating device and endpoint security as an event raised the event total to 0.471, and separating recovery failure (0.163) from preventive control failures (0.078 per criterion) produced an apparent contrast between recovery and preventive barriers. Within levels, device and endpoint security accounted for 0.403 of the source total and crisis response and recovery failure for 0.513 of the control-failure total. The contrast between recovery and preventive control failures is driven by improper data disposal policies, whose weight may reflect the instrument; erroneous risk assessment and analysis alone received its uniform share (0.125).

Table 6. Distribution of the aggregated weights by causal level.

Causal Level	Criteria [1]	Level Total (95% Bootstrap Interval)	Uniform Share	Ratio to Uniform	Mean Weight per Criterion
Threat and vulnerability sources	C1, C2, C4	0.353 (0.287–0.432)	0.375	0.94	0.118
Information-compromise events	C3, C6	0.328 (0.254–0.408)	0.250	1.31	0.164
Management-control failures	C5, C7, C8	0.318 (0.240–0.398)	0.375	0.85	0.106

[1] Uniform share; number of criteria in the level divided by eight (the total expected under equal weights).

4. Discussion

Privacy and data breach should be interpreted beyond confidentiality and legal compliance. In a smart healthcare facility a breach may disrupt service delivery through system isolation, forensic investigation, regulatory procedures and loss of stakeholder trust [15,16]. The high weight assigned to this criterion suggests that some experts regard the consequences of unauthorised disclosure as extending into operational continuity rather than remaining confined to information governance. In the full panel, however, this weight was carried by the least consistent experts, who were largely the information-centred experts, so inconsistency and preference cannot be separated; among the six experts within the consistency thresholds the criterion ranked fifth (fourth under the alternative coding of expert 3; Section 3.5).

Crisis response and recovery failure suggests that some experts, notably the three who rated it best, placed substantial emphasis on resilience rather than prevention alone. Its high weight may indicate that complete prevention is considered unrealistic and that the ability to absorb disruption and restore critical services is central to operational sustainability. This interpretation is consistent with critical-infrastructure research emphasising tested continuity arrangements, resource prioritisation and demonstrated recovery capability rather than the mere existence of emergency documentation [19,21,32,33]. Among the four leading criteria, its position was the least sensitive to consistency corrections (first or second in analyses that weighted or selected experts according to judgement consistency; Section 3.5), but it fell to seventh when the three experts whose comparison vectors designated it as best were omitted (expert 7 ticked device and endpoint security).

Loss of data integrity and transparency represents a latent risk. Availability failures are visible, whereas integrity failures may remain undetected while systems continue to operate on corrupted information. Its position in the full-panel leading group is consistent with some experts recognising this asymmetry. Data-driven building controls and clinical-support processes depend on trustworthy records, secure transmission, protected audit logs

and reliable provenance [8,10]. It remained in the top four in every leave-one-out replication and in 86% of bootstrap resamples, but fell to sixth when the information-centred experts or the experts above the consistency thresholds were excluded (third under the alternative coding of expert 3).

Device and endpoint security completed the full-panel leading group. Compromised devices may become unavailable or, more insidiously, continue operating while generating inaccurate information. In sensor-intensive environments the authenticity and integrity of device outputs are therefore as important as their availability [4,8,9]. Recent security testing of portable connected medical devices has shown that weaknesses in their wireless implementations can expose patient data through paired devices [31]. Its membership of the leading group was conditional: it fell to fifth when expert 5 or both technical-asset-centred experts were omitted.

Erroneous risk assessment and analysis occupies a meta-risk position because it conditions how every other risk is interpreted and managed. Inaccurate asset identification, likelihood estimation or consequence assessment can direct budgets and managerial attention towards visible but comparatively unimportant threats. IoT risk-management frameworks accordingly emphasise structured identification of assets, vulnerabilities, threats, controls and consequences [16,35]. It was also the strongest challenger to the leading group in the non-Bayesian specifications (Section 3.5), although Bayesian aggregation ranked it seventh.

Infrastructure design vulnerability and personnel negligence and misconduct fell below the leading group in the full panel; personnel negligence and misconduct did so in every specification except the bootstrap. These results should not be read as evidence that architectural and workforce risks are unimportant. Network segmentation, redundancy, interoperability, firewall configuration and the separation of IT from OT determine whether a local failure remains contained or propagates across the facility [7,26,27], and technical safeguards cannot fully compensate for weak credentials, social-engineering susceptibility, excessive access rights or deliberate misuse [8,15,17]. One possible interpretation is that some experts treated these two domains as enabling conditions that are already addressed by established baseline controls, and reserved their highest priority for the consequences—informational compromise and failed recovery—that materialise when those baseline controls fail.

Improper data disposal policies received a distinctly lower weight than all other criteria and was ranked last by nine of ten experts. Two readings are possible. The first is substantive: within a facility that already operates encryption, access control and retention policies, end-of-life data destruction may be regarded as a comparatively narrow and procedurally contained exposure. The second is a limitation of expert perception: the reuse and disposal of decommissioned medical devices, storage media and building controllers is a documented vector for retained protected health information, and its low ranking may reflect limited salience rather than limited consequence. Its last rank persisted in the primary analysis and the reported non-bootstrap sensitivity specifications, but this describes the panel's judgements rather than measured consequences. Whether the low priority reflects a shared blind spot or a comparatively narrow exposure remains unresolved. The questionnaire features that may have influenced this result are considered together in Section 4.3. In practical terms, a low weight should translate into a minimum standard rather than neglect: secure decommissioning of devices, storage media and building controllers in line with media-sanitisation guidance [37], documented sanitisation certificates and disposal clauses in vendor and leasing contracts (Table 7).

These results describe perceived priority, not actual operational risk. The weights do not measure likelihood, consequence or exposure, nor the interdependence through which, for example, personnel negligence may facilitate an endpoint compromise that leads to

loss of data integrity and prolonged recovery. They may also be shaped by availability and salience: widely reported events such as ransomware attacks are more readily recalled than latent integrity failures or end-of-life data exposure [45]. A criterion may also rank low because responsibility for it lies outside the panel's remit; decommissioning, for example, is often handled by procurement, clinical engineering or external vendors, functions not explicitly represented in the eligibility criteria. The ranking therefore identifies domains judged to deserve managerial attention, not probabilities of occurrence or expected losses, and requires corroboration by objective data before it is used to allocate resources.

Taken together, the findings are consistent with a conception of operational sustainability that balances efficiency with safety, reliability, cybersecurity and resilience. A facility may appear efficient under normal conditions while remaining vulnerable to cyber incidents, inaccurate data, equipment failure or inadequate recovery capability, so smart-building performance should also be assessed through system availability, unplanned downtime, recovery time, data-integrity events, indoor environmental quality and the availability of safe manual operating procedures [3,5].

4.1. Benchmarking Against Documented Incident Evidence

Facility-level incident data were not available, so the ranking was compared with published evidence on healthcare cyber incidents, which is consistent with the priority given to recovery failure and data breach. Infected trusts in the 2017 WannaCry attack on the English National Health Service had about 6% fewer admissions per day and lost activity valued at £5.9 million [46]. Between 2016 and 2021, 374 ransomware attacks on United States healthcare delivery organisations exposed the personal health information of almost 42 million patients, and 44% disrupted care [30]. Ransomware attacks have been associated with a 17–24% fall in hospital volume during the initial attack week and a 34–38% increase in in-hospital mortality among patients already admitted [47], with falls in emergency department visits and inpatient admissions at attacked hospitals of about 8% in the first week and 16–17% in the second week, and with spill-over to neighbouring emergency departments [48,49]. In these events, harm accrued through the duration of disruption and the scale of data exposure.

The evidence is not uniformly concordant. Reviews identify human error as a leading source of vulnerability [6,17], and unauthorised internal disclosure is the second most prevalent cause of healthcare breaches after hacking and IT incidents [29], whereas the panel ranked personnel negligence and misconduct seventh, perhaps because it weighted events above the sources that produce them (Section 3.6). Registries capture integrity failures and disposal-related exposures only when they are detected and reported, so their scarcity is not evidence of low risk, and the published evidence comes largely from the United Kingdom and the United States. The ranking is therefore partly concordant with, but not validated by, documented incident evidence.

4.2. From Priorities to Differentiated Control Schemes

Table 7 translates each criterion into a differentiated control scheme for engineering operation, maintenance and safety management, with lead functions, reference frameworks [28,34,36,37,50–52] and monitoring indicators. The schemes are judgement-derived hypotheses, proposed for pilot implementation and evaluation rather than as validated recommendations. Ownership is shared by facility management, clinical engineering and IT, reflecting IT-OT convergence [7,8]; the Tier 1 schemes include a recovery or manual-fallback element, because documented harms arise largely from the duration of disruption [46,47]; and continuous monitoring [18,53] is linked to indicators whose routine collection would generate the objective data needed to validate the ranking. The weighting should be repeated after major technological or organisational change.

Table 7. Differentiated control schemes derived from the criterion ranking.

Tier, Horizon and Criterion [1]	Principal Control Measures	Lead Functions	Reference Frameworks	Monitoring Indicators
Tier 1 (pilot: 0–12 months, in parallel) C5 Crisis response and recovery failure	Business-impact analysis of critical building and information systems; recovery-time and recovery-point objectives; offline backups with restoration tests; manual operating procedures for HVAC, medical gases and access control; joint IT-FM-clinical exercises	Business continuity; FM; IT; clinical leadership	ISO 22301 [51]; NIST CSF 2.0 (RS, RC) [34]	Achieved versus target recovery time; critical systems with a tested restore in 12 months; staff trained in downtime procedures
C3 Privacy and data breach	Data-flow mapping across BMS/BAS, IoMT and clinical systems; quarterly access-rights review; MFA for remote and vendor access; encryption; tested breach detection and notification; restoration from verified clean backups after containment	Information security; data protection officer; FM	NIST CSF 2.0 (PR.AA, PR.DS, DE.CM) [34]; ISO/IEC 27001 [50]	Time to detect and notify breaches; privileged accounts reviewed per quarter; remote sessions with MFA
C6 Loss of data integrity and transparency	Write-once audit logs; time-synchronisation and provenance controls; scheduled sensor calibration; integrity checks on backups; plausibility rules for sensor values and alarms	FM; clinical engineering; IT	NIST CSF 2.0 (PR.DS, DE.CM) [34]; IEC 62443-3-3 [28]	Integrity events detected; sensors calibrated on schedule (CMMS); false or implausible alarm rate
C4 Device and endpoint security	Inventory of medical devices, sensors, controllers and gateways; segmentation of IoMT and BAS networks; contractual patch obligations; compensating controls for legacy devices; continuous network monitoring; documented manual fallback for safety-critical devices and BAS controllers	Clinical engineering; FM; IT security	IEC 80001-1 [52]; IEC 62443-3-3 [28]; NIST CSF 2.0 (ID.AM, PR.PS, DE.CM) [34]	Devices inventoried in the CMMS; devices patched or compensated; time to remediate critical vulnerabilities
Bridging tier (initial assessment: 0–12 months; full programme: 12–24 months) C7 Erroneous risk assessment and analysis	0–12 months: initial structured risk assessment of critical building and information systems using an asset-vulnerability-threat register shared by IT and FM, including local re-weighting of C4, C6 and C7. 12–24 months: re-weighting annually and after major change; independent review	Risk management; governance board	ISO 31000 [36]; NIST CSF 2.0 (GV, ID.RA) [34]	Date of last reassessment; assets with a current risk rating; audit findings closed; initial assessment completed within 12 months
Tier 2 (12–24 months) C1 Infrastructure design vulnerability	Security architecture review of segmentation, redundancy and IT-OT boundaries at design, refurbishment and commissioning	FM projects; IT architecture	IEC 62443-3-3 [28]; NIST CSF 2.0 (PR.IR) [34]	Projects with a security design review; single points of failure resolved
C2 Personnel negligence and misconduct	Role-specific training including FM and contractor staff; phishing simulation; least privilege; joiner-mover-leaver process	Human resources; information security; FM contracts	NIST CSF 2.0 (PR.AT, PR.AA) [34]	Phishing-simulation failure rate; training completion; orphaned accounts
Baseline (maintain; review annually) C8 Improper data disposal policies	Secure decommissioning of devices, storage media and controllers; certified sanitisation before resale, return or disposal; disposal clauses in vendor and leasing contracts	Clinical engineering; FM; procurement	NIST SP 800-88 Rev. 2 [37]	Retired assets with a sanitisation certificate; disposal-related audit findings

[1] **Bold text identifies the implementation tiers.** Tiers indicate a proposed implementation sequence for a pilot, not differences in importance within a tier, and are based on the stability of each criterion's position across the analyses in Tables 4 and 5 (Section 3.5). Tier 1 comprises the four criteria that formed the top four in all eight specifications retaining the full panel (primary analysis, geometric mean, consistency weighting, three Best-to-Others-only models, single best-versus-worst entry and Bayesian BWM), in 13–15 of the 16 alternative specifications, in at least nine of the ten leave-one-out replications and in 75–95% of bootstrap resamples. Erroneous risk assessment and analysis ranked fifth to seventh in every full-panel specification and entered the top four in one leave-one-out replication and 39% of bootstrap resamples, but entered the top four in seven of the nine specifications that excluded experts, including second place among the experts within the consistency thresholds and three of four group omissions; it is therefore placed in a bridging tier. Infrastructure design vulnerability and personnel negligence and misconduct entered the top four in two and none of the 16 alternative specifications, respectively. The horizons are planning assumptions (Section 4.2), not quantities estimated from the weights.

The tiers and horizons in Table 7 have different bases. The assignment of criteria to tiers reflects the stability of each criterion's position across the analyses in Tables 4 and 5, not the primary ranking alone (Table 7, footnote 1). The positions of loss of data integrity and transparency and of device and endpoint security are sensitive to analytical choices and panel composition: each left the top four in three of the nine specifications that excluded experts. Both, however, remained in the top four in all eight specifications that retained all ten experts, including Bayesian BWM, and in 75–86% of bootstrap resamples. Erroneous risk assessment and analysis showed the opposite pattern. It ranked second among the experts within the consistency thresholds and entered the top four in three of the four group omissions, but ranked fifth to seventh whenever all ten experts were retained and entered the top four in 39% of bootstrap resamples. Because these data do not establish whether it belongs to the leading group, it is placed in a bridging tier: its initial structured risk assessment is scheduled within the first 12 months, in parallel with Tier 1, and its full programme in the following 12 months. Bringing this assessment forward is consistent with its meta-risk role (Section 4) and provides the local evidence needed to confirm or revise, in a given facility, the order of the three criteria whose positions were least stable. The horizons themselves are planning assumptions and are not estimated from the weights. The 0–12-month horizon corresponds to one annual planning, budgeting and management-review cycle, consistent with the annual reassessment and 12-month indicators in Table 7; the 12–24-month horizon schedules the Tier 2 measures, which are tied to design, refurbishment and commissioning projects or to workforce training cycles, within the second cycle.

4.3. Limitations

Several limitations should be acknowledged. First, the analysis relies on expert judgement and is therefore influenced by participants' professional backgrounds, organisational experience and technological familiarity; the panel was drawn from public and private hospitals in Istanbul, Türkiye, which may limit transferability. Although public or private hospital affiliation was known, individual professional roles and other participant characteristics were not recorded; the professional composition of the panel therefore could not be verified, and selection bias towards particular professional perspectives cannot be ruled out; the leading group was sensitive to which experts were retained (Section 3.5). Second, the consistency ratios were driven by products $a_{Bj} \cdot a_{jW}$ exceeding a_{BW}, most plausibly from large Others-to-Worst values; for three experts the two vectors were also ordinally incoherent (Table A2), four experts exceeded the Liang et al. thresholds under the Best-to-Others coding, and the threshold-based subset was itself fragile (Section 3.5). We therefore restrict our firmest claims to the statements identified in Section 3.5 and treat the remaining order, including the first position of privacy and data breach, as provisional.

Third, the criteria combine risk sources, adverse events and control failures, a structure suitable for managerial prioritisation but not for establishing causal relationships. The bow-tie classification (Tables 1 and 6) makes this heterogeneity explicit but does not remove it; it was introduced a posteriori, and the elicitation contained no comparisons between levels.

Fourth, the paper questionnaire had several limitations. C8 appeared last in the fixed C1–C8 sequence and lacked an Others-to-Worst row. For the nine experts whose coded worst criterion was C8, this self-comparison equalled 1 by definition; for expert 6, whose worst criterion was C1, the C8-to-C1 comparison was not elicited and its constraint was omitted. The ticked selections disagreed with the comparison-vector coding for two experts: expert 7 ticked C4 as best but the vector coded C5, and expert 10 ticked C1 as worst but the vector coded C8. The duplicated best-versus-worst entries also differed for experts 3 (8 versus 9), 5 (8 versus 7) and 10 (9 versus 3), with the Best-to-Others value stated first. The

single administration did not include repeat elicitation to resolve these discrepancies; coding and sensitivity analyses make them traceable but cannot recover the participants' intended judgements. The fixed order, final position and narrower scope of C8 may have produced order, salience or scope effects [45]; their contribution cannot be separated from substantive preferences in these data. The reproducible coding procedures remain in Section 2.4.2 and the comparison vectors in Appendix A and Supplementary Material S1.

Fifth, the conclusions rest exclusively on expert perception; they were not triangulated against facility-level incident records, downtime statistics, audit findings or patient-safety indicators, and the comparison with published incident evidence (Section 4.1) is indirect. Sixth, BWM does not estimate dependencies among criteria, so cascading pathways such as personnel negligence leading to endpoint compromise and loss of data integrity are not represented. Seventh, the additional robustness analyses introduced during revision are post hoc exploratory analyses; their role is to characterise uncertainty in the primary estimates rather than to establish a new confirmed ranking.

4.4. Directions for Future Research

Table 8 links each limitation to a targeted design response. The priorities are a role-stratified multicentre replication with recorded aggregate descriptors, a hierarchical elicitation on the bow-tie structure, and a coupling analysis of the leading criteria using DEMATEL or interpretive structural modelling combined with Bayesian networks, each triangulated against institutional incident, downtime, maintenance and audit data.

Table 8. Targeted research agenda linked to the limitations of the present study.

Limitation of the Present Study	Targeted Improvement	Expected Contribution
Single-city panel in Türkiye; ten experts; professional composition not recorded	Multicentre, cross-national panel stratified by role (FM and technical services, clinical engineering, IT and security, management, procurement) with recorded aggregate descriptors, a minimum quota per role and comparison of role-specific weights	Tests generalisability; quantifies the effect of professional background
Criteria at mixed causal levels	Hierarchical BWM elicited at two levels (causal level, then criteria within level) on a bow-tie structure, or separate models for sources, events and barriers	Replaces a posteriori decomposition with elicited between-level comparisons
No analysis of risk coupling	DEMATEL or interpretive structural modelling to elicit influence among criteria; Bayesian networks to propagate cascades (e.g., C2 → C4 → C6 → C5); integration with BWM weights	Distinguishes drivers from consequences; identifies leverage points
High inconsistency on a paper instrument	Digital instrument with real-time consistency and ordinal checks; consistency thresholds and Bayesian BWM specified a priori as the aggregation rule	Fewer incoherent responses; pre-specified rather than post hoc corrections
Perception-only evidence	Triangulation with institutional incident logs, maintenance-management records, downtime statistics, audit findings, recovery-exercise results and patient-safety indicators; longitudinal repetition	Converts judgement-derived hypotheses into validated priorities
Omitted risk domains	Inclusion of vendor concentration, regulatory non-compliance, environmental hazards, physical security and financial constraints	More complete coverage of institution-specific risk

5. Conclusions

The operational sustainability of smart healthcare facilities depends not merely on technological adoption but on the governance of institution-specific vulnerabilities created by digital integration. In this expert panel, privacy and data breach, crisis response and recovery failure, loss of data integrity and transparency, and device and endpoint security

carried the highest aggregate weights, but neither their order nor the membership of this group was stable. Improper data disposal policies ranked last in the primary analysis and the reported non-bootstrap sensitivity specifications. Crisis response and recovery failure ranked first or second in analyses that weighted or selected experts according to judgement consistency, whereas privacy and data breach did not rank first in those analyses. These post hoc exploratory findings do not establish a confirmed alternative ranking, and both positions depended on the experts whose comparison vectors prioritised the respective criteria. Prioritising non-systematic risks through the Best-Worst Method offers healthcare managers a structured and transparent basis for directing limited resources towards the domains judged most critical, provided the resulting priorities are read as provisional, judgement-derived hypotheses rather than as an exact ranking, and validated against incident and downtime data. The weights may serve as provisional inputs to a decision-support process, subject to corroboration by dependency analysis, incident and downtime data, and periodic reassessment as the technological and organisational environment evolves.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/buildings16214370/s1, Supplementary Material S1 (supplementary-S1.xlsx): raw Best-Worst Method data, individual weights, consistency indicators, aggregated results and all sensitivity analyses, including those added in revision. Supplementary Material S2 (S2-analysis-code.py): Python analysis code, tested with (Python 3.12, *NumPy 2.5*, *SciPy 1.18*) that re-computes the values in Tables 3 and 4 from the raw comparison vectors independently of the Excel Solver workbook and performs all post hoc exploratory analyses (Tables 5, 6 and A2).

Author Contributions: Conceptualisation, E.G. and Y.U.; methodology, E.G. and E.Y.; validation, Y.U. and E.G.; formal analysis, E.Y.; investigation, R.Ö.; resources, R.Ö.; data curation, R.Ö. and E.Y.; writing—original draft preparation, E.Y. and R.Ö.; writing—review and editing, E.G., Y.U. and E.Y.; visualisation, E.Y.; supervision, E.G. and Y.U. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and the protocol was approved by the Non-Interventional Clinical Research Ethics Committee of Istanbul Medipol University (decision number 872; project identification code: E-10840098-50.04-3939) on 14 May 2026.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The de-identified comparison matrices, intermediate calculations, derived results, and analysis code are provided in the Supplementary Materials (Supplementary Material S1, Excel workbook; Supplementary Material S2, Python analysis code). Source instruments and consent records are not publicly available because they contain personal identifiers. Anonymised copies of available source records may be requested from the corresponding author, subject to applicable ethical and privacy requirements.

Acknowledgments: The authors thank the experts who participated in the elicitation exercise for their time and expertise. During the preparation of this manuscript, the authors used Claude 3.7 Sonnet (Anthropic) for the purposes of language translation, proofreading, and improving narrative flow. During the revision, Claude Opus 5.5 (Anthropic) was additionally used to assist with drafting revised text and the response to reviewers, preparing the re-analysis code (Python; see Sections 2.4.2 and 2.7, where its role is described in detail) and checking references. The tool was not used to generate or alter study data, to select analyses or to interpret the results. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

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

Abbreviations

The following abbreviations are used in this manuscript:

AHP	Analytic hierarchy process
ANP	Analytic network process
BAS	Building automation system
BMS	Building management system
BO	Best-to-Others
BWM	Best-Worst Method
CI	Consistency index
CMMS	Computerised maintenance management system
CR	Consistency ratio
CR^I	Input-based consistency ratio
CSF	Cybersecurity Framework
DANP	DEMATEL-based analytic network process
DEMATEL	Decision-Making Trial and Evaluation Laboratory
ESS	Effective sample size
FM	Facility management
HVAC	Heating, ventilation and air-conditioning
IEC	International Electrotechnical Commission
IoMT	Internet of Medical Things
IoT	Internet of Things
ISO	International Organisation for Standardisation
IT	Information technology
MFA	Multi-factor authentication
NIST	National Institute of Standards and Technology
OT	Operational technology
OW	Others-to-Worst

Appendix A

Table A1. Best-to-Others and Others-to-Worst comparison vectors reported by each expert (best and worst are the coded selections).

Expert	Best	Worst	Best-to-Others Vector (C1 ... C8)	Others-to-Worst Vector (C1 ... C7)
E1	C5	C8	4, 5, 2, 3, 1, 3, 6, 9	6, 7, 8, 7, 9, 6, 4
E2	C3	C8	4, 3, 1, 3, 5, 2, 6, 8	5, 7, 8, 4, 8, 6, 3
E3	C6	C8	5, 4, 2, 4, 3, 1, 5, 8	6, 7, 9, 6, 7, 9, 5
E4	C7	C8	5, 6, 4, 5, 4, 3, 1, 9	6, 4, 5, 5, 6, 4, 9
E5	C4	C8	3, 4, 2, 1, 5, 3, 6, 8	6, 7, 8, 7, 9, 4, 3
E6	C7	C1	8, 4, 3, 5, 4, 3, 1, 6	1, 4, 4, 5, 6, 3, 8
E7	C5	C8	4, 5, 3, 3, 1, 4, 6, 9	5, 7, 8, 7, 9, 6, 4
E8	C1	C8	1, 4, 5, 2, 3, 6, 5, 9	9, 5, 6, 8, 7, 4, 5
E9	C5	C8	3, 4, 5, 2, 1, 3, 6, 9	7, 6, 5, 8, 9, 6, 4
E10	C3	C8	8, 4, 1, 5, 7, 2, 6, 9	9, 1, 3, 8, 2, 9, 8

Table A2. Judgement traceability diagnostics by expert (post hoc).

Expert	ρ [1] (BO [2], OW [3])	Reversed Pairs [4]	a_{BW} in BO/OW	Largest Triad Deviations ($a_{Bj} \cdot a_{jW} - a_{BW}$)	Classification [5]
E1	0.87	2/27 (7%)	9/9	C2 +26; C1 +15; C7 +15	Coherent
E2	0.63	6/27 (22%)	8/8	C5 +32; C2 +13; C1 +12	Coherent
E3	0.95	0/26 (0%)	8/9	C1 +22; C2 +20; C7 +17	Coherent
E4	0.60	5/26 (19%)	9/9	C1 +21; C4 +16; C2 +15	Coherent
E5	0.49	8/27 (30%)	8/7	C5 +37; C2 +20; C1 +10	Ordinally incoherent
E6	0.42	6/19 (32%)	8/8	C4 +17; C5 +16; C2 +8	Ordinally incoherent
E7	0.88	2/26 (8%)	9/9	C2 +26; C3 +15; C6 +15	Coherent

Table A2. *Cont.*

Expert	ρ [1] (BO [2], OW [3])	Reversed Pairs [4]	a_{BW} in BO/OW	Largest Triad Deviations ($a_{Bj} \cdot a_{jW} - a_{BW}$)	Classification [5]
E8	0.95	1/27 (4%)	9/9	C3 +21; C7 +16; C6 +15	Coherent
E9	0.98	0/27 (0%)	9/9	C3 +16; C2 +15; C7 +15	Coherent
E10	0.16	11/28 (39%)	9/3	C1 +63; C7 +39; C4 +31	Ordinally incoherent

[1] ρ = Spearman correlation between the importance orders implied by the two vectors. [2] BO: Best-to-Others vector; [3] OW: Others-to-Worst vector. [4] Reversed pairs = criterion pairs strictly reversed between the vectors, among pairs not tied in the BO vector (for E6 the C8 comparison was not elicited). [5] Classification: ordinally incoherent if $\rho < 0.50$ (threshold chosen post hoc); the rule of more than 25% reversed pairs identifies the same experts.

References

1. Lin, C.L.; Chen, J.K.C.; Ho, H.H. BIM for smart hospital management during COVID-19 using MCDM. *Sustainability* **2021**, *13*, 6181. [CrossRef]
2. Zhang, X.; Zhang, Y.; Peng, Y.; Au-Yong, C.P.; Awang, N.A. Transforming healthcare facility management with digital technologies: A systematic review and future roadmap. *Adv. Eng. Inform.* **2026**, *71*, 104404. [CrossRef]
3. Chen, J.K.C.; Ho, H.H. Asset resource optimization solution for smart hospital facilities and energy management through an interpretive structural model. *Buildings* **2023**, *13*, 3064. [CrossRef]
4. Adibi, S.; Rajabifard, A.; Shojaei, D.; Wickramasinghe, N. Enhancing healthcare through sensor-enabled digital twins in smart environments: A comprehensive analysis. *Sensors* **2024**, *24*, 2793. [CrossRef]
5. Ibrahim, F.; Samsudin, E.Z.; Ishak, A.R.; Sathasivam, J. Hospital indoor air quality and its relationships with building design, building operation, and occupant-related factors: A mini-review. *Front. Public Health* **2022**, *10*, 1067764. [CrossRef]
6. Ewoh, P.; Vartiainen, T. Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. *J. Med. Internet Res.* **2024**, *26*, e46904. [CrossRef]
7. Ciholas, P.; Lennie, A.; Sadigova, P.; Such, J.M. The security of smart buildings: A systematic literature review. *arXiv* **2019**, arXiv:1901.05837.
8. Huda, S.; Islam, M.R.; Abawajy, J.; Kottala, V.N.V.; Ahmad, S. A cyber risk assessment approach to federated identity management framework-based digital healthcare system. *Sensors* **2024**, *24*, 5282. [CrossRef]
9. Yaqoob, T.; Abbas, H.; Atiquzzaman, M. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices-A review. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3723–3768. [CrossRef]
10. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.N.; Mullins, M.; Murphy, F.; Materne, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap. Risk Insur. Issues Pract.* **2022**, *47*, 698–736. [CrossRef]
11. Kruse, C.S.; Frederick, B.; Jacobson, T.; Monticone, D.K. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technol. Health Care* **2017**, *25*, 1–10. [CrossRef]
12. Jalali, M.S.; Kaiser, J.P. Cybersecurity in hospitals: A systematic, organizational perspective. *J. Med. Internet Res.* **2018**, *20*, e10059. [CrossRef]
13. He, Y.; Aliyu, A.; Evans, M.; Luo, C. Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *J. Med. Internet Res.* **2021**, *23*, e21747. [CrossRef]
14. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Secur. Appl.* **2023**, *1*, 100016. [CrossRef]
15. Lehto, M.; Neittaanmäki, P.; Pöyhönen, J.; Hummelholm, A. Cyber security in healthcare systems. In *Cyber Security: Critical Infrastructure Protection*; Lehto, M., Neittaanmäki, P., Eds.; Computational Methods in Applied Sciences; Springer: Cham, Switzerland, 2022; Volume 56, pp. 183–215. [CrossRef]
16. Liu, Y. Risk management of smart healthcare systems: Delimitation, state-of-arts, process, and perspectives. *J. Patient Saf. Risk Manag.* **2022**, *27*, 129–148. [CrossRef]
17. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors* **2021**, *21*, 5119. [CrossRef]
18. Hernandez-Jaimes, M.L.; Martinez-Cruz, A.; Ramírez-Gutiérrez, K.A.; Feregrino-Uribe, C. Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. *Internet Things* **2023**, *23*, 100887. [CrossRef]
19. Hosseini, S.; Barker, K.; Ramirez-Marquez, J.E. A review of definitions and measures of system resilience. *Reliab. Eng. Syst. Saf.* **2016**, *145*, 47–61. [CrossRef]

20. Mottahedi, A.; Sereshki, F.; Ataei, M.; Nouri Qarahasanlou, A.; Barabadi, A. The resilience of critical infrastructure systems: A systematic literature review. *Energies* **2021**, *14*, 1571. [CrossRef]
21. Khalil, M.; Ravaghi, H.; Samhouri, D.; Abo, J.; Ali, A.; Sakr, H.; Camacho, A. What is "hospital resilience"? A scoping review on conceptualization, operationalization, and evaluation. *Front. Public Health* **2022**, *10*, 1009400. [CrossRef]
22. Fallah-Aliabadi, S.; Ostadtaghizadeh, A.; Ardalan, A.; Fatemi, F.; Khazai, B.; Mirjalili, M.R. Towards developing a model for the evaluation of hospital disaster resilience: A systematic review. *BMC Health Serv. Res.* **2020**, *20*, 64. [CrossRef]
23. Rezaei, J. Best-worst multi-criteria decision-making method. *Omega* **2015**, *53*, 49–57. [CrossRef]
24. Rezaei, J. Best-worst multi-criteria decision-making method: Some properties and a linear model. *Omega* **2016**, *64*, 126–130. [CrossRef]
25. de Ruijter, A.; Guldenmund, F. The bowtie method: A review. *Saf. Sci.* **2016**, *88*, 211–218. [CrossRef]
26. Demertzi, V.; Demertzis, S.; Demertzis, K. An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. *Appl. Sci.* **2023**, *13*, 790. [CrossRef]
27. Javed, A.R.; Shahzad, F.; Rehman, S.U.; Zikria, Y.B.; Razzak, I.; Jalil, Z.; Xu, G. Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects. *Cities* **2022**, *129*, 103794. [CrossRef]
28. *IEC 62443-3-3:2013*; Industrial Communication Networks-Network and System Security-Part 3-3: System Security Requirements and Security Levels. International Electrotechnical Commission: Geneva, Switzerland, 2013.
29. Seh, A.H.; Zarour, M.; Alenezi, M.; Sarkar, A.K.; Agrawal, A.; Kumar, R.; Khan, R.A. Healthcare data breaches: Insights and implications. *Healthcare* **2020**, *8*, 133. [CrossRef]
30. Neprash, H.T.; McGlave, C.C.; Cross, D.A.; Virnig, B.A.; Puskarich, M.A.; Huling, J.D.; Rozenshtein, A.Z.; Nikpay, S.S. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum* **2022**, *3*, e224873. [CrossRef]
31. Akinbi, A.; Raj, P.P. A systematic security analysis of medical internet of things (MIoT) ecosystems in threat modeling scenarios. *Front. Internet Things* **2025**, *4*, 1712430. [CrossRef]
32. Galbusera, L.; Cardarilli, M.; Giannopoulos, G. The ERNCIP survey on COVID-19: Emergency & business continuity for fostering resilience in critical infrastructures. *Saf. Sci.* **2021**, *139*, 105161. [CrossRef]
33. Rostek, K.; Wiśniewski, M.; Skomra, W. Analysis and evaluation of business continuity measures employed in critical infrastructure during the COVID-19 pandemic. *Sustainability* **2022**, *14*, 15388. [CrossRef]
34. National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*; NIST Cybersecurity White Paper 29; NIST: Gaithersburg, MD, USA, 2024. [CrossRef]
35. Parsons, E.; Panaousis, E.; Loukas, G.; Sakellari, G. A survey on cyber risk management for the Internet of Things. *Appl. Sci.* **2023**, *13*, 9032. [CrossRef]
36. *ISO 31000:2018*; Risk Management-Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018.
37. Chandramouli, R.; Hibbard, E. *Guidelines for Media Sanitization*; NIST Special Publication 800-88 Rev. 2; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2025. [CrossRef]
38. Saaty, T.L. Decision making with the analytic hierarchy process. *Int. J. Serv. Sci.* **2008**, *1*, 83–98. [CrossRef]
39. Mi, X.; Tang, M.; Liao, H.; Shen, W.; Lev, B. The state-of-the-art survey on integrations and applications of the best worst method in decision making: Why, what, what for and what's next? *Omega* **2019**, *87*, 205–225. [CrossRef]
40. Si, S.-L.; You, X.-Y.; Liu, H.-C.; Zhang, P. DEMATEL technique: A systematic review of the state-of-the-art literature on methodologies and applications. *Math. Probl. Eng.* **2018**, *2018*, 3696457. [CrossRef]
41. Liang, F.; Brunelli, M.; Rezaei, J. Consistency issues in the best worst method: Measurements and thresholds. *Omega* **2020**, *96*, 102175. [CrossRef]
42. Mohammadi, M.; Rezaei, J. Bayesian best-worst method: A probabilistic group decision making model. *Omega* **2020**, *96*, 102075. [CrossRef]
43. Efron, B.; Tibshirani, R.J. *An Introduction to the Bootstrap*; Chapman & Hall: New York, NY, USA, 1993. [CrossRef]
44. Kendall, M.G.; Babington Smith, B. The problem of m rankings. *Ann. Math. Stat.* **1939**, *10*, 275–287. [CrossRef]
45. Montibeller, G.; von Winterfeldt, D. Cognitive and motivational biases in decision and risk analysis. *Risk Anal.* **2015**, *35*, 1230–1251. [CrossRef]
46. 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. [CrossRef]
47. Neprash, H.; McGlave, C.; Nikpay, S. Hacked to pieces? The effects of ransomware attacks on hospitals and patients. *Am. Econ. J. Econ. Policy* **2026**, *18*, 256–281. [CrossRef]
48. Abouk, R.; Powell, D. Ransomware attacks, ED visits and inpatient admissions in targeted and nearby hospitals. *JAMA* **2024**, *331*, 2129. [CrossRef]
49. Dameff, C.; Tully, J.; Chan, T.C.; Castillo, E.M.; Savage, S.; Maysent, P.; Hemmen, T.M.; Clay, B.J.; Longhurst, C.A. Ransomware attack associated with disruptions at adjacent emergency departments in the US. *JAMA Netw. Open* **2023**, *6*, e2312270. [CrossRef]

50. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection-Information Security Management Systems-Requirements. International Organization for Standardization: Geneva, Switzerland, 2022.
51. *ISO 22301:2019*; Security and Resilience-Business Continuity Management Systems-Requirements. International Organization for Standardization: Geneva, Switzerland, 2019.
52. *IEC 80001-1:2021*; Application of Risk Management for IT-Networks Incorporating Medical Devices-Part 1: Safety, Effectiveness and Security in the Implementation and Use of Connected Medical Devices or Connected Health Software. International Electrotechnical Commission: Geneva, Switzerland, 2021.
53. Bellini, E.; D'Aniello, G.; Flammini, F.; Gaeta, R. Situation awareness for cyber resilience: A review. *Int. J. Crit. Infrastruct. Prot.* **2025**, *49*, 100755. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.