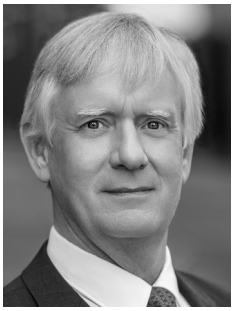
# Zur Cybersicherheit von Krankenhäusern – Eine empirische Bestandsaufnahme



*Daniel Zängerle und Dirk Schiereck*

**Schlagwörter:** Cyberrisiken, Experteninterviews, Gesundheitswesen, Krankenhäuser, Cyberrisikomanagement, Cybersicherheitsbewusstsein

**Zusammenfassung:** In Anbetracht der stetig steigenden Bedrohungslage durch Cyberrisiken untersucht dieser Beitrag Implikationen für das Cyberrisikomanagement in deutschen Krankenhäusern. Aufgrund des Facettenreichtums dieser Herausforderungen und der bislang noch unzureichenden Berücksichtigung in der wissenschaftlichen Forschung werden explorative Interviews mit Experten aus deutschen Krankenhäusern sowie des Gesundheitswesens geführt. Die Ergebnisse dieser Interviews verdeutlichen, dass Cyberrisiken als reale Bedrohung für Krankenhäuser wahrgenommen werden. Allerdings mangelt es noch an einer ausgeprägten Cyber Security Awareness sowie einer systematischen Implementierung und Integration des Cyberrisikomanagements.

**On the Cybersecurity of Hospitals – An Empirical Review**

**Keywords:** Cyber risks, expert interviews, healthcare, hospitals, cyber risk management, cyber security awareness

**Summary:** In light of the ever-increasing threat posed by cyber risks, this paper explores implications for cyber risk management in German hospitals. Given the multifaceted nature of these challenges and the insufficient consideration in scientific research, exploratory interviews are conducted with experts from German hospitals as well as the healthcare sector. The results of these interviews illustrate that cyber risks are perceived as a real threat to hospitals. However, there is still a lack of pronounced cyber security awareness as well as systematic implementation and integration of cyber risk management.

## 1 Ausgangssituation und Problemstellung

Die voranschreitende Digitalisierung und Integration von Informationstechnologie (IT) verbessert einerseits die Dienstleistungsqualität in vielen Sektoren, andererseits resultieren daraus neuartige Gefahren (Argaw et al., 2020). Cyberrisiken stellen dabei nach Einschätzung des World Economic Forum (2021) die wohl größte, neue Bedrohungsart des 21. Jahrhunderts dar. Aktuelle Lageberichte nationaler Institute beobachten eine weitere Anspannung der Bedrohungslage, die sich durch Cyberkrieg und die Professionalisierung der digitalen Angreifer zuspitzt (Bundesamt für Sicherheit in der Informationstechnik, 2022). Diese Entwicklungen sind für Industrien, die regelmäßig mit zahlreichen vertraulichen,

personenbezogen Daten umgehen, von besonderer Relevanz und werden dort auch in verschiedenen Ländern mit sektorspezifischen Regulierungen adressiert. Neben der Finanzdienstleistungsindustrie trifft dies insbesondere auf den Gesundheitssektor zu, wo ein großes Risiko für alle Gesundheitsprozesse erkannt wird (Sardi et al., 2020), was mit jüngsten Angriffen auf das Gesundheitswesen in den Vereinigten Staaten (Tully et al., 2020), Großbritannien (Clarke & Youngstein, 2017) sowie Deutschland (Argaw et al., 2020; Kucera, 2020) sehr sichtbar wurde. Die Bedeutung der IT- und Cybersicherheit wird gerade für Krankenhäuser wohl noch weiter zunehmen, insbesondere vor dem Hintergrund der digitalen Abbildung der gesamten patientenorientierten Prozesskette, der Masse an täglich erzeugten Daten sowie der regelmäßigen Handhabung mobiler Geräte (Darms et al., 2019). Während sich bislang die Investitionen bei der Digitalisierung auf die (medizinischen) Kernprozesse fokussiert haben, ergeben sich durch Cyberrisiken zusätzliche Herausforderungen in der Verteilung knapper IT-Ressourcen im Krankenhaus (Hoppe et al., 2021).

Cyberrisiken sind nicht nur für öffentliche und private Unternehmen im Gesundheitswesen von höchster Relevanz, sondern auch für Menschen und deren Wohlbefinden (Zängerle & Schiereck, 2023a), und fordern durch die gesellschaftliche Relevanz die Politik zum Handeln auf. Diese Bedeutung des Schutzes von Patienten- und Gesundheitsdaten wurde in den Vereinigten Staaten durch den Health Insurance Portability and Accountability Act (HIPAA) sowie den Health Information Technology for Economic and Clinical Health Act (HITECH) früh erkannt (Bohn & Schiereck, 2023). In Europa und Deutschland hat die Einführung der Datenschutzgrundverordnung (DSGVO) einen ersten einheitlichen Rahmen zur Verarbeitung personenbezogener Daten geschaffen. Zudem leistet das IT-Sicherheitsgesetz und dessen jüngste Erweiterung einen wichtigen Beitrag zur allgemeinen Erhöhung der Cybersicherheit sowie zum Schutz der Bürgerinnen und Bürger im Internet (Kosub, 2015; Darms et al., 2019). Trotz dieser Initiativen hat mit der Einführung der elektronischen Gesundheits- und Krankenakte das kriminelle Ausbeutungsrisiko von Patientendaten aber zugenommen (Li et al. 2019). Jenseits externer Bedrohungen für die IT-Systeme von Unternehmen erhöhen unternehmensinterne Verhaltensweisen häufig das Cyberrisiko. Dabei vernachlässigt das Enterprise Risk Management (ERM) vieler Unternehmen die mit der Digitalisierung einhergehenden Risiken, und es finden sich Vorwürfe, nach denen einige Akteure nicht nur die Schadenswirkungen von Cyberrisiken unzureichend wahrnehmen (Wrede et al., 2018), sondern generell nur eine passive Haltung gegenüber Cyberrisiken einnehmen (Ashby et al., 2018; Pooser et al., 2018; Zängerle & Schiereck, 2023b).

Die wissenschaftliche Forschung hat sich den Herausforderungen des Cyberrisikomanagement zwar schon aus verschiedenen Richtungen angenommen, und es finden sich in der Informatik, den Wirtschaftswissenschaften und der Versicherungsmathematik einige Forschungsarbeiten (Eling, 2020). Im Gegensatz zu den sektorspezifischen Regulierungsansätzen der Politik und den Untersuchungen über operationelle Risiken im Finanzsektor gibt es jedoch bislang kaum Erkenntnisse zur Cybersicherheit im Gesundheitswesen, insbesondere für den deutschsprachigen und europäischen Raum (Sardi et al., 2020) sowie über den Umgang mit Cyberrisiken in diesem Sektor (Wrede et al., 2018).

Tanriverdi et al. (2020) zeigen, wie verschiedene Komplexitätstreiber in der Krankenhausinfrastruktur die Risiken von Datenschutzverletzungen vorantreiben. Angst et al. (2017) betonen die Bedeutung kohärenter, tief integrierter IT-Sicherheitspraktiken, indem

sie die anhaltende Anfälligkeit von Krankenhäusern für IT-Risiken aufzeigen, wo die mitigierenden Maßnahmen lediglich symbolisch sind. Darauf aufbauend berichten Li et al. (2019), dass die Abweichung der Sicherheitsinvestitionen von Industriestandards eine wichtige Rolle bei der Bewertung der Wahrscheinlichkeit von Sicherheitsverletzungen spielt. Jedoch basieren Erkenntnisse dieser Studien auf Datenschutzverletzungen in den USA, was zu zwei Einschränkungen führt: 1) Cyberrisiken umfassen mehr als nur Datenschutzverletzungen (Eling, 2018), und: 2) Aufgrund des regionalen Fokus und der unterschiedlichen regulatorischen Anforderungen ist die Verallgemeinerbarkeit auf den europäischen und deutschen Raum in Frage zu stellen. Basierend auf Fallstudien zeigen Argaw et al. (2020) wichtige Handlungsfelder im Bereich der Cybersicherheit auf, wobei es an methodologischer Klarheit und Vollständigkeit der vorgeschlagenen Ansätze aber noch fehlt. Blanke & McGrady (2016) entwickeln eine Prüfliste, die in der initialen Bewertung des Status Quo helfen kann. Jedoch liegt der Fokus auf präventiven Maßnahmen und vernachlässigt organisatorisch konzeptionelle Gegenmaßnahmen aufgrund der ambivalenten Natur des Cyberrisikos (Boyer, 2020).

Vor diesem Hintergrund ist das Ziel dieses Beitrags, eine umfassendere Bestandsaufnahme der Cybersicherheit im deutschen Gesundheitswesen zu liefern. Dabei werden nicht nur neue Erkenntnisse und Good Practices des Cyberrisikomanagements identifiziert, sondern auch die zugrundeliegenden Problematiken von Cyberrisiken im Gesundheitswesen genauer erforscht und allgemeingültige Auffassungen im Sinne der Problematisierung hinterfragt (Alvesson & Sandberg, 2011). Basierend auf einem qualitativ empirischen Forschungsansatz werden 19 IT- und Cybersicherheitsexperten[1] aus führenden deutschen Krankenhäusern und des Gesundheitswesens befragt. Konkret werden vier Themengebiete beleuchtet: 1) Begriffsverständnis über den Terminus „Cyberrisiko“, 2) Organisatorischer Hintergrund, 3) Cyberrisikomanagement und 4) Herausforderungen und Trends zur Cybersicherheit im Gesundheitswesen. In diesem Kontext gibt diese Studie als erste ihrer Art Aufschluss über den aktuellen Status quo deutscher Krankenhäuser und deren Cyberrisikomanagement sowie über die aktuellen Herausforderungen, um das Gesundheitswesen vor zukünftigen Cyberangriffen zu schützen.

Zur Erreichung der angeführten Zielsetzung wird in Abschnitt 2 der Terminus Cyberrisiko begrifflich eingeordnet sowie ein Überblick über die relevante Literatur zum Management von Cyberrisiken und der Herausforderungen im Gesundheitswesen gegeben. Abschnitt 3 stellt das Forschungsdesign und das Vorgehen der Datenerhebung und -auswertung vor. In Abschnitt 4 werden die Ergebnisse der analysierten Experteninterviews vorgestellt sowie im folgenden Abschnitt 5 diskutiert. Abschnitt 6 fasst die Ergebnisse und Limitationen dieses Beitrages abschließend zusammen.

## 2 Stand der Forschung

Eine Bestandsaufnahme zum Umgang mit Cyberrisiken im Gesundheitswesen setzt die Erfassung des Begriffsverständnisses voraus, der in einer Industrie für diese Risiken vorherrscht. Dementsprechend ist zunächst der Stand der Literatur über Definition und Abgrenzung von Cyberrisiken kurz zu umreißen. Auf dieser Basis ist im nächsten Schritt

1 In diesem Beitrag wird aus Gründen der leichteren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.

die Literatur zur Implementierung von Risikomanagementprozessen für Cyberrisiken zu dokumentieren, um ein Benchmarking für das Gesundheitswesen vorzunehmen und zu klären, was im Gesundheitswesen anders gemacht wird als in anderen Wirtschaftszweigen. Nach einer Darlegung der allgemein beobachteten Vorgehensweisen beim Umgang mit Cyberrisiken gilt es deshalb, bisherige Einsichten der Forschung aus dem Gesundheitswesen zu erläutern und die bestehende Forschungslücke nochmals zu verdeutlichen.

### 2.1 Begriffsverständnis

Der Begriff Cyberrisiko wurde zwar schon mehrfach neu- und umdefiniert,[2] aber die Diskussion ist keinesfalls abgeschlossen und ein einheitliches Begriffsverständnis fehlt. Nach Gordon et al. (2003) handelt es sich um das „Geschäftsrisiko aus der Verbindung mit dem Internet", während Biener et al. (2015) – in Anlehnung an Cebula und Young (2010) – Cyberrisiken als „operationelle Risiken für Informations- und Technologieanlagen, die Auswirkungen auf die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder Informationssystemen haben" bezeichnen. Eine weiter gefasste Definition liefern Eling und Schnell (2016), die unter Cyberrisiken alle „Risiken, die sich aus der Nutzung von IT ergeben und die Vertraulichkeit, Verfügbarkeit oder Integrität von Daten oder Diensten gefährden" verstehen. Darauf aufbauend haben Zängerle & Schiereck (2023a) eine neue, ebenfalls umfassend angelegte Definition des Terminus Cyberrisiko vorgeschlagen, die Cyberrisiken nicht ausschließlich auf operationelle oder IT-Risiken beschränkt, sondern auch den Faktor Mensch als Bedrohung sowie Schadensobjekt versteht. Für die weiteren Untersuchungsschritte mit den Experteninterviews werden in Anlehnung an Zängerle und Schiereck (2023a) unter Cyberrisiko alle Bedrohungen aus dem Cyberraum verstanden, „die aufgrund einer Schwachstelle, sowohl materielle als auch immaterielle Werte als auch Menschen gefährden, was zu direkten und indirekten Schäden einer betroffenen Einheit und von Dritten führen kann" (Zängerle & Schiereck, 2023a). Im Gegenzug zielt die Cybersicherheit darauf ab, die Konsequenzen aus Cyberrisiken zu begrenzen.

### 2.2 Cyberrisikomanagement

Cyberrisiken gefährden Unternehmen, unabhängig von ihrer Größe, ihrem Geschäftsmodell oder der Industrie (Lloyd, 2020; Hoppe et al., 2021), aber die individuelle Gefahrenlage hängt von der spezifischen Anfälligkeit eines Unternehmens für Cybervorfälle ab, sodass vorhandene Schwachstellen in der IT-Sicherheit die Wahrscheinlichkeit eines Cybervorfalls erhöhen (Marotta et al., 2017). Allerdings besteht Einigkeit darüber, dass selbst ein hohes IT-Sicherheitsniveau ein Unternehmen nicht vollständig vor Cybervorfällen schützen kann, da Cyberrisiken nicht nur durch technische Fehler ausgelöst werden (Bandyopadhyay et al., 2009; Camillo, 2017; Smidt & Botzen, 2018; Falco et al., 2019; Hoppe et al., 2021). Entsprechend der Komplexität dieses Risikofeldes und den möglichen existenzbedrohenden Schäden zielt das IT-Sicherheitsmanagement zunächst darauf ab, die Vertraulichkeit, Verfügbarkeit und Integrität von Daten zu schützen (Whitman & Mattord, 2014; International Standard Organisation, 2018; Bitzer et al., 2021). Da die meisten Unternehmen offensichtlich große Probleme in der Erkennung und Bewertung von Cyberbedrohungen haben (Berger et al., 2020), erscheint zudem die Etablierung eines

2 Für eine umfassende Auseinandersetzung mit der Begriffsbestimmung des Terminus Cyberrisiko wird auf Zängerle & Schiereck (2023a) verwiesen.

spezifischen Cyberrisikomanagements unabdingbar (International Standard Organisation, 2018). Nach Hubbard & Seiersen (2016) umfasst ein Risikomanagement allgemein die „Identifizierung, Bewertung und Priorisierung von Risiken, gefolgt von einem koordinierten und wirtschaftlichen Einsatz von Ressourcen zur Minimierung, Überwachung und Kontrolle der Wahrscheinlichkeit und/oder der Auswirkungen". Daran angelehnt analysiert Kosub (2015) die zentralen Elemente eines ganzheitlichen Cyberrisikomanagements unter Berücksichtigung relevanter Sicherheitsstandards und diskutiert weiterführend existierende Herausforderungen für die Absicherung von Cyberrisiken. Anspruchsvolle Risikomanagement-Strategien berücksichtigen hier potenzielle IT-Sicherheitsbedrohungen, um Verluste durch etwaige IT-Sicherheitsvorfälle zu minimieren, und bilden die Grundlage für die Auswahl geeigneter Gegenmaßnahmen (International Standard Organisation, 2018).

Da sich Technologien und Cyberrisiken dynamisch verhalten (Eling, 2020), ändert sich die Gefahrenlage fortlaufend, und Unternehmen müssen ihre Bedrohungslandschaft und Gegenmaßnahmen kontinuierlich überwachen, um ihre Daten vor möglichen Cybervorfällen zu schützen (International Standard Organisation, 2018). Eine Herausforderung stellen dabei zunehmend die eigenen Mitarbeitenden als zentrale Schwachstelle der internen Cybersicherheit dar (Biener et al., 2015; Wrede et al., 2018). Daher zählt die Schaffung eines ausgeprägten Risikobewusstseins der Mitarbeitenden für alle Belange der IT- und Cybersicherheit – die sogenannte Cyber- bzw. Information Security Awareness – zu den wichtigsten Aufgaben des IT- und Informationssicherheitsmanagements (Thomson & Solms, 1998; Nosworthy, 2000; Kritzinger & Smith, 2008; Tsohou et al., 2012; Abawajy, 2014; Wrede et al., 2018). Hierbei kann das Management von Cyberrisiken nicht gänzlich an die IT-Abteilung delegiert werden, sondern muss in den gesamten Risikomanagementprozess eines Unternehmens integriert werden (Marotta & McShane, 2018; Shetty et al., 2018; Poyraz et al., 2020; Zängerle & Schiereck, 2023b).

Um einen Risikomanagementprozess zu etablieren, können Risikomanagementrichtlinien helfen, um sich organisatorischen Fragen zu widmen, den Prozess und die beteiligten Parteien zu beschreiben, die wichtigsten Begrifflichkeiten zu definieren sowie unterstützende Dokumente und Prozessbeschreibungen zu erstellen (Marotta et al., 2017). Taylor et al. (2012) betonen hierzu den Risikomanagementzyklus, bestehend aus 1) Identifikation, 2) Analyse, 3) Priorisierung, 4) Planung, 5) Überwachung und 6) Kontrolle. Während einige praktisch implementierte Leitlinien allgemein gehalten sind, geben andere spezifische Angaben zu technischen Details und stellen Instrumente für die Risikobewertung bereit (National Institute of Standards and Technology, 2012; Marotta et al., 2017). Zudem kann die in der Praxis bekannte ISO/IEC 27001-Norm als Leitfaden betrachtet werden, da sie alle Schritte des Risikomanagements beschreibt (International Standard Organisation, 2018).

Begrenzte Ressourcen machen es erforderlich, Prioritäten auf Grundlage von Kosteneffizienz bei Sicherheitsmaßnahmen zu setzen (Paté-Cornell et al., 2018). Dabei werden vorwiegend qualitative Cyberrisikomanagementprozesse implementiert (Palsson et al., 2020). Es existieren aufgrund der begrenzten Datenlage zu Cybervorfällen bislang nur wenige quantitative Ansätze zur Bewertung und Modellierung von Cyberrisiken (Zängerle & Schiereck, 2023b), was beispielsweise einen Risikotransfer im Sinne einer Cyberversicherung erschwert. Sowohl die Versicherbarkeit von Cyberrisiken als auch die Cyberversicherung als Instrument des Risikomanagements sind in der wissenschaftlichen Literatur bereits in Ansätzen untersucht worden (Eling & Schnell, 2016; Marotta et al., 2017; Wrede

et al., 2018). So zeigt Samhan (2017), dass der Abschluss einer Cyberversicherungspolice auch helfen kann, die aktuelle Bedrohungslage zu verstehen sowie die Einführung neuer Technologien zu legitimieren. Der begrenzte praktische Einsatz dieses Instruments des Risikomanagements zeigt aber, dass Cyberversicherungen noch mit verschiedenen Problemen zu kämpfen haben, beispielsweise auch bei der Prämienfindung.

### 2.3 Herausforderungen des Gesundheitswesens

Die zunehmende Integration von Technologie in den Gesundheitsbereich führt einerseits zu einer kontinuierlichen Verbesserung der Gesundheitsversorgung, andererseits erhöht sich die Exponierung vor Cybervorfällen (Argaw et al., 2020). Insbesondere weisen medizinische Geräte aufgrund der zunehmenden Konnektivität Schwachstellen in der Cybersicherheit auf, vor denen sie bisher geschützt waren (Williams & Woodward, 2015). Die Folgen eines potenziellen Cyberangriffs können sowohl operativ als auch finanziell katastrophal sein (McDonough, 2007), denn Cyberangriffe können eine Vielzahl von Dienstleistungen innerhalb eines Krankenhauses bedrohen, von Operationen bis hin zur Medikamentenabgabe, indem sie auf moderne Geräte wie Kühlschränke für Blutprodukte, bildgebende Geräte, automatische Medikamentenabgabegeräte und elektronische Gesundheitsakten abzielen, aber auch auf unterstützende kritische Systeme wie Heizung, Belüftung und Klimatisierung (Argaw et al., 2020). Seit der Einführung von Informationssystemen im Gesundheitswesen wird deren Sicherheit als wichtiges Thema betrachtet, insbesondere angesichts der Tatsache, dass es sich bei den Daten um äußerst sensible Informationen handelt (Smith & Eloff, 1999). Jedoch erschweren der Umfang und die Komplexität der Unternehmensabläufe in Verbindung mit zahlreichen veralteten und inkompatiblen Systemen die Umsetzung wirksamer Cybersicherheitsmaßnahmen im Gesundheitswesen (Abraham et al., 2019). Die Fokussierung auf rechtliche Vorgaben, Compliance-Vorschriften und Sicherheitsrichtlinien erschwert die Berücksichtigung angemessener technologischer Lösungen, was nach Abraham et al. (2019) oft dazu führt, dass die Führungsebene einen Zustand glücklicher Unwissenheit einnimmt.

Die jüngsten Vorfälle, wie zum Beispiel am Lukaskrankenhaus Neuss (Argaw et al., 2020) und am Universitätsklinikum Düsseldorf (Kucera, 2020), zeigen deutlich, dass Einrichtungen des Gesundheitswesens nicht nur gefährdet, sondern auch ein wahrscheinliches Ziel von Cyberangriffen sind (Holden, 2015). Das zeigen auch Etges et al. (2018) im Rahmen einer Befragung von 15 Chief Risk Officers (CRO), wo Cyberangriffe von den Teilnehmern als das größte Risiko eingestuft wurden. Ferner ergeben sich erste Indizien, dass große Krankenhäuser, gemessen an der Bettenzahl, mehr als doppelt so häufig von Cybervorfällen betroffen sind wie kleinere (McLeod & Dolezel, 2018). Daher schlagen Boudko & Abie (2019) vor, dass Gesundheitsorganisationen einen dynamischen Cybersicherheitsrahmen einführen sollten, um die vielfältigen Ökosysteme des Gesundheitswesens zu schützen und effizienter sowie widerstandsfähiger gegen Datenschutz- und Informationssicherheitsrisiken aufgestellt zu sein. Aufgrund der Vielzahl an potenziellen Angriffen ist laut Priestman et al. (2019) eine kontinuierliche Aufklärung über das gesamte Spektrum der Cybersicherheit erforderlich.

Vor dem Hintergrund geringer Ressourcen für IT- und Cybersicherheit ist die Risikoanalyse ein wichtiges Instrument, um erforderliche Maßnahmen abzuleiten und Investitionen zu legitimieren (Davey, 1995). Beispielsweise entwickeln Kamoun & Nicho (2014) ein Modell, um die technischen, organisatorischen und menschlichen Faktoren von Cyberver-

stößen im Gesundheitssystem zu beleuchten. Blanke & McGrady (2016) schlagen eine Checkliste vor, die Gesundheitsorganisationen zur Bewertung bestehender Praktiken und zur Ermittlung verbesserungsbedürftiger Sicherheitslücken verwenden können. Die qualitative Studie von Fernando & Dawson (2009) zeigt übergreifende Schwachstellen von Gesundheitseinrichtungen auf, wie zum Beispiel unzureichende Schulungen der Mitarbeiter, komplexe rechtliche Rahmenbedingungen und organisatorische Einschränkungen von Krankenhäusern.

Weitere Studien fokussieren sich auf technische Maßnahmen zur Verbesserung der Cybersicherheit. Beispielsweise nennen Argaw et al. (2020) neben einer hochwertigen IT und regelmäßiger Schulungen das Incidence Response Planning und Vulnerability Scanning als wichtiges proaktives Vorgehen. Zudem muss der Faktor Mensch und das menschliche (Fehl-)Verhalten bei der Bewertung der Cybersicherheit in Krankenhäusern berücksichtigt werden (Pfleeger & Caputo, 2012). Weitere Handlungsmaßnahmen erkennen Williams & Woodward (2015) in der Governance, der konsolidierten Berichterstattung sowie in der Standardisierung von Vorschriften und Normen zur proaktiven Bewältigung komplexer Cybersicherheitsvorfälle. Zudem ist der Austausch von Erfahrungen mit anderen Häusern ein wertvolles Instrument, um eigene Praktiken zu überdenken und (neu) zu bewerten (He & Johnson, 2015; Williams & Woodward, 2015). Standardisierte Sicherheitsdokumente können helfen, um die aus Sicherheitsvorfällen gewonnenen Erkenntnisse an Dritte weiterzugeben (He & Johnson, 2015). Eine besondere Herausforderung stellen die Medizinprodukte dar (Fu & Blum, 2013; Coronado & Wong, 2014), wobei der Aspekt der Sicherheit bereits in der Beschaffungsphase umfassend zu berücksichtigen ist (Coronado & Wong, 2014). Dabei kann ein einheitlicher Fragenkatalog in der Bewertung und Auswahl geeigneter Medizinprodukte helfen (Fu & Blum, 2013).

Weitere wissenschaftliche Beiträge befassen sich mit dem sicheren Austausch und der Verwendung von Patientendaten (Huang et al., 2009; Neubauer & Heurix, 2011; Almulhem, 2012; Shoffner et al., 2013), Ende-zu-Ende-verschlüsselten und mobilen Gesundheitsnetzwerken (Wozak et al., 2007; Iwaya et al., 2019; Moshi et al., 2019) sowie sicherem Cloud-Computing im Gesundheitswesen (Haufe et al., 2014). Ferner können moderne biologische Institute und Prozesse von Cyberangriffen betroffen sein (Moritz et al., 2020). Beispielsweise zeigen Fayans et al. (2020) wie das Next Generation Sequencing (NGS) in der Mikrobiologie von möglichen kriminellen Cyberakteuren angegriffen und manipuliert werden können.

Zusammenfassend zeigt Abbildung 1 die in der Literatur identifizierten Herausforderungen des Gesundheitswesens. Allerdings findet sich in der Literatur bislang keine ganzheitliche Untersuchung der dargestellten Themenfelder Cyberrisikomanagement, Verständnis von Cyberrisiken und daraus resultierenden Herausforderungen im Gesundheitswesen, die die zwischen diesen Bereichen bestehenden inhaltlichen Zusammenhänge umfassend analysiert. Diese Einschätzung bestätigen die Beiträge von Kim et al. (2018) und Sardi et al. (2020). Zwar gibt es erste Forschungsbeiträge über Cybersicherheitsmaßnahmen im Gesundheitswesen, jedoch besteht die Notwendigkeit, das Cyberrisiko im Krankenhausumfeld empirisch zu untersuchen, um den Gesundheitseinrichtungen praktische Lösungen zu offerieren (Sardi et al., 2020).

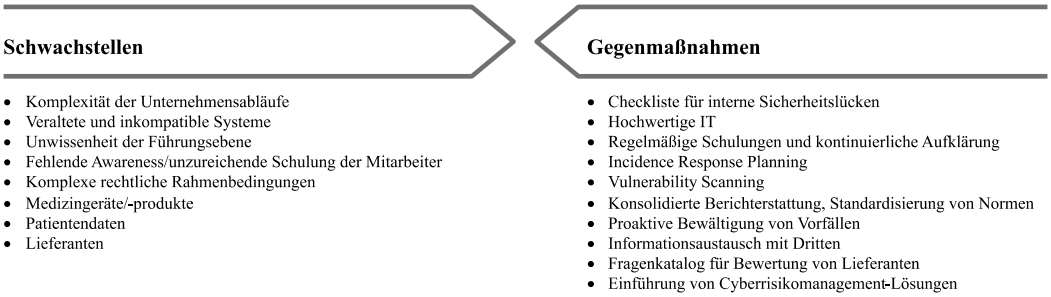



*Abbildung 1:* In der Literatur identifizierte Herausforderungen des Gesundheitswesens

## 3 Methodologie

Das Ziel dieses Beitrages besteht darin, Experten aus dem Krankenhausumfeld zu ihren Einschätzungen bezüglich des Managements von Cyberrisiken und der Herausforderungen und Implikationen zur Sicherstellung der Cybersicherheit zu befragen. Um komplexe Sachverhalte zu verstehen, haben sich Expertenbefragungen in der qualitativen Sozialforschung etabliert (Kruse, 2015). Der Begriff Experte beschreibt dabei „die spezifische Rolle des Interviewpartners als Quelle von Spezialwissen über die zu erforschenden sozialen Sachverhalte. Experteninterviews sind eine Methode dieses Wissen zu erschließen“ (Gläser & Laudel, 2012). Vor diesem Hintergrund werden mithilfe einer systematischen Auswertung des erhobenen Handlungs- und Erfahrungswissens der Befragten neue Erkenntnisse generiert sowie neue Theorien und Hypothesen abgeleitet (Diekmann, 2007; Finfgeld-Connett, 2014; Schnell et al., 2018; Wrede et al., 2018). Einen Überblick über das Forschungsdesign ist in Abbildung 2 dargestellt.

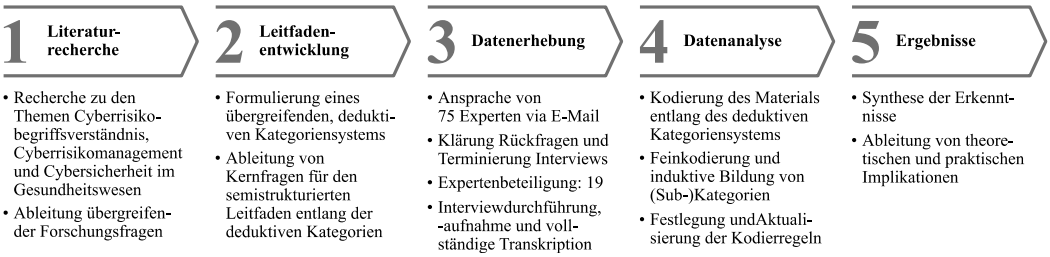



*Abbildung 2:* Methodologisches Vorgehen und Forschungsdesign

Aus der Literaturrecherche (Schritt 1 in Abbildung 2) wird ein deduktives Kategoriensystem abgeleitet, das die Grundlage der Untersuchung bildet (Cepeda & Martin, 2005; Yin, 2018; Wrede et al., 2018). Entlang dieser deduktiven Kategorien werden anschließend die Kernfragen für den Interviewleitfaden abgeleitet und formuliert (Schritt 2). Als Befragungsform wird die mündliche Befragung mittels teilstandardisierter Interviews gewählt (Kaiser, 2014). Da Interviews mit Experten aufgrund schneller und präziser Antworten als besonders herausfordernd gelten (Liebold & Trinczek, 2009), wurde bei der Gestaltung des semi-strukturierten Interviewleitfadens auf drei Aspekte geachtet (Baur & Blasius, 2014): plötzliche Themenwechsel zu vermeiden, um einen Erzählfluss herzustellen, dem Befragten durch eine klare Struktur und eine begrenzte Anzahl von Fragen genügend

Zeit zum Sprechen zu geben und den Befragten zum freien Erzählen zu ermutigen. Der semistrukturierte Leitfaden, der in Abbildung 3 dargestellt ist, ist in vier Kategorien unterteilt. Der erste Fragenblock beschäftigt sich mit dem Begriffsverständnis der Experten, um ein gemeinsames Verständnis über den Untersuchungsgegenstand herzustellen. Die zweite Kategorie umfasst allgemeine Fragen zum Unternehmen und der befragten Person sowie zum organisatorischen Aufbau. Im dritten Fragenblock wird das Management von Cyberrisiken des Unternehmens diskutiert. Konkret werden Maßnahmen zur Prävention, Mitigation, Reaktion sowie zum Transfer von Cyberrisiken herausgearbeitet. Die letzte Kategorie fokussiert aktuelle Herausforderungen und relevante Trends, die das Themengebiet der Cybersicherheit im Gesundheitswesen beeinflussen.

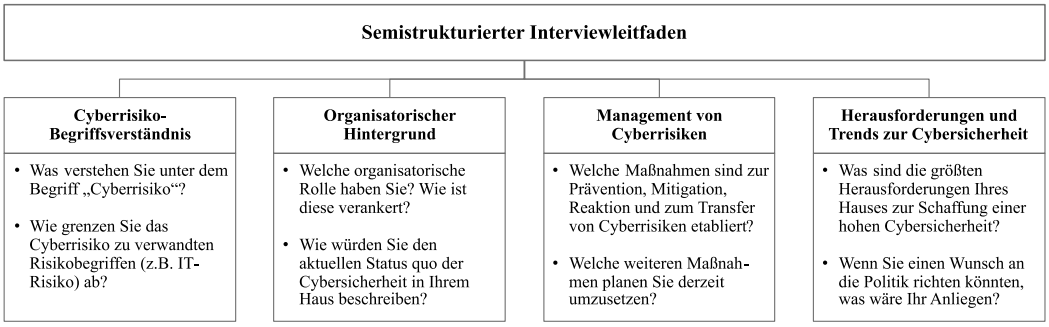



*Abbildung 3:* Deduktives Kategoriensystem und ausgewählte Fragen des semistrukturierten Leitfadens

Im Hinblick auf die Datenerhebung und Auswahl der Experten (Schritt 3) werden alle deutsch- oder englischsprachigen Mitarbeiter von deutschen Krankenhäusern, die einen technischen oder medizinischen Hintergrund haben und in ihrer aktuellen Rolle für die Cybersicherheit der Organisation zuständig sind, als relevante Experten verstanden. Ferner werden IT- und Cybersicherheitsexperten, vorwiegend aus dem Gesundheitswesen, ergänzend berücksichtigt. Basierend auf einer umfassenden Internetrecherche wurden die 75 größten privaten, öffentlichen und frei gemeinnützigen Krankenhäuser sowie Universitätskliniken in Deutschland identifiziert. Sofern aus dem Internetauftritt erkennbar, wurden die Cybersicherheitsverantwortlichen respektive die Geschäftsführung per E-Mail mit einer kurzen Beschreibung des Forschungsprojekts sowie dessen Zielsetzung kontaktiert. Zudem wurden ausgewählte Experten vorab telefonisch kontaktiert, um den Mehrwert der Studie darzulegen, etwaige Rückfragen zu besprechen sowie das Interview zu terminieren. Auf die Durchführung eines Pretests wurde verzichtet, da der Interviewleitfaden im Laufe der Interviewserie weiter angepasst sowie ergänzt werden konnte (Gläser & Laudel, 2012). Vor Durchführung der Interviews wurde der Fragenkatalog für die Vorbereitung und frühzeitige Klärung offener Fragen den Experten zur Verfügung gestellt. Im Zeitraum von September 2021 bis Januar 2022 fanden insgesamt 19 Interviews statt und wurden per Videokonferenzsoftware (18/19) beziehungsweise per Telefon (1/19) in deutscher Sprache und zur Wahrung der Vertraulichkeit der erhobenen Informationen als Einzelbefragung durchgeführt (Lamnek & Krell, 2016). Nach Einholen des Einverständnisses der Befragten wurden alle Interviews aufgezeichnet sowie anschließend transkribiert und anonymisiert (Meuser & Nagel, 2009; Kuckartz & Rädiker, 2022). Nach der Transkription aller

Interviews fand eine abschließende inhaltliche Überprüfung der Transkripte auf Vollständigkeit und Korrektheit statt (McLellan et al. 2003; Kuckartz & Rädiker, 2022). Die durchschnittliche Interviewdauer betrug 66 Minuten, wobei das kürzeste Interview 49 Minuten und das längste Interview 103 Minuten dauerte. Insgesamt wurden mehr als 20 Stunden Datenmaterial gesammelt. Tabelle 1 zeigt einen Überblick der befragten Experten in anonymisierter Form.

Zu Beginn eines Interviews wurde das Forschungsprojekt und dessen Zielsetzung vorgestellt. In den Gesprächen wurde das „Mirroring"-Konzept (deutsch: „Spiegeln") angewendet (Myers & Newman, 2007). Das bedeutet, dass die von der befragten Person verwendeten Phrasen und Wörter anschließend von dem Interviewer verwendet werden, um nachfolgende Fragen oder Kommentare zu formulieren. Vor dem Gesprächsabschluss konnten verbleibende Fragen seitens des Befragten gestellt werden. Abschließend wurde den Interviewpartnern für die bereitgestellten Erkenntnisse gedankt (Myers, 2020; Witte et al., 2020). Die Datenanalyse (Schritt 4) erfolgte gemäß dem Ablaufmodell der inhaltlich strukturierenden qualitativen Inhaltsanalyse nach Kuckartz & Rädiker (2022) und wurde mithilfe der Standardsoftware zur computergestützten qualitativen Datenanalyse MAXQDA durchgeführt (Kuckartz & Rädiker, 2020). Ziel der Textauswertung ist die Generierung neuer Erkenntnisse durch systematische Auswertung der erhobenen Daten (Schnell et al., 2018) und die Ableitung erkennbarer Strukturen im Textmaterial (Kuckartz & Rädiker, 2022). Im ersten Analyseschritt wurde das Textmaterial entlang des deduktives Kategoriensystem kodiert. Zur eindeutigen Zuordnung des Materials wurden Kodierregeln mit Ankerbeispielen konstruiert. Diese Kodierregeln wurden von beiden Autoren unabhängig voneinander getestet und im Laufe der qualitativen Auswertung verfeinert bzw. angepasst. Darauffolgend wurde das gesamte Textmaterial erneut kodiert und das Kategoriensystem um induktive (Sub-)Kategorien erweitert. Das deduktive Kategoriensystem wurde also durch induktiv gebildete Subkategorien ergänzt und weiterentwickelt. Abschließend wurde das analysierte Datenmaterial auf korrekte Zuordnung zum deduktiv-induktiv gebildeten Kategoriensystem durch beide Autoren überprüft und etwaige Unklarheiten gemeinsam abgestimmt.

| Experte | Branche | Trägerschaft/ Detailbranche | Position |
|---|---|---|---|
| A | Krankenhaus | Frei-gemeinnützig | Leitung IT |
| B | Krankenhaus | Frei-gemeinnützig | Leitung IT |
| C | Krankenhaus | Frei-gemeinnützig | Leitung IT |
| D | Krankenhaus | Öffentlich | Chief Digital Officer (CDO) |
| E | Krankenhaus | Öffentlich | Chief Medical Information Officer (CMIO) |
| F | Krankenhaus | Öffentlich | Chief Information Security Officer (CISO) |
| G | Krankenhaus | Öffentlich | Chief Information Security Officer (CISO) |
| H | Krankenhaus | Öffentlich | Chief Information Security Officer (CISO) |
| I | Krankenhaus | Öffentlich | Chief Information Security Officer (CISO) |
| J | Krankenhaus | Öffentlich | Chief Information Security Officer (CISO) |
| K | Krankenhaus | Öffentlich | Manager IT-Sicherheit |

| Experte | Branche | Trägerschaft/ Detailbranche | Position |
|---|---|---|---|
| L | Krankenhaus | Privat | Chief Information Officer (CIO) |
| M | Krankenhaus | Privat | Chief Information Security Officer (CISO) |
| N | Krankenhaus | Privat | Leitung IT |
| O | Krankenhaus | Privat | Leitung IT |
| P | Sonstige | Beratungsunternehmen | Experte Cybersicherheit |
| Q | Sonstige | Krankenhausgesellschaft | Leitung IT |
| R | Sonstige | Kriminalpolizei | Kriminalhauptkommissar Cybercrime |
| S | Sonstige | Medizinische Informationssysteme | Geschäftsführer (CEO) |

*Tabelle 1:* Teilnehmer der Expertenbefragung

## 4 Ergebnisse

Nachfolgend werden die Ergebnisse der qualitativen Expertenbefragung wiedergegeben. Dabei orientiert sich die Strukturierung der Erkenntnisse am deduktiven Kategoriensystem.[3]

### 4.1 Begriffsverständnis

Die Gespräche haben gezeigt, dass sich in der Praxis weder eine umfassende Definition des Terminus Cyberrisiko noch ein einheitliches Begriffsverständnis herausgebildet hat.

> *Es ist in aller Munde, jeder spricht irgendwie darüber und keiner weiß so wirklich, was dahintersteckt. (Experte G)*

Die Experten sind sich einig, dass Cyberrisiken eine Vielzahl an potenziellen Gefahren subsumieren, die im weitesten Sinne aus der Verwendung von IT, Technik beziehungsweise digitalisierten Systemen einhergehen.

> *Das ist halt ein riesiger Blumenstrauß, Cyberrisiken. (Experte C)*

Jedoch zeigt sich, dass jeder Gesprächspartner etwas anderes unter dem Begriff Cyberrisiko versteht. Während einige Experten unter dem Begriff Cyberrisiko den Fokus auf kriminelle Angriffe, wie zum Beispiel Trojaner, Ransomware und Distributed Denial of Service (DDoS)-Attacken legen, verstehen andere das Cyberrisiko als Abfluss von Daten und Informationen. Ein weiterer Experte sagt, „dass [das] Cyberrisiko gleich dem IT-Risiko ist“, ein anderer Experte wiederum definiert Cyberrisiko gleich dem Informationssicherheitsrisiko. Ferner legen andere Experten den Fokus auf die Cybersicherheit, also die Begrenzung und Prävention von Cyberrisiken. Nur einzelne Gesprächspartner erkennen einen Unterschied zwischen dem Cyberrisiko, IT-Risiko und Informationssicherheitsrisiko:

3 Wird in den folgenden Abschnitten von „einigen“ Experten gesprochen, so sind weniger als fünf Experten gemeint, während unter „vielen“ Experten fünf oder mehr Experten verstanden.

*Informationssicherheit ist […] das globale Thema, […] was den Schutz im Sinne der Vertraulichkeit, Verfügbarkeit und Integrität, auch Authentizität von Daten oder Informationen zum Ziel hat. Die IT-Sicherheit ist für mich die Operationalisierung, also die technische Umsetzung zum Schutz der Informationssicherheitsziele. (Experte G)*

Über die vergangenen Jahre waren einige der befragten Häuser bereits mit einem Cybervorfall konfrontiert.

*Es gibt [...] nur zwei Kategorien von Unternehmen: die einen haben es schon hinter sich und die anderen haben es noch vor sich und versuchen den Termin, wo es passiert, möglichst lange hinauszuschieben. (Experte L)*

Neben täglichen Angriffen wie zum Beispiel Phishing-Mails und technischer Scans, gab es ebenso DDoS- sowie vereinzelt Ransomware-Angriffe. Größere Schäden, insbesondere der Ausfall des operativen Betriebs oder der Verlust von Patientendaten, konnten bisher abgewendet werden. Die Experten sehen insbesondere den Faktor Mensch als Hauptschwachstelle.

*Die Schnittstelle für mich ist und bleibt der Mensch. Das ist für mich der Dreh- und Angelpunkt. (Experte R)*

Weitere Einfallstore ergaben sich durch interne Sicherheitslücken (z.B. unverschlüsselte Drucker) und die Anbindung von Dritten. Letztere offenbart eine hohe Exponierung gegenüber Supply-Chain Attacken, beispielsweise auf medizinische Software-Angebote und Büroanwendungen (z.B. Microsoft Office). Ferner ermöglicht die Nutzung privater Webanwendungen (z.B. Whatsapp, Dropbox, Mailprogramme) den Einfall von Schadsoftware. Größere Schäden durch Cyberangriffe konnten vermieden werden. Lediglich ein befragtes Krankenhaus stand aufgrund eines Virus-Angriffes vor der Totalabschottung, was letztlich verhindert werden konnte. Darüber hinaus besteht unter den Befragten Konsens darüber, dass von Cyberrisiken weitreichende Gefahrenpotenziale ausgehen. Insbesondere der Ausfall des klinischen Systems aufgrund von Ransomware, Supply-Chain Attacken, Cyberkrieg oder Cyberspionage nennen die Interviewteilnehmer als besonders relevante Angriffsformen. Zudem referenzieren einige Experten auf bekannte Cybervorfälle, wie zum Beispiel am Universitätsklinikum Düsseldorf oder am Lukaskrankenhaus Neuss, die als Worst-Case Szenario angesehen werden. Nach Einschätzung der Experten handelte es sich in der Vergangenheit meist um flächendeckende (Massen-)Angriffe über alle Branchen hinweg, weshalb es relativ wenige gezielte Angriffe auf das Gesundheitswesen gab. Zudem besteht nach Auffassung einiger Experten eine Hemmschwelle bei Cyberkriminellen, Krankenhäuser anzugreifen und Patienten zu gefährden. Als weiteren Grund sehen die Mehrheit der Befragten andere Wirtschaftsbereiche, insbesondere der freien Wirtschaft, aufgrund größerer finanzieller Mittel als attraktiveres Angriffsziel.

*Cyberkriminelle haben nur eine Sache vor Augen [...], die wollen eigentlich nur Geld. (Experte O)*

### 4.2 Organisatorischer Hintergrund

Die befragten Krankenhäuser unterscheiden sich in der organisatorischen Verankerung der IT-Abteilung. Während die kleineren Häuser meist eine zentrale IT-Abteilung besitzen, hat sich bei den größeren Häusern die Ausgliederung der IT in eine Dienstleistungs-GmbH

etabliert, wobei das Personal teils zentral, teils dezentral über die Standorte verteilt ist. Nur wenige Häuser – meist aufgrund der komplexen Organisationsstruktur – besitzen eine dedizierte Abteilung oder Stabsstelle für Informations- beziehungsweise Cybersicherheit. Alle befragten Häuser haben zwar einen Chief Information Security Officer (CISO) (deutsch: Informationssicherheitsbeauftragter; ISB), jedoch wird dessen Rolle sehr unterschiedlich gelebt. Positiv zu erwähnen ist zum Beispiel Experte I, der nebst zentraler Stabsstelle dezentrale Informationssicherheitskoordinatoren über die gesamte Organisation hinweg installierte. Laut Experten kann die zentrale Einheit organisatorisch und konzeptionellen Fragestellungen nachgehen, während die dezentralen Koordinatoren sich um die Umsetzung und bereichspezifischen Fragen kümmern.

Die Gesprächspartner empfinden das Verständnis des Managements für das Thema Cybersicherheit als sehr unterschiedlich. Während einige den hohen Stellenwert der Cybersicherheit im Vorstand betonen, bemängeln andere Experten die Auffassung des Vorstandes für IT- und Cybersicherheitsthemen.

> *Die meisten Geschäftsführer haben überhaupt keine Awareness auf Digitalisierung, geschweige denn auf Cyber-Security. Es ist jetzt ein bisschen anders geworden, weil sie jetzt Fördergelder kriegen, aber wenn sie einen fragen, was der dann unter Informationssicherheit versteht, dann würde der sagen, ja dann machen wir eine Firewall davor. (Experte S)*

Ein Grund für dieses Phänomen könnte in der unterschiedlichen Auslebung der CISO-Rolle liegen. Je öfter und regelmäßiger über die aktuelle Sicherheitslage an den Vorstand berichtet wird, desto höher scheint die Sensibilisierung des Topmanagements zu sein. Zudem haftet das Management für etwaige Schäden durch Cybervorfälle und ist für die finanzielle Ausstattung der IT- und Informationssicherheit verantwortlich. Bezüglich der internen Finanzierungsmöglichkeiten liegen die Ausgaben für die IT bei den Befragten im Durchschnitt zwischen 1 % und 2 % des Umsatzes. Nur wenige Häuser investieren mehr als 2 %. Insgesamt entfallen circa 10–20 % des IT-Budgets auf die IT-Sicherheit. Aufgrund der weiter voranschreitenden Digitalisierung und der damit erwarteten Erhöhung der IT-Ausgaben fordern einige Experten die Verdoppelung beziehungsweise Verdreifachung des IT-Budgets.

> *Wir gehen heute davon aus, dass wir für den normalen, sicheren Betrieb 4–6 % des Jahresumsatzes benötigen. (Experte N)*

Als größte Kostentreiber werden übereinstimmend das Personal sowie die technische Umsetzung gesetzlicher Auflagen genannt. Aufgrund der jahrelangen Unterfinanzierung des Krankenhaussektors müssen viele Häuser nicht nur eine Vielzahl an Sicherheitsmaßnahmen zeitnah umsetzen, sondern auch zusätzliches Fachpersonal, zum Beispiel Cybersicherheitsexperten, einstellen. Die in der Breite bekannte Annahme, dass sich die Kosten von IT-Projekten durch spätere Einsparungen amortisieren, trifft bei Investitionen in die Cybersicherheit laut Experten – unabhängig der Unternehmensgröße und Trägerschaft – grundsätzlich nicht zu.

In Zusammenfassung lässt sich festhalten, dass einerseits die organisatorischen Gegebenheiten nicht unterschiedlicher sein könnten, andererseits die finanzielle Ausstattung gemessen am Umsatzvolumen in allen Häusern noch relativ gering ausfällt.

### 4.3 Cyberrisikomanagement

Bezüglich des Managements von Cyberrisiken folgen die befragten Experten dem klassischen Risikomanagement-Ansatz:

*Risiken identifizieren, bewerten [und] Gegenmaßnahmen einleiten. (Experte G)*

Insbesondere die Identifikation von Schwachstellen, im Sinne von Sicherheitslücken und neuen Angriffsvektoren, wird von den meisten Experten genannt. Dabei werden Sicherheitsrisiken priorisiert geschlossen, teilweise in Zusammenarbeit mit externen Sicherheitsfirmen. Jedoch zeigen sich in den Interviews Unterschiede in der konkreten Ausgestaltung des Cyberrisikomanagements. Nur die Hälfte der befragten Häuser besitzt ein (teil-)etabliertes (Cyber-)Risikomanagement innerhalb der Organisation. Zwar besitzt der Großteil der Häuser ein medizinisches, betriebswirtschaftliches und IT-Risikomanagement, jedoch in vielen Fällen ohne einheitliche Standards und Vorgaben. Diese strikte Trennung stellt die Experten insbesondere in der Verschmelzung von Medizintechnik und IT vor neue Herausforderungen. Zudem werden Cyberrisiken in den aktuellen Risikobewertungen nur bedingt berücksichtigt und das Informationssicherheitsmanagement (ISM) ist organisatorisch in unterschiedlichen Bereichen, wie zum Beispiel in der IT, dem Qualitätsmanagement, der Compliance- oder Controlling-Abteilung, verankert. Zudem sind die bestehenden Risikomanagementaktivitäten operativ getrieben und es fehlt den meisten Krankenhäusern an einer unternehmensweiten Risikomanagement-Strategie.

Eine Möglichkeit des Risikotransfers bieten Cyberversicherungen. Lediglich fünf der befragten Häuser haben angegeben, eine Cyberversicherung zu besitzen. Die Versicherungslimits bewegen sich, abhängig der Unternehmensgröße, im niedrigen bis mittleren zweistelligen Millionenbereich. Die befragten Experten sind sich einig, dass sich die Bedingungen am Cyberversicherungsmarkt in den vergangenen Jahren stark verändert haben. Konkret nennen die Experten neben geringeren Versicherungslimits, gestiegene Prämien und erhöhte Anforderungen seitens der Versicherungen. Einige Experten bestätigen, dass sich die Versicherer in der initialen Risikoprüfung an Standards wie zum Beispiel ISO 27001 orientieren. Aufgrund dieser Entwicklungen hinterfragen viele Experten die zukünftige Wirtschaftlichkeit einer Cyberpolice, sowohl in der Prolongation als auch im Neuabschluss.

*Das Cyberrisiko wird immer unversicherbarer. [...] Deswegen weiß [ich] noch nicht, ob wir nächstes Jahr überhaupt noch eine Cyberversicherung haben können. (Experte L)*

Im Mittelpunkt des Umgangs mit Cyberrisiken steht bei allen befragten Experten die Prävention von möglichen Cybervorfällen, welche in drei Gruppen gegliedert werden können: 1) Organisatorisch konzeptionell, 2) Technisch sowie 3) Awareness und Sensibilisierung. Übergreifende konzeptionelle Maßnahmen umfassen beispielsweise die Konsolidierung und Reduktion der Anwendungslandschaften sowie die Harmonisierung der Unternehmensprozesse. Ziel dabei ist die Reduktion der Komplexität und die Schaffung einheitlicher Strukturen. Ferner haben einige Häuser ein umfassendes Sicherheitskonzept und diversifizieren ihre kritische Infrastruktur zur Prävention möglicher Kumulrisiken. Das von einigen Experten genannte Sicherheitskonzept beinhaltet beispielsweise das Abschalten externer Datenträger (USB-Sticks), einheitliche Regelungen zur Passwortvergabe (Länge und Gültigkeit), ein Berechtigungsmanagement, Zwei-Faktor-Authentifizierung sowie die Deaktivierung von externen Makros und Mail-Anhängen.

Bezüglich der technischen Prävention zeigt Abbildung 4 die von den Experten genannten Vorhaben. Besonders häufig wird die Modernisierung der Firewall sowie die Themen Netzwerksegmentierung und Patch-Management erwähnt. Eine weitere Komponente bildet das Intrusion Detection System (IDS) und Information Security Management System (ISMS), die seit 1. Januar 2022 für alle KRITIS-Häuser gemäß IT-Sicherheitsgesetz 2.0 respektive für alle Krankenhäuser gemäß § 75c SGB V verpflichtend ist. Ferner befinden sich einige Häuser zum Zeitpunkt der Gespräche im Aufbau eines Security Operation Center (SOC) oder eines SIEM. Außerdem setzt die Mehrheit der befragten Experten auf die präventive Simulation von Vorfällen, beispielsweise durch sogenannte Pen-Tests, Vulnerability-Scans sowie durch interne Phishing- und Spam-Kampagnen. Während einige Experten stolz über Ihre Risikomaßnahmen berichten, sehen andere besonders die Kritikfähigkeit und das Anpassungsvermögen des eigenen Sicherheitskonzeptes oftmals als besondere Herausforderung. Trotz der Fülle an (präventiven) Maßnahmen sind sich die Experten einig, dass ein Cybervorfall dennoch nicht ausgeschlossen werden kann.

> *Irgendwann mal trifft es einen vielleicht und dann muss ich hinter dem Wall was haben. (Experte R)*

Daher sehen die Experten die Mitarbeitersensibilisierung als weiteren wichtigen Baustein in der Prävention von Vorfällen.

> *Genauso wichtig ist tatsächlich die Mitarbeitersensibilisierung. (Experte M)*

Aufgrund der ambivalenten Hintergründe der Mitarbeiter und des teils fehlenden Verständnisses für Cybersicherheitsmaßnahmen stellt sich die Sensibilisierung als „kraftraubend und aufwändig" (Experte B) heraus.

> *Wir haben einen sehr breiten Querschnitt der Bevölkerung, der bei uns als Mitarbeiter an Bord ist, [...] Trotzdem werden alle mit digitalen Systemen arbeiten müssen und auch mit Systemen, die komplexer als ein Handy sind. (Experte A)*


*Abbildung 4:* Wortwolke der präventiv technischen Maßnahmen der befragten Experten

Daher setzen einige Häuser auf eine regelmäßige Kommunikation von aktuellen Sicherheitsmaßnahmen und Cybervorfällen.

*Wir sehen sehr viel Bedarf an Hilfestellungen und Schulungen [...]. Das ist eine sehr kraftraubende Aktion auf Dauer, weil [...| man immer wieder nachfassen muss, [um] das immer wieder ins Bewusstsein [zu] rufen. (Experte B)*

Weitere Praktiken umfassen den Versand von falschen Spam- und Phishing-Mails an die Belegschaft, um auf typische Einfallstore und Schwachstellen aufmerksam zu machen. Ungeachtet der von den Experten genannten Bedeutung von Sensibilisierungsmaßnahmen, besitzen die wenigsten Häuser ein umfassendes Schulungskonzept. Bei einigen befindet sich dieses jedoch im Auf- und Ausbau. Dabei setzen die Experten auf einzelne IT- und Sicherheitsschulungen bis hin zu mehrdimensionalen Schulungskonzepten.

*Es gibt [...] verschiedene Ebenen von Schulungen: Erstschulungen, Nachschulungen, Präsenzschulungen und Sonderschulungen, E-Mail und Newsletter sowie das E-Learning. (Experte I)*

So es zu einem Vorfall kommt, setzen die befragten Häuser mehrheitlich auf das sogenannte Business Continuity Management (BCM). Viele Häuser besitzen ein Ausfallkonzept oder Notfallpläne, jedoch nur die wenigsten für das Szenario Cyberrisiko.

*Und aufgrund aktueller Ereignisse [...] wäre es mir persönlich jetzt ein Anliegen [...] das Szenario Ransomware bei uns [...] in die Ablaufpläne aufzunehmen. (Experte H)*

Andere Häuser haben bereits umfassendere Notfallpläne.

*Daraufhin gibt es dann Disaster Recovery Pläne, die gebaut werden, Notfallpläne. Jede Klinik hat auch nochmal eigene Notfallpläne. Es gibt einen Gesamtnotfallplan. (Experte I)*

Andererseits besitzen nur die wenigsten Häuser eine Rufbereitschaft oder greifen auf (forensische) 24/7-Unterstützung zurück. Noch seltener gibt es in den befragten Krankenhäusern einen Katastrophenschutzbeauftragten oder Krisenstäbe, die bestimmte Szenarien, zum Beispiel Ransomware, in regelmäßigen Abständen vorbereiten. Basierend auf den Erläuterungen der Experten scheinen die befragten Häuser ihren Fokus auf die Prävention zulegen, was in der Zukunft zu Problemen führen könnte:

*So erfolgreich wie die Hacker sind, muss man davon ausgehen, dass ganz egal wie gut man sich schützt, man zu 50 % Prävention und 50 % Notfallmanagement organisiert sein muss. Und so sind schon diese Normen gar nicht aufgebaut und das ist schon der große Fehler. (Experte P)*

Es gibt eine Vielzahl an Normen im Krankenhausumfeld, wobei sich hinsichtlich der Cybersicherheit zwei etabliert haben: Branchenspezifischer Sicherheitsstandard (B3S) und ISO 27001. Circa die Hälfte der Häuser haben nach Aussage der Experten eine ISO 27001-Zertifizierung, der Rest folgt Vorgaben und Leitlinien des B3S oder IT-Grundschutzes (BSI). Als Vorteile des B3S nennen die Experten die Praktikabilität und pragmatische Forderung gewisser Sicherheitsstandards und -tools, wie zum Beispiel eines ISMS, des Notfallmanagements oder eines Druckkonzepts. Andererseits bietet die ISO 27001 einen branchenübergreifenden Standard mit internationaler Bekanntheit und größerem Handlungsspielraum für die einzelnen Häuser. Unabhängig davon, welcher Standard verfolgt wird, geben die Experten übereinstimmend an, dass die Einführung dieser Standards bei der Sensibilisierung der Mitarbeiter und des Vorstandes geholfen hat, jedoch die Zertifizierung

keinen wirtschaftlichen Mehrwert oder Wettbewerbsvorteil bietet. Zudem bemängeln die Experten, dass die Zertifizierungen einen hohen initialen und kontinuierlichen Dokumentationsaufwand erzeugen, welcher im Tagesgeschäft nicht immer gedeckt werden kann. Weiter argumentieren die Experten, dass die Zertifizierungen lediglich die Angemessenheit, jedoch nicht die Wirksamkeit beziehungsweise risikoadäquate Ausgestaltung der internen Betriebssicherheit prüfen.

> *Der Gesetzgeber überprüft standardgemäß die Dokumentation, dementsprechend dokumentieren alle auch nur. Erst wenn wir anfangen im KRITIS-Umfeld wie generell bei der DSGVO das Thema risikoadäquat in den Fokus zu nehmen, wird es dazu kommen, dass die Unternehmen wirklich anfangen, auch risikoadäquat abzusichern, weil die Gelder sind ja nicht in die Absicherung der Risiken geflossen, sondern in die Dokumentation. Und sowohl bei den ISMS-Lösungen als auch beim Datenschutz. (Experte P)*

Daher stehen einige Experten Zertifizierungen kritisch gegenüber.

> *Wenn ich morgen gehackt werde und unsere Kliniken stehen für ein paar Tage oder Wochen still, dann bin ich mit oder ohne Zertifizierung mein Job los, um es mal nüchtern zu sagen. (Experte L)*

Zusammenfassend stellt Tabelle 2 die in den Gesprächen identifizierten Good Practices der befragen Häuser entlang der organisatorischen, technischen und menschlichen Dimension dar.

| Dimension | Good Practices |
|---|---|
| Organisatorisch/ Konzeptionell | ▪ Trennung der Abteilungen IT- und Cybersicherheit<br>▪ Zentrale Stabsstelle oder Einheit für Cyber- und Informationssicherheit<br>▪ Etablierung von dezentralen Informationssicherheitskoordinatoren<br>▪ Direkter Berichtsweg des CISO/Leiter Cyber- und Informationssicherheit an Vorstand/CEO<br>▪ Jährliches Budget von mehr als 5 % des Jahresumsatzes<br>▪ Konsolidierung und Reduktion der Anwendungslandschaft<br>▪ Harmonisierung von Unternehmensprozessen<br>▪ Cyberstrategie<br>▪ Sicherheitskonzepte und Dokumentation<br>▪ Cyberrisikomanagementsystem<br>▪ Zertifizierungen (z.B. ISO 27001)<br>▪ Cyberversicherung<br>▪ Diversifikation der kritischen Infrastruktur<br>▪ Katastrophenschutzplan (inkl. Szenario „Cyberangriff“)<br>▪ Notfallpläne/Disaster Recovery Management<br>▪ Informationssicherheitsmanagementsystem (ISMS)<br>▪ Rufbereitschaft<br>▪ 24/7-forensicher Notruf |

| Dimension | Good Practices |
|---|---|
| Technisch | ▪ Vulnerability Management<br>▪ Netzwerksegementierung<br>▪ Patch-Management<br>▪ Firewall/Virenscanner<br>▪ Sandboxing<br>▪ Druckkonzept<br>▪ Intrusion Detection<br>▪ Backup-Management<br>▪ Zugriffskonzept (NAC)<br>▪ Mail-Filter<br>▪ Data Loss Prevention<br>▪ Geoblocking<br>▪ Identity Life Cycle Management<br>▪ Pen-Testing<br>▪ Mobile Device Management<br>▪ Logging<br>▪ Kennzeichnung externer Mails<br>▪ Security Operation Center (SOC)<br>▪ Security Incidence and Event Management (SIEM)<br>▪ Videoüberwachung<br>▪ Virtualisierung |
| Mensch | ▪ Awareness bei Vorstand und Management (z.B. durch regelmäßiges Reporting)<br>▪ Mehrdimensionales Schulungsangebot an alle Mitarbeiter<br>▪ Spezialschulungen für IT- und Cyberexperten<br>▪ Regelmäßiger Versand von Phishing und Spam-Mail (Test)<br>▪ Kommunikation<br>▪ Einbindung externer Experten |

*Tabelle 2:* Übersicht der identifizierten Good Practices

### 4.4 Herausforderungen und Trends zur Cybersicherheit

Aufgrund der Vielzahl an genannten Herausforderungen im weiteren Umgang mit Cyberrisiken und zur strukturierten Vorstellung der Ergebnisse wurde auf Basis der induktiven Kategorienbildung (zweiter Kodierdurchlauf) das in Abbildung 5 dargestellte Kategorienmodell in Anlehnung an Gioia et al. (2013) entwickelt. Nachfolgend werden die gewonnenen Erkenntnisse entlang der sechs Kategorien zweiter Ordnung vorgestellt.

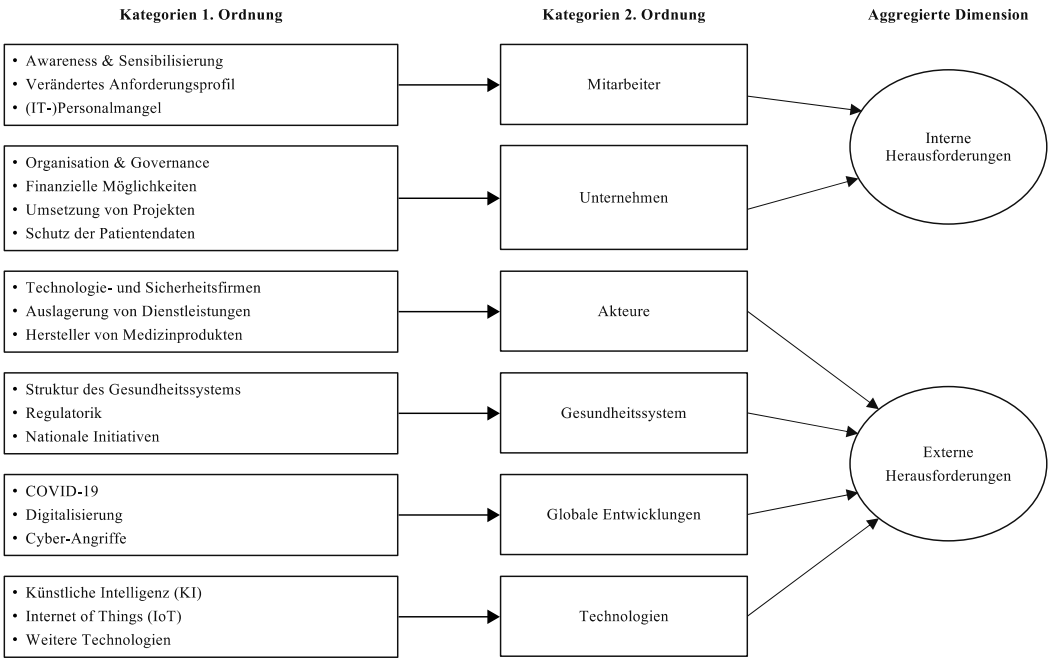



*Abbildung 5:* Kategorisierung der Trends und zukünftigen Herausforderungen

### 4.4.1 Mitarbeiter

Eine der größten Herausforderungen sehen die befragten Experten übereinstimmend in der kontinuierlichen Sensibilisierung von Mitarbeitern.

> *Ich glaube, zum einen die Awareness bei den Mitarbeitern zu haben, nicht auf bestimmte Links zu klicken oder irgendwelche Webseiten aufzurufen. Und gleichzeitig die Experten zu finden, die eben solche Systeme wie moderne Intrusion Detection Systeme dann steuern können. (Experte D)*

Um diese Durchdringung im Unternehmen zu erhalten, bedarf es einer umfassenden digitalen Kompetenz aller Mitarbeiter, insbesondere in IT-fernen Bereichen wie der Pflege oder Medizin. Zugleich ändert sich das Anforderungsprofil für eine sichere Arbeit im Krankenhaus, denn alle Mitarbeiter müssen mit IT arbeiten können. Dieser Wandel zeigt sich ebenso in den Anforderungen an das IT- und Cybersicherheitspersonal, da in Zukunft ein höheres Experten- und Spezialwissen erforderlich ist.

> *Da hat sich auch bei uns die Rolle der [...] IT mittlerweile stark geändert, vom klassischen Systemadministrator aus der Historie heraus zum Informationsmanager. (Experte S)*

Laut den Befragten verschärft diese Entwicklung den akuten Fachkräftemangel in der IT. Es finden sich kaum noch IT-Spezialisten.

> *Der IT-Markt ist in Ballungsräumen [...] vollständig leer. Die Gehälter für IT-Professionals sind enorm und ich sehe nicht, wann die Nachfrage mit Angebot wieder im Einklang sein wird, weil natürlich auch die Industrie die Leute abschöpft. (Experte A)*

Aufgrund der hohen Nachfrage an IT- und Cybersicherheitsexperten explodieren deren Gehaltsforderungen, die mit klassischen Krankenhaustarifstrukturen nicht realisiert werden können. Daher versuchen die befragten Häuser Fachkräfte mit anderen Besonderheiten, wie zum Beispiel das Arbeitsklima oder die Work-Life-Balance, für sich zu gewinnen.

*Die Leute, die bei uns arbeiten, die haben alle eine persönliche Motivation. (Experte R)*

Weiter erläutern die Experten, dass die Personalsituation in einigen Häusern aufgrund zusätzlicher Einsparungen und nicht genehmigter Planstellen zusätzlich belastet wurde.

*Es ist so, dass wir nicht mehr in der Lage sind, an jedem Haus einen Security-Spezialisten vorzuhalten. (Experte N)*

### 4.4.2 Unternehmen

Die Experten sehen die Resilienz ihres Hauses und der Organisation als eine der wichtigsten Eigenschaften und Erfolgsfaktoren der Cybersicherheit an. Jedoch berichten die Befragten übereinstimmend, dass die vorliegenden Organisationsstrukturen komplex sind und das Thema Cybersicherheit, bis auf wenige Ausnahmen, eine eher untergeordnete Rolle spielt. Vor diesem Hintergrund schlagen die Experten einerseits vor, eine unternehmensweite IT- und Cybersicherheitsstrategie zu entwickeln, andererseits eine klare organisatorische Abgrenzung der IT, der Informationssicherheit und der Medizintechnik zu schaffen.

*Es ist sehr viel komplizierter, vor allem weil Medizinprodukte kein IT-Thema sind, sondern Thema der Medizintechnik. Es gibt mittlerweile eine ganze Reihe von Kliniken, die das Thema IT und Medizintechnik zusammengeführt haben. [...] Medizintechnik ist heutzutage zu 85–90 % IT. (Experte A)*

Einige Gesprächspartner sehen zudem die kontinuierliche Standardisierung und Zentralisierung von Prozessen als wichtige organisatorische Aufgabe, um die Komplexität und somit die Fehleranfälligkeit für mögliche Einfallstore zu verringern. Vor allem kleinere Häuser können unter Umständen ihre IT-Infrastruktur nicht mehr kosteneffizient selbst gestalten. Hier schlagen die Experten vor, auf gemeinsame Dienste (Shared-Services) oder externe Dienstleister (Cybersecurity-as-a-Service) zuzugreifen.

*Jedes Krankenhaus will alles immer selbst machen, das müsste man ein bisschen mehr zentralisieren. (Experte S)*

Außerdem bemängeln einige Experten, dass eine kontinuierliche Finanzierung von Cybersicherheitsmaßnahmen bisher nicht sichergestellt ist. Zwar gibt es in allen Häusern ein geplantes IT-Budget, jedoch übersteigen die anfallenden Investitionen für Cybersicherheitsmaßnahmen dieses. Während die einen Experten unterjährig zusätzliche Gelder bewilligt bekommen, müssen die anderen jede weitere Investition detailliert rechtfertigen. In der Regel erfolgt eine Priorisierung der Projekte sowie eine Verteilung von größeren Vorhaben über mehrere Jahre. Bis dato werden die meisten Maßnahmen aus unterschiedlichen (Sonder-)Töpfen, wie zum Beispiel dem Krankenhauszukunftsfonds (KHZF) im Rahmen des Krankenhauszukunftsgesetzes (KHZG) finanziert.

*Auf der einen Seite finde ich es gut, dass Geld investiert wird seitens des Staats. Auf der anderen Seite haben wir natürlich das Problem, dass wir keine Anschlussfinanzierung dafür haben. (Experte F)*

Zwar unterstützt das KHZG wichtige Sicherheitsmaßnahmen, wie zum Beispiel die Modernisierung der IT-Infrastruktur und die Anschaffung moderner Medizinprodukte und -geräte. Jedoch reichen die individuellen Fördermittel für eine umfassende Modernisierung nicht aus.

*Die 4,3 Milliarden sind bei rund 800 Krankenhäusern ein Tropfen auf den heißen Stein. (Experte C)*

Die Mehrheit der Experten berichtet, dass die tatsächlichen Investitionsbedarfe um ein Vielfaches über den zugeteilten Finanzierungsgeldern liegen. Insbesondere die Modernisierung der Netzwerktechnik oder die Einführung eines Security Information and Event Management (SIEM) sind kostspielige Projekte. Zudem wird spezialisiertes Fachpersonal benötigt, was in den meisten befragten Häusern fehlt. Ein weiterer Kritikpunkt der Experten zeigt sich in der Antragsstellung und Bewilligung der Fördermittel, was eine zusätzliche Herausforderung darstellt.

*Dieses Krankenhauszukunftsgesetz ist eine tolle Sache, ist aber in der Verteilung und der Genehmigung oder Freigabe der Anträge gerade sehr schwierig. (Experte M)*

Aufgrund hoher bürokratischer Hürden und der Masse an Anträgen – teilweise über verschiedene Bundesländer hinweg – haben viele der befragten Häuser externe Berater und Anwälte beauftragt. Zusätzliche Komplexität ergibt sich in der Vergabe von Aufträgen durch Ausschreibungen und der fehlenden Transparenz über die Bewilligung von Geldern. Übereinstimmend bemängeln die Experten, dass das KHZG die historisch gewachsenen Investitionsstaus nicht vollständig decken kann und es an der Anschlussfinanzierung der umzusetzenden Maßnahmen fehlt. Getätigte Investitionen verursachen über den Förderzeitraum von 2024 hinaus weitere laufende Kosten. Zudem wird das zusätzlich benötigte Personal ebenso nur bis 2024 gefördert. Gemäß einiger Experten findet keine Gesamtkostenbetrachtung (Total Cost of Ownership) in der Investitionsentscheidung statt. Aufgrund der umfassenden Anforderungen und der zeitkritischen Umsetzung des KHZG haben sich einige Häuser gegen eine Förderung entschieden und nehmen so entsprechende Strafzahlungen in Kauf.

Außerdem stellt die operative Umsetzung gesetzlich verpflichtender Maßnahmen, wie zum Beispiel der Telematikinfrastruktur, die befragten Häuser vor weitere Herausforderungen.

*Telematikinfrastruktur, [..] das ist sehr aufwendig, und das ist im Moment gerade die größte Herausforderung, die wir so zu stemmen haben. (Experte Q)*

Besonders schwierig ist der Spagat zwischen der Gestaltung sicherer Systeme und der (maximalen) Benutzerfreundlichkeit digitaler Dienstleistungen. Weiter erörtern die Experten, dass die derzeit implementierten Initiativen eine Vielzahl an Einzelmaßnahmen darstellen, was zu punktuellen Verbesserungen führt, jedoch im Gesamtblick die Erarbeitung einer umfassenden digitalen Basisarchitektur oftmals vernachlässigen. Ferner wird zur Umsetzung komplexer und mehrjähriger Vorhaben ein professionelles Multiprojektmanagement erforderlich, was die befragten Krankenhäuser vor weitere Herausforderungen stellt.

*Da gibt es jetzt viele Maßnahmen, sowohl um die eigene Infrastruktur abzusichern. Da kommt jetzt noch das Krankenhauszukunftsgesetz dazu. Das heißt, plötzlich sind diese Krankenhäuser mit einem Multiprojektmanagement gefordert, dass sie überhaupt nicht mehr im Griff haben. (Experte P)*

Darüber hinaus sehen die Interviewteilnehmer den Schutz der Patientendaten als weitere Herausforderung an. Dabei sind sich die Experten einig, Patientendaten nur im Haus (on-premise) zu speichern und sprechen sich mehrheitlich gegen eine zentrale Patientendatenbank aus. Uneinigkeit herrscht jedoch über die Monetarisierung von kriminell erlangten Patientendaten. Während der Großteil der Befragten Patientendaten lediglich zur Erlangung von Erpressungen (Ransomware) gefährdet sieht, ist der (kontinuierliche) Verkauf von Patientendaten im Darknet für die anderen Gesprächspartner ein realistisches Szenario.

### 4.4.3 Akteure

Im Hinblick auf externe Herausforderungen empfinden die Experten die steigende Abhängigkeit von großen Technologie- und Sicherheitsanbietern, wie zum Beispiel Microsoft, als problematisch. Einerseits bieten solche standardisierten Produkte viele Vorteile, unter anderem Kosteneffizienz und höhere Sicherheit. Andererseits entsteht ein Klumpenrisiko, das zu weitreichenden, globalen Ausfällen führen kann.

*Das Allheilmittel kann nicht ein externer Dienstleister sein. (Experte K)*

Daher sehen die befragten Experten die Auslagerung von (Sicherheits-)Dienstleistungen, beispielsweise durch sogenannte Cloud-Lösungen, zwiegespalten. Die Fürsprecher betonen die Schonung interner Ressourcen sowie den Einsatz eines doppelten Schutzmechanismus durch on-premise und Cloud-Sicherheitsstandards. Die Widersprecher argumentieren, dass der Perimeterschutz geöffnet wird und somit das Sicherheitsniveau sinkt. Zudem wird die Abhängigkeit von Dritten erhöht. Dennoch erkennen die Gesprächspartner übereinstimmend die Cloud als Zukunftslösung an.

*Die Cloud wird nicht die Lösung aller Probleme, die wird die Lösung vieler Herausforderungen sein. (Experte C)*

Derzeit befinden sich vorwiegend standardisierte Randsysteme in der Cloud, wie zum Beispiel E-Mail, Mobile-Device-Management-Lösungen oder das Bewerbermanagement. Um zukünftig weitere Dienstleistungen in die Cloud auszulagern, haben die ersten Häuser einen Kriterienkatalog entworfen. Beispielsweise muss der Cloud-Anbieter zertifiziert sein, ein ISMS besitzen und dem Krankenhaus ein Audit-Recht zusagen. Zudem nutzen bereits einige die sogenannte private Cloud oder experimentieren mit Sub-Clouds, die eine stärkere Absicherung bei gleichzeitiger Nutzung externer Dateninfrastrukturen ermöglichen. Eine weitere, sehr bedeutsame Herausforderung stellt laut den Gesprächspartnern die Medizintechnik dar.

*Und Medizintechnik: Auch das ist ja kein Geheimnis, ist ja oft uralte Technik, die nicht verändert werden darf. Das heißt also, wir haben die letzte Windows XP Maschine erst vor kurzem hier rausgekriegt, weil wir eben kein Update machen dürfen, weil es dann gegen das Medizinproduktegesetz verstößt. (Experte C)*

Anpassungen und Veränderungen, inklusive Softwareaktualisierungen, sind gemäß der Gesetzeslage nicht erlaubt, beziehungsweise bedürfen einer Rezertifizierung.

> *Im Medizinproduktegesetz haben [sie] keine Adaption. Die haben zwar Fehlerbehebungen berücksichtigt in ihrem Zyklus aber sie haben keine Bedrohungsszenarien in ihrem Zyklus berücksichtigt. (Experte S)*

Laut Experten werden Altgeräte zwar technisch vom Netz segmentiert, jedoch führt die lange Lebensdauer der Medizinprodukte, insbesondere im Hinblick auf die steigende Vernetzung im Krankenhaus, zu einem unbekannten und steigenden Risiko. Zudem gelten neue Gesetze und Maßnahmen, wie zum Beispiel die Vorgabe einiger Häuser, Neugeräte nur noch mit Wartungsverträgen zu kaufen, nicht für den Bestand. Die Mehrheit der Interviewpartner fordert daher, die Hersteller von Medizinprodukten stärker zu incentivieren, um sichere Medizinprodukte zu liefern. Eine in den Gesprächen rege diskutierte Möglichkeit wäre die gesetzliche Verpflichtung der Herstellerhaftung:

> *Also die Incentivierung, sichere Systeme zu programmieren, ist einfach nicht da. Da hätte [...] das KHZF oder die Bundesregierung lieber Geld dahingehend ausgeben sollen, dass man tatsächlich Hersteller in die Haftung bringt. Also, wenn du ein unsicheres System lieferst, dann [...] bist du schadensersatzpflichtig, lieber Hersteller. (Experte L)*

Andererseits, so argumentieren insbesondere die externen Krankenhausexperten, bieten die Hersteller nur Einzelkomponenten an und können somit nur schwer für die Cybersicherheit eines einzelnen Hauses geradestehen. Zusätzlich würde eine solche Verpflichtung einen schwerwiegenden Nachteil im internationalen Wettbewerb mit sich bringen. Ernüchternd ergibt sich die Erkenntnis:

> *Der Geschäftsführer ist also in der Haftung und muss im Einkauf einfach ganz genau hingucken. (Experte P)*

### 4.4.4 Gesundheitssystem

Die Experten sehen ferner das deutsche Gesundheitssystem in seiner aktuellen Ausgestaltung an seinen Grenzen. Besonders der Mangel an einer umfassenden Gesundheits- und IT-Sicherheitsstrategie sowie die Verteilung der Verantwortlichkeit zwischen Bund, Ländern und den jeweiligen Städten und Landkreisen bemängeln die Gesprächspartner. Zudem wird die Umsetzung der stetig zunehmenden gesetzlichen Anforderungen auf europäischer und nationaler Ebene als herausfordernd bezeichnet. Eine besondere Schwierigkeit stellt die duale Finanzierung von Krankenhäusern dar. Die Investitionskosten werden grundsätzlich von den Bundesländern finanziert, jedoch sind die Investitionsmittel in den letzten 10 Jahren zurückgegangen. Ferner wird weder die Digitalisierung noch die Cybersicherheit in den finanziellen Kalkulationen berücksichtigt:

> *Digitalisierung ist derzeit nicht als Kostenblock oder als Kosten im Gesundheitswesen verankert. (Experte S)*

Daher schlagen einige Experten eine Anpassung des Vergütungssystems vor, indem die Cybersicherheit zum Bestandteil der Leistungserbringung wird und Refinanzierungen ermöglicht werden. Eine rege diskutierte Möglichkeit bietet die Cyber-Fallpauschale, die pro Patienten einen gewissen Sicherheitsaufschlag abrechnet. Dieser Vorschlag wurde von den

weiteren Gesprächspartnern begrüßt, obgleich Einigkeit besteht, dass die Sicherheitskosten nicht linear mit der Anzahl an Betten korreliert und die Finanzierung einer solchen Pauschale weiter ungeklärt ist.

Eine weitere Möglichkeit, um Sicherheitsmaßnahmen (kosten-)effizient zu gestalten, würde laut Experten in der Einführung von nationalen Standards und zentralen Dienstleistungen liegen. Es gibt zwar diverse Arbeitskreise und Allianzen auf Bundes- und Länderebene, jedoch werden bisher keine gemeinsamen Projekte über verschiedene Häuser hinweg geschaffen, bis auf wenige Ausnahmen. Kooperationen ermöglichen die flächendeckende Abstimmung des Versorgungsangebots sowie die Möglichkeit gemeinsame Dienstleistungen (Shared Services) zu etablieren. Als besonders wichtig sehen die Gesprächspartner nicht nur den Austausch innerhalb des Gesundheits- und Krankenhaussektors, sondern wünschen sich eine bessere Zusammenarbeit mit industrieübergreifenden IT-Sicherheitsexperten.

> *Ein Wahnsinn, dass es jetzt jedes Krankenhaus für sich selbst macht, weil damit natürlich jede dieser Lösungen wird schlechter sein als eine gebündelte Lösung und jede dieser Lösungen wird nicht nur funktional schlechter sein, sondern auch unsicherer sein. (Experte P)*

Daher bedarf es laut Experten an europäischen und deutschlandweiten Standards, um die Wettbewerbsfähigkeit und Cybersicherheit der deutschen Krankenhäuser sicherzustellen.

### 4.4.5 Globale Entwicklungen

Laut den Expertenausführungen wurden aufgrund der globalen COVID-19 Pandemie wichtige Projekte verschoben. Zudem hat sich die Gefahrenlage durch Home-Office und einer geringeren Aufmerksamkeit der Mitarbeiter signifikant erhöht. Bedingt durch die Pandemie und nationalen Förderinitiativen, wie das KHZG, hat die Digitalisierung in den befragten Krankenhäusern einen spürbaren Schub erhalten. Vor diesem Hintergrund sehen die Experten derzeit eine besondere Herausforderung in der sicheren Umsetzung aller Maßnahmen, insbesondere aufgrund der weiter zunehmenden Komplexität und Vernetzung der Krankenhausinfrastruktur. Der Auf- und Ausbau einer konsistenten und sicheren digitalen Architektur, während die Peripherie nicht steuerbar ist und die Cybersicherheit eines Systems nur so gut ist, wie das schwächste Glied innerhalb des Systems, stellt die Gesprächspartner vor besondere Herausforderungen. Ferner sind sich die Experten einig, dass die Gefährdung durch Cyberrisiken weiter steigen wird. Insbesondere neue Angriffsszenarien, wie zum Beispiel gezielte Ransomware-Angriffe, Cybercrime-as-a-Service und Cyberkrieg, werden auf die befragten Häuser zukommen. Dabei ist und bleibt der Faktor Mensch die größte Unbekannte. Aufgrund der dynamischen Natur des Cyberrisikos wird es laut Experten zum Wettrüsten kommen:

> *Die größten Herausforderungen sehe ich im Augenblick [...] in den externen Angriffen, Stichwort Ransomware. [...] Wir werden ein Wettrennen haben zwischen Sicherheitssystemen und den Entwicklern von Schadsoftware und Angriffs-Software. (Experte A)*

### 4.4.6 Technologien

Hinsichtlich moderner Technologien, die den weiteren Umgang mit Cyberrisiken beeinflussen, nennen die Experten besonders häufig Künstliche Intelligenz (KI) und das Internet

of Things (IoT). Bezüglich IoT sind die Ansichten der Interviewteilnehmer zwiegespalten. Einerseits sind viele Befragte offen gegenüber IoT, sehen jedoch als besondere Herausforderung, sichere Systeme in der hochkomplexen Vernetzung anzubieten. Dabei kann KI neue Möglichkeiten schaffen, diese Komplexität zu meistern. Laut den Gesprächen werben zwar erste Anbieter von Cybersicherheitssoftware mit KI, jedoch ist nicht gänzlich erkenntlich, ob und wieviel KI in den Produkten vorliegt. Ferner müssen die Algorithmen von den Häusern selbst trainiert werden, was wiederum interne Kapazitäten erfordert, die nicht zur Verfügung stehen. Andererseits wird KI laut Befragten beutender für Cyberkriminelle, weshalb das genannte Wettrüsten eine neue Dimension erreichen könnte. Weitere Herausforderungen werden moderne Quantencomputer und Cloud-Computing mit sich bringen, die aktuelle Sicherheitsstandards und Passwörter in wenigen Minuten knacken können.

## 5 Diskussion

Die Ergebnisse dieser Studie zeigen, dass Krankenhäuser aufgrund einer Vielzahl interner und externer Faktoren gegenüber Cybervorfällen besonders exponiert sind. Neben der mangelnden Cyber Security Awareness, vor allem in der Pflege und Medizin (Priestman et al., 2019), fehlt es den befragten Krankenhäusern an einer eindeutigen Begriffsabgrenzung des Terminus Cyberrisiko von verwandten Begrifflichkeiten wie IT- und Informationssicherheitsrisiko (Zängerle & Schiereck, 2023a). Dabei ist ein ausgeprägtes Sicherheitsbewusstsein ein elementarer Bestandteil zur Prävention von Cybervorfällen (Osborn & Simpson, 2017; Wrede et al., 2018). Zwar hat sich in den Interviews gezeigt, dass der Faktor Mensch eine bedeutende Rolle als interne und externe Risikoquelle einnimmt (Tsohou et al., 2012), jedoch werden in der Regel nur sehr wenige Maßnahmen zur Mitarbeitersensibilisierung umgesetzt (Wrede et al., 2018). Beispielsweise gibt es in den meisten Häusern kein umfassendes Schulungskonzept. Zudem mangelt es vielen Krankenhäusern einerseits an IT- und Cybersicherheitsexperten, andererseits erschweren die historisch gewachsene Komplexität der Unternehmensabläufe und die Vielzahl an veralteten und inkompatiblen Systemen die wirksame Einführung von Cybersicherheitsmaßnahmen (Abraham et al., 2019). Ferner zeigte sich in den Interviews, dass vor allem größere Häuser neue Organisationsstrukturen schaffen, zum Beispiel Dienstleistungs-GmbHs, um der steigenden Komplexität entgegenzuwirken. Dies kann jedoch nur als erster Schritt in Richtung eines effektiven Cyberrisikomanagements betrachtet werden, wenn größere Häuser häufiger von Cyberangriffen betroffen sind (McLeod & Dolezel, 2018). Vor dem Hintergrund der dynamischen Natur des Cyberrisikos (Boyer, 2020) erscheint die Einführung eines umfassenden und abgestimmten Cyberrisikomanagements unerlässlich (International Standard Organisation, 2018).

Weiter hat sich gezeigt, dass Krankenhäuser Defizite in der Erkennung und Bewertung von Cyberbedrohungen aufweisen (Berger et al., 2020). Trotz der Fülle an identifizierten Good Practices (Tabelle 2) und technischen Maßnahmen (Abbildung 4) fehlt es an einem konzeptionellen und risikoadäquaten Gesamtblick auf das Risikomanagement, also an der risikoorientierten Bewertung der vielfältigen Schadenspotenziale von Cybervorfällen sowie der Identifikation neuer Angriffsszenarien, die sich aus der ständigen Weiterentwicklung der IT ergeben (Wrede et al., 2018). Hier ist zunächst die Absicherung der wichtigsten Unternehmensprozesse und -werte sowie die Ableitung von effektiven Schutzmaßnahmen anzugehen. Wenn in den meisten Häusern die IT-Abteilung für das Management von

Cyberrisken verantwortlich ist und es weder einen Cyberrisikomanagementprozess noch ein einheitliches Risikomanagement in den befragten Häusern gibt, ist auch hier die Organisationsstruktur zu hinterfragen (Marotta & McShane, 2018; Shetty et al., 2018; Poyraz et al., 2020; Zängerle & Schiereck, 2023b). Gegenwärtig ist es kaum verwunderlich, dass Supply-Chain-Attacken im bestehenden Risikomanagement nur unzureichend adressiert werden und somit nur wenige effektive Maßnahmen zur Risikoprävention solcher Schäden verfügbar sind (Smith et al., 2007; Deane et al., 2009; Bandyopadhyay et al., 2009; Wrede et al., 2018).

Angesichts der möglichen existentiellen Konsequenzen von Cybervorfällen sollte die Unternehmensleitung unbedingt in die Risikoanalyse einbezogen sein, um die vermittelten Ergebnisse verständlich darzulegen (Davey, 1995). Hierbei kann die Einführung eines regelmäßigen Berichtsweges an den Vorstand über die aktuelle Gefahrenlage helfen, was sowohl die Cyber Security Awareness (Wrede et al., 2018) als auch das gemeinsame Begriffsverständnis (Zängerle & Schiereck, 2023a) verbessern kann. Zudem erhalten Maßnahmen durch die Vorstandseinbindung die notwendige Priorisierung. Darüber hinaus verstehen viele Experten die Einführung eines Sicherheitsstandards, wie zum Beispiel des B3S oder ISO 27001, als ein effektives Risikomanagementinstrument. Solche Richtlinien können die Etablierung von Risikomanagementprozessen fördern (Marotta et al., 2017), doch zielen diese Standards auf die Schaffung einheitlicher Minimalanforderungen an das Cybersicherheitsniveau eines Unternehmens ab (International Standard Organisation, 2018). Zudem hat sich gezeigt, dass aufgrund der dynamischen Entwicklung des Cybersicherheitsumfeldes und der langwierigen Überarbeitung und Neuveröffentlichung (internationaler) Normen die etablierten Standards Mängel aufweisen (Anderson & Williams, 2018). Ebenso werden Cyberversicherungen oftmals als Äquivalent eines effektiven Cyberrisikomanagements angesehen, jedoch bieten solche Versicherungen weder einen vollumfänglichen Schutz, noch investieren Unternehmen ausreichend in die eigene Absicherung gegen Cybergefahren (Wrede et al., 2018). Dennoch kann eine Cyberversicherungspolice dabei helfen, die aktuelle Gefahrenlage besser zu verstehen (Samhan, 2017).

Die Entwicklung hin zu einem modernen, informationstechnologischen Gesundheitswesen ist eine besondere Herausforderung in Bezug auf Sicherheit und Datenschutz (Smith & Eloff, 1999). Aufgrund der weiter voranschreitenden Vernetzung von Medizingeräten mit internen und externen Netzwerken, erhöht sich die Anfälligkeit der Geräte gegenüber Cybergefahren in mehrfacher Hinsicht (Caruso & Masters, 2014). Medizinische Geräte müssen nicht nur ihre eigene Sicherheit gewährleisten, sondern auch vor Angreifern geschützt werden, die Schwachstellen ausnutzen und in das größere IT-System des Krankenhauses eindringen wollen (Holden, 2015). Daher muss die Cybersicherheit nicht nur ein integrativer Bestandteil der internen Beschaffung werden (Coronado & Wong, 2014), vielmehr sollten Hersteller und Gesundheitsdienstleister Maßnahmen zur Identifizierung, Erkennung und Prävention vor und nach der Markteinführung in Betracht ziehen (Webb & Dayal, 2017). Trotz der starken Regulierung der Medizinprodukteindustrie, stellt die Gerätesicherheit eine besondere Herausforderung dar, die Änderungen und Ergänzungen der aktuellen Prozesse erfordert, um die spezifischen Erwartungen an die Cybersicherheit zu erfüllen (Jump, 2019). Aufgrund der Unvorhersehbarkeit der Bedrohungslage bedarf es eines Paradigmenwechsels, um proaktiv neue Bedrohungen und Schwachstellen zu erkennen, die sich in kürzester Zeit zu globalen Ereignissen entwickeln könnten (Jump, 2019). Somit ist ein regelmäßiger Informationsaustausch sowie eine verstärkte Zusammenarbeit

zwischen allen Beteiligten von grundlegender Bedeutung für das Sicherheitsmanagement von Medizinprodukten, die zukünftige Cybersicherheit des Gesundheitswesens sowie der Gewährleistung einer optimalen Patientenversorgung (Coronado & Wong, 2014; Webb & Dayal, 2017; Jump, 2019). Der Austausch von Erfahrungen hilft Organisationen, ihre eigenen Praktiken zu bewerten und geltende Sicherheitsstandards weiterzuentwickeln (He & Johnson, 2015). Kooperationen und Zusammenschlüsse mit anderen Krankenhäusern und Institutionen des Gesundheitswesens auf regionaler, nationaler und europäischer Ebene können diesen Wandel nicht nur unterstützen, sondern auch neuartige, zentrale Angebote und Dienstleistungen schaffen, um den weiter steigenden Kostendruck zu meistern.

Ferner zeigte sich in den Gesprächen, dass das Prinzip der dualen Krankenhausfinanzierung an ihre Grenzen stößt. Trotz erheblicher ökonomischer Anstrengungen konnten die Kostensteigerungen der vergangenen Jahre nicht durch dieselben Ertragssteigerungen im Fallpauschalen basierten Vergütungssystem (DRG) ausgeglichen werden (AG Hochschulmedizin, 2014). Besonders kritisch ist die Tatsache, dass die Bundesländer seit Einführung der dualen Finanzierung vor knapp 50 Jahren ihrer Finanzierungspflicht, der Übernahme anfallender Investitionskosten der Krankenhäuser, nicht vollumfänglich nachgekommen sind und sich ein Investitionsstau von mehr als 50 Mrd. Euro angesammelt hat (Schmitz & Pedell, 2013). Daher fordert beispielsweise die Arbeitsgemeinschaft Hochschulmedizin, dass im Rahmen einer Grundgesetzänderung die Investitionskosten durch Bund und Länder hälftig zu übernehmen sind (AG Hochschulmedizin, 2014). Eine weitere Alternative bietet die in den Gesprächen genannte Cybersicherheitspauschale, die pro Patienten zu entrichten wäre. Offen bleibt jedoch die Finanzierung und die Problematik, dass die Kosten für Cybersicherheit wegen eines hohen Fixkostenanteils nicht linear mit der Anzahl an Patienten steigen. Nichtsdestotrotz bedarf es einer zeitnahen Lösung, um die Finanzierung von sogenannten Vorhalteleistungen, wie der Cybersicherheit, sicherzustellen. Erste politische Überlegungen zur Reform der Krankenhausvergütung wurden seitens der Bundesregierung getätigt (Augurzky et al., 2022), jedoch beziehen sich diese Änderungen lediglich auf die Vergütung der medizinischen Versorgung und nicht auf die Finanzierung der Investitionskosten oder infrastruktureller Sicherheitsleistungen.

## 6 Zusammenfassung und Schlussbemerkung

Aufgrund des Mangels an umfassenden wissenschaftlichen Studien über das Cyberrisikomanagement im deutschen Gesundheitswesen untersucht dieser Beitrag anhand qualitativer Expertenbefragungen aktuelle Good Practices des Cyberrisikomanagements und analysiert die elementaren Herausforderungen der Branche zur langfristigen Sicherstellung der Cybersicherheit. Cyberbedrohungen sind für Krankenhäuser und das Gesundheitswesen real und müssen umfassend analysiert und behandelt werden. Die vorliegende Studie zeigt in ausführlicher Weise den aktuellen Stand des Gesundheitswesens und bestehende Good Practices im Rahmen des Cyberrisikomanagements auf. Im Hinblick auf die weiter voranschreitende Digitalisierung von medizinischen und Unternehmensprozessen, kombiniert mit einer höheren Vernetzung innerhalb und außerhalb des Krankenhauses steht das Gesundheitswesen jedoch am Scheideweg, die vorliegenden Herausforderungen zur Sicherstellung der Cybersicherheit zu meistern.

Neben einer ausgeprägten Cyber Security Awareness bedarf es einer systematischen Integration von ERM-Lösungen, die ein unternehmensweites Rahmenwerk schaffen (Kosub, 2015), sowie der Implementierung eines funktionierenden Cyberrisikomanagement-Kon-

zeptes (Eling, 2018). Letzteres sollte nicht an die IT-Abteilung delegiert werden, sondern muss in das unternehmensweite ERM integriert werden (Marotta & McShane, 2018; Shetty et al., 2018; Poyraz et al., 2020; Zängerle & Schiereck, 2023b). Zudem sind die Entwicklung von qualitativen und quantitativen Risikomanagementansätzen (Wrede et al., 2018) sowie von einheitlichen Begriffsabgrenzungen des Terminus Cyberrisiko (Zängerle & Schiereck, 2023a) erforderlich. Zur Schaffung solcher Strukturen bedarf es sowohl einer kontinuierlichen Finanzierung, insbesondere vor dem Hintergrund der jahrzehntelangen Unterfinanzierung von Krankenhäusern, als auch regionaler, nationaler und internationaler Zusammenschlüsse und Partnerschaften. Denn Cyberrisiken sind dynamisch und beschränken sich nicht auf einzelne Institute, Unternehmen oder Länder (Eling, 2020).

In Anbetracht der qualitativ ausgerichteten Vorgehensweise weist die vorliegende Untersuchung Limitationen auf. Zum einen basiert unsere Analyse auf den mündlichen Erfahrungen von IT- und Cybersicherheitsexperten von führenden deutschen Krankenhäusern. Aufgrund der zielgerichteten Stichprobe und der relativ kleinen Stichprobengröße kann die Verallgemeinerung der Ergebnisse eingeschränkt sein. Zum anderen beruhen die Erkenntnisse über das Management von Cyberrisiken auf den Antworten einzelner Personen und sind daher möglicherweise nicht repräsentativ für alle Bemühungen in den befragten Krankenhäusern sowie im Gesundheitswesen im Allgemeinen. Um die Objektivität zu erhöhen und ein noch tieferes Verständnis der Ansätze und Initiativen zu erhalten, könnte die Analyse durch die Befragung weiterer Personen aus den jeweiligen Häusern erweitert werden. Vor allem Interviews mit Personen aus verschiedenen Hierarchieebenen, Funktionsbereichen oder mit unterschiedlichen Verantwortlichkeiten könnten vielversprechende Erkenntnisse liefern. Auch andere Informationsquellen, wie Jahresberichte oder Auszüge aus der internen Kommunikation der Krankenhäuser, könnten die Analyse bereichern.

Die theoretischen und praktischen Implikationen dieser Studie sind vielfältig. Für die wissenschaftliche Forschung bieten die aufgezeigten Ergebnisse, als erste ihrer Art, eine recht umfassende, empirisch basierte Bestandsaufnahme, die als Grundlage für weitere Forschungsarbeiten herangezogen werden kann. Beispielsweise kann die zukünftige Forschung auf den vorgestellten Ergebnissen ansetzen und weitere Erkenntnisse aus der systematischen Zuordnung von Herausforderungen und Maßnahmen ableiten.[4] Ferner können konkrete Einzelaspekte der vorliegenden Studie näher beleuchtet werden. Einerseits bedarf es neuer wissenschaftlicher Erkenntnisse über die effektive Ausgestaltung von Cyberversicherungen. Andererseits ergeben sich mit Blick auf resiliente Organisationen im Gesundheitswesen weitere Forschungsfragen, etwa zu Vorteilen und Grenzen der Auslagerung von IT-Systemen und zur effektiven Schulung des Personals für eine dauerhaft hohe Awareness.

Für die Praxis schafft die Analyse einen transparenten Überblick über den aktuellen Status quo und sogenannte Good Practices des Cyberrisikomanagements. Chief Information Security Officers sowie Cybersicherheitsverantwortliche von Krankenhäusern können sich an diesen Praktiken orientieren, um das interne Cyberrisikomanagement zu verbessern oder die Bewilligung von Investitionsmaßnahmen wissenschaftlich zu fundieren. Zudem bietet die Studie eine empirische Diskussionsgrundlage für Politik, Krankenhäuser und Krankenkassen, insbesondere vor dem Hintergrund der ungeklärten Finanzierung von Cybersicherheitsmaßnahmen.

4 Wir danken unserer anonymen Gutachterin bzw. unserem anonymen Gutachter für diesen wichtigen Hinweis.

## Literatur


Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Abraham, C., Chatterjee, D. & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

AG Hochschulmedizin (2014). Neue Finanzierung der Universitätsklinika dringend notwendig. *Orthopädie und Unfallchirurgie – Mitteilungen und Nachrichten*, *03*(01), 13–14. https://doi.org/10.1055/s-0034-1368736

Almulhem, A. (2012). Threat modeling for electronic health record systems. *Journal of Medical Systems*, *36*(5), 2921–2926. https://doi.org/10.1007/s10916-011-9770-6

Alvesson, M. & Sandberg, J. (2011). Generating Research Questions Through Problematization. *The Academy of Management Review, 36*(2), 247–271. https://doi.org/10.5465/amr.2009.0188

Anderson, S. & Williams, T. (2018). Cybersecurity and medical devices: Are the ISO/IEC 80001–2–2 technical controls up to the challenge? *Computer Standards & Interfaces*, *56*(C), 134–143. https://doi.org/10.1016/j.csi.2017.10.001

Angst, C. M., Block, E. S., D'Arcy, J. & Kelley, K. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly, 41*(3), 893–916. https://doi.org/10.25300/MISQ/2017/41.3.10

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B. & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1), 146. https://doi.org/10.1186/s12911-020-01161-7

Ashby, S., Buck, T., Nöth-Zahn, S. & Peisl, T. (2018). Emerging IT Risks: Insights from German Banking. *The Geneva Papers on Risk and Insurance – Issues and Practice*, *43*(2), 180–207. https://doi.org/10.1057/s41288-018-0081-8

Augurzky, B., Bschor, T., Busse, R., Dötsch, J., Evans, M., Felix, D., Gürkan, I., Haeske-Seeberg, H., Hasseler, M., Huster, S., Karagiannidis, C., Kingreen, T., Kroemer, H., Münkler, L., Schmitt, J., Somasundaram, R. & Sundmacher, L. (2022). *Grundlegende Reform der Krankenhausvergütung: Dritte Stellungnahme und Empfehlung der Regierungskommission für eine moderne und bedarfsgerechte Krankenhausversorgung*. http://www.bundesgesundheitsministerium.de/krankenhauskommission-stellungnahme-krankenhausverguetung.pdf. Zugegriffen: 03.01.2023

Bandyopadhyay, T., Mookerjee, V. S. & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, *52*(11), 68–73. https://doi.org/10.1145/1592761.1592780

Baur, N. & Blasius, J. (Hrsg.). (2014). *Handbuch Methoden der empirischen Sozialforschung*. Springer VS Wiesbaden.

Berger, S., Bürger, O. & Röglinger, M. (2020). Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy. *Computers & Security*, *93*, 101790. https://doi.org/10.1016/j.cose.2020.101790

Biener, C., Eling, M. & Wirfs, J. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Bitzer, M., Stahl, B. & Strobel, J. (2021). Empathy for Hackers – An IT Security Risk Assessment Artifact for Targeted Hacker Attacks. *ECIS 2021 Research Papers*(41). https://aisel.aisnet.org/ecis2021rp/41. Zugegriffen: 04.10.2022

Blanke, S. J. & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of Healthcare Risk Management*, *36*(1), 14–24. https://doi.org/10.1002/jhrm.21230

Bohn, L. & Schiereck, D. (2022). Regulation of data breach publication: the case of US healthcare and the HITECH act. *Journal of Economics and Finance*. https://doi.org/10.1007/s12197-022-09607-6

Boudko, S. & Abie, H. (2019). Adaptive Cybersecurity Framework for Healthcare Internet of Things. In *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT),* Oslo, Norway. https://doi.org/10.1109/ISMICT.2019.8743905

Boyer, M. M. (2020). Cyber insurance demand, supply, contracts and cases. *The Geneva Papers on Risk and Insurance – Issues and Practice*, *45*(4), 559–563. https://doi.org/10.1057/s41288-020-00188-1

Bundesamt für Sicherheit in der Informationstechnik. (2022). *Die Lage der IT-Sicherheit in Deutschland 2022*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410. Zugegriffen: 11.01.2023

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53–63. https://doi.org/10.1080/23738871.2017.1296878

Caruso, R. J. & Masters, M. (2014). Applying cyber risk management to medical device design. *Biomedical Instrumentation & Technology*, 32–37. https://doi.org/10.2345/0899-8205-48.s1.32

Cebula, J. J. & Young, L. R. (2010). *A taxonomy of operational cyber security risks*. Technical Note CMU/SEI-2010-TN-028. Software Engineering Institute. https://apps.dtic.mil/sti/pdfs/ADA537111.pdf. Zugegriffen: 10.02.2021

Cepeda, G. & Martin, D. (2005). A review of case studies publishing in Management Decision 2003-2004. *Management Decision*, *43*(6), 851–876. https://doi.org/10.1108/00251740510603600

Clarke, R. & Youngstein, T. (2017). Cyberattack on Britain's National Health Service – A Wake-up Call for Modern Medicine. *The New England Journal of Medicine*, *377*(5), 409–411. https://doi.org/10.1056/NEJMp1706754

Coronado, A. J. & Wong, T. L. (2014). Healthcare cybersecurity risk management: keys to an effective plan. *Biomedical Instrumentation & Technology*, *48*, 26–30. https://doi.org/10.2345/0899-8205-48.s1.26

Darms, M., Haßfeld, S. & Fedtke, S. (2019). *IT-Sicherheit und Datenschutz im Gesundheitswesen*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-21589-7

Davey, J. (1995). The role of risk analysis in European harmonisation of security for healthcare information systems. *Computer Methods and Programs in Biomedicine*, *48*(1), 133–137. https://doi.org/10.1016/0169-2607(95)01673-H

Deane, J. K., Ragsdale, C. T., Rakes, T. R. & Rees, L. P. (2009). Managing supply chain risk and disruption from IT security incidents. *Operations Management Research*, *2*(1–4), 4–12. https://doi.org/10.1007/s12063-009-0018-2

Diekmann, A. (2007). *Empirische Sozialforschung: Grundlagen, Methoden, Anwendungen* (14. Aufl.). *rororo: Rowohlts Enzyklopädie*. Rowohlt Taschenbuch Verlag.

Eling, M. (2018). Cyber Risk and Cyber Risk Insurance: Status Quo and Future Research. *The Geneva Papers on Risk and Insurance – Issues and Practice*, *43*(2), 175–179. https://doi.org/10.1057/s41288-018-0083-6

Eling, M. (2020). Cyber risk research in business and actuarial science. *European Actuarial Journal*, *10*(2), 303–333. https://doi.org/10.1007/s13385-020-00250-1

Eling, M. & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

Etges, A. P. B. d. S., Grenon, V., Lu, M., Cardoso, R. B., Souza, J. S. de, Kliemann Neto, F. J. & Felix, E. A. (2018). Development of an enterprise risk inventory for healthcare. *BMC Health Services Research*, *18*(1), Artikel 578, 1–16. https://doi.org/10.1186/s12913-018-3400-7

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G. & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. *Science*, *366*(6469), 1066–1069. https://doi.org/10.1126/science.aaz4795

Fayans, I., Motro, Y., Rokach, L., Oren, Y. & Moran-Gilad, J. (2020). Cyber security threats in the microbial genomics era: implications for public health. *Eurosurveillance*, *25*(6), 1900574. https://doi.org/10.2807/1560-7917.ES. 2020.25.6.1900574

Fernando, J. I. & Dawson, L. L. (2009). The health information system security threat lifecycle: an informatics theory. *International Journal of Medical Informatics*, *78*(12), 815–826. https://doi.org/10.1016/j.ijmedinf.2009.08.006

Finfgeld-Connett, D. (2014). Use of content analysis to conduct knowledge-building and theory-generating qualitative systematic reviews. *Qualitative Research*, *14*(3), 341–352. https://doi.org/10.1177/1468794113481790

Fu, K. & Blum, J. (2013). Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, *56*(10), 35–37. https://doi.org/10.1145/2508701

Gioia, D. A., Corley, K. G. & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Gläser, J. & Laudel, G. (2012). *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen*. *Lehrbuch*. VS, Verl. für Sozialwiss.

Gordon, L. A., Loeb, M. P. & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85. https://doi.org/10.1145/636772.636774

Haufe, K., Dzombeta, S. & Brandis, K. (2014). Proposal for a Security Management in Cloud Computing for Health Care. *The Scientific World Journal*, *2014*, 146970. https://doi.org/10.1155/2014/146970

He, Y. & Johnson, C. (2015). Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template. *International Journal of Medical Informatics*, *84*(11), 941–949. https://doi.org/10.1016/j.ijmedinf.2015.08.010

Holden, W. L. (2015). The vital role of device manufacturers as cybercitizens. *Biomedical Instrumentation & Technology*, *49*(6), 410–422. https://doi.org/10.2345/0899-8205-49.6.410

Hoppe, F., Gatzert, N. & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. *The Journal of Risk Finance*, *22*(3/4), 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Huang, L.-C., Chu, H.-C., Lien, C.-Y., Hsiao, C.-H. & Kao, T. (2009). Privacy preservation and information security protection for patients' portable electronic health records. *Computers in Biology and Medicine*, *39*(9), 743–750. https://doi.org/10.1016/j.compbiomed.2009.06.004

Hubbard, D. W. & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. Wiley.

International Standard Organisation. (2018). *ISO/IEC 27000:2018: Information technology – Security techniques – Information security management systems – Overview and vocabulary*. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en. Zugegriffen: 20.04.2021

Iwaya, L. H., Fischer-Hübner, S., Åhlfeldt, R.-M. & Martucci, L. A. (2019). Mobile health systems for community-based primary care: Identifying controls and mitigating privacy threats. *JMIR mHealth and uHealth*, *7*(3), e11642. https://doi.org/10.2196/11642

Jump, M. (2019). AAMI TIR97: A vital resource in the postmarket management of medical device security. *Biomedical Instrumentation & Technology*, *53*(6), 462–464. https://doi.org/10.2345/0899-8205-53.6.462

Kaiser, R. (2014). *Qualitative Experteninterviews: Konzeptionelle Grundlagen und praktische Durchführung*. *Elemente der Politik*. Springer. https://doi.org/10.1007/978-3-658-02479-6

Kamoun, F. & Nicho, M. (2014). Human and organizational factors of healthcare data breaches: The Swiss cheese model of data breach Causation And Prevention. *International Journal of Healthcare Information Systems and Informatics*, *9*(1), 42–60. https://doi.org/10.4018/ijhisi.2014010103

Kim, H.-W., Park, J. H. & Jeong, Y.-S. (2018). Human-intelligence workflow management for the big data of augmented reality on cloud infrastructure. *Neurocomputing*, *279*, 19–26. https://doi.org/10.1016/j.neucom.2017.04.082

Kosub, T. (2015). Components and challenges of integrated cyber risk management. *Zeitschrift für die gesamte Versicherungswissenschaft*, *104*(5), 615–634. https://doi.org/10.1007/s12297-015-0316-8

Kritzinger, E. & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, *27*(5–6), 224–231. https://doi.org/10.1016/j.cose.2008.05.006

Kucera, M. (2020). Uniklinik Düsseldorf: Cyberangriff verursacht Todesfall. *kma – Klinik Management aktuell*, *25*(10), 6. https://doi.org/10.1055/s-0040-1718794

Kuckartz, U. & Rädiker, S. (Hrsg.). (2020). *Fokussierte Interviewanalyse mit MAXQDA: Schritt für Schritt* (1. Aufl.). Springer Fachmedien Wiesbaden; Springer VS.

Kuckartz, U. & Rädiker, S. (2022). *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung* (5. Aufl.). *Grundlagentexte Methoden*. Beltz Juventa.

Lamnek, S. & Krell, C. (2016). *Qualitative Sozialforschung: Mit Online-Material* (6., überarbeitete Auflage). Beltz.

Li, H., Yoo, S. & Kettinger, W. (2019). The Changing Tides of Investments and Strategies and Their Impacts on Security Breaches. *ICIS 2019 Proceedings, 33*. https://aisel.aisnet.org/icis2019/cyber_security_privacy_ethics_IS/cyber_security_privacy/33. Zugegriffen: 20.06.2023Liebold, R. &

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud & Security*, *2020*(2), 14–17. https://doi.org/10.1016/S1361-3723(20)30019-1

Marotta, A., Martinelli, F., Nanni, S., Orlando, A. & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35–61. https://doi.org/10.1016/j.cosrev.2017.01.001

Marotta, A. & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach: A Holistic Cyber Risk Management Approach. *Risk Management and Insurance Review*, *21*, 435–452. https://doi.org/10.1111/rmir.12109

McDonough, W. J. (2007). Cyber risk and privacy liability: A click in the right direction? *Journal of Healthcare Risk Management*, *27*(4), 9–12. https://doi.org/10.1002/jhrm.5600270403

McLellan, E., MacQueen, K. M. & Neidig, J. L. (2003). Beyond the Qualitative Interview: Data Preparation and Transcription. *Field Methods*, *15*(1), 63–84. https://doi.org/10.1177/1525822X02239573

McLeod, A. & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57–68. https://doi.org/10.1016/j.dss.2018.02.007

Meuser, M. & Nagel, U. (2009). The Expert Interview and Changes in Knowledge Production. In A. Bogner, B. Littig & W. Menz (Hrsg.), *Research Methods Series. Interviewing Experts*. Palgrave Macmillan.

Moritz, R. L., Berger, K. M., Owen, B. R. & Gillum, D. R. (2020). Promoting biosecurity by professionalizing biosecurity. *Science*, *367*(6480), 856. https://doi.org/10.1126/science.aba0376

Moshi, M. R., Parsons, J., Tooher, R. & Merlin, T. (2019). Evaluation of mobile health applications: Is regulatory policy up to the challenge? *International Journal of Technology Assessment in Health Care*, *35*(4), 351–360. https://doi.org/10.1017/S0266462319000461

Myers, M. D. (2020). *Qualitative research in business & management* (Third edition). SAGE.

Myers, M. D. & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

National Institute of Standards and Technology. (2012). *Guide for Conducting Risk Assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

Neubauer, T. & Heurix, J. (2011). A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics*, *80*(3), 190–204. https://doi.org/10.1016/j.ijmedinf.2010.10.016

Nosworthy, J. D. (2000). Implementing Information Security In The 21st Century — Do You Have the Balancing Factors? *Computers & Security*, *19*(4), 337–347. https://doi.org/10.1016/S0167-4048(00)04021-9

Osborn, E. & Simpson, A. (2017). On small-scale IT users' system architectures and cyber security: A UK case study. *Computers & Security*, *70*, 27–50. https://doi.org/10.1016/j.cose.2017.05.001

Palsson, K., Gudmundsson, S. & Shetty, S. (2020). Analysis of the impact of cyber events for cyber insurance. *The Geneva Papers on Risk and Insurance – Issues and Practice*, *45*(4), 564–579. https://doi.org/10.1057/s41288-020-00171-w

Paté-Cornell, M.-E., Kuypers, M., Smith, M. & Keller, P. (2018). Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis : an official publication of the Society for Risk Analysis*, *38*(2), 226–241. https://doi.org/10.1111/risa.12844

Pfleeger, S. L. & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Pooser, D. M., Browne, M. J. & Arkhangelska, O. (2018). Growth in the Perception of Cyber Risk: Evidence from U.S. P&C Insurers. *The Geneva Papers on Risk and Insurance – Issues and Practice*, *43*(2), 208–223. https://doi.org/10.1057/s41288-017-0077-9

Poyraz, O. I., Canan, M., McShane, M., Pinto, C. A. & Cotter, T. S. (2020). Cyber assets at risk: monetary impact of U.S. personally identifiable information mega data breaches. *The Geneva*

*Papers on Risk and Insurance – Issues and Practice*, *45*(4), 616–638. https://doi.org/10.1057/s41288-020-00185-4

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S. & Sebire, N. J. (2019). Phishing in healthcare organisations: threats, mitigation and approaches. *BMJ Health & Care Informatics*, *26*(1). https://doi.org/10.1136/bmjhci-2019-100031

Kruse, J. (2015). *Qualitative Interviewforschung: Ein integrativer Ansatz* (2. Aufl.). *Grundlagentexte Methoden*. Beltz Juventa.

Samhan, B. (2017). Can cyber risk management insurance mitigate healthcare providers' intentions to resist electronic medical records? *International Journal of Healthcare Management*, *13*(1), 12–21. https://doi.org/10.1080/20479700.2017.1412558

Sardi, A., Rizzi, A., Sorano, E. & Guerrieri, A. (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability*, *12*(17), 7002. https://doi.org/10.3390/su12177002

Schmitz, R.-M. & Pedell, B. (2013). Steuerung eines Krankenhauses der Maximalversorgung. *Controlling*(2), 121–124. https://doi.org/10.15358/0935-0381_2013_2_121

Schnell, R., Hill, P. B. & Esser, E. (2018). *Methoden der empirischen Sozialforschung* (11. Aufl.). *De Gruyter Studium*. De Gruyter Oldenbourg.

Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K. & Njilla, L. L. (2018). Reducing Informational Disadvantages to Improve Cyber Risk Management. *The Geneva Papers on Risk and Insurance – Issues and Practice*, *43*(2), 224–238. https://doi.org/10.1057/s41288-018-0078-3

Shoffner, M., Owen, P., Mostafa, J., Lamm, B., Wang, X., Schmitt, C. P. & Ahalt, S. C. (2013). The secure medical research workspace: An IT infrastructure to enable secure research on clinical data. *Clinical and Translational Science*, *6*(3), 222–225. https://doi.org/10.1111/cts.12060

Smidt, G. de & Botzen, W. (2018). Perceptions of Corporate Cyber Risks and Insurance Decision-Making. *The Geneva Papers on Risk and Insurance – Issues and Practice*, *43*(2), 239–274. https://doi.org/10.1057/s41288-018-0082-7

Smith, E. & Eloff, J. (1999). Security in health-care information systems—current trends. *International Journal of Medical Informatics*, *54*(1), 39–54. https://doi.org/10.1016/S1386-5056(98)00168-3

Smith, G. E., Watson, K. J., Baker, W. H. & Pokorski II, J. A. (2007). A critical balance: collaboration and security in the IT-enabled supply chain. *International Journal of Production Research*, *45*(11), 2595–2613. https://doi.org/10.1080/00207540601020544

Tanriverdi, H., Kwon, J. & Im, G. (2020). Data Breaches in Multihospital Systems: Antecedents and Mitigation Mechanisms. *ICIS 2020 Proceedings*, *10*. https://aisel.aisnet.org/icis2020/cyber_security_privacy/cyber_security_privacy/10. Zugegriffen: 21.06.2023

Taylor, H., Artman, E. & Woelfer, J. P. (2012). Information Technology Project Risk Management: Bridging the Gap between Research and Practice. *Journal of Information Technology*, *27*(1), 17–34. https://doi.org/10.1057/jit.2011.29

Thomson, M. E. & Solms, R. von (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security*, *6*(4), 167–173. https://doi.org/10.1108/09685229810227649

Trinczek, R. (2009). Experteninterview. In S. Kühl, P. Strodtholz & A. Taffertshofer (Hrsg.), *Handbuch Methoden der Organisationsforschung* (S. 32–56). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91570-8_3

Tsohou, A., Karyda, M., Kokolakis, S. & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology & People*, *25*(3), 327–352. https://doi.org/10.1108/09593841211254358

Tully, J., Selzer, J., Phillips, J. P., O'Connor, P. & Dameff, C. (2020). Healthcare Challenges in the Era of Cybersecurity. *Health Security*, *18*(3), 228–231. https://doi.org/10.1089/hs.2019.0123

Webb, T. & Dayal, S. (2017). Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia. *Computer Law & Security Review*, *33*(4), 559–563. https://doi.org/10.1016/j.clsr.2017.05.004

Whitman, M. & Mattord, H. (2014). Information Security Governance for the Non-security Business Executive. *Journal of Executive Education*, *11*, 97–111.

Williams, P. & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, *8*, 305–316. https://doi.org/10.2147/MDER.S50048

Witte, A.-K., Fuerstenau, D. & Zarnekow, R. *Digital Health Ecosystems for Sensor Technology Integration – A Qualitative Study on the Paradox of Data Openness*. Hyderabad, India. 41st International Conference on Information Systems (ICIS) 2020.

World Economic Forum. (2021). *The global risks report 2021: 16th edition. Insight report*. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf. Zugegriffen: 10.05.2021

Wozak, F., Schabetsberger, T. & Ammmenwerth, E. (2007). End-to-end security in telemedical networks – A practical guideline. *International Journal of Medical Informatics*, *76*(5), 484–490. https://doi.org/10.1016/j.ijmedinf.2006.09.020

Wrede, D., Freers, T. & Graf von der Schulenburg, J.-M. (2018). Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken – Eine empirische Analyse. *Zeitschrift für die gesamte Versicherungswissenschaft*, *107*(4), 405–434. https://doi.org/10.1007/s12297-018-0425-2

Yin, R. K. (2018). *Case study research and applications: Design and methods* (Sixth edition). SAGE.

Zängerle, D. & Schiereck, D. (2023a). Cyberrisiken – Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis. *HMD Praxis der Wirtschaftsinformatik, 60*(1), 214–229. https://doi.org/10.1365/s40702-022-00888-3

Zängerle, D. & Schiereck, D. (2023b). Modelling and predicting enterprise-level cyber risks in the context of sparse data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice, 48*(2), 434–462. https://doi.org/10.1057/s41288-022-00282-6

**Daniel Zängerle**, Dr., ist ehemaliger Doktorand am Fachgebiet Unternehmensfinanzierung der Technischen Universität Darmstadt.

*Anschrift*: Hochschulstr. 1, 64289 Darmstadt, Deutschland, Tel.: +49 (0)160/744–2143, E-Mail: daniel.zaengerle@t-online.de

**Dirk Schiereck**, Prof. Dr., ist Professor und Leiter des Fachgebietes Unternehmensfinanzierung der Technischen Universität Darmstadt.

*Anschrift*: Hochschulstr. 1, 64289 Darmstadt, Deutschland, Tel.: +49 (0)6151/16–24291, E-Mail: dirk.schiereck@tu-darmstadt.de