Spotlight on Information Security Integration in the German Health Sector

Margit SCHOLL
Business Computing and Administrative Informatics
Faculty of Business, Computing, and Law
Technical University of Applied Sciences Wildau (TH Wildau)
Wildau, 15745, Germany

ABSTRACT [1]

Based on extensive research of the literature on the current status of the health sector in Germany, the four spotlight areas of CRITIS, the pandemic situation, pandemic planning, and communication and learning are discussed in more detail in connection with information security. They may be used to create an integrative research map for holistic approaches in future research projects. With this in mind, the aim of this paper is to summarize key aspects of the spotlight areas based on a sound understanding of the literature. The focus here is on general lessons learned from previous awareness-raising projects in information security.

Keywords: Information Security, Health Sector, E-Health, Pandemic Situation, Research Map.

1. INTRODUCTION

Increased information technology (IT), a necessary and comprehensive process of digital transformation (DT), and—as an unavoidable result—information security (ISec) have been of great importance in recent years for medicine and the healthcare system in their pursuit of process optimization and cost reduction. For example, the Internet has had a major influence on the way people work in the medical environment and in some cases has completely changed it [1]. ISec has been an important topic for hospitals for several years and is becoming increasingly relevant as networking becomes ever more prevalent, denser, and more heterogeneous [1:175]. In particular, the question of ISec for patient data and data protection is becoming more and more important. However, there are currently no suitable concepts for integrating the requirements of IT security and risk identification related to business processes into a process-oriented and data-oriented view [2]. Training and awareness programs are immensely important in the healthcare sector, whereby the half-life of memory must be taken into account—regular repetition is essential, and even more important is the example set on a daily basis by those in charge [1]. Raising the awareness of internal and external employees is essential [1]. However, studies show that awareness-raising approaches that only focus on knowledge transfer without experience-oriented and interactive elements are not sufficient to create lasting awareness (see [3], for example). It is thus necessary to come up with new concepts for increasing people's sensitivity to the issues as they manifest in practical terms.

In Germany, SMEs make up over 99 percent of German companies and employ around 60 percent of all workers subject to social security [4:64]. However, the increased attention ISec is receiving nowadays is not reflected in the implementation of in-company measures [5:80]. The human factor in ISec has not been given sufficient attention so far in most SMEs. In order to motivate employees to be more observant of ISec in their individual behavior, it is necessary that managers and supervisors model the desired behavior [5:79]. This is confirmed by Gocke (2020) for the Charité hospital in Berlin: "If a real digital transformation is to take place in the clinics, then this is a major project and there will be conflicts over resources and schedules. The project is doomed to failure without good guidance from the clinic's board of directors" [6]. DT and ISec are a matter for the top management. The German police registered over 100,000 cases of cybercrime in the narrower sense in 2019, an increase of over 15 percent on the previous year [7]. The estimated damage caused by such acts is high—the German digital industry association Bitkom (2019) estimates that cyberattacks resulted in over 100 billion euros' worth of damage to the German economy [8]. The security risks are also increasing because three out of four companies now operate cloud computing [9], while complex, advanced attacks are discovered very late [10:3]. Companies around the world need an average of 280 days to detect and contain a cyberattack [11] [10].

The healthcare sector is one of the so-called critical information infrastructures in terms of security (CRITIS). "The failure of a CRITIS would restrict fundamental public processes, so that its protection is of paramount importance in the context of police security and criminal

[1] I would like to thank the following people for their stimulating and motivating input during the process of developing this article: Regina Schuktomow and Peter Koppatz from my research team, Dietmar Pokoyski (known_sense), the subcontractor in many of my projects, and Jan Seitz from the team of my colleague Prof. Gillert. I would like to thank the reviewers for their recommendations and Simon Cowper for his detailed peer-editing of this paper.

prosecution" [7:42]. According to a Roland Berger study, two-thirds of German clinics have already become victims of cyber criminals [12]. A greater understanding and more conscious handling of ISec would help relieve the healthcare sector. The importance of ISec in this sector must be expanded in the long term in order to minimize the risks coming from cyberattacks and from people's ignorance. Attacks on the healthcare system have increased by more than 60 percent in recent years [13]. During the Covid-19 pandemic, which has necessitated increased use of the Internet, "numerous new variants of cyberattacks developed, which all used the coronavirus crisis as a common denominator for their attacks" [7:1]. Attack tools such as blackmail Trojans remind us that ISec in hospitals is not a sure-fire success—this is especially true for the future Hospital 4.0 [14].

In section 2, the initial situation is clarified based on a literature search. In particular, four spotlight areas in the healthcare sector are identified that should be made the focus of research in a more integrated manner than has previously been the case. Section 3 summarizes the proposed integration of the interlinked spotlight areas. A general summary and outlook can be found in section 4.

2. LITERATURE SEARCH ON THE INITIAL SITUATION

Health should be understood in its full range—in physical, psychological, and social terms—and embedded in a holistic concept of quality of life. Attacks on hospitals have increased in recent years [15], especially in the course of the coronavirus crisis. Cyber incidents pose a dangerous threat to the healthcare system [16] [17] [18] [19]. Nowadays, there is no question that governance, risk management, and compliance activities are key challenges for all institutions—however, as Barafort et al. (2019) show, the challenge lies primarily in integrating risk management into organizational processes and thus making it possible to easily comply with the necessary ISO standards [20]. Back in 2010, Gabriel et al. pointed out that because of the sensitive data and information they process, healthcare organizations will feel the consequences of these changes even more than companies or public authorities [2]. On the one hand, these organizations are exposed to severe financial constraints—making it difficult for them to implement appropriate ISec measures—while, on the other, they operate in an environment in which it is impossible to completely exclude the public [2120].

The starting point of the literature search is the social vulnerability caused by increasing digital penetration and our dependence on it in almost all areas of life. Security of supply in the sense of fail-safe security is therefore of great importance: ensuring security precautions and the protection of critical infrastructures has thus been a core task of the German Federal State since the end of the 1990s [22] [23]. The literature search is also shaped by current circumstances relating to the Covid-19 pandemic and questions about planning safety. It was also motivated by questions about what and how one should learn from the pandemic. In the following, four spotlight areas are described in more detail as the starting point for tackling the issues in the healthcare sector.

2.1 First spotlight area: CRITIS

European and national laws assign the healthcare sector to CRITIS [24]. Ignorance of, violation of, or nonexistent ISec policies are major threats to institutions of all types and sizes. Because of the delay between an attack and its consequences, a long-term mindset is an important factor in reducing these security deficiencies. According to [25], long-term orientation comprises the three dimensions of continuity, future viability, and perseverance, which must be established in institutions as a function of ISec. In the healthcare sector, personal and highly sensitive data are recorded to allow an appropriate therapy to be determined for each individual patient. However, hospitals have a complex structure with many different clinical areas, which are mostly organized individually, and the understanding of information security varies accordingly [26]. We need to define new ways of increasing awareness, with the aim of making the primarily abstract contents of ISec clear and understandable. The simple transfer of knowledge will fail to achieve this goal [27]. Rather, it should also include direct involvement, exchange, and interaction between the participants. According to psychology-based research results on corporate ISec, which is a relatively new discipline, this combination is crucial in order to achieve sustainable awareness raising for employees and managers [27].

Krüger-Brand (2019) also emphasizes that *medical technology* in hospitals represents an increased security risk. Medical devices, like computers, work with programs and operating systems, and it is sometimes impossible for regular patches and updates to be implemented [28]. Hospitals also need to set up an information security management system (ISMS). The first general ISec specifications for CRITIS companies were set out in the German IT Security Law in 2015 [29]. The German legal landscape is congruent with the draft directive for network and information systems (NIS) first issued by the EU Commission in 2013 [30]. Hospitals with more than 30,000 inpatient cases per year have been required to screen their systems and adapt them to the guideline in order to protect themselves. "The NIS directive affects around 100 hospitals in Germany" [31].

However, it took several more years for the German Hospital Association (DKG), together with other institutions in the hospital sector, to develop the so-called B3S standard "Medical Care," which was confirmed by the Federal Office for Information Security (BSI) in October 2019. In principle, the B3S standard includes the imple-

mentation of an ISMS based on the requirements of the ISO/IEC 27001 and ISO/IEC 27799 standards—though the latter is relevant for the healthcare sector, it is comparatively unknown [32]. The B3S standard is valid for two years—so the BSI will have to review it this year. However, the threat landscape can be considered critical, meaning that more effective security mechanisms for networked medical devices and mobile healthcare applications must continue to be developed in the future [17:65]. In the worst-case scenarios, cyberattacks can endanger human life if medical devices are deactivated. Moreover, the current Patient Data Protection Law (PDSG) is not fully compatible with the GDPR [33]. This could also have an impact on the *acceptance* of digitization. The federal government hopes that another four years with electronic patient records and a secure exchange of sensitive health data will lead to acceptance of DT [34].

2.2 Second spotlight area: The pandemic situation and ISec

In the current Covid-19 pandemic, the healthcare sector is revealing itself to be *systemically relevant for human life* and demands a great deal from medical and nursing staff as well as from psychotherapists. On-site workers are also challenged in a variety of ways in different stressful situations. In addition to the current exceptional workload, there has always been a high level of responsibility, and wages are usually too low [35], which is why there has been a long-term lack of staff in this area, especially nursing staff [36]. The Federal Ministry of Health and the German Care Network have therefore started a campaign to support care workers. This allows local mayors to enter into dialogue with nursing staff via an online action platform, and local/regional traders can express their appreciation [37]. However, that will not be enough. Active relief should be provided to staff by building up skills among the general population.

ISec must be integrated into operational processes, and this should certainly apply during times of pandemic. However, even in a non-pandemic situation, ISec training for staff in the healthcare sector is limited to the bare minimum, as appropriate exemptions immediately create gaps in the care system. Concepts of resilience and sustainable awareness raising and training for exceptional situations are largely lacking. Attempts have been made in the last few decades to integrate so-called *health literacy* into school education through special events, and companies have also increasingly taken on responsibility for *health awareness*, but only selectively. Moreover, it should be noted that awareness is essential both for healthcare workers and for the overall population. Shang (2013) suggests that both local and contact awareness can raise the epidemic thresholds, while global awareness cannot **[38].** The result supports the previous findings of Wu et al. (2012), whose conclusion is that individual awareness contributes to the inhibition of epidemic transmission **[39]**. There is a lack of ongoing, sustainable concepts for seamlessly integrating health competence in schools and everyday work, and this is mirrored in the consciousness of the population as a whole. This makes it clear that an awareness of health and the state of health itself is increasingly becoming a *communication issue* [40].

Obviously, there are distinct communication *deficits and needs* affecting staff and the general public, which is why new ways of raising awareness and creating training measures with interactive methods for employees and managers should be explored and established in everyday working life. It is not just a matter of providing information. Rather, it is about targeting specific groups and sustainably increasing the individual level of knowledge about health within that group. With the help of new methods and classic discursive or constructivist didactics, so-called *empowerment*—in the sense of a development of the community/common good—should be enabled and given strategic support. In our opinion, we need to work together to increase general healthcare skills, with the aim of increasing the *self-efficacy* of the population at the same time.

Psychological research defines self-efficacy as a person's subjective certainty of being able to cope with new or challenging situations based on their individual skills, and it often depends precisely on whether the individual successfully masters what they set out to do [41]. The concept of self-efficacy goes back to [42]. It concerns the subjective assessment of an individual's competences and their ability to carry out a task or achieve a goal. Self-efficacy can be favorably influenced by a person's individual positive experiences and feelings of achievement, by vicarious experiences based on observations and stories from third parties, and through feedback and encouragement from third parties [43] [44]. This means that self-efficacy can be strengthened and maintained through *simple* measures [41]. In psychology, the investigation of motivation has also led to the concept of self-efficacy expectations. This relates to the ability for a certain behavior to be carried out competently [45]. It is also postulated that in addition to the positive assessment of one's own effectiveness, it is primarily a matter of whether and to what extent the individual personally identifies with the tasks they are given and the degree of autonomy they feel as a result [46].

2.3 Third spotlight area: Pandemic planning

Owing to the complexity of its processing procedures and its heterogeneous IT infrastructure, a hospital cannot avoid setting up an appropriate data-protection management system, in which ISec should play an essential part [29]. In addition, the pending sanctions—such as the fines stipulated by the GDPR—are significantly higher (10 to 20 million euros or 2 to 4 percent of the total an-

nual group turnover) than those under BSI law ("only" up to a maximum of 50,000 euros) [29]. The data-protection requirements are the same in both cases, and in both cases it is essential for there to be comprehensive transparency in the processing, the data flows, the IT used, and the technical and organizational protective measures taken [29].

The novel situation created by the current pandemic shows very clearly the fragility of the status quo in all institutions within the healthcare system (and beyond) based on a lack of security planning. A preliminary master plan for pandemics was first published by the World Health Organization (WHO) in 1999, and bodies such as the Robert Koch Institute (RKI) and the Federal Office for Civil Protection and Disaster Aid (BBK) followed suit (2001–5, with updates in 2017 and for Covid-19 in 2020) [47]. The focus is on protecting the population and maintaining the public health system [48] [49] [50] [51]. However, precautionary pandemic planning is only evident in the case of influenza. The Covid-19 pandemic involves *learning by doing*—an approach that broad sections of the population find more and more difficult to understand. There was no effective and comprehensive preparation for a situation like this, but the current pandemic should be an opportunity to better prepare actors and those affected. In addition, options for action by or for companies in which a large segment of the population works are rarely subject to scientific investigation in crisis situations like pandemics. So far, there have been specific studies of decision-making [52] [53] [54] [55] [56] [57] [58] [59] and shopping behavior [60], social responsibility [61], and IT security [62]. However, the question of resilience has not yet been considered.

A hospital can only survive pandemics in the long term if its employees are made aware of the issues and offered information and training: they should have the general competence to enable them to transparently implement the necessary measures, which they should also be involved in developing. New hybrid interaction techniques for systematic, systemic, and sustainable learning processes are also required in this spotlight area. Reichl-Streich (2020) emphasizes in his article that even before the Covid-19 pandemic, the increase in cyberattacks was posing problems for German hospitals and their awareness programs for employees. "At the latest with Covid-19 and the accelerating process of digitization, the question arises as to whether classical training formats such as e-learning and face-to-face events are still sufficient or whether new approaches are required" [63]. A hospital can only survive attacks in the long term if its employees are more sensitive to the design and development of ISec in-house and are also involved in it [63]. In addition, the connection between ISec, the pandemic situation, and pandemic planning must be made clearer and linked in an integrative way. More research is necessary.

2.4 Fourth spotlight area: Communication and learning

The population was *not* prepared for such a pandemic. In addition, there are *increasing communication deficits* in politics and science in conveying and weighing up the necessary measures, and these are coupled with the phenomenon of *fake news and disinformation campaigns*, an aspect of the Internet with which we are all familiar. A look at the corresponding scientific literature [64] [65] [66] [67] [68] quickly reveals that there are a large number of publications on the *subject* of fake news. However, the various publications are mainly concerned with describing (i.e., defining) and identifying the problem. Any discussion of *awareness raising*, which we consider to be of central importance, is secondary. The deletion of content and the education of the population are mentioned again and again as suitable countermeasures against disinformation [69]. However, that alone is not enough. The population must be *actively* involved in awareness-raising campaigns for sustainable learning, and the politicians, who are also learning, must significantly improve their communication with the population.

Given the author's perceptions at the beginning of the Covid-19 pandemic and the technologies and platforms that have been developed, it seems that there was a lack of clear, targeted communication and online learning units, as well as explicit instructions for staff and the population at large on how to reduce the spread of the virus. This is confirmed by [70]. Afterwards, public administrations put together collections of guidelines for different areas on their websites. However, according to our own research and testing, there was seldom a filter for specific questions and locations. A general hotline could be referenced for direct questions, although this was likely to be overloaded. Apart from contact tracking, the author's perception in 2020 was that current information, services, and applications do not directly help the public to answer their questions. Vogel (2020) points out that language and communication are in a state of emergency during a pandemic crisis that impacts everyday life [71].

In the author's opinion, users of the developed technology (i.e., people) should not be left to their own devices but should receive suitable suggestions for action. In a pandemic, technologies should be developed that lead to learning success among the population, answering their direct questions in a focused manner, presenting structured information that covers all eventualities, and offering clear simulations. This would not only serve to increase the quality of life for the public at large and raise their awareness of security issues but would also lead to a general unburdening of medical staff and the healthcare system.

For years, the *D21-Digital-Index* study has served as the basis for current and future decisions by political, eco-

nomic, scientific, and civil society actors in Germany [72]. The current edition for 2020/21 shows that problem-solving skills in the digital world, which overall has a higher degree of complexity, are relatively low among the German population [72:28]. There are significant differences between those with a low level of formal education and the highly educated [72:28], with the result that the *digital division* within the German population remains a key focus. However, after two years of stagnation, informal learning about the Internet and computers is clearly gaining in importance: some two out of three people are teaching themselves new skills by trying things out and making targeted use of the help of friends and acquaintances [72:29].

3. RESEARCH INTEGRATION

The status of research in Germany on the four spotlight areas was presented above in section 2. An explanation was also given of the deficits that can be identified. In this section, these four research areas are summarized and put together. In the interests of modeling the ongoing process of improvement, a circular design has been chosen for figure 1, which can be interpreted as an integrative research map, because resilience, just like awareness, cannot be achieved with a one-off project. Rather, it is a continuous process in which the individual awareness-raising projects should consistently contribute to the overall effect and must also reflect this (fig. 1).

Overall, the article proposes the following results in response to the key areas identified in fig. 1:

1. Increase understanding among the population and company employees of the importance of ISec in the healthcare sector, especially in times of a pandemic. There are new funding opportunities with the Hospital Future Act (Krankenhauszukunftsgesetz, KHZG) launched in January 2021. Fifteen percent of the funding amount must be demonstrably used for increased ISec, with a focus on IT and cybersecurity [73]. It is important that hospitals do not simply apply for a collection of projects side by side but rather pursue *strategic* and operational goals for digitization as part of an overall concept [73]. The development of a strategy is the task of the management. Moreover, the management delegates operational tasks to responsible bodies such as the ISec team or officers. However, the public must be actively involved in educational ISec measures, and the processes must also become more transparent and comprehensible.

2. Promote increased resilience and self-efficacy in the population and among employees through sustainable, experience-oriented learning scenarios covering exceptional situations in analog, digital, and hybrid form. “Hybrid” means a smart combination of analog and digital communication options. Short, experience-oriented learning scenarios are therefore necessary for the population as a whole, with a focus on a consensus-based level of knowledge and well-founded argumentation as a new means of clarification and education—the connection to the first spotlight area is obvious. This new, hybrid communication method must offer the public support and answer their questions concretely. Trust needs to be developed.

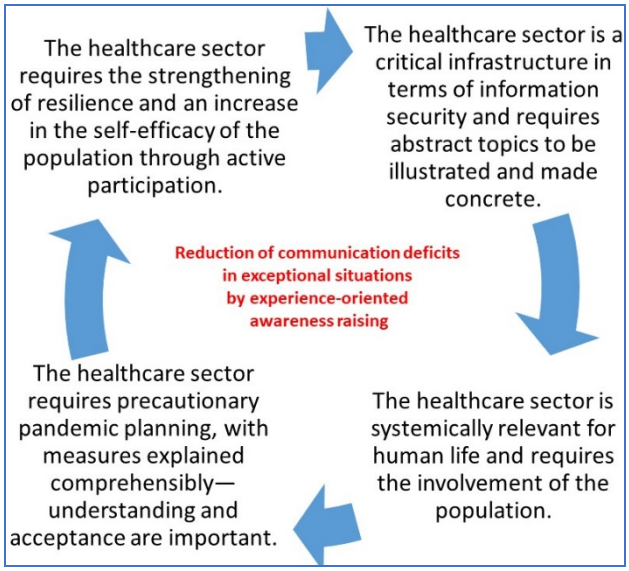

Fig. 1 Four spotlight areas that are currently relevant in the healthcare sector, as addressed in this article, integratively combined as a possible research map

3. Support and unburden the healthcare system through the clear communication of concrete action measures via a hybrid platform for the population as medical laypeople. Understood as a network, initial contact points could be named, guidelines explained, instructions illustrated, experience-oriented learning scenarios deployed, personal experiences processed, and self-assessments carried out. In the federal system, it is up to the individual states to draw up, interpret, and implement pandemic plans. This has been confusing for large segments of the population. Legal texts, regulations, and rationales have not always been comprehensible. As with the first two spotlight areas, an attempt must also be made here to make abstract topics tangible and concrete. Evidently, this has not happened enough in the political arena. A certain degree of helplessness has been developing as a counterpoint to self-efficacy. This corresponds to people’s assumptions that they are helpless and have no control and are thus unable to influence certain aspects of their lives [41]. This gives disinformation a possible foothold—with obvious connections to the fourth spotlight area.

4. Eliminate communication deficits through the active involvement of pilot testers—as representatives of the patients and the population at large—who bring in their own experience, skills, and know-how to help develop the plot. A traffic-light system for the hybrid platform might be used to give feedback on the "severity" of an incident to the specialist staff, who can then enter into an appropriate process of active exchange. Expectations and experiences must be made transparent.

4. SUMMARY AND OUTLOOK

Without a functioning IT system, a hospital is largely disabled, as is proven by numerous examples of hacker attacks [74]. An information security officer must be appointed and an ISMS set up [74] [75]. IS officers act as coordinators for the framework ISMS, for its reporting systems, the ISMS protection level, and the security concepts, for monitoring the continuous improvement of an ISMS, and for planning further education and training. However, the question of ISMS should not only be a matter for the IT department, because it clearly affects the system as a whole [76]—the responsibility for this falls to top management. We should combine the experience of raising awareness in ISec with the pandemic situation in an integrative way, shown in the article as a possible research map. Moreover, healthcare employees and members of the public should be actively involved in order to reduce the lack of understanding and prevent disinformation from prospering. "In promoting health, spreading knowledge is as essential as tackling typical problems of implementation. Both aspects can be addressed using game-based learning approaches" [77]. However, sustainable awareness raising does not succeed through the simple process of imparting knowledge—rather, those affected must be emotionally and actively involved in the process (see [78], for example). As Bruce Schneier, a US American ISec expert, puts it, "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" [79] [80]. The focus must be placed on the human being.

The author referred to Germany because she has a clearer overview of her home country. For further research, however, it would be very interesting to find out whether the four spotlight areas are also seen as generally applicable in other countries—an international research project would certainly make sense. With all the different experiences in the different countries, an overarching discussion is required about how information security in healthcare is viewed in other countries.

The aim of this paper is to summarize certain aspects—using an approach that has a sound basis in the literature—of four spotlight areas connecting ISec and the healthcare sector in times of pandemic. The aspects are mapped to general lessons learned from previous awareness-raising projects. The findings of the paper should be verified in future through empirical and statistical approaches with surveys and interviews so that the assumptions are made more reliable.

5. REFERENCES

[1] M. Darms, S. Haßfeld, and S. Fedtke, "Krankenhäuser und Kliniken–groß, anonym und damit ideal für Angreifer" / "Hospitals and clinics—large, anonymous and therefore ideal for attackers," in: **IT-Sicherheit und Datenschutz im Gesundheitswesen**, Wiesbaden: Springer Vieweg, 2019, pp. 175–195.

[2] R. Gabriel, A. Wagner, T. Lux, "Informationssicherheit im Krankenhaus—eine prozessorientierte Analyse der Patientendaten" / "Information security in the hospital—a process-oriented analysis of patient data," **INFORMATIK 2010. Service Science–Neue Perspektiven für die Informatik**, Vol. 1, 2010, https://dl.gi.de/bitstream/handle/20.500.12116/19209/241.pdf?sequence=1&isAllowed=y, last accessed 2021/2/23.

[3] T. San Nicolas-Rocca, B. Schooley, and J.L. Spears, "Designing Effective Knowledge Transfer Practices to Improve Security Awareness and Compliance," in: Sprague, R. H. (ed.), **Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS)**, Vol. 47, 2014, pp. 3432–3441, IEEE, Piscataway, NJ.

[4] D.C. Leeser, **Digitalisierung in KMU kompakt—Compliance und IT-Security** / Digitization in SMEs in a nutshell—compliance and IT security, Springer Vieweg, 2019.

[5] A. Hillebrand, A. Niederprüm, S. Schäfer, S. Thiele, I. Henseler-Unger, **Aktuelle Lage der IT-Sicherheit in KMU. Kurzfassung der Ergebnisse der Repräsentativbefragung, Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste** / Current situation of IT security in SMEs: Brief summary of the results of the representative survey, Scientific Institute for Infrastructure and Communication Services, WIK, 2017, https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/Aktuelle_Lage_der_IT-Sicherheit_in_KMU_-_WIK.pdf, last accessed 2021/2/13.

[6] P. Gocke, "Digitalisierung in der Praxis in der Charité: Digitalisierung ist Chefsache: 'Wir brauchen mehr Führung'" / "Digitization in practice at the Charité: Digitization is a top priority: 'We need more leadership,'" **kma-Klinik Management aktuell**, Vol. 25, No. 11, 2020, pp. 29–31.

[7] Bundeskriminalamt (BKA) (ed.), **Bundeslagebild Cybercrime 2019** / Federal Cybercrime Report

2019, September 2020, https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html, last accessed 2021/2/25.

[8] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom e. V.), **Wirtschaftsschutz in der digitalen Welt** / Economic protection in the digital world, 2019, https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf, last accessed 2021/2/25.

[9] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom e. V.), **Drei von vier Unternehmen nutzen Cloud-Computing** / Three out of four companies use cloud computing, 2020, https://www.bitkom.org/Presse/Presseinformation/Drei-von-vier-Unternehmen-nutzen-Cloud-Computing, last accessed 2021/2/25.

[10] O. Schonschek, "Warum es ohne Security Intelligence nicht mehr geht. Erkennung, Abwehr und Prognose komplexer Attacken" / "Why security intelligence is now essential: Detection, defense, and the prognosis in complex attacks," in: Security Insider (ed.), **Security Intelligence, eBook**, www.security-insider.de, Augsburg: Vogel IT-Medien GmbH, December 2020.

[11] Ponemon-Instituts (ed.), **Cost of a Data Breach 2020**, https://www.ibm.com/security/data-breach, last accessed 2021/2/25.

[12] C. Russo, "Krankenhausstudie" / "Hospital Study," in: **Roland Berger Study**, 2017. https://www.rolandberger.com/de/Media/Deutsche-Krankenhäuser-in-der-Zwickmühle-Kliniken-wollen-digitaler-werden-aber.html, last accessed 2021/1/2.

[13] W. Greiner, "60 Prozent mehr Angriffe auf das Gesundheitswesen" / "60 percent more attacks on healthcare," November 2019, **LANline** https://www.lanline.de/, https://www.lanline.de/60-prozent-mehr-angriffe-auf-das-gesundheitswesen, last accessed 2021/1/2.

[14] T. Eisenbarth and I. Bruhns, "IT-Sicherheit: Lücken schliessen" / "IT security: closing the gaps," **Klinik Management aktuell**, Vol. 23, No. 12, 2018, pp. 46–49.

[15] Radware (ed.), **Global Application and Network Security Report 2018/2019**, 2019, https://www.radware.com/ert-report-2018/, last accessed 2021/1/2.

[16] M. Kucera, "Uniklinik Düsseldorf: Cyberangriff verursacht Todesfall" / "Uniklinik Düsseldorf: Cyberattack causes death," **Klinik Management aktuell**, Vol. 25, No. 10, 2020, p. 6, (2020).

[17] Bundesamt für Sicherheit in der Informationstechnik (BSI) /Federal Office of Information Security (ed.), **The State of IT Security in Germany in 2019**, 2020, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2019.html, last accessed 2021/5/5.

[18] C. Spies, "Nach Hacker-Angriff: Uniklinik Düsseldorf kehrt zum Normalbetrieb zurück" / "After a hacker attack: Düsseldorf University Hospital returns to normal operation," https://www.bibliomedmanager.de/news/nach-hacker-angriff-uniklinik-duesseldorf-kehrt-zum-normalbetrieb-zurueck, last accessed 2021/5/30.

[19] M. Darms, S. Haßfeld, and S. Fedtke, "Informationssicherheit und Datenschutz in der Medizin" / "Information security and data protection in medicine," **Der MKG-Chirurg**, 2020, pp. 1–7.

[20] B. Barafort, A.L. Mesquida, and A. Mas, "ISO 31000-based integrated risk management process assessment model for IT organizations," **Journal of Software: Evolution and Process**, 2019, Vol. 31, No. 1, e1984, https://doi.org/10.1002/smr.1984.

[21] Deutsches Institut für Normung, **DIN EN ISO 27799: 2008-10**, "Medizinische Informatik – Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002" / "Health informatics—healthcare safety management using ISO/IEC 27002," Berlin: Beuth, 2008.

[22] **Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)** / National strategy for the protection of critical infrastructures (CRITIS strategy), June 2009, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html, last accessed 2021/5/29.

[23] Bundesamt für Sicherheit in der Informationstechnik (BSI) /Federal Office of Information Security (ed.), **Security in focus**, BSI Magazine 2018/02, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2018-02.html**,** last accessed 2021/05/29.

[24] Bundesamt für Sicherheit in der Informationstechnik (BSI) /Federal Office of Information Security (ed.), **Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS /** Protection of critical infrastructures through the IT Security Act and UP CRITIS, 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITISec.pdf?__blob=publicationFile&v=7, last accessed 2020/12/17.

[25] Y. Li, N. Zhang, and M. Siponen, "Keeping secure to the end: a long-term perspective to understand employees' consequence-delayed information security violation," **Behaviour & Information Technology**, 2018. DOI: 10.1080/0144929X.2018.1539519

[26] S. Wittjen, "Organisation von Informationssicherheit im Krankenhaus" / "Organization of informati-

on security in hospitals," in: Dünn et. al (eds.), **Cybersicherheit im Krankenhaus /** Cybersecurity in hospitals, Berlin: MWV Medizinisch Wissenschaftliche Verlagsgesellschaft mbH & Co. KG, 2020.

[27] M. Helisch and D. Pokoyski, (eds.), **Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung**/ Security awareness: New ways to successfully raise employee awareness, Wiesbaden: Vieweg+Teubner, 2009.

[28] H.E. Krüger-Brand, "Medizinische IT-Netzwerke: Cybersicherheit als Herausforderung" / "Medical IT networks: The challenge of cybersecurity," in: Dtsch Arztebl 2016; 113(9): A-364 / B-309 / C-309, **Ärzteverlag GmbH** (ed.), 2016, https://www.aerzteblatt.de/archiv/175147/Medizinische-IT-Netzwerke-Cybersicherheit-als-Herausforderun, last accessed 2020/11/15.

[29] G. Spyra, "Digitalisierung und IT-Sicherheit: Wo Licht ist, ist auch Schatten" / "Digitization and IT security: Where there is light, there are also shadows", **Klinik Management aktuell**, Vol. 24, No. 12, 2019, pp. 46–48.

[30] **DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**, English / German, https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016L1148&from=DE https://eur-lex.europa.eu/legalcontent/DE/TXT/PDF/?uri=CELEX:32016L1148&from=DE, last accessed 2021/2/25.

[31] x-tention (www.x-tention.at), "Von ausbaufähig zu NISec-konform—Das IT-Sicherheitssystem im Check" / "From expandable to NISec-compliant—The IT security system under review," **Klinik Management aktuell**, Produkte und Dienstleistungen, Vol. 23, No. 4, 2018, p. 76.

[32] Deutsche Krankenhausgesellschaft (DKG), **Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (2019)** / Industry-specific security standard for healthcare in hospitals (2019), https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf, last accessed 2021/5/5.

[33] M. Klein, "Patientenakte verstößt gegen DSGVO" / "Patient record violates GDPR," **eGovernment Computing**, 2020/8/25, https://www.egovernment-computing.de/patientenakte-verstoesst-gegen-dsgvo-a-958491/?print, last accessed 2020/12/17.

[34] P. von Braunmühl and M. Klein, "Warum ein Datentreuhänder so wichtig ist" / "Why a data trustee is so important," **eGovernment Computing**, 2020/4/28, https://www.egovernment-computing.de/warum-ein-datentreuhaender-so-wichtig-ist-a-927892/?print, last accessed 2020/12/17.

[35] A. Stettner, "Gehalt: Wie viel verdienen Krankenschwestern und Pfleger?" / "Salary: How much do nurses earn?," **Merkur online**, 2020, https://www.merkur.de/leben/karriere/gehalt-krankenschwester-krankenpfleger-zr-9532931.html, last accessed 2020/12/19.

[36] kna/aerzteblatt.de, "Zahl der Beschäftigten in Pflegeberufen im Lockdown gesunken" / "Number of employees in nursing professions fell during lockdown," 2020, https://www.aerzteblatt.de/treffer?mode=s&wo=1041&typ=1&nid=119573&s=Personalmangel, last accessed 2020/12/19.

[37] kna/aerzteblatt.de "Kampagne zur Unterstützung von Pflegekräften gestartet" / "Campaign started in support of nurses," 2020, https://www.aerzteblatt.de/nachrichten/119567/Kampagne-zur-Unterstuetzung-von-Pflegekraeften-gestartet, last accessed 2020/12/19.

[38] Y. Shang, "Modeling epidemic spread with awareness and heterogeneous transmission rates in networks," **Journal of biological physics**, 2013, 39(3), 489-500. DOI: 10.1007/s10867-013-9318-8

[39] Q. Wu, X. Fu, M. Small, and X.-J. Xu, "The impact of awareness on epidemic spreading in networks," **Chaos**, 2012; 22:13101. DOI: 10.1063/1.3673573.

[40] T. Abel, E. Bruhin, K. Sommerhalder, and S. Jordan, "Health Literacy/Gesundheitskompetenz," **Bundeszentrale für gesundheitliche Aufklärung** (online), 2018, https://www.leitbegriffe.bzga.de/alphabetisches-verzeichnis/health-literacy-gesundheitskompetenz, last accessed 2020/5/5.

[41] K.N. Barysch, "Selbstwirksamkeit" / "Self-efficacy." In: **Psychologie der Werte** / Psychology of values, Berlin/Heidelberg: Springer, 2016, pp. 201–211.

[42] A. Bandura, **Social Foundations of Thought and Action: A Social Cognitive Theory**, Englewood Cliffs, NJ: Prentice Hall, 1986.

[43] A. Bandura, "Exercise of Personal and Collective Efficacy in Changing Societies," in: Bandura, A. (ed.), **Self-efficacy in Changing Societies**, Cambridge: Cambridge University Press, 1995, pp. 1–45.

[44] R. Schwarzer and M. Jerusalem, "Das Konzept der Selbstwirksamkeit" / "The concept of self-efficacy," **Zeitschrift für Pädagogik** (ZfPäd), Vol. 44, 2002, pp. 28–53.

[45] F. Becker, "Selbstwirksamkeit und Motivation" / "Self-efficacy and motivation," in: **Mitarbeiter wirksam motivieren**, Berlin/Heidelberg: Springer, 2019, pp. 177–183.

[46] A. Krapp, R.M. Ryan, "Selbstwirksamkeit und Lernmotivation" / "Self-efficacy and the motivation

to learn," **Zeitschrift für Pädagogik. Selbstwirksamkeit und Motivationsprozesse in Bildungsinstitutionen**, Vol. 44, 2002, pp. 54–82, last accessed 2020/12/19.

[47] Robert-Koch-Institut (RKI): **Nationaler Pandemieplan**. Strukturen und Massnahmen: Ergänzung zum Nationalen Pandemieplan – Covid-19 – neuartige Coronaviruserkrankung / National pandemic plan. Structures and measures: Supplement, 2020.

[48] S. Kuo, H.-T. Ou, and C.J. Wang, "Managing medication supply chains. Lessons learned from Taiwan during the Covid-19 pandemic and preparedness planning for the future," **Journal of the American Pharmacists Association**, 2020.

[49] J. Madrigano, A. Chandra, T. Costigan, and J.D. Acosta, "Beyond Disaster Preparedness: Building a Resilience-Oriented Workforce for the Future," **International Journal of Environmental Research and Public Health**, Vol. 14, No. 12, 2017. DOI: 10.3390/ijerph14121563.

[50] K. Nikolopoulos, S. Punia, A. Schäfers, C. Tsinopoulos, and C. Vasilakis, "Forecasting and planning during a pandemic: Covid-19 growth rates, supply chain disruptions, and governmental decisions," **European Journal of Operational Research**, 2020.
DOI: 10.1016/j.ejor.2020.08.001.

[51] S. Simpson, MC. Kaufmann, V. Glozman, and A. Chakrabarti, "Disease X. Accelerating the development of medical countermeasures for the next pandemic," **The Lancet Infectious Diseases**, Vol. 20, No. 5, e108-e115, 2020. DOI: 10.1016/S1473-3099(20)30123-7

[52] M. Obal and T. Gao, "Managing business relationships during a pandemic. Conducting a relationship audit and developing a path forward," **Industrial Marketing Management**, Vol. 88, 2020, pp. 247–254. DOI: 10.1016/j.indmarman.2020.05.025.

[53] F. Pantano, G. Pizzi, D. Scarpi, and C. Dennis, "Competing during a pandemic? Retailers' ups and downs during the Covid-19 outbreak," **Journal of Business Research**, Vol. 116, 2020, pp. 209–213.
DOI: 10.1016/j.jbusres.2020.05.036.

[54] C.I. Pedersen, T. Ritter, C.A. Di Benedetto, "Managing through a crisis. Managerial implications for business-to-business firms," **Industrial Marketing Management**, Vol. 88, 2020, pp. 314–322. DOI: 10.1016/j.indmarman.2020.05.034.

[55] V. Ratten, "Coronavirus and international business. An entrepreneurial ecosystem perspective," **Thunderbird Int. Bus. Rev.**, Vol. 62, No. 5, 2020, pp. 629–634. DOI: 10.1002/tie.22161.

[56] P.W. Smith, K. Hansen, L. Spanbauer, and D.F. Shell, "Pandemic influenza preparedness: a survey of businesses," **American Journal of Infection Control**, Vol. 35, No. 7, 2007, pp. 484–485.
DOI: 10.1016/j.ajic.2006.11.008.

[57] S. Thorgren and T.A. Williams, "Staying alive during an unfolding crisis. How SMEs ward off impending disaster," **Journal of Business Venturing Insights**, Vol. 14, e00187, 2020. DOI: 10.1016/j.jbvi.2020.e00187.

[58] F. Giones, A. Brem, J.M. Pollack, T.L. Michaelis, K. Klyver, and J. Brinckmann, "Revising entrepreneurial action in response to exogenous shocks. Considering the Covid-19 pandemic," **Journal of Business Venturing Insights**, Vol. 14, e00186, 2020.
DOI: 10.1016/j.jbvi.2020.e00186.

[59] H. Kachali, I. Storsjö, I. Haavisto, and G. Kovács, "Inter-sectoral preparedness and mitigation for networked risks and cascading effects," **International Journal of Disaster Risk Reduction**, Vol 30, 2018, pp. 281–291.
DOI: 10.1016/j.ijdrr.2018.01.029.

[60] J. Habel, V. Jarotschkin, B. Schmitz, A. Eggert, and O. Plötner, "Industrial buying during the coronavirus pandemic. A cross-cultural study," **Industrial Marketing Management**, Vol. 88, 2020, pp. 195–205.
DOI: 10.1016/j.indmarman.2020.05.015.

[61] H. He and L. Harris, "The impact of Covid-19 pandemic on corporate social responsibility and marketing philosophy," **Journal of Business Research**, Vol. 116, 2020, pp. 176–182. DOI: 10.1016/j.jbusres.2020.05.030.

[62] G. Blokdijk, **Disaster recovery 100 success secrets. IT business continuity, disaster recovery planning and services**, S.l.: Emereo, 2008.

[63] A.J. Reichl-Streich, "Schulungen Gegen Cybercrime: Cybersicherheit ist kein Spiel" / "Training courses against cybercrime: cybersecurity is not a game," **Klinik Management aktuell**, Vol. 25, No. 10, 2020, pp. 46–47.

[64] C.T. Bergstrom and J.D. West, **Calling Bullshit: The Art of Skepticism in a Data-Driven World**, Random House, 2020.

[65] K. Nocun, P. Lamberty, **FAKE FACTS - Wie Verschwörungstheorien unser Denken bestimmen** / How conspiracy theories determine our thinking, Cologne: Bastei Lübbe AG, 2020.

[66] NEWS4TEACHER, "Woran erkennt man seriöse Informationen? Was Lehrer ihren Schülern beibringen sollten" / "How do you recognize legitimate information? What teachers should teach their students,"
https://www.news4teachers.de/2020/09/woran-erkennt-man-serioese-informationen-was-lehrer-ihren-schuelern-beibringen-sollten, last accessed 2021/5/30.

[67] C. Hertel, "Den Lügen auf der Spur" / "On the trail of lies," in: Deutsche Rentenversicherung (ed.), **zukunftjetzt, 02/20**, 2020, pp. 6–11.

[68] A. Brandolini, "The bullshit asimmetry [*sic*]: the amount of energy needed to refute bullshit is an order of magnitude bigger than to produce it," https://twitter.com/ziobrando/status/289635060758507521,

last accessed 2021/5/5.
[69] Pricewaterhouse Coopers GmbH (ed), **Fake news Ergebnisse einer Bevölkerungsumfrage** / Fake news results of a population survey, 2020, https://www.pwc.de/de/technologie-medien-und-telekommunikation/pwc-bevoelkerungsbefragung-fake-news.pdf, last accessed 2020/9/8.
[70] D. Schaeffer, K. Hurrelmann, and S. Schmidt-Kaehler, "Gesundheitsbildung: Corona zeigt Lücken auf" / "Health education: Corona 19 reveals gaps," retrieved from https://www.apotheken-umschau.de/krankheiten-symptome/infektionskrankheiten/coronavirus/gesundheitsbildung-corona-zeigt-luecken-auf-724111.html, last accessed 2021/5/29.
[71] F. Vogel, "Wenn Virologen alle paar Tage ihre Meinung ändern, müssen wir in der Politik dagegenhalten" - Thesen zur politischen Sprache und (strategischen) Kommunikation im Pandemie-Krisendiskurs / "If virologists change their mind every few days, we in politics have to counter this"—theses on political language and (strategic) communication in the pandemic crisis discourse, https://ids-pub.bsz-bw.de/frontdoor/deliver/index/docId/10043/file/Vogel_Thesen_zur_politischen_Sprache_und_Kommunikation_im_Krisendiskurs_2020.pdf, last accessed 2021/5/29.
[72] Initiative D21 (ed.), **D21 DIGITAL INDEX 2020/2021 – Jährliches Lagebild zur Digitalen Gesellschaft in Deutschland** / D21 DIGITAL INDEX 2020/2021—Annual situation report on the digital society in Germany, 2020, https://initiatived21.de/app/uploads/2021/02/d21-digital-index-2020_2021.pdf, last accessed 2021/2/25.
[73] W. Riedel and H. Riedel, "Krankenhauszukunftsgesetz: Die große Digitalisierungsoffensive" / "Hospital Future Act: The great digitization offensive," **Klinik Management aktuell**, Vol. 25, No. 12, 2020, pp. 55–57.
[74] T. Schütz, "CHIEF INFORMATION SECURITY OFFICER: Steuermann durch den IT-Sicherheitsprozess" / "Navigator through the IT security process," **Klinik Management aktuell**, Vol. 25, No. 03, 2020, pp. 54–57.
[75] M.C. Scholl and E.-P. Ehrlich, **Information Security Officer: Job profile, necessary qualifications, and awareness raising explained in a practical way**—Basis: ISO/IEC 2700x, BSI Standards 200-x, and IT-Grundschutz Compendium, Frankfurt: Buchwelten Verlag, 2021.
[76] T. Klagge, "IT-Sicherheitsgesetz: So geht die KRITISReise weiter" / "IT Security Act: The KRITIS journey continues," **Klinik Management aktuell,** Vol. 24, No. 6, 2019, pp. 46–48.
[77] E. Mir and H. Penz, "Gesundheitsförderung – lohnt sich das? Ein Diskussionsspiel für Ausbildung und Praxis / "Health promotion: Is it worth it? A discussion game for training and practice," **Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen**, 2021.
[78] P.S. Buffum, K.E, Boyer, E.N. Wiebe, B.W. Mott, and J.C. Lester, "Mind the Gap: Improving Gender Equity in Game-Based Learning Environments with Learning Companions," Artificial Intelligence in Education: 17th International Conference (AIED), C. Conati, N. Heffernan, A. Mitrovic, and M. F. Verdejo (eds.), Madrid, Spain, 2015, pp. 64–73. DOI: https://doi.org/10.1007/978-3-319-19773-9_7
[79] A. Reichl and S. Schwinger, "Informationssicherheit im Krankenhaus: Auch für 'die Kleinen' heißt es: Handeln!" / "Information security in hospitals: even for 'kids' it means: Action!" **Klinik Management aktuell**, Vol. 24, No. 05, 2019, 50–52.
[80] B. Schneier, **Secrets and Lies: Digital Security in a Networked World**, Indianapolis, IN: Wiley, 2015, p. xxiv.