doi: 10.36689/uhk/hed/2024-01-033

# Systematic Review of Current Risk Management Methods in Cybersecurity for Healthcare

Marie SOUKUPOVÁ* and Radek DOSKOČIL

Brno University of Technology, Brno, Czech Republic; Marie.Soukupova1@vut.cz; Radek.Doskocil@vut.cz

* Corresponding author: Marie.Soukupova1@vut.cz

Abstract: Presented systematic review is analyzing cyber risk management, more specifically economic aspect of the measures resulting from the risk analysis, through search of Web of Science and Scopus databases. The article questions the current scientific knowledge in the field of applicability of quantitative methods on measuring of the negative impact of successful cyberattacks. The purpose of the article is to define how these shall be improved for real application in the environment of healthcare, being specific not only by operating with sensitive patient data, but also by the urgency with which system malfunctions must be dealt with in order to prevent threatening the health and lives of patients (the fact that is providing the attacker with a unique position of privilege). While it is apparently necessary to invest more resources into the cybersecurity in healthcare, it is at the same time essential to ensure that these measures are profitable and the resources for them are spent economically. While cost of human life cannot easily be quantified, it is now time to search for methods on how to define an appropriate cybersecurity investment as opposed to the costs of a potential cyberattack.

Keywords: risk management; cybersecurity; healthcare; measure; cost

JEL Classification: G32; I15; K24

## 1. Introduction

Cyberattacks on hospitals are something that one can come across very often these days. With increasing number of attacks, followed by increase of costs for ransom and/or repairs and decrease of availability of health services, the question of how these situations can be prevented naturally comes to mind. The causes of these situations (meaning specific examples of the lack of cybersecurity measures in the current healthcare) together with the possible methods of prevention (meaning the risk management approaches) will be discussed in this article.

The aim of this paper is to assess whether the level of scientific knowledge in the field of economic optimization of measures in the cyber risk management process in healthcare is sufficient and whether the current methods developed for measuring cyber risks are useful. The basic condition of the cyber risk management process indicates that the costs of security measures adopted in order to prevent cyberattacks shall be proportional to the amount of damage done in case of a successful cyberattack (ENISA, 2012). Thus, analyzing the economical aspect of security measures and especially the methods used to quantify it is the aim of this article.

The topic of the article concerns multiple scientific fields consisting of risk management on one side, and cybersecurity in healthcare on the other. While cybersecurity is an urgent and current topic among organizations around the world, one cannot only understand it from the perspective of technical and technological improvements, but must also always consider the costs of the measures. That is where risk management and its methods step in. Vice versa, cybersecurity plays an indispensable role in risk management, cyberattacks being often defined as the most serious and at the same time probable risks known to organizations. The most common cost of cyberbreaches in healthcare does not concern the purchase of new hardware, but the disruption of operations which means cutting the hospital off its funding from the health insurance companies which are financing the treatments (Lee, 2021).

### *1.1. Cybersecurity in Healthcare*

Quite a few specifics of the field of cybersecurity can be found, among all else seeing that it is not something that organizations would proudly proclaim. For obvious reasons, if the level of security is low and proven by recent cyberbreach, the organization will have no desire to publicly talk about it, but even if the level of security is considered high in an organization, it is advised not to be very specific especially about its vulnerabilities. This fact makes research on the topic complicated. As well as digitalization, the cybercrime has also been rising exponentially in the course of the past few years. With the widening of the cyberspace in the recent years, frequent introduction of new technologies, the quantity of devices in a network, with wireless ones playing a major role, it has become easier to threaten organizations.

The state of cybersecurity in healthcare is inadequate to the state of security in other organizations, although interest in this topic from the side of senior management of healthcare facilities has changed considerably in the past few years as severe (especially ransomware) attacks on hospitals have been successful and gravely damaging (Pears & Konstantinidis, 2021). Nevertheless, cybersecurity, not being the primary service that the medical sector focuses on, still gets less attention and funding than necessary (Vukotich, 2023).

Moreover, what some senior managers do not realize is that cybersecurity does not only affect the IT department, but the entire patient care. As a matter of fact, close attention of the management should be paid to every aspect of the system that it is overlooking, from the perspective of its vulnerabilities to its defense mechanisms. The problem with rising investments in cybersecurity is the lacking data-driven strategy (Rothrock et al., 2017). Indeed fear, rather than a clear vision, should certainly not be the primary reason for cybersecurity investments. Additionally, it is necessary for the management to own responsibility for cybersecurity policies that it should ratify and comply with (Abraham et al., 2019).

It is no wonder that without constructive guidance from the authorities and with the shortage of cybersecurity specialists on the labor market, the facilities are uncertain about the security decisions and purchases that they should convey. As a consequence, most facilities lack cybersecurity strategies and since public spendings are being cut due to government's efforts for savings in almost all sectors (*[Czech] Government approved the state budget for 2024, decided to purchase F-35 supersonic aircraft and took another step to strengthen energy security*, 2023), cybersecurity budgets of hospitals can also be expected to decrease in the current calendar year.

Furthermore, the specific vulnerability of the healthcare sector is caused by the sensitive patient data that it operates with. Considering that sensitive data is even more valued by hackers than the data in banking or retail sectors (Symantec, 2017) puts extra stress on security in this industry. Henceforth, the human factor continues to prove as the weakest point of a security system in any organization (Lord, 2018), which, in case of healthcare, is even amplified by the notorious overwork of staff (Branley-Bell et al., 2021).

### *1.2. Devices and Networks in Healthcare*

Although healthcare facilities usually do not operate with Internet of Things (IoT) devices since their technologies are more outdated and therefore, they do not face the severe threats of distributed denial-of-service (DDoS) attacks through IoT, they still face many problems concerning their networks. The problems are, of course, caused by the outdated technologies themselves together with a lack of surveillance (SCADA) systems, resulting in the fact that the administrators often do not operate with an up-to-date overview of the networks that it is their responsibility to monitor. In some sense, one can understand medical facilities as underdeveloped and/or family businesses in terms of their level of cybersecurity, main difference between the two categories being the size of the actual organization where hospitals ensure a wide range of processes varying from healthcare through catering to administration.

However, the current security concerns consist not only of staff and established technological measures (such as firewalls, antivirus or encryption) since these are not sufficient anymore (Branley-Bell et al., 2021), but also of increasingly common wearable devices, especially those connected to the cloud. These are a version of IoT that is beginning to be used in healthcare. As with technological innovations in general, pressing focus of developers on delivering the solutions first to market pushes product security to the sidelines (Mills et al., 2016).

Wearable devices are unique in many ways. First of all, they can not only be compromised in the sense of a data breach, but they also have the potential to physically hurt the patient wearing them (Mills et al., 2016), being in direct contact with their bodies (Mills et al., 2016). Although wearables are not the reality of the majority of hospitals today, they are definitely the long-term goal of healthcare (since they provide the patients with additional possibility of mobility during the recovery or monitoring phase of treatment) which is why it is necessary to take their vulnerabilities into consideration, especially since they can serve as means of compromising the entire network (Abraham et al., 2019).

### *1.3. Data and Regulations*

Recent inevitable tightening of regulations concerning data protection (GDPR, 2018) has made it even more difficult for medical (as well as other) facilities to navigate themselves in the cybersecurity issues (Lee, 2021) which also increased requirements for already understaffed cybersecurity specialists. At the same time, more recommendations from the government in order to reduce the diversity of systems in each medical facility is advisable. A regulation named HIPAA (*Health Insurance Portability and Accountability Act of 1996*, 1996) which is in force in the USA can be used as a best practice, apparently taking into consideration the differences that the healthcare systems in the USA and in European countries have.

Nowadays, data is the most valuable asset of organizations and therefore needs to be protected with special care. At the same time, in each organization, there are definitely various categories of data with different value. A breach of cafeteria menus will surely cost the healthcare facility less than the breach of results of screenings of patients including their social security numbers. That is why data within an organization shall be classified and protected based on its importance.

Healthcare sector, to a certain extent comparable to underdeveloped companies, can in some perspective benefit from its outdated technologies in use. Since there are increasing risks with new technologies (such as cloud services), the fact that those are not commonly used in this sector might be recognized as a risk reduction. However, this argument is false since often, the issue that the cloud services do not cover must still be replaced by another, often unsystematic and therefore even less secure solution.

For instance, oftentimes, the patient's data (such as screenings or scans) is not stored on a shared cloud storage, however multiple departments of the medical facility need to access it in order to provide the patient with further treatment. What they do is often either send the data physically (by printing each paper out or writing the conditions down by hand), or send it through personal, unsupervised online communication tools (such as WhatsApp or email) while neither of these solutions complies with any basic security rules. This is one of the processes that shall without a doubt be replaced by a robust controlled system so that the entire healthcare can share necessary sensitive information in a considerably safer way (Draper & Raymond, 2020).

The healthcare sector is now therefore facing a crucial question: how to fully digitalize its processes and data. The main risks of the digital transformation are apparent, most serious of them being unauthorized access to sensitive data. However, those risks (in limited sense) already occur in the current (insufficient) state of digitalization. What digitalization comes with is the solution for backups counting with high volumes of data being stored a safe, accessible cyberspace so that they are available even in case of crisis. Concluding that digitalization is certainly the way to go.

### *1.4. Risk Management*

While all the aspects of cybersecurity mentioned above can be economically perceived as a cost, the question how to measure whether the cost is adequate to the risk and cost of potential damage done is still present. That is what the following chapters of the article are discussing.

## 2. Methodology

The systematic review includes synthesis of publications that had to fulfill predetermined eligibility criteria such as belong to the category "Economics and Business" within the Web of Science database, or be published in 2018 or more recently. The articles were searched within the Web of Science and Scopus databases using the keywords "cybersecurity" AND "hospitals" and "cyber risk management" AND "healthcare".

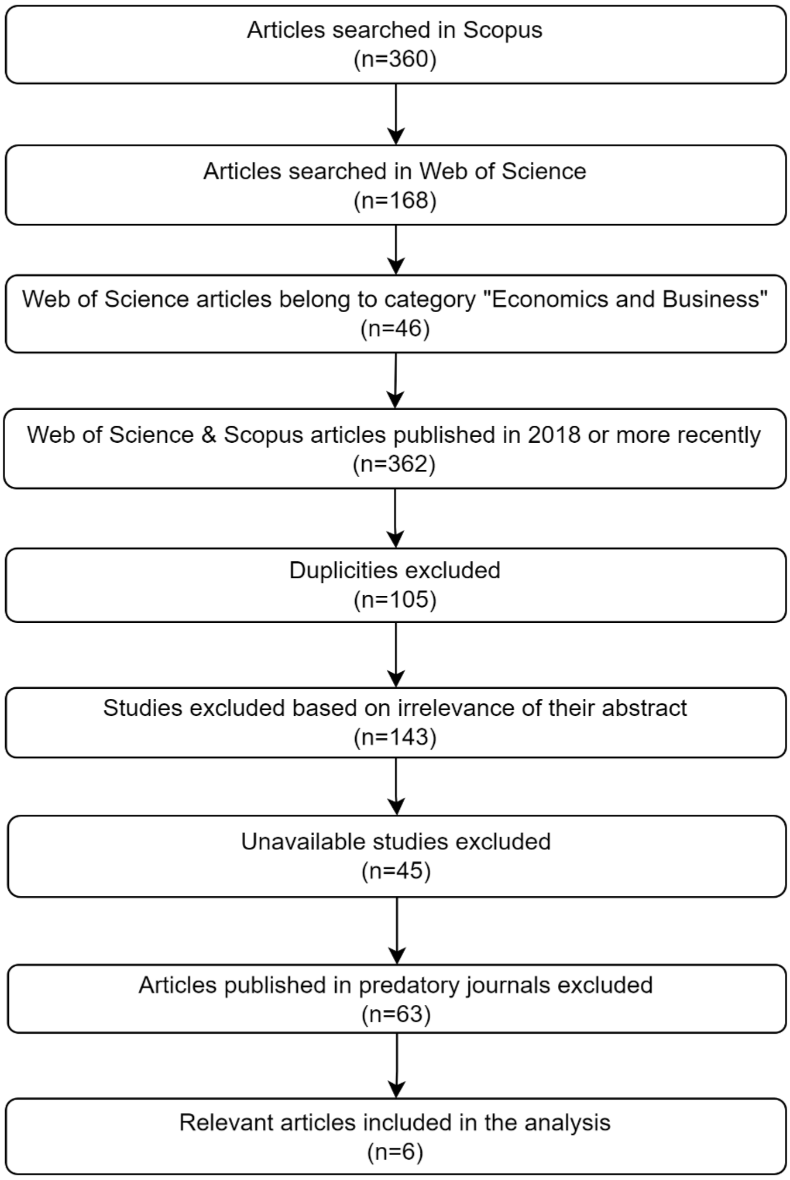
Articles searched in Scopus
(n=360)
Articles searched in Web of Science
(n=168)
Web of Science articles belong to category "Economics and Business"
(n=46)
Web of Science & Scopus articles published in 2018 or more recently
(n=362)
Duplicities excluded
(n=105)
Studies excluded based on irrelevance of their abstract
(n=143)
Unavailable studies excluded
(n=45)
Articles published in predatory journals excluded
(n=63)
Relevant articles included in the analysis
(n=6)

Figure 1: Flowchart of selection process of relevant articles

The findings were summarized and the subsequent outputs were analyzed. Implications were drawn based on them. Relevant studies were selected while excluding duplicities, irrelevant studies based on the content of their abstract, and unavailable studies were excluded as well as studies published in predatory journals. Useful references from suitable articles were used for further extension of the review.

Apart from the Web of Science and Scopus databases, a number of respectable websites of regulatory institutions was inspected (such as the official ENISA websites) for the purpose of this review.

## 3. Results

The review has concluded that there are quite a few approaches to cyber risk management. Some of them highlight the technological measures (Lockheed, 2009), some others point out the security of the entire supply chain (NIST, 2018) and other ones consider

Table 1: Bibliometric analysis of articles

| Author | Title of Article | Title of Journal | Year of publication |
|---|---|---|---|
| Lee, In | Cybersecurity: Risk management framework and investment cost analysis | Business Horizons | 2021 |
| Abraham, Chon, Chatterjee, Dave, Sims, Ronald R. | Muddling through cybersecurity: Insights from the U.S. healthcare industry | Business Horizons | 2019 |
| Eaton, Tim V., Grenier, Jonathan H., Layman, David | Accounting and Cybersecurity Risk Management | Current Issues in Auditing | 2019 |
| Draper, Chris, Raymond, Anjanette H. | Building a risk model for data incidents: A guide to assist businesses in making ethical data decisions | Business Horizons | 2019 |
| Branley-Bell, Dawn, Coventry, Lynne, Sillence, Elizabeth | Promoting Cybersecurity Culture Change in Healthcare | The 14th Pervasive Technologies Related to Assistive Environments Conference | 2021 |
| Vukotich, George | Healthcare and Cybersecurity: Taking a Zero Trust Approach | Health Services Insights | 2023 |

the human factor and consequent organizational measures as well. While all of that makes perfect sense, the problem in question is not only the definition of the measures themselves, as much as measuring of their costs and the costs of a potential cyberbreach, followed by a cost-benefit analysis.

Cybersecurity departments should thrive to quantify the impacts of risks as well as measures in order to justify investments into them (Lee, 2021) which is where the review found a blind spot. Not having access to accurate quantified data makes the work of cybersecurity managers in all sorts of organizations considerably more difficult especially in the aspect of negotiations on funding of cyber measures with the top management.

A few of the papers that were analyzed for the purpose of this review offer somewhat of a solution. The proposed cyber risk management framework designs four layers consisting of cyber ecosystem (outside of the organization itself), cyberinfrastructure (organization, employees, technologies), cyber risk assessment (designing the risk management together with investments needed) and cyber performance (consisting of the implementation, monitoring and continuous improvement of the cyber risk management) (Lee, 2021) that are to be governed by the cyber risk management.

Beyond doubt, the ecosystem layer (Lee, 2021) is a rather important one in case of healthcare, taking into account the different stakeholders in- and outside of its own field. Different healthcare facilities shall be able (under the condition of accessing only the data relevant for their own work – meaning the data of the patients that are in their care – not the data of all patients as is often the case) to exchange and discuss information related to the patient.

There are also ongoing debates about whether healthcare data should be used for other public service purposes (such as giving tax benefits to payers that prove that they attend check-ups). These debates are of course highly hypothetical at the moment since there are considerable problems accompanying the transfer of data within the healthcare sector itself, let alone its transfer beyond it. However, this only proves the importance of taking the surroundings of a single hospital into account when designing a cyber risk management framework in it.

In case of healthcare, the ecosystem consists mainly of its global supply chain management, patients, authorities, and the health insurance companies which are usually the main providers of income of the hospitals. Regarding cybersecurity area specifically, one shall also take into account the consulting specialists and the hackers.

Next on the list, the cyberinfrastructure layer, consisting of IT and non-IT staff as well as technologies within the organization (Lee, 2021), shall in opinion of the authors of this review be more specified by the public authorities, especially from the technological point of view. First of all, IT staff in hospitals could use guidelines to follow whereas minimalization of the diversity of networks in healthcare would help increase security overall. Cyber defense strategies followed by recurring trainings of all staff and possibly most importantly, a culture of positive cybersecurity behavior, are a part of this layer (Lee, 2021). Of course, keeping the technologies updated together with an overview of their vulnerabilities is essential here as well. Data also falls under this layer, nowadays being the primary target of the cyberattacks in healthcare and outside of it (Lee, 2021).

Cyber risk assessment layer is where this review can get inspired by standard risk management approaches, through risk identification, its quantification and cyber investment analysis (Lee, 2021). Identification of cyber risks can be done by learning from successful cyberattacks carried out on similar organizations (of course, the details of which the victims usually want to keep private because of the damage done to their corporate reputation). This is where experienced cybersecurity consulting specialists can prove very useful since they usually overlook a number of somewhat similar organizations. Once again, risk quantification is necessary for efficiency of investments into security (Chen et al., 2011).

While the method of cyber layers analyzed above, being one of the scarce number of methods published in scientific circles in recent years, describes the cyber risk management from all the different perspectives that need to be taken into consideration, it lacks a specific quantification method that could be used in the healthcare sector. The reason for quantification is as follows: security can never be established up to the point of elimination of all risks, both from technological point of view, where all risks can never be foreseen, and from the cost-benefit point of view, where cost of some measures exceeds the cost of damage done by certain risks.

Therefore, the realistic security approach must be to reduce the risk as long as implementation of measures against this risk has the same value as additional savings from possible incidents caused by it. Indeed, the process of estimating this value is where quantitative methods are needed, the issue with them being the lack of a standard that would help determine the costs of security measures as well as costs of assets that are being protected by them (Bojanc & Jerman-Blažič, 2008).

Some of the variables that the papers analyzed for the purposes of this review mentioned as appropriate for quantification were namely frequencies of cyberattacks as well as financial losses resulting from each of them (Lee, 2021). Naturally, statistical methods (such as the probability density function) can also be used, although data from a SCADA monitoring system may be considerably more accurate.

Above all, the cost of a cyberbreach shall include fines, costs of lawyers and consultants hired to settle the problem and the value of data released (Lee, 2021), in case of healthcare extended by the ransom, relocation of patients to other sites, the cost of government penalties, recovering data and replacing equipment together with damage of reputation (Abraham et al., 2019).

While scientifically discussing different possible variables that could be included in a quantitative model, we cannot forget to take the reality in practice into account. It is possible that a given cybersecurity manager might not have access to all finance-related information in the organization. Before designing a feasible quantitative cyber risk model, it is therefore necessary to interview the professionals thoroughly.

The more precisely the risk is quantified, the easier it should be to advocate for the investment in the security measures through an elaborate cost-benefit analysis. Another approach mentioned in the analyzed papers describes comparing financial loss in case of a cyberbreach to the cyber investment cost, meaning the expenses for cybersecurity (Lee, 2021), suggesting a rather broad and unspecified variable.

## 4. Discussion

The review proved that there is a scientific gap in the sense of a quantitative cyber risk model that is currently missing. A number of scientific papers published in respectable journals was analyzed in order to confirm the need for a quantitative approach in the defined topic. A few of them indicated suitable variables to be included in such a quantitative model, though often without a proper consideration of whether the values of these variables are accessible to the cybersecurity experts within the organization which is applying the model in practice.

The apparent recommendation of the authors of this review concerns consulting an external cybersecurity specialist rather than assigning the cybersecurity role to a randomly selected member of the IT department. While learning from previous cyberattacks in similar facilities might be difficult due to their will to keep the details of the incidents private, cybersecurity experts are the ones able to share the lessons learned since they were often the ones witnessing it happen.

Clearly, there is space for future research in this area. One of the apparent directions includes cooperation among different departments of a healthcare facility. As described in more detail above, cyberattacks are not just the issue of one department since they effect the entire facility. Therefore, it is only logical to support cooperation of multiple parts of the facility to prevent them. What the authors of the review find especially potentially fruitful is the cooperation of cybersecurity managers and accountants who may be more competent to quantify certain risks and costs associated with cyberattacks. Accountants, being experts in this field, shall offer their advisory and/or assurance capacities (Eaton et al., 2019). Only with specific and measurable impact of cyberattacks serving as proof can cybersecurity managers obtain better financial support for the protection of the networks from the side of the senior management. And that is why a quantitative cyber risk model is needed.

Furthermore, another research direction is at hand: during the design of the new model, authors must not forget to consult the cybersecurity experts in practice in order to include variables that they have access to and ensure the model's feasibility and usefulness. Thus, a set of interviews or questionnaires shall be conducted and analyzed for future steps of the research. The authors of the review would, among all else, like to statistically verify their assumption that cybersecurity staff in healthcare may benefit from advanced level of government support in the form of official recommendations regarding network resilience etc. A tool whose applicability in the field of cybersecurity in healthcare shall be examined from the point of view of scientific research is also the artificial intelligence. Many are discussing its security risks, but forgetting that it might be used as a part of security itself, especially in the context of shortage of staff and experts in cybersecurity, namely visible in healthcare.

The review defined a need for a feasible quantitative cyber risk model usable in healthcare which the practice is now lacking, resulting in low security overall. While defining the new model, not only shall the experts in practice be interviewed, but emphasis on continuous improvement shall be remembered since every model becomes less accurate with time passed, especially when it concerns the rapidly developing field of IT.

One does not need to be a cybersecurity expert to notice the fact that cyberattacks on hospitals have been rising in the past years. By being able to measure the costs and benefits of security as well as the costs of damage done, hospitals (as well as other organizations) will be able to make informed and strategic decisions concerning their security and their patients will be able to recover in a safe space. By building resilient networks supported by verified providers, the cyberattacks shall become less and less successful, eventually making healthcare sector unappealing for hackers to whom it will be hard to affect it and hospitals shall once again become the places where citizens in their greatest need will come with full trust in the institutions of healthcare as well as the state itself.

Conflict of interest: none.

## References

[Czech] Government approved the state budget for 2024, decided to purchase F-35 supersonic aircraft and took another step to strengthen energy security. (2023). Vláda České republiky. Retrieved January 10, 2024, from https://vlada.gov.cz/cz/media-centrum/aktualne/vlada-schvalila-statni-rozpocet-na-rok-2024--rozhodla-o-nakupu-nadzvukovych-letounu-f-35-a-ucinila-dalsi-krok-k-posileni-energeticke-bezpecnosti-208775/

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

Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*(5), 413-422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

Branley-Bell, D., Coventry, L., & Sillence, E. (2021). Promoting Cybersecurity Culture Change in Healthcare. In *Proceedings of the 14th PErvasive Technologies Related to Assistive Environments Conference* (pp. 544-549). https://doi.org/10.1145/3453892.3461622

Draper, C., & Raymond, A. H. (2020). Building a risk model for data incidents: A guide to assist businesses in making ethical data decisions. *Business Horizons*, *63*(1), 9-16. https://doi.org/10.1016/j.bushor.2019.04.005

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and Cybersecurity Risk Management. *Current Issues in Auditing*, *13*(2), C1-C9. https://doi.org/10.2308/ciia-52419

ENISA. (2012). *Introduction to Return on Security Investment: Helping CERTs assessing the cost of (lack of) security*. European Union Agency for Cybersecurity. Retrieved January 10, 2024, from https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/@@download/fullReport

GDPR. (2018). *What is GDPR, the EU's new data protection law?* Retrieved January 10, 2024, from https://gdpr.eu/what-is-gdpr/

Health Insurance Portability and Accountability Act of 1996. (1996). ASPE. Retrieved January 10, 2024, from https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quarterly*, *35*(2), 397-422. https://doi.org/10.2307/23044049

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671. https://doi.org/10.1016/j.bushor.2021.02.022

Lockheed, M. (2009). *Cyber Kill Chain*. Retrieved January 10, 2024, from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Lord, N. (2018). Information Security: The top INFOSEC considerations for healthcare organizations today. *Digital Guardian*. Retrieved January 10, 2024, from https://www.digitalguardian.com/blog/healthcare-information-security-top-infosec-considerations-healthcare-organizations-today

Mills, A. J., Watson, R. T., Pitt, L., & Kietzmann, J. (2016). Wearing safe: Physical and informational security in the age of the wearable device. *Business Horizons*, *59*(6), 615-622. https://doi.org/10.1016/j.bushor.2016.08.003

NIST. (2018). *Framework documents*. National Institute of Science and Technology. Retrieved January 10, 2024, from https://www.nist.gov/cyberframework/framework

Pears, M., & Konstantinidis, S. T. (2021). Cybersecurity Training in the Healthcare Workforce – Utilization of the ADDIE Model. In *2021 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1674-1681). https://doi.org/10.1109/EDUCON46332.2021.9454062

Rothrock, R. A., Kaplan, J., & Van der Oord, E. (2017). The Board's Role in Managing Cybersecurity Risks. *MIT Sloan Management Review*. Retrieved January 10, 2024, from https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/

Symantec. (2017). *Addressing Healthcare Cybersecurity Strategically* [White Paper]. Mountain View, CA. Retrieved January 10, 2024, from https://www.carahsoft.com/application/files/8014/6194/0617/Addressing_Cybersecurity_Strategically_whitepaper.pdf

Vukotich, G. (2023). Healthcare and Cybersecurity: Taking a Zero Trust Approach. *Health Services Insights*, 16, 1-5. https://doi.org/10.1177/11786329231187826